Opinion of the Data Ethics Commission

daten
ethik
kommission

Opinion of the Data Ethics Commission

daten
ethik
kommission

Content overview

Table of contents

Executive Summary

Our society is experiencing profound changes brought about by digitalisation. Innovative data-based technologies may benefit us at both the individual and the wider societal levels, as well as potentially boosting economic productivity, promoting sustainability and catalysing huge strides forward in terms of scientific progress. At the same time, however, digitalisation poses risks to our fundamental rights and freedoms. It raises a wide range of ethical and legal questions centring around two wider issues: the role we want these new technologies to play, and their design. If we want to ensure that digital transformation serves the good of society as a whole, both society itself and its elected political representatives must engage in a debate on how to use and shape data-based technologies, including artificial intelligence (AI).

Germany's Federal Government set up the Data Ethics Commission *(Datenethikkommission)* on 18 July 2018. It was given a one-year mandate to develop ethical benchmarks and guidelines as well as specific recommendations for action, aiming at protecting the individual, preserving social cohesion, and safeguarding and promoting prosperity in the information age. As a starting point, the Federal Government presented the Data Ethics Commission with a number of key questions clustered around three main topics: algorithm-based decision-making (ADM), AI and data. In the opinion of the Data Ethics Commission, however, AI is merely one among many possible variants of an algorithmic system, and has much in common with other such systems in terms of the ethical and legal questions it raises. With this in mind, the Data Ethics Commission has structured its work under two different headings: **data** and **algorithmic systems** (in the broader sense).

In preparing its Opinion, the Data Ethics Commission was inspired by the following **guiding motifs**:

- Ensuring the human-centred and value-oriented design of technology
- Fostering digital skills and critical reflection in the digital world
- Enhancing protection for individual freedom, self-determination and integrity
- Fostering responsible data utilisation that is compatible with the public good
- Introducing risk-adapted regulation and effective oversight of algorithmic systems
- Safeguarding and promoting democracy and social cohesion
- Aligning digital strategies with sustainability goals
- Strengthening the digital sovereignty of both Germany and Europe.

1

General ethical and legal principles

Humans are morally responsible for their actions, and there is no escaping this moral dimension. Humans are responsible for the goals they pursue, the means by which they pursue them, and their reasons for doing so. Both this dimension and the societal conditionality of human action must always be taken into account when designing our technologically shaped future. At the same time, the notion that technology should serve humans rather than humans being subservient to technology can be taken as incontrovertible fact. Germany's constitutional system is founded on this **understanding of human nature**, and it adheres to the tradition of Europe's cultural and intellectual history.

Digital technologies have not altered our ethical framework – in terms of the basic values, rights and freedoms enshrined in the German Constitution and in the Charter of Fundamental Rights of the European Union. Yet the new challenges we are facing mean that we need to reassert these values, rights and freedoms and perform new balancing exercises. With this in mind, the Data Ethics Commission believes that the following ethical and legal principles and precepts should be viewed as indispensable and socially accepted benchmarks for action.

Human dignity
Human dignity is a principle that presupposes the unconditional value of every human being, prohibiting such practices as the total digital monitoring of the individual or his or her humiliation through deception, manipulation or exclusion.

Self-determination
Self-determination is a fundamental expression of freedom, and encompasses the notion of informational self-determination. The term "digital self-determination" can be used to express the idea of a human being a self-determined player in a data society.

Privacy
The right to privacy is intended to preserve an individual's freedom and the integrity of his or her personal identity. Potential threats to privacy include the wholesale collection and evaluation of data about even the most intimate of topics.

Security
The principle of security relates not only to the physical and emotional safety of humans but also to environmental protection, and as such involves the preservation of vitally important assets. Guaranteeing security entails compliance with stringent requirements, e.g. in relation to human/machine interaction or system resilience to attacks and misuse.

Democracy

Digital technologies are of systemic relevance to the flourishing of democracy. They make it possible to shape new forms of political participation, but they also foster the emergence of threats such as manipulation and radicalisation.

Justice and Solidarity

In view of the vast amounts of power being accumulated using data and technologies, and the new threats of exclusion and discrimination, the safeguarding of equitable access and distributive justice is an urgent task. Digitalisation should foster participation in society and thereby promote social cohesion.

Sustainability

Digital developments also serve sustainable development. Digital technologies should contribute towards achieving economic, ecological and social sustainability goals.

Ethics cannot be equated on a one-to-one basis with the law. In other words, not everything that is relevant from an ethical perspective can and should be enshrined in legislation; conversely, there are provisions of the law that are motivated purely by pragmatic considerations. Nevertheless, the law must, at all times, be heedful of the potential ethical implications of the legal provisions in force, as well as living up to ethical standards. The Data Ethics Commission holds the view that **regulation is necessary, and cannot be replaced by ethical principles**. This is particularly true for issues with heightened implications for fundamental rights that require the central decisions to be made by the democratically elected legislator. Regulation is also an essential basis for building a system where citizens, companies and institutions can trust that the transformation of society will be guided by ethical principles.

At the same time, regulation must not unduly inhibit technological and social innovation and dynamic market growth. Overly rigid laws that attempt to regulate every last detail of a situation may place a stranglehold on progress and increase red tape to such an extent that innovation by German companies can no longer keep pace with the rate of technological development on the international stage.

Yet legislation is only one of a range of tools that can be used to lend tangible shape to ethical principles. The **synergistic use of various governance instruments** at different levels (multi-level governance) is vital in view of the complexity and dynamism of data ecosystems. These instruments include not only legislative measures and standardisation, but also various forms of co-regulation or self-regulation. Technology and technological design can moreover function as governance instruments themselves, and the same applies to business models and options for steering the economy. Governance in the broader sense also encompasses policy-making decisions in the fields of education and research. It is important to consider each of the aforesaid governance instruments not only in a national context, but also (and in particular) in their **European and international** contexts.

In the view of the Data Ethics Commission, all of the key questions presented by the Federal Government belong to one of two different perspectives: questions that concentrate mainly on data (the **"data perspective"**) and questions that are primarily focused on algorithmic systems (the **"algorithms perspective"**). These two perspectives should not be regarded as competing views or two sides of the same coin; instead, they represent two different **ethical discourses, which both complement each other and are contingent upon each other**. These different ethical discourses are typically also reflected in different governance instruments, including in different acts of legislation.

2

Data

The **data perspective** focuses on digital data, which are used for machine learning, as a basis for algorithmically shaped decisions, and for a plethora of further purposes. This perspective considers data primarily with a view to their **origin** and to the potential **impact** their processing may have on certain parties who are involved with the data, such as by being the data subject, as well as on society at large. From an ethical and legal point of view, it is important to identify **standards for data governance**; typically, however, **rights** that parties involved with the data can enforce against others will play an even more significant role. A central distinction in this context is that between personal and non-personal data, since it determines whether the provisions of data protection law apply.

General standards for data governance

In the opinion of the Data Ethics Commission, responsible data governance must be guided by the following data ethics principles:

- **Foresighted responsibility:** Possible future cumulative effects, network effects and effects of scale, technological developments and changing actor constellations must be taken into account when gauging the potential impact of collecting, processing and forwarding data on individuals or the general public.

- **Respect for the rights of the parties involved:** Parties who have been involved in the generation of data – whether as data subjects or in a different role – may have rights in relation to such data, and these rights must be respected.

- **Data use and data sharing for the public good:** As a non-rivalrous resource, data can be duplicated and used in parallel by many different individuals for many different purposes, thereby furthering the public good.

- **Fit-for-purpose data quality:** Responsible use of data includes ensuring a high level of data quality that is fit for the relevant purpose.

- **Risk-adequate level of information security:** Data are vulnerable to external attacks, and it is difficult to recover them once they have gone astray. The standard of information security applied must therefore be commensurate with the potential for risk inherent to the situation in question.

- **Interest-oriented transparency:** Controllers must be prepared and in a position to account for their data-related activities. This requires appropriate documentation and transparency and, if necessary, a corresponding liability regime in place.

Data rights and corresponding obligations

For self-determined navigation in the data society, parties must have, and be able to enforce, certain data-related rights against others. First and foremost among these rights are those relating to an individual's **personal data**, which derive from the right to informational self-determination that is enshrined as a fundamental right, and which are guaranteed by the applicable data protection law. Digital self-determination in the data society also includes the self-determined economic exploitation of one's own data, and it includes self-determined management of **non-personal data**, such as non-personal data generated by one's own devices. The Data Ethics Commission takes the view that, in principle, a right to digital self-determination in the data society also applies to companies and **legal entities** and – at least to some extent – to groups of persons (collectives).

Data are often generated with contributions from different parties who are acting in different roles – be it as the data subject, be it as the owner of a data-generating device or be it in yet another role. In the opinion of the Data Ethics Commission such contributions to the generation of data should not lead to exclusive ownership rights in data, but rather to **data-specific rights of co-determination and participation**, which in turn may lead to corresponding obligations on the part of other parties. The extent to which an individual should be entitled to data rights of this kind, and the shape they should take, depends on the following general factors:

a) the nature and scope of that party's **contribution to data generation**,

b) the **weight of that party's legitimate interest** in being granted the data right,

c) the weight of any possibly **conflicting interests** on the part of the other party or of third parties, taking into account any potential compensation arrangements (e.g. protective measures, remuneration),

d) the **interests of the general public**, and

e) the **balance of power** between the parties involved.

Data rights may allow their holders to pursue a number of different goals, in particular the following:

- requiring that a controller **desist from data use** (up to a right to require erasure of the data),
- requiring that a controller **rectify the data**,
- requiring that a controller grant **access to data** (up to full data portability), or
- requiring an **economic share** in profits derived with the help of the data.

For each type of data right (desistance, rectification, access, economic share) there exists a **separate set of conditions** defining, e.g., what counts as a party's legitimate interest in being granted the data right. For determining whether a party has a right to require desistance from a particular data use, key considerations include the potential for harm associated with said use and the circumstances under which the party in question had contributed to generating the data. Potential for harm may also be relevant when a request is made to rectify data, but the benchmark is lower in this respect. Where a party requests access to data, there is a graded spectrum of interests that count as a legitimate interest to be granted such access, which is particularly relevant within existing value creation systems. Only under very narrowly defined conditions may a party have an independent claim to an economic share in profits derived by others. The **rights granted to data subjects** under the EU's General Data Protection Regulation (GDPR) are a particularly important manifestation of these data rights, aimed specifically at protecting the natural persons to whom the data pertain; they are also to some extent a standardised manifestation given that they hinge on the qualification of data as personal data.

Considering these principles, the Data Ethics Commission wishes to submit the following key recommendations for action:

Standards for the use of personal data

1

The Data Ethics Commission recommends that **measures be taken against ethically indefensible uses of data**. Examples of these uses include total surveillance, profiling that poses a threat to personal integrity, the targeted exploitation of vulnerabilities, addictive designs and dark patterns, methods of influencing political elections that are incompatible with the principle of democracy, vendor lock-in and systematic consumer detriment, and many practices that involve trading in personal data.

2

Data protection law as well as other branches of the legal system (including general private law and unfair commercial practices law) already provide for a range of instruments that can be used to prevent such ethically indefensible uses of data. However, in spite of the widespread impact and enormous potential for harm, too little has been done to date in terms of harnessing the power of these instruments, particularly against the market giants. The various factors contributing to this **enforcement gap** must be tackled systematically.

3

As well as steps to make front-line players (e.g. supervisory authorities) more aware of the existing options, there is an urgent need for the **legislative framework in force to be fleshed out more clearly and strengthened in certain areas**. Examples of recommended measures include the blacklisting of data-specific unfair contract terms, the fleshing out of data-specific contractual duties of a fiduciary nature, new data-specific torts, the blacklisting of certain data-specific unfair commercial practices and the introduction of a much more detailed legislative framework for profiling, scoring and data trading.

4

In order to allow supervisory authorities to take action more effectively, these authorities need significantly better human and material resources. Attempts should be made to strengthen and formalise cooperation between the different data protection authorities in Germany, thereby ensuring the uniform and coherent application of data protection law. If these attempts fail, consideration should be given to the **centralisation of market-related supervisory activities** within a federal-level authority that is granted a broad mandate and that cooperates closely with other specialist supervisory authorities. The authorities at *Land* level should remain responsible for supervisory activities relating to the public sector, however.

5

The Data Ethics Commission believes that **"data ownership"** (i.e. exclusive rights in data modelled on the ownership of tangible assets or on intellectual property) would not solve any of the problems we are currently facing, but would create new problems instead, and **recommends refraining from their recognition**. It also advises against granting to data subjects copyright-like rights of economic exploitation in respect of their personal data (which might then be managed by collective societies).

6

The Data Ethics Commission also argues that **data should not be referred to as "counter-performance"** provided in exchange for a service, even though the term sums up the issue in a nutshell and has helped to raise awareness among the general public. Regardless of the position that data protection authorities and the European Court of Justice will ultimately take with regard to the prohibition under the GDPR of "tying" or "bundling" consent with the provision of a service, the Data Ethics Commission believes that consumers must be offered **reasonable alternatives** to releasing their data for commercial use (e.g. appropriately designed **pay options**).

7

Stringent requirements and limitations should be imposed on the use of data for **personalised risk assessment** (e.g. the "black box" premiums in certain insurance schemes). In particular, the processing of data may not intrude on intimate areas of private life, there must be a clear causal relationship between the data and the risk, and the difference between individual prices charged on the basis of personalised and non-personalised risk assessments should not exceed certain percentages (to be determined). There should also be stringent requirements in respect of transparency, non-discrimination and the protection of third parties.

8

The Data Ethics Commission advises the Federal Government not to consider the issues falling under the heading of **"digital inheritance"** as having been settled by the Federal Court of Justice's 2018 ruling. The ephemeral spoken word is being replaced in many situations by digital communications that are recorded more or less in their entirety, and the possibility that these records will be handed over to a deceased's heirs adds a whole new dimension of privacy risk. A range of mitigating measures should be taken, including the imposition of new obligations on service providers, quality assurance standards for digital estate planning services and national regulations on post-mortem data protection.

9

The Data Ethics Commission recommends that the Federal Government should invite the social partners to work towards a common position on the legislative provisions that should be adopted with a view to **stepping up the protection of employee data**, based on examples of best practices from existing collective agreements. The concerns of individuals in non-standard forms of employment should also be taken into account during this process.

10

In view of the benefits that could be gained from **digitalising healthcare**, the Data Ethics Commission recommends swift expansion of digital infrastructures in this sector. The expansion of both the range and the quality of digitalised healthcare services should include measures to better allow patients to exercise their rights to informational self-determination. Measures that could be taken in this respect include the introduction and roll-out of an electronic health record, building on a participatory process that involves the relevant stakeholders, and the further development of procedures for reviewing and assessing digital medical apps in the insurer-funded and consumer-funded health markets.

11

The Data Ethics Commission calls for action against the significant enforcement gap that exists with regard to statutory **protection of children and young people** in the digital sphere. Particular attention should be paid to the development and mandatory provision of technologies (including effective identity management) and default settings that not only guarantee reliable protection of children and young people but that are also family-friendly, i.e. that neither demand too much of parents or guardians nor allow or even encourage excessive surveillance in the home environment.

12

Standards and guidelines on the handling of the personal data of **vulnerable and care-dependent persons** should be introduced to provide greater legal certainty for professionals in the care sector. At the same time, consideration should be given to clarifying in the relevant legal provisions on living wills that these may also include dispositions with regard to the future processing of personal data as far as such processing will require the care-dependent person's consent (e.g. for dementia patients who will not be in a position to provide legally valid consent).

13

The Data Ethics Commission believes that a number of binding requirements should be introduced to ensure the **privacy-friendly design of products and services**, so that the principles of privacy by design and privacy by default (which the GDPR imposes on controllers) will already be put into practice upstream, by manufacturers and service providers themselves. Such requirements would be particularly important with regard to consumer equipment. In this context, standardised icons should also be introduced so that consumers are able to take informed purchase decisions.

14

Action must also be taken at a number of different levels to provide manufacturers with adequate **incentives to implement features of privacy-friendly design**. This includes effective legal remedies that can be pursued against parties along the entire distribution chain to ensure that also manufacturers can be held accountable for inadequate application of the principles of privacy by design and privacy by default. Consideration should also be given, in particular, to requirements built into tender specifications, procurement guidelines for public bodies and conditions for funding programmes. The same applies to **privacy-friendly product development**, including the training of algorithmic systems.

15

While debates on data protection tend (quite rightly) to centre around natural persons, it is important not to ignore the fact that **companies and legal persons must also be granted protection**. The almost limitless ability to pool together individual pieces of data can be used as a means of obtaining a comprehensive picture of a company's internal operating procedures, and this information can be passed on to competitors, negotiating partners, parties interested in a takeover bid and so on. This poses a variety of threats – *inter alia* to the digital sovereignty of both Germany and Europe – in view of the significant volumes of data that flow to third countries. Many of the Data Ethics Commission's recommendations for action therefore also apply on a *mutatis mutandis* basis to the data of legal persons. The Data Ethics Commission believes that action must be taken by the Federal Government to **step up the level of data-related protection afforded to companies**.

Improving controlled access to personal data

16

The Data Ethics Commission identifies enormous potential in the use of data for research purposes that serve a public interest (e.g. to improve healthcare provision). Data protection law as it currently stands acknowledges this potential, in principle, by granting far-reaching privileges for the processing of personal data for research purposes. Uncertainty persists, however, in particular as regards the scope of the so-called research privilege for secondary use of data, and the scope of what counts as "research" in the context of product development. The Data Ethics Commission believes that appropriate **clarifications in the law** are necessary to rectify this situation.

17

The fragmentation of research-specific data protection law, both within Germany itself and among the EU Member States, represents a potential obstacle to data-driven research. The Data Ethics Commission therefore recommends that **research-specific regulations should be harmonised**, both between federal and *Land* level and between the different legal systems within the EU. Introducing a notification requirement for research-specific national law could also bring some improvement, as could the establishment of a European clearing house for cross-border research projects.

18

In the case of research involving particularly sensitive categories of personal data (e.g. health data), **guidelines** should be produced with information for researchers on how to obtain consent in a legally compliant manner, and **innovative consent models should be promoted and explicitly recognised by the law**. Potential options include the development and roll-out of digital consent assistants or the recognition of so-called meta consent, alongside further endeavours to clarify the scope of the research privilege for secondary use of data.

19

The Data Ethics Commission supports, in principle, the move towards a **"learning healthcare system"**, in which healthcare provision is continuously improved by making systematic and quality-oriented use of the health data generated on a day-to-day basis, in keeping with the principles of evidence-based medicine. If further progress is made in this direction, however, greater efforts must be made at the same time to protect data subjects against the significant potential for discrimination that exists when sensitive categories of data are used; this might involve **prohibiting the exploitation of such data** beyond the defined range of purposes.

20

The development of procedures and standards for data **anonymisation** and **pseudonymisation** is central to any efforts to improve controlled access to (formerly) personal data. A legal presumption that, if compliance with the standard has been achieved, data no longer qualify as personal, or that "appropriate safeguards" have been provided in respect of the data subject's rights, would improve legal certainty by a long way. These measures should be accompanied by rules that – on pain of criminal penalty – prohibit the de-anonymisation of anonymised data (e.g. because new technology becomes available that would allow the re-identification of data subjects) or the reversal of pseudonymisation, both in the absence of narrowly defined grounds for doing so. Also research in the field of **synthetic data** shows enormous promise, and more funding should be funnelled into this area.

21

Fundamentally speaking, the Data Ethics Commission believes that **innovative data management and data trust schemes** hold great potential, provided that these systems are designed to be robust, suited to real-life applications and compliant with data protection law. A broad spectrum of models falls under this heading, ranging from dashboards that perform a purely technical function (**privacy management tools**, PMT) right through to comprehensive data and consent management services (**personal information management services**, PIMS). The underlying aim is to empower individuals to take control over their personal data, while not overburdening them with decisions that are beyond their capabilities. The Data Ethics Commission recommends that research and development in the field of data management and data trust schemes should be identified as a funding priority, but also wishes to make it clear that adequate protection of the rights and legitimate interests of all parties involved will require additional **regulatory measures at EU level**. These regulatory measures would need to secure central functions without which operators cannot be active, since their scope for action would otherwise be very limited. On the other hand, it is also necessary to protect individuals against parties that they assume to be acting in their interests, but that, in reality, are prioritising their own financial aims or the interests of others. In the event that a feasible method of protection can be found, data trust schemes could serve as vitally important mediators between data protection interests and data economy interests.

22

As far as the right to **data portability** enshrined in Article 20 GDPR is concerned, the Data Ethics Commission recommends that industry-specific codes of conduct and standards on data formats should be adopted. Given that the underlying purpose of Article 20 GDPR is not only to make it more straightforward to change provider, but also to allow other providers to access data more easily, it is important to evaluate carefully the market impact of the existing right to portability and to analyse potential mechanisms by which it can be prevented that a small number of providers increase yet further their market power. Until the findings of this evaluation are available, expansion of the scope of this right (for example to cover data other than data provided by the data subject, or real-time porting of data) would seem premature and not advisable.

23

In certain sectors, for example messenger services and social networks, **interoperability or interconnectivity obligations** might help to reduce the market entry barriers for new providers. Such obligations should be designed on an asymmetric basis, i.e. the stringency of the regulation should increase in step with the company's market share. Interoperability and interconnectivity obligations would also be a prerequisite for building up or strengthening, within and for Europe, certain basic services of an information society.

Debates around access to non-personal data

24

Access by European companies to appropriate non-personal data of appropriate quality is a key factor for the growth of the European data economy. In order to benefit from enhanced **access to data**, however, stakeholders must have a sufficient degree of data-awareness and have the data skills that are necessary to make use of the data. Also, access to data proves to be disproportionately advantageous to stakeholders that have already built up the largest reserves of data and that have the best data infrastructures at hand. The Data Ethics Commission therefore wishes to stress that the factors referred to should always receive due attention when discussing whether and how to improve data access, in keeping with the **ASISA principle** *(Awareness – Skills – Infrastructures – Stocks – Access)*.

25

The Data Ethics Commission therefore supports the efforts already initiated at European level to promote and improve **data infrastructures** in the broadest sense of the term (e.g. platforms, standards for application programming interfaces and other elements, model contracts, EU Support Centre), and recommends to the Federal Government that these efforts should continue to be matched by corresponding efforts at national level. It would also be advisable to set up an ombudsman's office at federal level to provide assistance and support in relation to the negotiation of data access agreements and dispute settlement.

26

The Data Ethics Commission ascribes enormous importance to a holistically conceived, sustainable and strategic **economic policy** that outlines effective methods of preventing not only the exodus of innovative European companies or their acquisition by third-country companies, but also an excessive dependence on third-country infrastructures (e.g. server capacities). A balance must be struck in this context between much-needed international cooperation and networking on the one hand, and on the other a resolute assumption of responsibility for sustainable security and prosperity in Europe against the backdrop of an ever-evolving global power dynamic.

27

Also from the perspective of boosting the European data economy, the Data Ethics Commission does not see any benefit in introducing new exclusive rights ("data ownership", "data producer right"). Instead, it recommends affording **limited third-party effects to contractual agreements** (e.g. to restrictions on data utilisation and onward transfer of data by a recipient). These third-party effects could be modelled on the new European regime for the protection of trade secrets. The Data Ethics Commission also recommends the adoption of legislative solutions enabling European companies to cooperate in their use of data, for example by using data trust schemes, without running afoul of anti-trust law (**"data partnerships"**).

28

The data accumulated in existing value creation systems (e.g. production and distribution chains) are often of enormous commercial significance, both inside and outside that value creation system. In many cases, however, the provisions on data access that appear in the contractual agreements concluded within a value creation system are unfair and/or inefficient, or lacking entirely; in certain cases, there is no contractual agreement at all. Efforts must therefore be made to **raise awareness among businesses** in sectors far outside what is commonly perceived as the "data economy", and to provide practical guidance and support (e.g. model contracts).

29

The Data Ethics Commission furthermore recommends cautious **adaptations of the current legislative framework**. The first stage in this process should be to make explicit reference in Section 311 of the [German] Civil Code (*Bürgerliches Gesetzbuch*, BGB) to the special relationship that exists between a party that has contributed to the generation of data in a value creation system and the controller of the data, clarifying that such parties may have certain quasi-contractual duties of a fiduciary nature. These duties should normally include a duty to enter into negotiations about fair and efficient

data access arrangements. Consideration should also be given to whether additional steps should be taken, which could range from blacklisting particular contract terms also for B2B transactions, to formulating default provisions for data contracts, to introducing sector-specific data access rights.

30

The Data Ethics Commission believes that **open government data (OGD) concepts** hold enormous potential, and recommends that these concepts should be built on and promoted. It also recommends a series of measures to promote a **shift in mindset among public authorities** (something that has not yet fully taken place) and to make it easier in practice to share data on the basis of OGD concepts. These measures include not only the establishment of the relevant **infrastructures** (e.g. platforms), but also harmonisation and improvement of the existing **legal framework** that is currently fragmented and sometimes inconsistent.

31

Nevertheless, the Data Ethics Commission identifies a degree of tension between efforts to promote OGD (relying on principles such as "open by default" and "open for all purposes"), and efforts to enhance data protection and the protection of trade secrets (with legally enshrined concepts such as "privacy by default"). The Data Ethics Commission submits that, in cases of doubt, **priority should be given to the duty of protecting** individuals and companies who have entrusted their data to the State (often without being given any choice in the matter, e.g. tax information). The State must deliver on this duty by implementing a range of different measures, which may include technical as well as legal safeguards against misuse of data.

32

In particular, it would be beneficial to develop **standard licences and model terms and conditions** for public-sector data sharing arrangements, and to make their use mandatory (at least on a sector-specific basis). These standard licenses and model terms and conditions should include clearly defined safeguards for the rights of third parties who are affected by a data access arrangement.

Provision should also be made against data being used in a way that ultimately harms public interests, and also against still greater accumulation of data and market power on the part of the big players (which would be likely to undermine competition) and against the taxpayer having to pay twice.

33

As regards **open-data concepts in the private sector**, priority should be given to **promoting and supporting voluntary data-sharing arrangements**. Consideration must be given not only to the improvement of infrastructures (e.g. data platforms), but also to a broad range of potential incentives; these might include certain privileges in the context of tax breaks, public procurement, funding programmes or licensing procedures. Statutory data access rights and corresponding obligations to grant access should be considered as fall-back options if the above measures fail to deliver the desired outcomes.

34

Generally speaking, the Data Ethics Commission believes that a cautious approach should be taken to the introduction of statutory data access rights; ideally such rights should be developed only on a **sector-by-sector basis**. Sectors in which the level of demand should be analysed include the media, mobility or energy sectors. In any case, before a statutory data access right or even a disclosure obligation is introduced, a full impact assessment needs to be carried out, examining and weighing up against each other all possible implications; these include implications for data protection and the protection of trade secrets, for investment decisions and the distribution of market power, as well as for the strategic interests of German and European companies compared to those of companies in third countries.

35

The Data Ethics Commission recommends considering enhanced obligations of private enterprises to grant access to data **for public interest and public-sector purposes** (business-to-government, B2G). A cautious and sector-specific approach is, however, recommended in this respect as well.

3

Algorithmic systems

The **algorithms perspective** focuses on the architecture of data-driven algorithmic systems, their dynamics and the systems' impacts on individuals and society. The ethical and legal discourse in this area typically centres around the relationship between humans and machines, with a particular focus on automation and the outsourcing of increasingly complex operational and decision-making processes to "autonomous" systems enabled by AI. The algorithms perspective differs from the data perspective in that the data processed by the system might have no connection whatsoever with the persons affected by it; in particular, individuals may suffer ethically indefensible implications even if all of the data used (e.g. to train an algorithmic system) are non-personal. The current debates on "algorithmic oversight" or liability for AI are of central importance in this respect.

General standards for algorithmic systems

The Data Ethics Commission distinguishes between three different levels of algorithmic involvement in human decision-making, based on the distribution of tasks between the human and the machine in the specific case in question:

a) **algorithm-based** decisions are human decisions based either in whole or in part on information obtained using algorithmic calculations,

b) **algorithm-driven** decisions are human decisions shaped by the outputs of algorithmic systems in such a way that the human's factual decision-making abilities and capacity for self-determination are restricted,

c) **algorithm-determined** decisions trigger consequences automatically; no provision is made for a human decision in the individual case.

In the opinion of the Data Ethics Commission, the following principles should be observed to ensure the responsible use of algorithmic systems.

- **Human-centred design:** Systems must be centred around the human who uses them or who is affected by their decisions; they must prioritise his or her fundamental rights and freedoms, basic needs, physical and emotional well-being and skills development.

- **Compatibility with core societal values:** The process of system design must take account of the system's impact on society as a whole, and in particular its effects on the democratic process, on the citizen-centred nature of state action, on competition, on the future of work and on the digital sovereignty of Germany and Europe.

- **Sustainability:** Considerations relating to the availability of human skills, participation, environmental protection, sustainable resource management and sustainable economic activity are becoming increasingly important factors in the design and use of algorithmic systems.

- **Quality and performance:** Algorithmic systems must work correctly and reliably so that the goals pursued with their help can be achieved.

- **Robustness and security:** Robust and secure system design involves not only making the system secure against external threats, but also protecting humans and the environment against any negative impacts that may emanate from the system.

- **Minimisation of bias and discrimination:** The decision-making patterns upon which algorithmic systems are based must not be the source of systematic bias or the cause of discriminatory decisions.

- **Transparent, explainable and comprehensible systems:** It is vitally important to ensure not only that the users of algorithmic systems understand how these systems function and can explain and control them, but also that the parties affected by a decision are provided with sufficient information to exercise their rights properly and challenge the decision if necessary.

- **Clear accountability structures:** Questions of the allocation of responsibility and accountability including possible liability arising with the use of algorithmic systems must be unambiguously resolved.

System criticality

The level of **criticality of an algorithmic system** dictates the specific requirements it must meet, in particular with regard to transparency and oversight. System criticality is determined by assessing an algorithmic system's potential for harm, on the basis of a two-pronged investigation into the **likelihood that harm will occur** and the **severity of that harm**.

The **severity** of the harm that could potentially be sustained, for example as a result of a mistaken decision, depends on the significance of the legally protected rights and interests affected (such as the right to privacy, the fundamental right to life and physical integrity, the prohibition of discrimination), the level of potential harm suffered by individuals (including non-material harm or loss of utility that are hard to calculate in monetary terms), the number of individuals affected, the total figure of the harm potentially sustained and the overall harm sustained by society as a whole, which may go well beyond a straightforward summation of the harm suffered by individuals. The **likelihood** that harm will be sustained is also influenced by the properties of the system in question, in particular the role of the algorithmic system components in the decision-making process, the complexity of the decision, the effects of the decision and the reversibility of these effects. The severity and likelihood of the predicted harm may also be contingent on whether the algorithmic systems are operated by the State or by private enterprises and, particularly in a business context, on the market power wielded by the system's operator.

In conclusion, the Data Ethics Commission wishes to make the following recommendations for action on the basis of these principles:

Risk-adapted regulatory approach

36

The Data Ethics Commission recommends adopting a **risk-adapted regulatory approach** to algorithmic systems. The principle underlying this approach should be as follows: the greater the potential for harm, the more stringent the requirements and the more far-reaching the intervention by means of regulatory instruments. When assessing this potential for harm, the **sociotechnical system as a whole** must be considered, or in other words all the components of an algorithmic application, including all the people involved, from the development phase – for example the training data used – right through to its implementation in an application environment and any evaluation and adjustment measures.

37

The Data Ethics Commission recommends that the potential of algorithmic systems to harm individuals and/or society should be determined uniformly on the basis of a **universally applicable model**. For this purpose, the legislator should develop a **criteria-based assessment scheme** as a tool for determining the criticality of algorithmic systems. This scheme should be based on the general ethical and legal principles presented by the Data Ethics Commission.

38

Among other things, the **regulatory instruments and the requirements that apply to algorithmic systems** should include corrective and oversight mechanisms, specifications of transparency, explainability and comprehensibility of the systems' results, and rules on the allocation of responsibility and liability for using the systems.

39

The Data Ethics Commission believes that a useful first stage in determining the potential for harm of algorithmic systems is to distinguish between **five levels of criticality**. Applications that fall under the lowest of these levels (Level 1) are associated with zero or negligible potential for harm, and it is unnecessary to carry out special oversight of them or impose requirements other than the general quality requirements that apply to products irrespective of whether they incorporate algorithmic systems.

40

Applications that fall under Level 2 are associated with **some potential for harm**, and can and should be regulated on an as-needs basis; regulatory instruments used in this connection may include ex-post controls, an obligation to produce and publish an appropriate risk assessment, an obligation to disclose information to supervisory bodies or also enhanced transparency obligations and access rights for individuals affected.

41

In addition, the introduction of licensing procedures may be justified for applications that fall under Level 3, which are associated with **regular** or **significant potential for harm**. Applications that fall under Level 4 are associated with **serious potential for harm**; the Data Ethics Commission believes that these applications should be subject to enhanced oversight and transparency obligations. These may extend all the way through to the publication of information on the factors that influence the algorithmic calculations and their relative weightings, the pool of data used and the algorithmic decision-making model; an option for "always-on" regulatory oversight via a live interface with the system may also be required.

42

Finally, a complete or partial ban should be imposed on **applications with an untenable potential for harm** (Level 5).

43

The Data Ethics Commission believes that the measures it has proposed should be implemented in a new EU Regulation on algorithmic systems enshrining general **horizontal requirements (Regulation on Algorithmic Systems, EU-ASR)**. This horizontal regulation should incorporate the fundamental requirements for algorithmic sytems that the Data Ethics Commission developed. In particular, it should group together general substantive rules – informed by the concept of system criticality – on the admissibility and design of algorithmic systems, transparency, the rights of individuals affected, organisational and technical safeguards and supervisory institutions and structures. This horizontal instrument should be fleshed out in **sectoral instruments** at EU and Member State level, with the concept of system criticality once again serving as a guiding framework.

44

The process of drafting the EU-ASR (as recommended above) should incorporate a debate on how best to demarcate the respective scopes of this Regulation and the **GDPR**. A number of factors should be taken into account in this respect; firstly, algorithmic systems may pose specific risks to individuals and groups even if they do not involve the processing of personal data, and these risks may relate to assets, ownership, bodily integrity or discrimination. Secondly, the regulatory framework introduced for the future horizontal regulation of algorithmic systems may need to be more flexible and risk-adapted than the current data protection regime.

Instruments

45

The Data Ethics Commission recommends the introduction of a **mandatory labelling scheme** for algorithmic systems of enhanced criticality (Level 2 upwards). A mandatory scheme of this kind would oblige operators to make it clear whether (i.e. when and to what extent) algorithmic systems are being used. Regardless of system criticality, operators should always be obliged to comply with a mandatory labelling scheme if there is a risk of confusion between human and machine that might prove problematic from an ethical point of view.

46

An individual affected by a decision should be able to exercise his or her right to "meaningful **information** about the logic involved, as well as the scope and intended consequences" of an algorithmic system (cf. GDPR) not only in respect of fully automated systems, but also in situations that involve any kind of **profiling**, regardless of whether a decision is taken on this basis later down the line. The right should also be expanded in the future to apply to the algorithm-based decisions themselves, with differing levels of access to these decisions according to system criticality. These measures may require the clarification of certain legislative provisions or a widening of regulatory scope at European level.

47

It certain cases, it may be appropriate to ask the operator of an algorithmic system to provide an **individual explanation** of the decision taken, in addition to a general explanation of the logic (procedure) and scope of the system. The main objective should be to provide individuals who are affected by a decision with comprehensible, relevant and concrete information. The Data Ethics Commission therefore welcomes the work being carried out under the banner of "Explainable AI" (efforts to improve the explainability of algorithmic systems, in particular self-learning systems), and recommends that the Federal Government should fund further research and development in this area.

48

In view of the fact that, in certain sectors, society as a whole may be affected as well as its individual members, also particular **parties who are not individually affected** by an algorithmic system should be entitled to access certain types of information about it. It is likely that rights of this kind would be granted primarily for journalistic and research purposes; in order to take due account of the operator's interests, they would need to be accompanied by adequate protective measures. The Data Ethics Commission believes that consideration should also be given to the granting of unconditional rights to access information in certain circumstances, in particular when algorithmic systems with serious potential for harm (Level 4) are used by the State.

49

It is appropriate and reasonable to impose a legal requirement for the operators of algorithmic systems with at least some potential for harm (Level 2 upwards) to produce and publish a proper **risk assessment**; an assessment of this kind should also cover the processing of non-personal data, as well as risks that do not fall under the heading of data protection. In particular, it should appraise the risks posed in respect of self-determination, privacy, bodily integrity, personal integrity, assets, ownership and discrimination. It should encompass not only the underlying data and logic of the model, but also methods for gauging the quality and fairness of the data and the model accuracy, for example the bias or the rates of (statistical) error (overall or for certain sub-groups) exhibited by a system during forecasting/category formation.

50

To provide controllers and processors with greater legal clarity, further work must be done in terms of fleshing out the requirements to **document and log** the data sets and models used, the level of granularity, the retention periods and the intended purposes. In addition, operators of sensitive applications should be obliged in future to document and log the program runs of software that may cause lasting harm. The data sets and models used should be described in such a way that they are comprehensible to the employees of supervisory institutions carrying out oversight measures (as regards the origin of the data sets or the way in which they are pre-processed, for example, or the optimisation goals pursued using the models).

51

System operators should be required by the standard-setting body to guarantee a minimum level of **quality, from both a technical and a mathematical-procedural perspective**. The procedural criteria imposed must ensure that algorithmically derived results are obtained in a correct and lawful manner. For this purpose, quality criteria could be imposed, in particular as regards corrective and control mechanisms, data quality and system security. For example, it would be appropriate to impose quality criteria on the relationship between algorithmic data processing outcomes and the data used to obtain these outcomes.

52

The Data Ethics Commission believes that a necessary first step is to clarify and flesh out in greater detail the scope and legal consequences of Article 22 GDPR in relation to the use of algorithmic systems in the context of human decision-making. As a second step, the Data Ethics Commission recommends the introduction of additional **protective mechanisms for algorithm-based and algorithm-driven decision-making systems**, since the influence of these systems in real-life settings may be almost as significant as that of algorithm-determined applications. The prohibitory principle followed to date by Article 22 GDPR should be replaced by a more flexible and risk-adapted regulatory framework that provides adequate guarantees as regards the protection of individuals (in particular where profiling is concerned) and options for these individuals to take action if mistakes are made or if their rights are jeopardised.

53

Consideration should be given to expanding the **scope of anti-discrimination legislation** to cover specific situations in which an individual is discriminated against on the basis of automated data analysis or an automated decision-making procedure. In addition, the legislator should take effective steps to prevent **discrimination on the basis of group characteristics** which do not in themselves qualify as protected characteristics under law, and where the discrimination often does not currently qualify as indirect discrimination on the basis of a protected characteristic.

54

In the case of algorithmic systems with regular or significant (Level 3) or even serious potential for harm (Level 4), it would be useful – as a supplement to the existing regulations – for these systems to be covered by **licensing procedures or preliminary checks** carried out by supervisory institutions, in the interests of preventing harm to individuals who are affected, certain sections of the population or society as a whole.

Institutions

55

The Data Ethics Commission recommends that the Federal Government should expand and realign the competencies of existing supervisory institutions and structures and, where necessary, set up new ones. Official supervisory tasks and powers should primarily be entrusted to the **sectoral supervisory authorities** that have already built up a wealth of expert knowledge in the relevant sector. Ensuring that the competent authorities have the financial, human and technical **resources** they need is a particularly important factor in this respect.

56

The Data Ethics Commission also recommends that the Federal Government should set up a **national centre of competence for algorithmic systems**; this centre should act as a repository of technical and regulatory expertise and assist the sectoral supervisory authorities in their task of monitoring algorithmic systems to ensure compliance with the law.

57

The Data Ethics Commission believes that initiatives involving the development of technical and statistical **quality standards for test procedures and audits** (differentiated according to critical application areas if necessary) are worthy of support. Test procedures of this kind – provided that they are designed to be adequately meaningful, reliable and secure – may make a vital contribution to the future auditability of algorithmic systems.

58

In the opinion of the Data Ethics Commission, particular attention should be paid to innovative forms of **co-regulation and self-regulation**, alongside and as a complement to forms of state regulation. It recommends that the Federal Government should examine various models of co-regulation and self-regulation as a potentially useful solution in certain situations.

59

The Data Ethics Commission believes that an option worth considering might be to require operators by law (inspired by the "comply or explain" regulatory model) to sign a declaration confirming their willingness to comply with an **Algorithmic Accountability Code**. An independent commission with equal representation – which must be free of state influence – could be set up to develop a code of this kind, which would apply on a binding basis to the operators of algorithmic systems. Appropriate involvement of civil society representatives in the drafting of this code must be guaranteed.

60

Voluntary or mandatory evidence of protective measures in the form of a specific **quality seal** may also serve as a guarantee to consumers that the algorithmic system in question is reliable, while at the same time providing an incentive for developers and operators to develop and use reliable systems.

61

The Data Ethics Commission takes the view that companies and authorities operating critical algorithmic systems should be obliged in future to appoint a **contact person**, in the same way that companies of a specific size are currently obliged to appoint a data protection officer. Communications with the authorities should be routed through this contact person, and he or she should also be subject to a duty of cooperation.

62

To ensure that official audits of algorithmic systems take due account of the interests of civil society and any companies affected, suitable **advisory boards should be set up within the sectoral supervisory authorities**.

63

In the opinion of the Data Ethics Commission, technical standards adopted by **accredited standardisation organisations** are a generally useful measure, occupying an intermediate position between state regulation and purely private self-regulation. It therefore recommends that the Federal Government should engage in appropriate efforts towards the development and adoption of such standards.

64

The system of granting **competitors, competition associations or consumer associations the right to file an action** has been an important feature of the German legal landscape for many years, and could play a key role in civil society oversight of the use of algorithmic systems. In particular, private rights of this kind could allow civil

society players with a legitimate mandate to enforce compliance with legal provisions in the area of contract law, fair trading law or anti-discrimination law, without needing to rely on the authorities to take action and without needing to wait for individuals to authorise them.

Special topic: Algorithmic systems used by media intermediaries

65

Given the specific risks posed by media intermediaries that act as **gatekeepers to democracy**, the Data Ethics Commission recommends that options should be examined for countering these risks, also with regard to influencing EU legislation (→ see Recommendation 43 above). A whole gamut of risk mitigation measures should be considered, extending through to ex-ante controls (e.g. in the form of a licensing procedure).

66

The national legislator is under a constitutional obligation to protect the democratic system from the dangers to the free, democratic and pluralistic formation of opinions that may be created by providers that act as gatekeepers by establishing a binding normative framework for **media**. The Data Ethics Commission believes that the small number of operators concerned should be obliged to use algorithmic systems that allow users (at least as an additional option) to access an unbiased and balanced selection of posts and information that embodies pluralism of opinion.

67

The Federal Government should consider measures that take due account of the risks typically encountered in the media sector in respect of all media intermediaries and also in respect of providers that do not act as gatekeepers or whose systems are associated with a lower potential for harm. These measures might include mechanisms for **enhancing transparency** (for example by ensuring that information is available about the technical procedures used to select and rank news stories, **introducing labelling obligations for social bots**) and establishing a right to post countering responses on timelines.

Use of algorithmic systems by state bodies

68

The State must, in the interests of its citizens, make use of the best available technologies, including algorithmic systems, but must also exercise particular prudence in all of its actions in view of its obligation to preserve fundamental rights and act as a role model. As a general rule, therefore, the use of algorithmic systems by public authorities should be assessed on the basis of the criticality model as **particularly sensitive**, entailing at the very least a comprehensive risk assessment.

69

In the areas of **law-making** and the **dispensation of justice**, algorithmic systems may at most be used for peripheral tasks. In particular, algorithmic systems must not be used to undermine the functional independence of the courts or the democratic process. By way of contrast, enormous potential exists for the use of algorithmic systems in connection with **administrative** tasks, in particular those relating to the provision of services and benefits. The legislator should take due account of this fact by giving the green light to a greater number of partially and fully automated administrative procedures. Cautious consideration should therefore be given to expanding the scope of both Section 35a of the German Administrative Procedures Act (*Verwaltungsverfahrensgesetz*, VwVfG) (which is couched in overly restrictive terms) and the corresponding provisions of statutory law. All of these measures must be accompanied by adequate steps to protect citizens.

70

Decisions taken by the State on the basis of algorithmic systems must still be **transparent**, and it must still be possible to provide **justifications** for them. It may be necessary to clarify or expand the existing legislation on freedom of information and transparency in order to achieve these goals. Furthermore, the use of algorithmic systems does not negate the principle that decisions made by public authorities must generally be justified individually; on the contrary, this principle may impose limits on the use of overly complex algorithmic systems. Finally, greater priority should be accorded to open-source solutions, since the latter may significantly enhance the transparency of government actions.

71

From an ethical point of view, there is no general right to non-compliance with rules and regulations. At the same time, however, automated "total" enforcement of the law raises a number of different ethical concerns. As a general rule, therefore, systems should be designed in such a way that a human can override **technical enforcement** in a specific case. The balance struck between the potential transgression and the automated (and perhaps preventive) enforcement measure must at all times meet the requirements of the proportionality principle.

Liability for algorithmic systems

72

Liability for damages, alongside criminal responsibility and administrative sanctions, is a vital component of any ethically sound regulatory framework for algorithmic systems. It is already apparent today that algorithmic systems pose challenges to liability law as it currently stands, *inter alia* because of the complexity and dynamism of these systems and their growing "autonomy". The Data Ethics Commission therefore recommends that the current provisions of liability law should undergo in-depth checks and (where necessary) revisions. The scope of these checks and revisions should not be restricted on the basis of too narrowly defined technological features, such as machine learning or artificial intelligence.

73

The proposal for a future system under which legal personality would be granted to high-autonomy algorithmic systems, and the systems themselves would be liable for damages (**"electronic person"**), should **not be pursued further**. As far as this concept is, by some protagonists, based on a purported equivalence between human and machine it is ethically indefensible. And as far as it boils down to introducing a new type of company under company law it does not, in fact, solve any of the pertinent problems.

74

By way of contrast, if harm is caused by autonomous technology used in a way functionally equivalent to the employment of human auxiliaries, the operator's liability for making use of the technology should correspond to the otherwise existing vicarious **liability regime of a principal for such auxiliaries** (cf. in particular Section 278 of the German Civil Code). For example, a bank that uses an autonomous system to check the creditworthiness of its customers should be liable towards them to at least the same extent that it would be had it used a human employee to perform this task.

75

As the debate currently stands, it appears highly likely that appropriate amendments will need to be made to the **Product Liability Directive** (which dates back to the 1980s), and a connection established to new product safety standards; in addition, certain changes may need to be made to the rules relating to **fault-based liability** and/or new bases of **strict liability** may need to be introduced. In each case, it will be necessary to determine the liability regime that is most appropriate for particular types of products, digital content and digital services, and the exact shape that this regime should take (once again depending on the criticality of the relevant algorithmic system). Consideration should also be given to innovative liability concepts currently being developed at European level.

4

A European path

The Data Ethics Commission examined a great many different questions in the course of its work, and discussions on these questions have raised new ones in turn; this alone should serve to indicate that this Opinion can serve only as one out of many building blocks in the larger edifice of a **debate on ethics, law and technology** that will continue for many years to come. The Data Ethics Commission takes the view that it is important to remember that ethics, law and democracy must serve as a shaping force for change, both in the broader sense and more specifically in the field of technology. To achieve this goal, interdisciplinary discourse in politics and society is required, and care must be taken to ensure that any rules and regulations adopted are open enough to retain their regulatory clout and their ability to adapt, even in the face of fast-paced changes to technologies and business models. These rules and regulations must be enforced effectively by means of appropriate instruments, procedures and structures, and these latter must make it possible to intervene promptly in response to infringements or undesirable developments.

In the global contest for future technologies, Germany and Europe are being confronted with value systems, models of society and cultures that differ widely from our own. The Data Ethics Commission supports the **"European path"** that has been followed to date: the defining feature of European technologies should be their consistent alignment with European values and fundamental rights, in particular those enshrined in the European Union's Charter of Fundamental Rights and the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms.

The Data Ethics Commission believes that the State has a particular responsibility to develop and enforce ethical benchmarks for the digital sphere that reflect this value system. In order to deliver on this promise to citizens, it must act from a position of political and economic strength on the global stage; excessive dependence on others turns a nation into a rule taker rather than a rule maker, resulting in the citizens of this nation being subject to resulting in the citizens of this nation being subject to requirements imposed by players elsewhere in the world, or by private corporations that are, for the most part, exempt from democratic legitimacy and oversight. Embarking on **efforts to safeguard the digital sovereignty of Germany and Europe in the long term** is therefore not only a politically far-sighted necessity, but also an expression of ethical responsibility.

Part A

Introduction

Guiding motifs

Our society is experiencing profound changes brought about by digitalisation. Innovative data-based technologies may benefit us at both the individual and the wider societal levels, as well as potentially boosting economic productivity, promoting sustainability and catalysing huge strides forward in terms of scientific progress. At the same time, however, digitalisation poses risks to our fundamental rights and freedoms. It raises a wide range of ethical and legal questions centring around two wider issues: the role we want these new technologies to play, and their design. If we want to ensure that digital transformation serves the good of society as a whole, both society itself and its elected political representatives must engage in a debate on how to use and shape data-based technologies, including artificial intelligence (AI).

Germany's Federal Government set up the Data Ethics Commission *(Datenethikkommission)* on 18 July 2018. It was given a one-year mandate to develop ethical benchmarks and guidelines as well as specific recommendations for action, aiming at protecting the individual, preserving social cohesion, and safeguarding and promoting prosperity in the information age. As a starting point, the Federal Government presented the Data Ethics Commission with a number of key questions clustered around three main topics: algorithm-based decision-making (ADM), AI and data. In the opinion of the Data Ethics Commission, however, AI is merely one among many possible variants of an algorithmic system, and has much in common with other such systems in terms of the ethical and legal questions it raises. With this in mind, the Data Ethics Commission has structured its work under two different headings: **data** and **algorithmic systems** (in the broader sense).

In preparing its Opinion, the Data Ethics Commission was inspired by the following **guiding motifs**:

- Ensuring the human-centred and value-oriented design of technology
- Fostering digital skills and critical reflection in the digital world
- Enhancing protection for individual freedom, self-determination and integrity
- Fostering responsible data utilisation that is compatible with the public good
- Introducing risk-adapted regulation and effective oversight of algorithmic systems
- Safeguarding and promoting democracy and social cohesion
- Aligning digital strategies with sustainability goals
- Strengthening the digital sovereignty of both Germany and Europe.

1. Mission and basic understanding

Our society is experiencing profound changes brought about by digitalisation. Innovative data-based technologies may benefit us at both the individual and the wider societal levels, as well as potentially boosting economic productivity, promoting sustainability and catalysing huge strides forward in terms of scientific progress; in some cases, this has already happened. The digital transformation offers tremendous opportunities for all countries, in particular for Germany as a closely networked and high-tech economy, but it means that German companies are coming under increasing competitive pressure on the international market. At the same time, it is already becoming apparent that digitalisation poses risks to our fundamental rights and freedoms. It raises a wide range of ethical and legal questions centring around two wider issues: the role we want these new technologies to play, and their design. If we want to ensure that digital transformation serves the good of individuals and society as a whole, both society itself and its elected political representatives must engage in a debate on how to shape the design of data-based technologies, including AI.

On 18 July 2018, the Federal Government set up the Data Ethics Commission (*Datenethikkommission*) and named its 16 members (→ see Annex, 2). Christiane Wendehorst and Christiane Woopen were appointed as co-spokespersons. The Data Ethics Commission was given a one-year mandate to develop ethical benchmarks and guidelines, aiming at protecting the individual, preserving social cohesion, and safeguarding and promoting prosperity in the information age. It was also asked to put forward specific recommendations for action and suggestions for possible legislation with a view to allowing these ethical guidelines to be observed, implemented and supervised. As a starting point, the Federal Government presented the Data Ethics Commission with a number of key questions (→ see Annex 1) clustered around three main topics: (I) algorithm-based decision-making, (II) AI and (III) data.

In this context, "**AI**" is understood by the Data Ethics Commission to be a catch-all term for technologies and related applications based on digital methods which involve the machine processing of potentially very large and heterogeneous data sets in a complex procedure that mimics human intelligence; the results obtained from such a procedure may be applied in an automated way. Some of the most important methods underpinning AI (as just one aspect of a much wider computer science landscape) include sub-symbolic pattern recognition, machine learning, computer-based knowledge representation and knowledge engineering, which in turn encompasses heuristic search methods, inference techniques and action planning.

The Data Ethics Commission however believes that it would be wrong to restrict the ethical and legal debate to AI alone. It is merely one among many possible variants of an algorithmic system, and thus represents a subset of this field. Both AI systems and other types of algorithmic systems share a number of features that may give rise to ethical problems, meaning that regulations focused on AI alone would tackle only part of the problem. The feature of self-learning, which is in the foreground in AI, brings with it specific challenges, and due consideration must be given to them at the risk assessment stage; at the same time, however, there are many other features besides self-learning that require special attention. The following arguments therefore relate to **algorithmic systems of all kinds**.

Applications are rarely based on a single algorithm, and examining algorithms in isolation is rarely meaningful. Any ethical appraisal must be based on the **sociotechnical system as a whole**, or in other words all the components of an algorithmic application, including all the people involved, from the development phase – for example the training data used – right through to its implementation in an application environment and any evaluation and adjustment measures.

2. Working method

Between September 2018 and September 2019, the Data Ethics Commission met on a monthly basis. It discussed examples of use cases for new technologies in a range of different sectors, and analysed them in terms of both the technology involved and the ethical and legal issues raised. The findings obtained from this work and from fundamental debates made it possible to identify overarching topics and questions, which were used as a starting point for the development of an ethical appraisal framework and the drafting of specific recommendations for future political and legislative action. As early as October 2018, in response to a policy paper by the Federal Government, the Data Ethics Commission put forward two specific recommendations for points that should be included in the Artificial Intelligence Strategy, and these recommendations were taken up by the Federal Government. In November 2018, the Data Ethics Commission issued another recommendation, calling for the roll-out of an electronic health record, building on a participatory process.[1]

The Data Ethics Commission involved the public in two public conferences. The first took place on 7 February 2019 at the Federal Ministry of Justice and Consumer Protection (*Bundesministerium der Justiz und für Verbraucherschutz*), and centred around the issue of "Self-determination and external determination in the age of artificial intelligence". The second – an international round table under the title "Towards ethical shaping of our digital future" – was held on 9 May 2019 at the Federal Ministry of the Interior, Building and Community (*Bundesministerium des Innern, für Bau und Heimat*). Both events allowed the Data Ethics Commission to engage in in-depth discussions with experts and stakeholders as well as members of the public and interested citizens.[2]

On 14 November 2018, during the Federal Government's *Digitalklausur*, an exchange of views took place between the Federal Chancellor, all the members of the Federal Government, and the two co-spokespersons of the Data Ethics Commission. Ad-hoc discussions were also held with individual members of the Federal Government. In addition, the Data Ethics Commission organised expert hearings and consultation meetings with other institutions and bodies working on related topics, including the Study Commission "Artificial Intelligence", the Commission of Experts on Competition Law 4.0, the Federal Government's Digital Council, the Advisory Council for Consumer Affairs and many more.

One of the defining features of the Data Ethics Commission is that its work and advisory activities are fully independent and free from any external political influence. All of the viewpoints outlined in this report reflect either the personal opinions expressed by the Data Ethics Commission's individual members, or the opinions that emerged from internal discussions within its institutional members. The Data Ethics Commission has adopted all of the recommendations in this report by consensus.

1 Both documents are available on the Data Ethics Commission's website (at *www.datenethikkommission.de*).
2 Further information on the public conferences, including video recordings, can be found on the Data Ethics Commission's website (at *www.datenethikkommission.de*).

3. Objectives and scope of the report

The goal pursued by the Data Ethics Commission in publishing this report is to further the development of our **ethical and legal framework** in order to confront the challenges posed by digital technologies. The main concern is to ensure that the fundamental conditions are in place for the free democratic basic order to be preserved, and for the potential that exists to be leveraged so that sustainability-oriented goals can be achieved and our social market economy can flourish.

Given the increase in the volume of personal data being collected and the use of automated methods to process these data for different purposes, one of the main priorities of the Data Ethics Commission is to reconcile the need to protect the **individual's fundamental rights and freedoms** – including self-determination and integrity – with the need to promote progress, prosperity, the safeguarding of democracy and the shaping of a society that is fit for the future. Protecting individuals against data misuse and discrimination and guaranteeing the security of all parties involved are tasks that fall squarely within the remit of a State governed by the rule of law, and effective regulations must be adopted and institutions set up for this purpose. At the same time, however, the State must facilitate the emergence of innovative business models that safeguard future prosperity for everyone.

The Data Ethics Commission believes that digitalisation – in particular the rapidly increasing availability of data and the use of complex algorithmic systems, including AI – holds **enormous potential** for technical and social innovation and for achievement of the UN's Sustainable Development Goals. Promising avenues for action include promoting health, humanising the world of work, designing sustainable cities and communities, providing a decent education and implementing effective climate protection measures. At the same time, however, we must not forget the **major risks** that may face individuals, society as a whole and the free democratic basic order in connection with the extensive use of digital technologies. These risks include the possibility of high-granularity profiling (using techniques such as online tracking, voice analysis during remote job interviews, or even the diagnosis of pathological mental conditions on the basis of social media posts), the potential for these profiles to be exploited for the purpose of controlling and manipulating people (either on a small scale through individual pricing or on a larger scale by manipulating democratic opinion-building processes through "micro-targeting"), the potential for discrimination against different social groups, and the ability to delegate human responsibility to machines. With these factors in mind, the Data Ethics Commission believes that we must actively shape our future in such a way as to realise the potentials while avoiding the risks.

The Data Ethics Commission advocates for a multi-step approach to achieving these goals. The first step is an ethical reflection on the value of human activity in an environment shaped by technology, and a reaffirmation of the **key ethical principles and precepts** upon which our society is founded (→ Part B). In the view of the Data Ethics Commission, the key questions can be divided into questions that concentrate mainly on data (the "data perspective") and questions that are primarily focused on algorithmic systems (the "algorithms perspective"). These two perspectives represent ethical discourses which both complement each other and are contingent upon each other, and which are also each reflected in different **governance instruments** (→ Part D).

In the section devoted to the data perspective (→ Part E), the Data Ethics Commission outlines general ethical principles for **data governance** (→ E 1), in particular ethical principles governing **data rights and data obligations** (→ E 2); these serve as the basis for a series of specific recommendations for action regarding the use of data and data access (→ E 3 to 5). In the section devoted to the algorithms perspective (→ Part F), the Data Ethics Commission sets out general ethical requirements for the **design of algorithmic systems** (→ F 2) and the **risk-adapted regulation** of these systems (→ F 3). The instruments and institutions that would be required to implement regulations of this kind are examined in detail and summarised in recommendations to the legislator (→ F 4 to 8). A shared basic understanding of technical parameters and relationships (→ Part C) serves as an essential foundation for considerations of this kind. The report ends with a plea for the Federal Government to follow a "European path" (→ Part G).

As per its mission, the Data Ethics Commission's recommendations are targeted primarily at the German **Federal Government** and its associated institutions. At certain points, however, the target audience is widened to include other stakeholders, for example Länder and municipalities, research institutions or enterprises. The Federal Government is always the secondary target audience of any such recommendations, given the underlying recommendation for it to encourage and support these other stakeholders in their efforts. All of the recommendations should also be viewed in the context of the institutions and rules that have been or will be put in place at EU and international level, and in the context of further developments in these arenas. In cases where the Data Ethics Commission suggests that a recommendation should be implemented at **EU or international level**, it should be interpreted as a recommendation to the German Federal Government to make a vigorous and future-oriented contribution to the debate taking place within Europe and across the globe.

Part B

Ethical and legal principles

1. The fundamental value of human agency

Given the fast-paced development of digital technologies, including self-learning algorithmic systems ("artificial intelligence") which incorporate certain functions that can outperform the abilities of humans, the elementary question is raised **whether human agency poses an ethically relevant value in and of itself** which transcends considerations of effectiveness and efficiency, and which is inherently preferable to the functioning of machine systems. This question is all the more pressing as the momentum and internal logic of international competition are, for the most part, dictated solely by the goal of maximising economic efficiency.

Human agency derives its basic value from its moral significance. A human being can provide reasons for one's actions and decide whether or not to perform them, and must bear responsibility for these actions. It is only by taking action that individuals can develop and realise their full potential in accordance with their capabilities, preferences and understanding of a meaningful life. This **dimension of meaning** lends a value to human activity that could never be claimed for the functioning of technical systems. Technology can only ever be the means to achieving a goal that humans have set. Even if – hypothetically speaking – humans were to decide that algorithmic systems could set themselves goals, allowing them to do so would be a goal that had been set by humans. The use of technical systems may therefore be a component of human activity, and may even be ethically required in certain cases, but it will never be possible for technical systems to replace the moral dimension of human agency completely. Human agency and the human drive to develop as a living being are characterised by their multi-dimensional nature. Although the conceptions of man espoused by different cultures and different faiths vary significantly, they all incorporate the dimension of the living and of moral responsibility, and despite all the differences in the respective answers, they all embrace the question of the meaning of life whereas technical systems merely function.

We must weigh up many different criteria when identifying cases in which preference should be given to human activity over the use of algorithmic systems. As a basic principle, a higher level of effectivity should be prioritised only with regard to the performance of certain limited functions. **Effectiveness should not rule supreme.** It must not place material restrictions on the ability of humans to take action as a form of self-development, and it must take second place to the basic ethical dimension of a meaningful and flourishing life, both as an individual and as a member of society. For example, even if it were possible for a human to be cared for more effectively by a robot than by another human, care by a robot cannot be allowed to replace the human element of attention and affection for the person needing that care. At the same time, however, the use of robots to perform care-related tasks alongside humans may be deemed expedient if it makes the situation significantly safer for the person receiving care. Yet the effectiveness gains of technical systems must take a back seat if they entail an intrusion into the privacy or personal integrity of the individual, for example because they force an employee to modify all of his or her work processes in order to maximise effectiveness. People must be allowed to retain their subjectivity rather than morphing into objects that are "acted upon" by machines.

Humans are morally responsible for their actions, and there is no escaping this moral dimension. Humans are responsible for the goals they pursue, the means by which they pursue them, and their reasons for doing so. This dimension must always be taken into account when designing our technologically shaped future. At the same time, the notion that technology should serve humans rather than humans being subservient to technology can be taken as incontrovertible fact. Germany's constitutional system is founded on this **understanding of the human being**, and it adheres to the tradition of Europe's cultural and intellectual history.

2. Relationship between ethics and law

Exponential technical developments relating to the collection and use of digital data and the deployment of algorithmic systems and artificial intelligence are increasingly shaping the life of every individual and all aspects of our social coexistence. These developments give rise to far-reaching and profound questions, and the answers to these questions must be guided by the **fundamental legal and ethical principles** that a democratic society undertakes to uphold.

The benchmarks and guiding principles underpinning the processes by which society shapes and has to shape various sectors – the economy, education, public spaces, healthcare, finance, transport and energy – are fundamentally ethical in nature. Although liberal systems are characterised by a high degree of moral pluralism, a common ethical framework is nevertheless established in constitutional law, and more especially in fundamental rights as far as the relationship between the State and the individual is concerned. The significance of this ethical and legal framework in relation to an individual case and in the event of conflict between differing values or fundamental rights is not always clear-cut. Yet this does not relativise the binding nature and **fundamental importance of the ethical foundation of our community**. Instead, it merely goes to prove once again the crucial importance of an open and ongoing debate on the future shape of our society, and serves as a basis for democratic decision-making processes that acknowledge the possibility of different answers within the framework of the Constitution.

Ethics cannot be equated on a one-to-one basis with the law. In other words, not everything that is relevant from an ethical perspective can and should be enshrined in legislation; conversely, there are provisions of the law that are motivated purely by pragmatic considerations and are not ethically imperative. Nevertheless, legislation must, at all times, be heedful of its potential ethical implications and must live up to ethical standards – at the very least, the requirements outlined in constitutional law.

The Data Ethics Commission holds the view that regulation is necessary, and cannot be replaced by ethical principles and guidelines in cases where the constitutionally developed **principle of materiality** requires the enactment, in the form of parliamentary legislation, of democratically legitimate rules that can be enforced against anyone. Internet governance is also the governance of society. As algorithmic systems, including artificial intelligence, become an increasingly normal feature of the daily lives we lead together in society, we must also develop and enforce rules to govern them. This calls for an ongoing public debate, and also – particularly in cases where fundamental rights are at threat – parliamentary debate and legislative initiatives. Given past experiences of law enforcement in the Internet sphere, and in view of the experience that power tends to be accumulated in the hands of a few large corporations in certain sectors of markets dominated by digital technologies, a systematic move away from enforceable rules and towards voluntary regulation would appear to be a mistake.

At the same time, regulation must not unduly inhibit technological and social innovation and dynamic market growth. Overly rigid laws that attempt to regulate every last detail of a situation may place a stranglehold on progress and increase red tape to such an extent that innovative processes in Germany can no longer keep pace with the rate of technological development on the international stage. On the other hand, regulatory frameworks can and must protect fundamental rights and freedoms and create legal certainty. This is an essential first stage in building a system within which citizens, companies and institutions can trust in the fact that the transformation of society will be guided by ethical principles. In addition, the “toolbox-like” nature of the legal system with its options for regulating matters at many different levels, ranging from acts and ordinances right down to codes, self-governance options and voluntary obligations, makes it suitable for creating a framework that is adaptable and can keep up with technological progress.

However, the **need for guidance goes far beyond the regulatory sphere**. With this in mind, many different stakeholders – such as professional groups, companies and advisory boards at national, regional and international level – have responded to the manifold upheavals by drafting ethical codes or sets of guiding ethical principles, in some cases with an ensuing public debate.

The Data Ethics Commission welcomes the diversity of stakeholders taking action and the number of voices being heard in the discussion on how the process of digitalisation can be shaped in an ethical way, since this highlights the indispensability of public debate and **for everyone to take responsibility for the flourishing of our future lives together**. In keeping with the mission assigned to it in the coalition agreement, the Data Ethics Commission has based its recommendations for a "framework on how to develop data policy and deal with algorithms, artificial intelligence and digital innovations" not only on the precepts of constitutional law, but also on cross-cutting ethical principles that apply to differing degrees in all areas of society; these principles are briefly outlined below.[1]

1 By following this approach, the Data Ethics Commission is adhering to the same basic principles endorsed by the European Group on Ethics in Science and New Technologies (EGE) in its opinion: EGE: Statement on Artificial Intelligence, Robotics and "Autonomous" Systems, 2018, (available at: *http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf*).

3. General ethical and legal principles

3.1 Human dignity

Human dignity, which from an ethical viewpoint is synonymous with the unconditional value of every human being and which is enshrined as a "fundamental constitutional principle" in the constitutional order, is of foundational and supreme importance. It follows from the principle of human dignity that every individual merits respect, regardless of his or her attributes and achievements. Protecting the value which is inherent in every human being and which does not need to be acquired also implies that human beings are not ranked in a classifying system across various spheres of life and activities ("super scoring") or labelled like an object with a price and treated accordingly. The fact that each human is an individual rather than a pattern made up of data points must also be borne in mind at all times in situations where human behaviour is measured and these measurements are processed by algorithmic systems. Algorithmic systems must therefore always be designed in such a way that they can cater to each human's claim to individuality.

Acknowledging human dignity involves recognising that humans must always be "superior to technology", i.e. that they must not be completely or irrevocably subordinated to technical systems. The opportunities for configuration and intervention may be localised at different levels in each specific application, but the **principle of human sovereignty of action** must be upheld. Humans hold responsibility in human/machine interactions, and must not be regarded as defective beings that need to be optimised or perfected by the machine. Instead, human use of algorithmic systems aims at realising human ideas and objectives more effectively and rapidly and with fewer errors.

Protecting human dignity also involves ensuring that the **human as a relational being** is not misled by technology about the nature of a relationship; for example, it would be wrong for a human to be systematically deceived into thinking that he or she is speaking with another human when it is actually a bot. The **psychological integrity of the individual** is a particularly important factor in protecting human dignity. This rules out the use of data-driven systems for manipulative purposes, particularly when the systems draw on comprehensive and highly granular personality profiles. It also rules out the use of algorithmic systems to **discriminate systematically against individuals or groups**, for example by "downgrading" them, preventing them from using certain services for ethically untenable reasons or systematically misleading them as they participate in the democratic discourse.

3.2 Self-determination

The opportunity for self-determination is inextricably linked with human dignity. Humans **express their freedom** by determining their life goals and the way they lead these lives, as a basis for determining, developing and enacting the very essence of their self. A society that takes freedom seriously must put in place a framework within which its citizens can develop freely and respect each other's freedom, despite all their differences. For example, if people are to lead a self-determined life and develop in freedom, technical systems must not restrict and control human avenues for action without an ethically meaningful reason. Self-determination must not be viewed solely through an individualistic lens – humans are relational beings whose life unfolds through social interactions with others, on the basis of manifold reciprocal links and influences.

The rules that govern these interactions are shaped over time by the **cultural and socionormative framework** that serves as a basis for our life together in society. They are also shaped by law in a democratic society, especially where imbalances of power and information prevail.

The more information third parties have collected about an individual, the more difficult it becomes for that individual to act unselfconsciously in social situations or even to reinvent himself or herself completely. Steps must be taken to ensure that data collection and evaluation practices do not result in personal and social profiles being routinely created in multiple locations, thereby "cementing" a particular version of the individual. Self-determination therefore also encompasses the **right to develop and alter one's own identity**, and the possibility of starting one's life afresh. The right to self-determination thus also includes each individual's right to decide how he or she is perceived in public and to prevent public misrepresentations.

Another vital aspect of self-determination is that people must not only be allowed to assume **responsibility**, but must do so and do justice to the task. Responsibility always lies with a human – institutionally enshrined, if necessary – never with a machine. Even if a technical system is used to apply inferences based on automated evaluations (i.e. whether or not a loan should be granted), the responsibility for developing and using this system in an ethically sound manner must lie with humans.

An important manifestation of self-determination is **informational self-determination**. It includes the individual's right to determine who can collect and use which personal data, when they may do so and for what purpose. Informational self-determination allows an individual to protect his or her freedom of action and privacy to the extent he or she deems important, and also to determine as what personality he or she wants to be perceived and treated in public.

In this era of digitalisation, the special importance of individuals as self-determined actors in the data society goes beyond their informational self-determination. The term **digital self-determination** refers to this; it encompasses the skills needed by an individual to determine for himself or herself the content that should be used as a basis for interacting with his or her environment, and how he or she can unfold his or her own personality in an interactive way. Under certain circumstances, it may also include the self-determined economic exploitation of an individual's own data assets and the self-determined governance of non-personal data, for example the data generated when operating certain devices. Digital self-determination always goes hand in hand with digital accountability.

The Data Ethics Commission takes the view that **businesses and legal persons** should also be entitled to a right to digital self-determination. Legal persons cannot invoke the concept of human dignity granted by Article 1 paragraph 1 of the [German] Basic Law (*Grundgesetz*, GG) and protected in the framework of the general right of personality, and are therefore barred from referring to the associated core area of personality development, which enjoys absolute protection. Article 2 paragraph 1 of the Basic Law, in conjunction with Article 19 paragraph 3 of the Basic Law, does however grant legal persons a protected right of personality that also incorporates a right to informational self-determination.

The ability of consumers to take self-determined action and conscious consumption decisions is a vital prerequisite for optimum resource allocation and maximisation of the public good at macroeconomic level. Any erosion of the **skills needed by consumers** to exercise their right of self-determination, for example because of the excessive use of decision-making assistants and the associated habituation effects, raises ethical questions regarding external determination and the freedom of individuals to take decisions, and also regarding the ability of a small number of market-dominant firms to exert control over society.

3.3 Privacy

The **protection of human dignity and self-determination** are closely and materially linked with the protection of privacy. The individual's right to determine who may access which personal information relating to him or her, and when and for what purpose they may do so (informational self-determination, see section 3.2 above), is justified by the supreme ethical importance of the ability to prevent intrusions into one's private sphere and also to appear in public in the certainty that one's privacy is protected. Efforts to protect human dignity must include legislative measures to regulate the responsible use of personal data.

A further aspect of privacy is the need to **preserve the integrity of an individual's personal identity**. For example, this integrity may be violated if an algorithmic system – using data collected for entirely different purposes – "calculates" the personality of an individual together with his or her preferences and proclivities, and the system operator then uses these calculations for its own purposes, regardless of or even contrary to the individual's will.

Given that different spheres of society are being shaped more and more by data-driven technologies, it is important for us to **increase the amount of attention we pay to the use of data**. Many people are willing to make their personal data available for public or semi-public use because they will receive certain products and services in return, or because they wish to contribute to the public good. Merely telling the public to think twice before disclosing personal data is not effective. Instead, effective regulations must be adopted so that people can rely on the fact that their data will be used responsibly, and that steps will be taken to prevent any ethically unacceptable uses.

3.4 Security

Algorithmic systems also give rise to crucial security questions. The context of use may promote or jeopardise user security. Security is relevant from an ethical and legal perspective because of the role it plays in **protecting high-ranking values**, such as an individual's physical and mental health and his or her privacy, or public security, peace, and free and equal democratic elections.

Security can relate to collecting and using data, which means that the concept also has a bearing on the **protection of privacy**. The major data scandals that have hit the headlines in recent years have made it clear that privacy breaches and the use of personal data for manipulative purposes can have far-reaching – and sometimes political – consequences.

Consideration must also be given to the **physical and emotional safety** of an individual who operates and uses an algorithmic system. Stringent requirements apply in this respect, e.g. in connection with human/machine interactions. If a robot carer is used, for example, it must be ensured that neither the person receiving care nor the person providing care suffer any harm in terms of their physical and mental integrity.

Algorithmic systems may also have an impact on **environmental safety**. Malfunctions of algorithmically controlled public infrastructures, e.g. traffic or energy and water supply infrastructures, may cause enormous amounts of damage.

Algorithmic systems may also be innately unsafe, causing malfunctions or even functioning as **gateways for malicious attacks and manipulation**. Even beyond inherent system vulnerabilities of this kind, it must not be forgotten that an algorithmic system could be misused for harmful purposes.

3.5 Democracy

Digital technologies are in a complex manner **systemically relevant** for the development of fundamental rights (in particular freedom of expression and information, (informational) self-determination, confidentiality of telecommunications, freedom of assembly and association, freedom of occupation and right to property), for democracy, for the safeguarding of diversity, for an open societal debate and for free and equal elections. For example, social media sites serve as a low-threshold opportunity for every citizen to participate in debates on the shape of our future, and as such should in principle be welcomed. At the same time, however, there is a risk that they may be used for manipulation and radicalisation. The State should take decisive action to counter these risks by adopting rules and setting up institutions capable of preventing undesirable developments and misuse.

It is also an undeniable fact that the rise of the Internet has been accompanied by an economic decline in journalism and its privately funded plurality. Yet the electronic public sphere cannot in any way be considered a valid replacement for the role played by journalism in a democracy, namely that of a "fourth estate" or "watchdog of democracy" – i.e. an instance that exercises control of power and claim to truth on the basis of systematic and independent investigations and criticism. Under certain circumstances, powerful **media intermediaries playing a gatekeeper function** may exert a controlling influence over the democratic formation of will, posing a significant threat to democracy that – based on ethical considerations and the provisions of constitutional law – must be countered through legislative means.

Education and training must also play a prominent role in safeguarding the free democratic basic order, since they influence, in a wide variety of ways, the participation of citizens in the shaping of society – a process that is of critical and fundamental importance for democracy, these citizens' understanding and appraisal of socially relevant interrelationships and developments, and – ultimately – their level of confidence in a future that can be shaped and that is founded on values. Education and training must impart not only technical and mathematical skills, but also skills in the fields of ethics, law, economics and the social sciences.

3.6 Justice and solidarity

Observance of the principles of justice by society and its institutions is another fundamental factor that allows us to live together in peace, prosperity, freedom and democracy. Data and technology have placed enormous influence – both economic clout and the societal sway that results from the former – in the hands of a small number of large companies, and this has raised new questions about a fair economic order. The availability of large volumes of data and the digitalisation of processes e.g. in the workplace and the healthcare sector raises other questions relating to **equitable access and distributive justice**, however, for example in relation to income and the provision of healthcare; these developments may mean that scarce resources can be distributed more fairly, but they may also mean that individual groups of people suffer disadvantage or discrimination.

There is also a close link between justice and opportunities for participation. **Stronger participatory processes**, also supported by digital tools, can play an important role in promoting social innovations during a time of technology-induced social upheavals. Finally, questions of justice arise in connection with situations where the use of algorithmic systems – in particular self-learning algorithmic systems – means that individuals or groups of people suffer discrimination for no justifying reason.

A clear **assignment of responsibility and accountability** is an indispensable feature of a democratic State under the rule of law. An adequate level of transparency and explainability is an essential prerequisite for auditing algorithmic systems appropriately on the basis of their real potential for harm. Opportunities for seeking legal recourse and, if necessary, holding another party accountable, i.e. liable, must also be available under certain conditions.

In the world as it stands today, **access to digital resources** via the Internet is a fundamental requirement for digital and thus also social participation. As part of its public provision remit, the State is obliged to ensure that its citizens can access up-to-date Internet infrastructure anywhere in the country and to an adequate extent, using either a fixed or a mobile connection. As part of its educational remit, it must provide its citizens with the skills needed for self-determined navigation of the digital world and for accurate appraisal of the opportunities and risks of Internet use.

Opportunities for participation promote **social cohesion**, which is also based on a fundamental attitude of societal solidarity and integration of the latter into the institutional framework. Digital technologies may strengthen solidarity, but may also weaken or destroy it. When algorithmic systems are used in certain spheres of society such as the insurance sector or the provision of opportunities for social participation, care must be taken to avoid a systematic weakening of solidarity, which may, in some cases, be caused by very subtle effects. For example, it is perfectly possible for data-driven differentiation and unequal treatment that appears plausible and justified in individual cases to lead overall to a reduction in solidarity with certain groups of people, some of whom may be particularly reliant on society's support.

3.7 Sustainability

Digital technologies offer huge potential in terms of more efficient resource management and innovative business models. This economic aspect generally attracts the lion's share of attention in general debates on the topic. To date, however, less interest has been shown in the question of whether digital technologies can also contribute to economic sustainability. Consideration must also be given to issues relating to ecological and social sustainability. The UN has adopted **17 Sustainable Development Goals relating to economic, social and ecological aspects**, which apply to all the UN Member States and should be achieved by 2030. Digital technologies may make it easier to do so; this is the aim pursued by the International Telecommunication Union (ITU) with its "AI for Good" initiative, for example. Similarly, the German Advisory Council on Global Change (*Wissenschaftliche Beirat der Bundesregierung Globale Umweltveränderungen*) recently outlined its vision of an AI-based and highly granular network of environmental sensors that would allow unprecedented "comprehensive and real-time monitoring of the natural Earth systems, their condition and development", as a vital building block in a future digital sustainability policy.

Yet digital technologies do not only conserve resources; they also consume them, for example through the ever-rising demand for electricity and the reliance of digital products on certain rare earth elements that are only available in limited quantities and in certain countries. Rare-earth mining causes enormous damage to the environment. This raises questions with regard to sustainable economic and ecological development, and also **questions of international justice** concerning the use of natural resources and global responsibility for future generations.

Human knowledge and human skills are also resources whose sustainability must be safeguarded. The development of digital technologies and the concomitant reduction in the tasks that need to be performed by humans will mean that individuals gain certain new skills but lose other **competences of the human being**. A debate must be held on our responsibility towards the next generation, and measures are required to preserve and develop certain skills and avenues for independent action.

As noted elsewhere in this Opinion, there is a need for regular and comprehensive **technological impact assessments**, and these assessments must also consider the sustainability of new technologies in their various manifestations. It is incumbent upon the legislator to ensure that responsibility for sustainability is incorporated into the rules that govern the data economy and algorithmic systems, for example through the introduction of an obligation to disclose the entire energy footprint of an energy-hungry blockchain system.

The pursuit of sustainability goals set by the United Nations should be a particular focus of **public investments** into the data economy and algorithmic systems. When allocating government funding, priority should be given not to economic gains which are only short-term in nature, but to the development of data and algorithmic systems for purposes such as recording and monitoring environmental impacts and developments, or systems for optimising and reducing energy and resource consumption. In addition, more should be done to promote sustainability-oriented social innovations that foster social creativity and participation.

Part C

Technical foundations

Data-intensive IT applications have a lasting impact on our living and working environment, our economy, our scientific endeavours and our society. As well as being permanently tethered to our smartphones, we use search engines on a daily basis, rely on recommendation software, send text or voice messages to our family and friends, regulate the temperature in our home remotely and allow navigation devices to guide us from one place to another. We are able to do so because of a series of technological developments that have occurred over the past few decades. Some of the fundamental technical concepts underpinning these developments are described below; the aim is not to provide a comprehensive account but to highlight key points as a basis for identifying any resulting problems and starting points for potential governance approaches.

1. Status quo

Entirely new fields of application have been opened up thanks to the improved performance and miniaturisation of the physical components of IT systems (hardware) that are used to store and process data, along with continual enhancements to both wired and wireless connectivity. Smartphones, tablets and wearables are gradually infiltrating our workplaces and homes, along with sensors, actuators and, in some cases, "autonomous" systems such as robots. In many locations, the Internet is "always on" thanks to mobile access, making it possible – e.g. in combination with various sensors in smartphones, such as geolocators, gyrosensors, cameras, microphones, etc. – not only to input text, but also to upload image, video and audio recordings to the Internet at any time and from almost anywhere. This penetration of technology makes it possible not only to communicate and use social networking sites, but also to link devices to the Internet of Things (IoT).

It has become impossible to draw a clear dividing line between the analogue and the digital worlds; the former contains more and more components that transfer information into the latter, while digital information is becoming ever more widely available in the analogue world, bringing the two closer and closer together and creating a **hybrid world**.

Data volumes are increasing exponentially thanks to comprehensive arrays of sensors, the IoT and the falling price of storage capacity. Specialised tools are needed to process such large volumes of data. At the same time, the accumulation of so much data (together with the availability of high-performance hardware) has promoted the widespread use of machine learning procedures, and some of these have achieved impressive results, for example in the field of speech and image recognition.

Speech recognition and video processing have now seen such huge leaps forward in terms of performance that there is potential for the **boundaries between reality and computer-generated information** to become blurred. When this happens, people are no longer sure whether or not they are talking to a speech bot, or whether they are watching a normal video recording or a "deep fake", i.e. a synthesised human image saying things that the real person never actually said.

2. System elements

2.1 Data

2.1.1 Definition and properties of data

In keeping with the Data Ethics Commission's mission, this report concentrates on data that are **digital and machine-readable**. These data are made up of a stream of binary electrical impulses, which may be transient (signals that only exist for an instant, e.g. a control impulse for a technical system) or persistent (stored on a medium).

Data are multifaceted. The word "data" is an umbrella term that encompasses an enormous range of manifestations. For example, data can be categorised on the basis of data type (e.g. binary, nominal, ordinal, metric and textual data), the process used to generate the data (e.g. survey data, sensor data), the sector in which the data are collected (e.g. financial data, weather data) or their function in a digital system (e.g. login data, training data). They can be further categorised on the basis of their level of processing. Data that have not yet been processed are referred to as "raw data". Processed data are referred to as "structured" or "unstructured", depending on the level of structuring (normalisation). Data can function as the input into a system or the output from a system, and an output may, in turn, function as an input into another system. Data can also represent digital assets, such as multimedia content or units of cryptocurrency. A further distinction of enormous legal significance is that between personal and non-personal data.

The terms "data" and "information" are not always synonymous. To make sense of the **binary electrical impulses** that form the basis for digital data, i.e. to transform data into "information", it is necessary to know their **context** and **semantics** (meaning). One possible context would be the origin of a generated signal – knowing which precise sensor emitted a signal, for example. The term "semantics" refers to the information contained in a certain sequence of binary signals; for example, a "4" that appears in a survey may equally well represent the number of children in a household or the number of tubes of toothpaste bought in the past six months. Potential sources of context and semantics include metadata, domain tables, ontologies, identifiers and other technical specifications that supplement data values. Whenever the term "data" is used in the remainder of this report, familiarity with the context and semantics will always be implied.

Data are of varying quality. The purpose of most data – or, more accurately, the information contained therein – is to reflect reality as accurately as possible. This can for example be done by assigning attributes that are exhibited by entities in real life to the correct entities in the digital world (information objects). There are also many types of data that are intended to express the likelihood of something happening in reality (either now or in the future). Some types of data are intended to construct a hypothetical reality, while others have no relation to reality whatsoever. In all of these cases, the pool of data **may contain errors**. A distinction should be made between these errors and cases in which the data do what is expected of them but are **unsuitable** for achieving a specific goal, for example performing a particular analysis (e.g. the data are insufficiently granular, or outdated, or incomplete in some way).

The quality of the data used is of decisive importance for data-driven systems, since even a perfect algorithm cannot deliver high-quality results if it receives poor data as an input (i.e. inaccurate or inadequate data). Data quality is not an absolute value; the relevant data quality dimensions and their quality level depend on the specific use (see Figure 1).

Figure 1: Example of different use-specific quality requirements

2.1.2 Data management

Data are not some pre-existing entity – they are created. The process of collecting, preparing and processing data involves many different human decisions that have implications for the future use of the data. For example, the potential that might have been gained from data may be irretrievably lost if they are stored without any context or semantics. Careful **data management** is necessary to avoid situations of this kind.

Before collating data from different sources, it is vital to ensure that the collation will be possible from both a technical and a semantic perspective ("interoperability"). The data from these different sources must be mapped against each other in a way that reflects their semantics. In cases where interoperability is particularly important, efforts should be made to achieve **standardisation** of the technical specifications (formats, descriptive metadata, etc.). Reference data play an important role in this respect, i.e. standardised schemes or ontologies, some of which fall under the remit of national or international institutions (e.g. the International Classification of Diseases (ICD) published by the WHO).

2.1.3 Big data and small data

The term **"big data"** does not refer to a separate type of data, but instead to a new methodological approach for the identification of relationships. Laney[1] famously used the "three Vs" – volume, velocity and variety – to define this approach while it was still in its incipient stages; large volumes of varied data, potentially from a variety of sources, are generated at high velocity (often in real time). Special technologies are needed to process these large volumes of rapidly changing data that vary in terms of both their nature and their quality. The analysis of large data sets ("big data") is particularly well suited to situations where it is necessary to identify the most promising of a large number of potential correlations. In the field of medical research, for example, it is helpful to start with big data methods that identify a number of likely candidates from a long list of environmental factors that might increase risk for a disease, before going on to perform costly and high-precision experiments or studies that investigate only these candidates. A specific problem associated with this approach is that it initially shows only **correlations** rather than causalities, and completely unsuitable candidates may therefore be identified.

1 Doug Laney: 3D Data Management. Controlling Data Volume, Velocity, and Variety, META Group Inc., 2001.

In many areas, the volumes of data available will never be large enough to allow analysis using big data methods (for example, the client base of a small or medium-sized company may never exceed 200 customers, and the number of political parties in one country rarely reaches three figures). Suitable **"small data"** analytical methods can also be used to extract a great deal of knowledge and information from data. The quantity of data is not what matters; instead, the decisive factor is the availability of suitable tools that make it possible to combine data of an adequately high quality in quantities that are sufficient for the task at hand, as a basis for effective data analysis.

2.2 Data processing

2.2.1 Algorithms

From a data protection point of view, the term **"processing"** refers to the entire sequence of actions from data generation and extraction through to storage and any transformation of the actual data (Article 4(2) GDPR). By way of contrast, the mathematical and technical sciences mainly deploy the term to refer to the use of data. The following arguments are based on the latter of these two understandings of the term.

Any method of digital data processing follows the **IPO (input, processing, output) model** – data enter a system as an input, are processed, and then leave it as an output. Any form of internal processing within an IPO system is based on an algorithm, or in other words an operational processing sequence that specifies a procedure as a series of different processing steps, with the aim of achieving the desired result through successive transformations of the data inputs. Algorithms have been around since the time of Euclid, who specified a method for easily calculating the greatest common divisor of two natural numbers. The word "algorithm" is derived from the name of the Arabian mathematician al-Khwarizmi (formerly Latinised as "Algorithmi"), who published a collection of calculation rules for solving algebraic equations in 830 AD or thereabouts.

It is hard to overestimate the importance of the term "algorithm" in modern computer science. To solve a particular problem by processing data, an algorithm must not only be implemented correctly, but also used productively. This presumes a knowledge of the algorithm. In many cases, however, the algorithm that will ultimately deliver the desired result is not yet known, and the first and most important task is to **find a suitable algorithm**. For many situations of practical relevance, the processing specifications can be derived directly (i.e. deduced) from specialist knowledge, known models or legislative provisions. In other situations, our understanding of the context is not yet sophisticated enough to allow it to be described using more or less simple mathematical formulae.

If this framework of understanding is absent, various strategies can be applied to identify an algorithm. These include random chance, trial and error or data-based **inference**. The latter approach follows the principle of induction – an attempt is made to infer a general rule from individual cases (i.e. the data). If a general rule is found that can be used to solve the question, it can be assumed to be a suitable algorithm. It is worth remembering that there may well be several suitable rules, and furthermore that the result of this process of induction may not necessarily be correct. The result inferred from the individual cases may be partially or wholly inaccurate.

2.2.2 Statistical inference

A central concern of statistics is the drawing of inferences from data. **Statistical inference procedures** can be applied to data sets to investigate problems that lack a known inherent logic. More importantly, however, they can also be used for problems where random chance forms an integral part of the process to be modelled. Examples would be estimating the probability that it will rain on the following day, or identifying high-probability prospects for a particular product. There are many different statistical inference methods to choose among, starting with various forms of regression (linear regression, logistic regression or regularisation (ridge regression)), moving through support-vector machines (SVM), Bayesian networks and rule learners (such as Aprioiri, CART and random forest), and ending up with neural networks (NN). All of these procedures are suitable for extracting information from the available data. Some of them are specifically designed to solve regression questions, for example estimating the future height of a child based on the height of his or her parents, whereas others, such as SVM, CART and NN, are used for classification-type question, e. g. pregnant/not pregnant, dog/cat. Whether or not they represent a suitable means of answering a question depends on many factors, including the data volume and type.

Besides methods for induction, statistics offers a broad set of **tools for measuring the quality of the results (estimations) obtained**. These measurements can be used to estimate potential errors and to monitor actual errors in practice. Thus an estimate of a child's future height can be stated as 175 cm with a deviation range of +/– 4 cm. If a pregnancy test yields a positive result, this result might be deemed to be 93% accurate. A pregnancy test is a good example of the need to monitor two different parameters: the number of false positives (e. g. when the women is not pregnant but the pregnancy test is positive) and the number of false negatives (e. g. when the woman is pregnant but the pregnancy test is negative). The ideal statistical procedure would never result in any of these errors. In practice, it is necessary to weigh up the severity of the two errors and decide which false rate should be minimised. Is it worse for a woman to find out at a later date that she is, in fact, pregnant after being told that she is not, or for a woman to be told that she is pregnant when this is not true? The two error types cannot be minimised at the same time, since it is generally the case that the lower the frequency of one, the higher the frequency of the other. A balance must be struck, and this will look different depending on the context.

The quality characteristics of the methods themselves are used as a basis for assessing the quality of the results. It is even possible to **guarantee the quality** of the results obtained using certain methods; for example, estimation procedures that use a uniformly minimum-variance unbiased estimator (UMVUE) ensure that the best possible results are obtained using the data available. If a regression using UMVUE-based parameters supplies a result stating that the expected height of a child is 175 cm +/− 4 cm, no other estimator would have achieved a smaller error margin. Similarly, if a support-vector machine is used, the model determined on the basis of the relevant data (provided that a model can be found at all) is guaranteed to be the best possible model for the method in question. In certain cases, well-founded procedures for assessing the quality of either the model itself or the estimates generated using the model are yet to be developed – this applies, in particular, to the method class of neural networks. Quality indications can also be provided for neural networks, however. Measurements of how well a model functions using data that were previously unknown are particularly important. The model is taught using one data set (training data) and assessed for quality using a different data set (test data). This approach can be used to identify models that do not reflect the general rule because they have learned their training data too thoroughly. Cases of this kind are referred to as overfitting; an overfitted model will achieve significantly better quality values for the training data than for the test data.

Many statistical procedures can be solved analytically. This means that the question can be formulated as a mathematical equation or a system of equations and solved through transformations (even though this often requires a great deal of skill). However, a direct analytical solution is impossible for many other methods (for example if additional conditions such as a regularisation term are applied, see below). In these cases, use can be made of **optimisation procedures** that approximate the solution through many small steps. Optimisation procedures are not necessarily optimal; for example, the calculated result may be only a local optimum and not the global optimum (or one of them).

Different classes of problems: analytical procedures and optimisation procedures

A direct analytical solution is possible for tasks such as “Find the value of y for the equation $y=4 \cdot x+3$ where $x=3$”.

A solution of this kind is not possible for the task “Solve the linear equation $a \cdot x_1 + b \cdot x_2 + \cdots + h \cdot x_8 = y$, in which as many parameters as possible a, b, ..., g, h are equal to 0”.

An additional regularisation term is applied for this purpose: $\min((a \cdot x_1 + b \cdot x_2 + \cdots + h \cdot x_8 - y) + \text{sum}(\text{parameter} \neq 0))$.

Optimisation procedures are used to find solutions.

2.2.3 Machine learning

The boundary between traditional statistics and **machine learning**, a term first defined by Mitchell,[2] is difficult to delineate. The scales tip towards machine learning at the latest when optimisation procedures (→ see section 2.2.2 above for further details) are used to solve inductive inference problems.

The different approaches to **estimation or "learning" strategies** that fall under the heading of machine learning can be differentiated on the basis of the formulation of the optimisation problem to be solved. A distinction is made between a number of different learning procedures:

- **Supervised learning:** Supervised learning procedures require knowledge of the correct output (the "O" in the IPO model) for each piece of information used as input (the "I"). Height is a classic example: before inferring the height of a child (output) from the height of his or her parents (input), it is necessary to know the height of the child in advance. It is also necessary to know the correct result of a pregnancy test, the actual weather that follows a weather forecast, the properties of the soil predicted by a soil analysis, etc. In practice, the real challenge often lies in obtaining the correct output information and assessing its quality. This output information is frequently referred to as a **label**. The majority of machine learning algorithms currently in use were trained using supervised learning procedures.
- The decisive questions with regard to these learning procedures are how to formulate the actual optimisation problem, which regularisation terms to use and how to define the loss function (i.e. are all errors treated the same, or are there different weightings and levels of severity, e. g. when comparing false negatives for patients with cancer who are incorrectly diagnosed as healthy and false positives for healthy patients who are incorrectly diagnosed with cancer?).

Quality of labels

Labels can also contain errors. Several levels of complexity can be defined for data labelling:

1. Labels whose accuracy can be verified when the data are collected. Example: only one correct and relevant value exists for physical systems or properties such as the speed of an object, the temperature of a room or an individual's date of birth. In principle, therefore, these values can be ascertained as labels by an algorithm.
2. Labels whose accuracy cannot be verified when the data are collected and may, in certain cases, not be verifiable at a later date.
3. Labels with a construed and non-verifiable relationship to the real world. Example: concepts such as social milieus or character types have been developed with a view to achieving a better understanding and analytical grasp of humans and their behaviour. These concepts are abstractions that are not necessarily an accurate representation of the "truth" (in so far as it exists).

2 Tom Mitchell: Machine Learning, McGraw-Hill, 1997.

Identifying an optimisation goal

A public transport company is planning to alter its bus routes to reflect recent changes in the city where it operates; many residents have moved to peripheral areas, large inner-city brownfield sites have been developed, and gentrification has brought about huge changes in the composition of the population in various districts. The project manager has collected data in the form of passenger and usage figures, and is attempting to optimise the routes served so that the city's needs can be met as effectively as possible without needing to use extra buses. He is aware that a range of different goals or constraints could be imposed on the optimisation, such as using fewer buses, using fewer drivers or avoiding the creation of new routes. For example, depending on how the optimisation problem is formulated, it might be possible to achieve a solution whereby densely populated neighbourhoods are served by more bus lines compared to other districts, but anyone living in a suburb is forced to put up with longer travel times or a lower frequency of buses. Since the project manager himself lives in the affluent commuter belt, he has a personal preference for an optimisation strategy that minimises the longest travel time. A strategy of this kind would result in faster connections to all areas of the city, including the outlying districts. His line manager is unimpressed by both of these models. He believes that the goal should be to transport as many passengers as possible. This puts short-distance routes with plenty of passengers at an advantage, but is bad news for longer routes with more than four stops. It should be readily apparent from the above that decisions on the optimisation function can have social impacts. Many questions are raised, including the following: Who should decide on the goal of optimisation? Who else should have a say in the decision? How can the matter be debated with the general public, and is it necessary and meaningful to do so? Should certain groups/neighbourhoods have access to legal remedies if they feel that they have been placed at an unfair disadvantage compared to others?

- **Reinforcement learning** involves assessing an agent's actions and imposing a punishment or reward. An agent selects from a pool of different actions and performs whichever action it has selected; this action changes the state of the system and functions as an optimisation input. In addition to the state (or change in state) of the system that is brought about by the agent's actions, there must also be a clearly defined reward function. In the case of supervised learning, the correct and optimal solution is available for every input; this is not necessarily true in the case of reinforcement learning. Instead, the optimisation goal pursued is that of finding the action strategies that lead to the best end state with reference to the optimisation problem. Actions that deliver only short-term improvements may need to be rejected to achieve this goal. Alongside the optimisation problem itself and the relevant loss factor, the reward function plays a particularly important role in this learning strategy.
- **Unsupervised learning** involves searching for structures in a particular quantity of input data. There is no need for the correct structures to be known or for a reward function to exist. A precise definition of the structure being searched for is required, however. For example, a search can be carried out for clusters (i.e. groups in the data) by imposing the requirement that the difference between all the data points in a cluster should be minimised while the difference between the clusters should be maximised. The optimisation problem for unsupervised learning is identified on this basis. Unsupervised learning is also referred to as **data mining**.

Decisive factors include not only the learning procedures but also the availability of sufficient volumes of data that are adequately high in quality and broad in scope, since close approximation of an optimisation goal cannot otherwise be achieved. In many cases, the volume, quality or scope of the data are lacking in some way, meaning that other avenues must be pursued to ensure that good outcomes can nevertheless be obtained using machine learning techniques.

For example, **synthetic data** can be used, i.e. data that are generated artificially rather than being collected directly in the real world and that boast several advantages over real-world data.[3] They can be produced in any quantity, which is particularly important when dealing with simulations for which real-world data cannot yet be generated. When they are created, steps can be taken to ensure that the entire range of possible values is included in the synthetic data, e. g. in order to test how a technical system would behave when confronted with unusual data combinations. Their quality can be measured, and if necessary it can be guaranteed in individual cases that the properties of a set of real-world reference data are retained; alternatively, distortions occurring in sets of real-world data can be pinpointed and removed in order to avoid discrimination. If the set of synthetic data contains no references to persons, it is anonymous and does not fall within the scope of the GDPR. Synthetic data can also be used to train algorithms or test systems; there is, however, a risk that the algorithm will be influenced by properties of the artificially generated data that have no counterpart in reality. Separate functional testing must therefore be carried out before the algorithm is used for practical applications.

A middle course is frequently adopted in the form of **augmentation**. This involves creating new data from the real-world data so that a greater range of situations can be covered at the training stage; the pool of data is enlarged, but the relationship to the real-world data is preserved. The term "augmentation" describes the process of generating new data that deviate slightly from the original data. For example, a characteristic feature of augmented images is that they have been shifted, rotated or distorted in some way.

2.2.4 Artificial intelligence

In the current parlance, the field of machine learning – and more specifically neural networks – is referred to as **artificial intelligence (AI)**, but this term often gives rise to confusion. Machine learning is only one specific procedure that falls under the heading of "weak AI" and that is used to solve well-specified tasks. By way of contrast, "strong AI" methods are expected not just to tackle a single task, but to handle a broad spectrum of tasks, potentially without human intervention. Despite the hopes raised by the term "artificial intelligence", machine learning methods are not capable of such feats.

Historically speaking, the concept of **artificial intelligence** first appeared in the Dartmouth Proposal, published back in 1956 in the USA,[4] to refer to a broad area of research within the field of computer science. The decades since AI first emerged as a field of research have been marked by repeated cycles of unrealistic expectations followed by disillusionment. AI left the ivory towers and made inroads into the economy and everyday life (both workplaces and homes) at the latest in the 1970s and 1980s, in the form of "expert systems", and research efforts in Germany stepped up a gear in the 1980s.

Achievements that can be chalked up to AI research include not only machine learning techniques, but also a large number of other vitally important methods, such as procedures for **pattern recognition, knowledge representation, inferences, action planning and user modelling**. Applications for these procedures include speech, image and dialogue comprehension, robotics and multi-agent systems.

3 Jörg Drechsler/Nicola Jentzsch: Synthetische Daten: Innovationspotenzial und gesellschaftliche Herausforderungen [Synthetic data: potential for innovation and societal challenges], Stiftung Neue Verantwortung, May 2018 (available at: *https://www.stiftung-nv.de/sites/default/files/synthetische_daten.pdf*).

4 John McCarthy/Marvin Minsky/Nathaniel Rochester/Claude Shannon: A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, 1955.

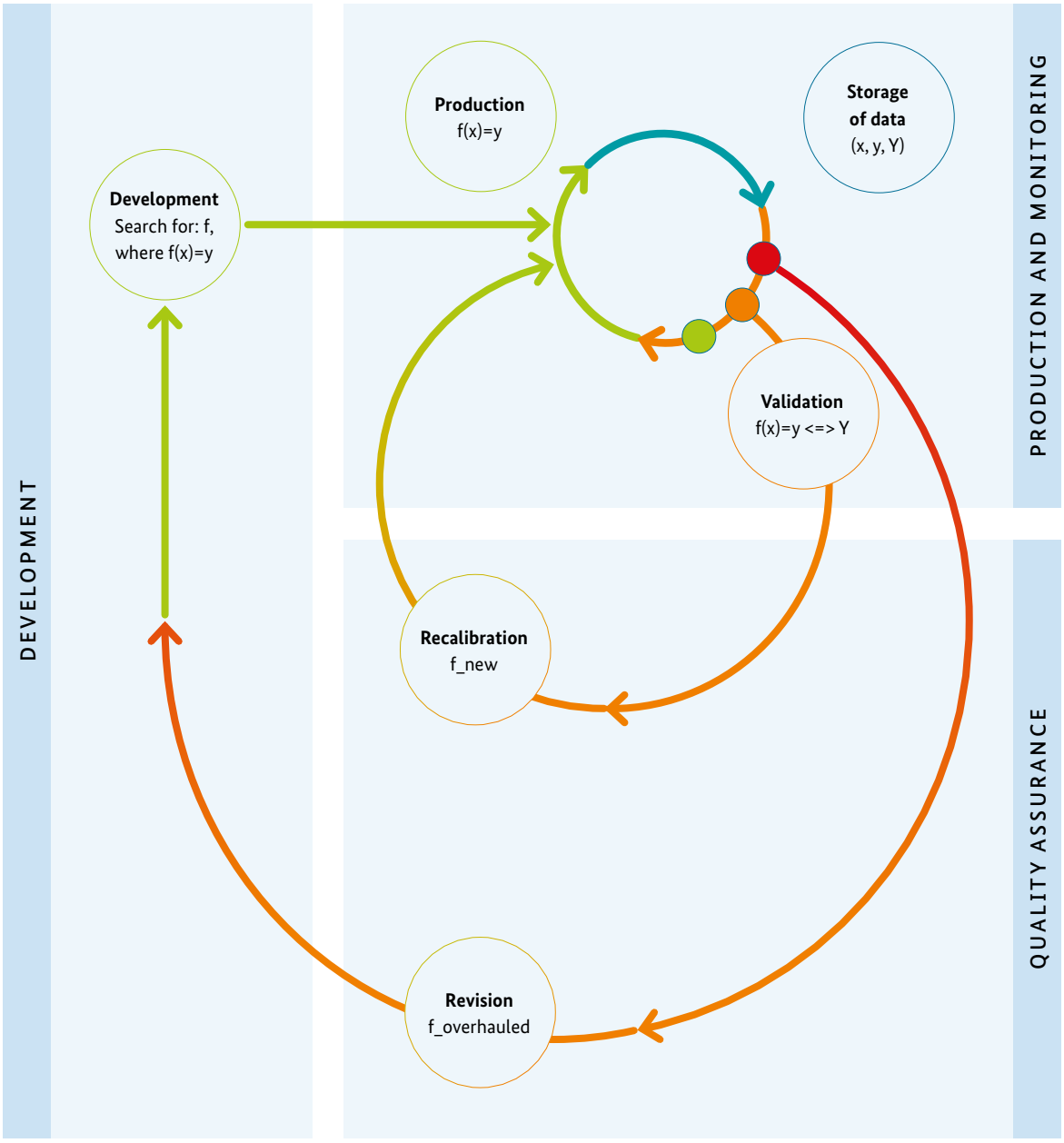
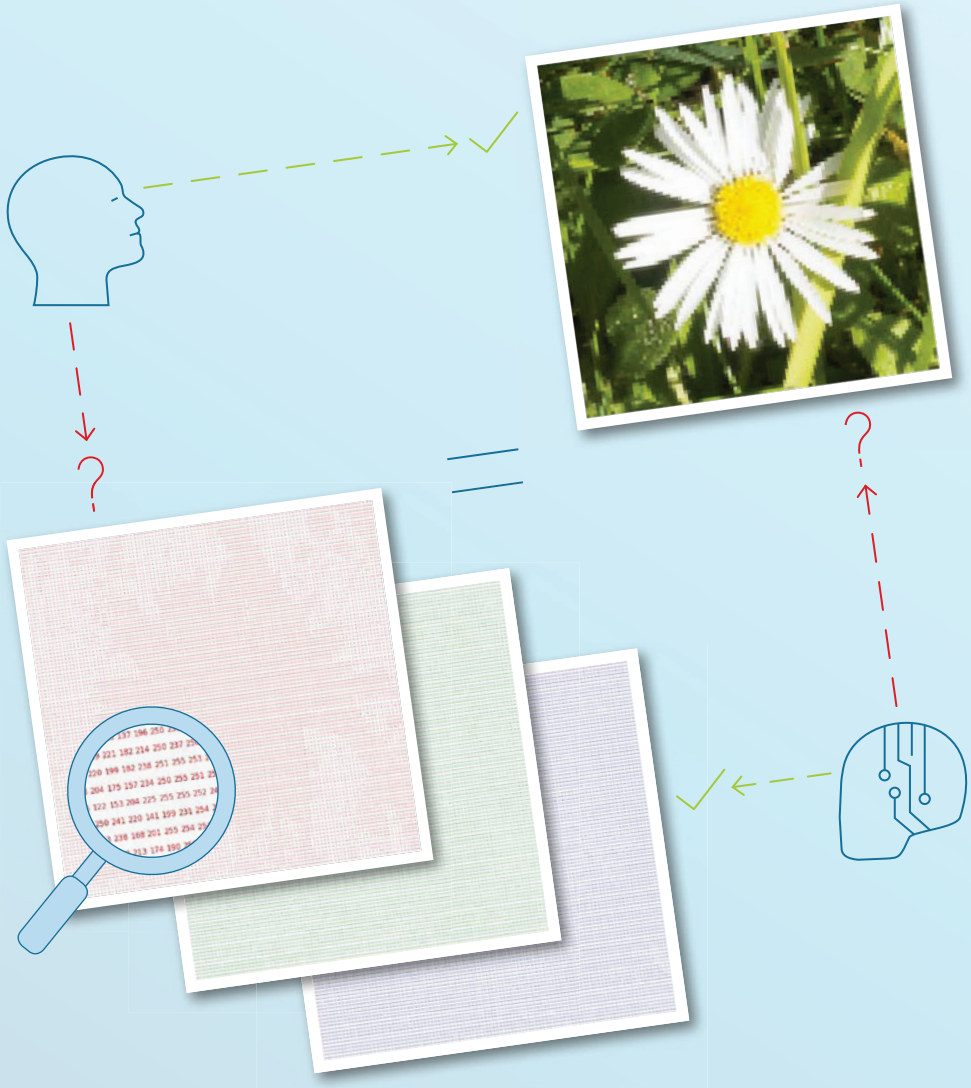


Figure 2: Process model of an algorithm based on machine learning: ongoing monitoring and assessment. The process starts when an algorithm (f) is developed using the training data. Once an algorithm has been identified that meets the desired quality standards, it is put into production. To ensure monitoring and quality control capabilities the production process must make it possible to record the input (x) that enters the algorithm, the output (y) that leaves the algorithm, and the relevant correct value (Y). This information can be used as a basis for monitoring the algorithm in a production environment. To do so, a comparison is carried out to determine the extent to which the output of the algorithm (y) reflects the expected value (Y). The algorithm can continue to be operated without changes in the event of non-critical deviations between these values. If significant deviations are detected, it may be necessary to re-evaluate (i.e. recalibrate) the parameters of the algorithm. If critical deviations are detected, an algorithmic redesign is recommended.

The problem of understanding and comprehending

Humans often find it difficult or impossible to understand methods intuitively if they are described in mathematical or technical terms. This even goes for experts in the field of modelling. Even in the case of relatively simple classification methods that are well understood mathematically (such as logistic regression), almost no one can intuit which result they will return for a given set of input values.

Neural networks for image recognition are a good example of this phenomenon; a human can generally look at a photograph and understand immediately what he or she is looking at, but a human looking at the data structures used as an input for a neural network intended to classify the same photograph is likely to understand almost nothing. This means that, even if a human is familiar with all the digital input values and comprehends all the steps in a neural network, he or she will not necessarily understand the recognition process. If an error occurs, for example, he or she may not be able to determine why recognition has failed and how the problem can be fixed. Humans and machines recognise objects and patterns according to different sets of rules, and it is not always easy to translate between the two.



2.2.5 Algorithmic systems

An algorithmic system generally incorporates multiple algorithms that can work together rather than a single algorithm, and the term "component" is used to describe an executable part of such a system. Different components of an algorithm might be based on different technical implementations. The architectural style known as microservices is a good example. It is important to remember that the individual components of a system of this kind might be subject to different regulatory requirements or protection objectives during their development. In addition, different stakeholders might be responsible for different components of an algorithmic system, for example as suppliers, operators or manufacturers. It should be borne in mind that different requirements or different sets of rules might apply to the individual components, e. g. in respect of data quality, non-discrimination or freedom of contract.

2.3 Software

If an algorithm is formulated in a programming language (formal language) rather than natural language, it is executable in automated form on a computer as a **program** (or **software**). The functioning of software depends not just on the data it processes, but also on the context in which it is executed (cf. concepts such as the "technology stack", which contains all the hardware and software components used for execution) and its parameterisation. Parameters are an "outside-in" method of configuring software. They make it possible to pass information to the software, ranging from simple data (such as display options or path names) through to complex models. More extensive parameterisation options generally go hand in hand with more flexible software use and a more complex development process, making parameters all the more important. For example, software that can be parameterised can be adapted to different contexts with a relatively small amount of effort, and without modifying the source text (i.e. the actual implementation). There are special variants of adaptive systems which over time automatically adapt to their context – such as the individual using these systems or the environment in which they are used.

In order to guarantee or improve the efficiency of high-quality software development processes in spite of increasingly complex framework conditions, and in order to reduce communication problems during these processes, **model-driven development approaches** have been pursued successfully for many years. A generic software component is parameterised on the basis of a complex model, using a language specific to the application context. Mathematical and statistical models represent a special case, and differ from domain-specific languages in that a model is not explicitly specified or programmed; instead, the mathematical or statistical model is (implicitly) taught or trained using data (→ see section 2.2.3 above on machine learning).

2.4 Hardware

Software is executed by hardware, and in particular by **processors**. In recent years, these processors have seen steady gains in performance, while the devices themselves have seen continual reductions in size, meaning that the array of potential applications has become ever wider. Moore's Law (according to which performance should increase a hundredfold every 10 years) is subject to physical constraints, however. When chip components become so small that they are barely bigger than individual atoms, fulfilling Moore's predictions using silicon as a transistor material becomes an increasingly costly and technically challenging task. Researchers are therefore currently investigating alternative materials such as graphene in conjunction with new computing concepts such as photonic quantum computing. The question of whether these will be suitable for everyday use remains open, however. Solutions focusing on parallel computing are more established, and include multi-core and many-core processors or the use of graphics processing units (GPUs). In order to accelerate machine learning using bulk data, application-specific chips (such as tensor processing units, TPUs) that are optimised to handle the highly parallel addition and multiplication of matrices for neural networks have been developed.

The increasingly parallel nature of computing is not without its problems, however; humans find it very difficult to identify any related processor errors, and the calculations performed at the hardware level are **almost impossible to reproduce and comprehend.**

2.5 System architecture

Applications today rarely run on a single computer. Instead, many different software components run on different computers and interact with each other to perform a task. The term **"distributed system"** is used to refer to this method of distributing the work across different hardware nodes. A distributed system is made up of different software and hardware components that interact within a network. The network nodes communicate with each other over wired or wireless links.

A wide range of **protocols and standards** exist for network communication, and are used as a basis for processing data at the network nodes and forwarding these data through the network (i.e. transporting them to other nodes). Specifications outlining the requests that can be submitted to a server are published in an application programming interface (API), for example. As a general rule, steps must be taken to prevent these interfaces being used incorrectly or accessed by attackers.

IT infrastructures that can be reached via the Internet are referred to as the **cloud**, and cloud applications can be accessed by billions of users. Groups of related cloud applications are often referred to as **digital platforms**, and many – such as the "Big Four" or "GAFA" (Google, Apple, Facebook, Amazon or "GAFAM" if Microsoft is also included) – have a high level of name recognition.

In the early days of the Internet of Things, most data were sent directly to the cloud and processed there on large digital platforms. By way of contrast, an increasing number of solutions are currently being developed that involve the processing (or at least pre-processing) of data immediately and as close as possible to the place where they are collected, or in other words "on the edge" of the Internet. This practice of processing data near to where they are collected is referred to as **edge computing**, to distinguish it from situations in which the data are processed in the cloud (cloud computing). Data pre-processing is particularly important, since it allows not only the minimisation of communication effort, but also the creation of more privacy-friendly systems, since any references to individuals that are not required can be removed at this point (close to where the data are collected).

The complex system landscape that has emerged in recent years (incorporating the Internet, edge computing and IoT) entails a high level of interconnection, making it hard to distinguish the individual systems from one another.

The way in which the architecture of distributed systems is designed also has a significant **impact on the business processes** supported by the system, since it acts as a factor in decisions on the technology that is used, the network nodes on which the software runs, the interfaces and protocols used for communications and the other parties involved in these communications. For example, if manufacturers want to use the hardware data collected by their devices for the purpose of long-term efforts to improve those devices, they have the choice of setting up their own communication infrastructure, making use of the user's own infrastructure (where available) or asking the user to make the data available via an interface. The way in which data of this kind are handled in cooperative processes should be transparent and agreed contractually if necessary. Technical parameters may place constraints on the contractual provisions governing the exchange of data.

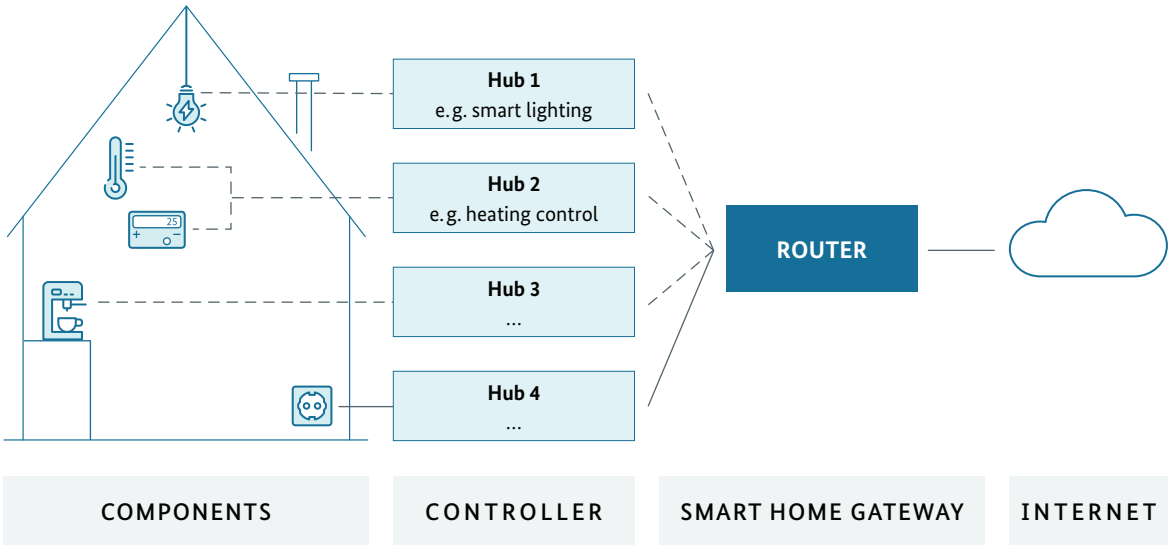


Figure 3: Example of system architecture in the smart home

Blockchain and other distributed ledger technologies

Significant improvements in the field of distributed systems have made it possible to use **distributed ledger technologies (DLT)**. These technologies involve the management of multiple identical copies of a ledger by different partners, instead of the centralised management of a single ledger. New ledger entries are added to all of the copies, and the current accuracy of the database is confirmed by consensus. The underlying architecture of systems of this kind varies from linear approaches to a wide range of graph-based solutions, depending on their intended purpose and the structure of the transactions. A consensus can also be achieved using different methods. These methods are outlined in consensus protocols.

One of the most famous examples of a DLT architecture is the **blockchain** concept, implementations of which include Bitcoin and Ethereum. Blockchains are used to store data as a list of records (“blocks”). The blocks are linked to each other using cryptography, meaning that a transaction stored as a block implicitly confirms the accuracy of previous transactions (i.e. the entire chain), making it extremely difficult for fraudsters to manipulate the data by modifying it or deleting entries. Use of a decentralised consensus protocol eliminates the need for an additional instance that confirms the integrity of transactions.

Part D

Multi-level governance of complex data ecosystems

The high level of complexity and dynamism of data ecosystems means that new challenges must be overcome in terms of regulating, controlling and designing these systems before the ethical and legal framework upon which the Data Ethics Commission has based its work can be implemented in practice; this will require cooperation between different stakeholders and interaction between different governance instruments at many different regulatory levels (multi-level governance). Part D examines **relevant governance instruments and stakeholders**, with further details provided in the following two parts on data and algorithmic systems (in particular regarding the interplay between different instruments and stakeholders).

1. General role of the State

All those who are entitled to exercise ethically justified rights and who are obliged to comply with the corresponding obligations – be they citizens, companies or government agencies – must actually be able to do so in practice. This presents the State with a wide range of tasks. First and foremost, the State is responsible for establishing a **legal framework** within which a data society geared towards the public interest can develop. The speed at which algorithmic systems are developing and infiltrating ever more areas of life poses major challenges for the legislature and the courts that hand down rulings clarifying the legislative provisions. The State must ensure that any regulations adopted in an environment of this kind are sufficiently hard-hitting to steer developments, while at the same time being flexible enough to continue fulfilling their purpose even if the technological parameters change. Statutory provisions must therefore be formulated in a **technology-neutral manner**, and **innovative regulatory models** must be developed.

In addition, the **appropriate infrastructural and technological prerequisites** must be in place – such as enabling technologies, institutions and intermediaries, complemented by the involvement of a broad gamut of civil society actors. The Data Ethics Commission believes that, here too, the State must play a key role in guaranteeing and safeguarding these services of general interest.

The new opportunities opened up by the data society also impose a far-reaching **educational remit** on the State. It is necessary to identify the skills required to take a creative yet reflective approach to the use of digital technologies, and to determine the framework conditions that must be put in place before appropriate training can be offered to a diverse range of target groups. The State's educational remit should be understood in a broad sense, and should incorporate **public outreach work** with the aim of raising awareness in this area.

Furthermore, the State is also generally responsible for encouraging **research and development** (R&D). It is particularly important here to support R&D with regard to ethically sound technologies (e.g. those that uphold the principles of accountability, transparency and anti-discrimination). Extensive research and development programmes are needed to ensure that ethical and legal principles are taken into account, and more funding must be channelled towards these programmes.

Not all of the funding needs to be provided by the State itself or by institutions that are closely aligned with the State, but the State must put in place the **framework** (legal and otherwise) for a data society in which individuals and businesses alike can operate in a self-determined fashion on the basis of ethical values and principles, in which these individuals and businesses are provided with adequate protection, and in which the potential of data and algorithmic systems are harnessed to shape a worthwhile future.

Germany's efforts in the direction of ethically sound and multi-level governance should also include active contributions to **debates at the European and international level**. The global dimension of technological developments means that action by a single nation state or regulations adopted at the national level alone are inadequate. The Data Ethics Commission therefore welcomes the European and international initiatives that have already been launched (by the European Commission and the OECD, for example) with a view to ensuring that our future is shaped on the basis of ethical principles. Safeguarding the **digital sovereignty** of Germany and Europe in the international context is a vitally important task in this regard (→ see Part G for further details).

2. Corporate self-regulation and corporate digital responsibility

Responsibility for mitigating the risks of digitalisation and for leveraging its significant potential should not be placed solely at the feet of the State and its legislators. This **responsibility** should also be shared with the parties that develop, disseminate and use the technologies, even **in the absence of any legal obligation**. Although the State must shoulder most of the responsibility, not least because it is obliged to protect its citizens by guaranteeing the confidentiality and integrity of IT systems and safeguarding other fundamental rights, self-regulation tools are also vitally important, particularly in the context of the digital transformation process.

The term **"corporate digital responsibility" (CDR)** is used at a theoretical and practical level to refer to the idea that companies, as manufacturers and operators of digital technologies, should each assume their own responsibility for the consequences of digitalisation. Like corporate social responsibility (CSR), CDR falls under the broader umbrella of corporate responsibility; in this case, the focus is on voluntary corporate activities in the digital sphere which go beyond what is currently prescribed by law, and which actively shape the digital world to the benefit of society in general, and of customers and employees in particular. To further this aim, in October 2018, the Federal Ministry of Justice and Consumer Protection launched an initiative to clarify the principles and concepts of corporate digital responsibility (*www.bmjv.de/cdr*). According to this initiative, CDR can encompass many topics,[1] including the protection of personal data, inclusion in the digital sphere, transparency (e.g. in relation to algorithms or data protection), the development of digital innovations that help to achieve sustainability objectives, algorithmic use that is geared to the public interest, open data and information security.

The responsible development of digital products and services must be a central priority in all corporate decisions taken at all levels of the company. Ethical questions must not be a matter for legal departments and compliance officers alone. Instead, they must be viewed as a **cross-cutting task** and **integrated into all processes**. All of the parties involved must be aware of their responsibility to consider ethical values such as participation, fairness, equal treatment, self-determination and transparency. The negative social and societal impacts of digitalisation and digital business models on employees, suppliers, clients, society as a whole and the wider environment should thus be minimised, and the new opportunities that digitalisation offers for the achievement of macrosocial goals should be leveraged. When applied correctly, the concept of CDR can lead to improvements in terms of consumer protection, digital participation and the **sustainable development of the digital economy**.

CDR is fundamentally similar to corporate social responsibility (CSR) in that it requires companies to take self-regulatory action on a voluntary basis. Internal strategies such as in-house or industry-specific codes of values are therefore a particularly effective way of implementing CDR. In this respect, the Data Ethics Commission welcomes the proliferation of professional and ethical standards and codes of conduct published by associations and companies in the data-processing industry, with the proviso that these standards and codes must help to clarify exactly what needs to be done; CDR must not be reduced to a metaphorical fig leaf that allows companies to pretend that they are upholding the principles of digital ethics when the truth is very different.

1 Corporate Digital Responsibility Initiative: Shaping the digitalization process responsibly: A joint platform, 2018 (available at: *https://www.bmjv.de/SharedDocs/Downloads/DE/News/Artikel/100818_CDR-Initiative_EN.pdf?__blob=publicationFile&v=3*).

In the Data Ethics Commission's view, the data protection impact assessment that must (under the relevant circumstances) be carried out pursuant to the GDPR while a digital product is still at the development stage should be accompanied by a more comprehensive and general **societal impact assessment** focused on the assumption of foresighted responsibility (including the impact on any employees and customers of a company that are particularly affected by the digital transformation process) which also takes into account the long-term social effects of data-driven business models. It might be a good idea for companies commanding a large market share to set up an advisory panel (along the lines of consumer and customer advisory panels) that could be consulted when drawing up impact assessments of this kind; the panel should be made up of representatives of the groups of people most affected by the relevant business model.

3. Education: boosting digital skills and critical reflection

Digital self-determination presupposes digital skills. The Data Ethics Commission therefore unreservedly welcomes the efforts undertaken by the Federal Government, by consumer protection associations, by legal professional groups and by other bodies to raise public awareness of the importance of the **self-determined use of data and digital technologies** (from smartphone settings through to digital inheritance planning) and to provide straightforward and easy-to-understand information on the available options as well as practical guidance. It also welcomes the steps taken to raise awareness among consumers of the potential inherent to data, and to provide them with much-needed information about their rights and about the real opportunities and risks involved in the economic exploitation of their data. The Data Ethics Commission recommends that all of these efforts should be continued and stepped up.

School pupils should also be made aware of the issues connected with digitalisation as early as possible. Digital skills should be integrated into the **curriculum**, and teachers must be provided with comprehensive training on the subject at regular intervals. This is the only way to ensure that new generations will grow up to become competent "digital natives", able to assess both the opportunities and the risks of new digital applications, to take informed decisions and to assert their rights effectively.

In addition, **lifelong education** on the use of data and digital technologies must be provided to all age groups and social groups. It must be borne in mind that digital skills require not only a basic knowledge of the underlying technology (which, in turn, requires ongoing education in technical and mathematical subjects), but also an adequate familiarity with the economic, legal, ethical and social sciences; this broad spectrum of knowledge is necessary to comprehend, discuss and assess the various opportunities and risks in all their complexity.

Education and training in computer science, data science and software development is of particular relevance in this respect. As well as basic instruction on ethical and legal issues, more in-depth teaching on statistics, methodology and scientific theory is needed. It is particularly important to ensure that questions relating to data ethics and research ethics are embedded in discipline-specific methodological training, and there must be a major push in this area to ensure that ethical and legal considerations are incorporated into early-stage discussions by the parties that develop digital products and services or are involved in decisions on their development.

An essential first step towards achievement of these goals is cooperation between as many different entities as possible, including **government agencies, bodies that are closely aligned with the State and private actors** at federal, State (Bundesland) and municipal levels. The challenges involved in providing the general public with digital skills, maintaining these skills in the long term, and adapting them to each individual's lived experience are so great that they could never be tackled successfully by a single, centralised body. That said, a key role must be played by supervisory authorities (data protection authorities and/or the relevant specialist supervisory authorities), the Foundation for Data Protection, consumer protection associations and training providers. The media and institutions involved in media regulation also have a large part to play in this connection; they must not only provide society with information about the new technologies and cast a critical eye over technical progress, but also establish new forums for debate.

Although government agencies must remain chiefly responsible for imparting digital skills to the general public, this task cannot be realised in full unless the necessary **civil society structures** are put in place, such as digital volunteering, tech accountability journalism and consumer-focused market observation. The Data Ethics Commission therefore recommends that the Federal Government should provide long-term support for the establishment of structures of this kind.

Companies also have a responsibility to provide training to their staff. For example, a company can attain high ethical standards only if its employees (particularly those in management and in product development) have an adequate awareness of potential ethical and legal issues. As far as education and training is concerned, questions relating to data ethics and data law should also be included in a **broad spectrum of academic and professional training routes** and in workplace training. Particular attention should be given to technical and business professions, with a view to ensuring that ethical and legal considerations are incorporated into early-stage discussions by the parties that develop digital products and services or are involved in decisions on their development.

4. Technological developments and ethical design

Efforts to impart more advanced digital skills to the general population must not end up shifting the weight of responsibility away from manufacturers and digital service providers and towards users, not least because users have only limited opportunities to grasp and comprehend all the steps involved in the processing of their data and the underlying business models. Responsibility should be laid first and foremost at the feet of those who are able to exert an influence over the development of products and services. This concept is embodied in the principle of **ethics by design** or **ethics in design**, and appears in the GDPR (with reference to data protection and intrusions into the private sphere) under the heading of data protection by design and by default. Aligning the development of technologies and products (including services and applications) with the ethical values and principles outlined above is also a good way of increasing public confidence in digital products and acceptance of these products.

At the same time, however, the design of every product must be **tailored to the target user groups**. Involving user groups and their needs at an early stage of product development **(participatory product development)** may be helpful in this respect. It is particularly important for products that are targeted at vulnerable and/or less digitally literate user groups to have an **inclusive design**, including privacy-friendly default settings, with a view to protecting the digital self-determination of these user groups. Inclusive design allows manufacturers and operators to meet the constitutional requirement for informational self-determination as enshrined in Article 1 paragraph 1 of the German Basic Law (Human dignity), according to which protection must not be contingent upon individual capabilities and personal circumstances.

The most popular methods and platforms used to develop technologies, the most commonly used libraries and other code components have rarely supported the requirements of ethics by design to date. Components with a "better" design from the perspective of ethics or data protection law are at best a niche interest. There is a need for change in this area so that compliance with ethical principles in general and data protection principles in particular becomes the rule rather than continuing to be the exception. Ethics by design requires the gap between different communities to be bridged, and this has certain implications for the professions affected. The goals of this approach could be furthered not only by information on methods and catalogues, but also by **best-practice concepts, supporting tools, development frameworks** and **(open-source) code components**. Platforms with repositories of these components and usable pools of data (which, in some cases, are a necessary prerequisite for checks) would make it possible to highlight the specific properties required, supply the documentation needed and provide opportunities for exchanging know-how and experience.

Although ethics by design is a crucial governance instrument that allows the process of designing products, processes and services to be aligned with individual and public interests from the outset, it provides no guarantee that the resulting products and services will be ethical. Ethical principles can and should have a positive influence on technological developments, but **ethics is not a task that can be delegated to technology**. Furthermore, decisions about which ethical principles should be implemented and how they should be implemented (for example whether fairness metrics should be applied to algorithmic systems, and if so which metrics) should not be left to developers alone; instead, these decisions should be negotiated on a context-specific basis, if necessary with the involvement of the parties affected.

5. Research

Although data-processing systems with a more ethical design are frequently developed and showcased by researchers, there is a gulf between the world of research and the real world. One of the reasons for this may be the fact that some of these technical solutions (for example those based on cryptographic mechanisms) are counterintuitive in nature and more difficult for many people to understand than conventional methods; a prime example is a digital identification document that changes in appearance every time it is shown, making it impossible to "join the dots" between its holder's observed behaviours. Many people attempt to **understand** these innovative technologies by drawing on **conceptual models** from the surrounding (analogue) world, but these latter provide an insufficient basis for comprehending them or appraising their added value. Despite the advantages offered by these technologies in terms of ethics and data protection law, it is unlikely that their use will become widespread until the public gains a better understanding of them and is more confident in their use.

In many cases, **cross-cutting (and therefore interdisciplinary) cooperation** is an essential starting point for understanding the implications of new developments and designing ethical systems, but cooperation of this kind is not adequately rewarded by the discipline-bound metrics for good science and research. In many areas, interdisciplinary research will be given due recognition only if a shift in mindset occurs (this applies to universities, peer reviews and expert opinions, for example). Research funding should be funnelled towards interdisciplinary cooperation which delivers results that would have been impossible to achieve within the silos of the individual disciplines, and should allow the necessary institutional frameworks and long-term career paths to be established.

In many cases, high-quality and promising technical solutions have already emerged from the research sector, but the demand for these solutions is currently still lacking. There is also a need for methodologies or technologies that **signpost a route** from the current implementation status to an **improved state of technology**. Once again, **funding should be channelled into development and innovation** so that improved solutions can move from the drawing board to reality. Instead of providing support for only a few outstanding success stories, the need for broad-based progress in the field of ethical design must be acknowledged.

6. Standardisation

At the very latest when Lawrence Lessig coined the aphorism "Code is Law",[2] thereby emphasising the relevance of technical reality, it should have been obvious that **technical standardisation** is an essential factor in the implementation of legal and ethical requirements. Bodies responsible for the technical standardisation of communications networks have been established at international level (ISO/IEC, IEEE, IETF, ITU, ETSI or W3C), European level (CEN) and national level (DIN being the prime example in Germany, alongside other specific standards for public bodies). A technical standard by itself has no legal force, and anyone who uses a technical system must also comply with the applicable legislation, even if the provisions of this legislation run counter to the requirements imposed by a global technical standard. Nevertheless, standardisation is hugely influential in terms of what is available on the market; wherever possible, therefore, steps should be taken to avoid adopting standards that infringe the current legislation.

The standardisation process is often criticised for its lack of democratic legitimacy, and it is true that the groups within society that stand to be most affected are often deprived of any opportunity for **representative participation**. For example, non-governmental organisations or other civil society representatives are seldom involved in the standardisation process, and generally speaking even data protection authorities are only rarely involved in the standardisation of technical systems. In a worst-case scenario, this may mean that the operation of a technical system complies with the standards but violates the legislation. Another point of criticism is that a number of international standards that manufacturers or operators are supposed to comply with are not **available free of charge in the public domain**, but must instead be purchased.

Past standardisation efforts in the field of information security served as a major contributing factor to the addition of extra security features and gradual improvements in the level of security, for example of online banking. Yet the Snowden revelations made it clear that a number of intelligence services and government agencies were deliberately attempting to weaken standards by including security loopholes or backdoors as a way of safeguarding access in the future. The role of technical standardisation can be expected to gain in importance over coming years, for example as a result of the GDPR-imposed requirement to take due regard of state-of-the-art technology, or as a consequence of the German IT Security Act (*IT-Sicherheitsgesetz*). The political influence exerted by a number of different countries (not all of which are in Europe) can also be expected to increase.

An **impact assessment** of standards that are currently in existence or are still being debated must go beyond purely technical and economic considerations, and be **expanded** to include ethical and societal factors. The State should ensure that civil society actors, data protection authorities, consumer protection experts or spokespersons for organisations representing the parties affected can play a role in the standardisation process alongside the stakeholders that have dominated it to date.

2 Lawrence Lessig: Code and other Laws of Cyberspace, 1999.

7. Two governance perspectives: the data perspective and the algorithms perspective

In the following two parts, the arguments set out above are applied to data-based algorithmic systems on the basis of two different but complementary approaches. The **general ethical principles and precepts** used as a basis by the Data Ethics Commission (see Part B above) are important in two respects: firstly, they must guide data governance measures, in particular with a view to ensuring that procedures for collecting, accessing and using data are ethically sound; secondly, they must guide the design of algorithm-based systems used to process data (including the oft-cited "artificial intelligence" systems). The perspective that focuses primarily on data (the "data perspective") and the perspective that concentrates mainly on algorithmic systems (the "algorithms perspective") should not be regarded as competing views or two sides of the same coin; instead, they represent two different **ethical discourses, which both complement each other and are contingent upon each other**. These different ethical discourses are typically also reflected in different governance instruments, including in different acts of legislation.

The **data perspective** focuses on the data that are used to train algorithmic systems, as a basis for algorithmically shaped decisions, or for a plethora of other purposes specifically associated with the **context of meaning and the semantics of data** (Part C, section 2.1). In particular, it requires thinking about the origin of these data and the potential impact their processing may have on individuals involved with the context and semantic content of the data. From an ethical and legal perspective, it is important to identify standards for data governance; typically, however, the **rights** that these individuals can assert against others will play an even more significant role. A central distinction in this context is that between personal and non-personal data, since it determines whether the rights granted to data subjects under data protection law apply. Current debates that are pertinent in this connection include those on "data ownership rights" or open data, for example.

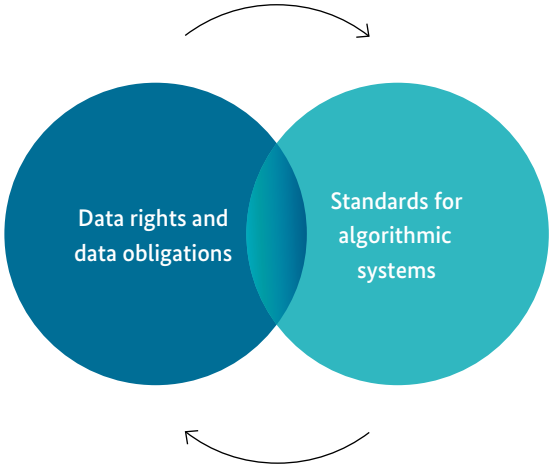


Figure 4:
Data perspective and algorithms perspective

By way of contrast, the **algorithms perspective** focuses on the architecture of data-driven algorithmic systems, their dynamics and the systems' impacts on individuals and society. The ethical and legal discourse in this area typically centres around the relationship between **humans and machines**, with a particular focus on automation and the outsourcing of increasingly complex operational and decision-making processes to autonomous systems enabled by artificial intelligence (AI). The algorithms perspective differs from the data perspective in that the data subjects affected by the system may not necessarily have anything to do with the original training or processing data; even if they do, they are not the focus of attention. The focus is on the **objective requirements** that apply, observance of which may be enforced and failure to comply with which may lead to liability and sanctions. The current debate on "algorithmic oversight" is relevant and important in this respect.

Part E

Data

Data provide access to information, information can lead to knowledge, and knowledge bestows influence and power. In the light of new capabilities of automated data processing and an exponential increase in memory and computing capacity, having access to data can mean an enormous increase in power and opportunities. Controlling important resources is inherently associated with a certain level of responsibility. Thus data, like other resources, may be used only for lawful and ethically acceptable purposes, and, like other resources, the impact of their use on individuals and the general public as a whole must always be assessed. Yet data also exhibit certain characteristics that differentiate them from other resources.

In the following sections, the Data Ethics Commission will therefore take these specific characteristics of data as a starting point, and develop, on the basis of the principles outlined in Part B and without claiming to be exhaustive, general standards of data governance (→ section 1 below) as well as data rights and corresponding data obligations (→ section 2 below). It will then set out specific recommendations for action in relation to standards for the use of personal data (→ section 3 below), improvements to controlled access to personal data (→ section 4 below) and general access to data, in particular non-personal data (→ section 5 below).

1. General standards of data governance

Any attempt to identify specific principles of data governance must start with the differences between data and traditional resources such as oil or goods. The unique characteristics of data include, in particular, the following:

- data are created and processed further in a **distributed and dynamic process**, through the interaction of a number of different players acting in very different roles (e. g. the data subject, the operator of a data-generating system, the developer); this process is, in principle, **never fully complete**;
- data are a **non-rivalrous resource**, i. e. they can be duplicated as often as necessary and used in parallel by multiple different players for multiple different purposes;
- data are **multifunctional and can be used across different sectors**, and the potential and risks inherent to them depend, to an exceptionally large extent, on each data controller's specific goals and opportunities and, in particular, given the importance of effects of scale, the ability to combine them with other data.

1.1 Foresighted responsibility

The special characteristics of data, such as their unusually dynamic nature and the unusually high context dependence of opportunities and risks associated with them, mean that there is a particular need for foresighted responsibility when making decisions about collecting, using or forwarding data. When assessing the potential impacts, including the risk of infringing the rights of third parties, particular consideration should be given to the following points:

- the **volume** of the emerging collections of data, with a particular focus on any cumulative effects, network effects or effects of scale;
- the **technological means** for processing data, with a particular focus on the technological options that are, or will be, available to large corporations and government bodies (especially in relation to the recombination and decryption of data);
- the **purposes** of data processing, with a particular focus on potential changes to the context of data use and the players involved (e. g. as a result of access by government agencies or following a corporate takeover).

In the case of personal data, the principle of foresighted responsibility has found its standardised expression in the maxims of data minimisation and storage limitation that are enshrined in the GDPR. A range of further duties under the GDPR, from the need to carry out a data protection impact assessment to mandatory requirements for controller-to-processor contracts, likewise follow from this principle.

1.2 Respect for the rights of the parties involved

The use of data must always be underpinned by respect for the rights of others. Acts or omissions that are ethically unacceptable or unlawful in general terms, because they violate the **rights of others**, do not become acceptable or lawful simply because they are committed by way of using data (e.g. fraud is a criminal offence regardless of whether it is committed by use of data or otherwise). As data are generated in distributed processes and through the interaction of many different players, parties who have in any way been involved in the process of data generation, for example as the data subject or as the owner of a data-generating device, may – from an ethical and possibly also from a legal perspective – be entitled to **genuinely data-specific rights (data rights)** in relation to these data (→ for further details, see section 2 below). Such data rights must be respected whenever data are used.

Respect for the rights of others implies much more than simply avoiding intrusion into legally protected spheres, such as another party's copyright. What is needed instead from an ethical perspective is in-depth **consideration** for the data-related legitimate interests of parties who are specifically linked to the data and who may therefore have certain rights of co-determination and participation concerning the data. This in-depth consideration may also imply duties to take action, for example by granting another party access to the data in certain ways.

In the case of personal data, the principle of respect for third-party data rights is expressed particularly clearly in the **principles of lawfulness, fairness and purpose limitation** enshrined in the GDPR. The GDPR itself sets out a number of data rights vested in the data subject, e.g. the right to be informed, the right to rectification, the right to restriction of processing, the right to erasure or the right to data portability.

1.3 Data use and data sharing for the public good

Resources that could be used to further key legally protected interests of individuals (e.g. health) or to promote the public good, particularly in pursuit of the UN's 17 Sustainable Development Goals relating to economic, social and ecological aspects, should not be neglected. As a basic principle, there is an **ethical imperative** to use these resources in cases where to do so would increase overall prosperity and where there are no overriding and conflicting interests of other parties (particularly data rights).

One of the special features that make data unique is that they are a non-rivalrous resource. They do not "wear out", even if they are used in parallel by many different players for many different purposes, and they can be duplicated an almost infinite number of times. **Sharing data** can mean that the player who first shares the data is at the very least no worse off, and everyone else involved (however loosely) is better off than they would have been had the data not been shared. An ethically responsible approach to data governance must take this fact into account. Data sharing is also enormously important in terms of safeguarding **fair and efficient competition**.

At the same time, however, conflicts can sometimes arise between the principle of furthering the public good by data use and data sharing on the one hand, and the principles of foresighted responsibility and respect for other parties' data rights, including considerations of appropriate investment protection, on the other. The creation of incentives for **voluntary data sharing** should therefore always be prioritised, and legislative requirements to share data should be the exception.

1.4 Fit-for-purpose data quality

Data, together with their context and semantics, are stored information. Information regularly purports to be the most accurate possible representation of reality as it currently stands, or the most accurate possible prediction of future reality. In situations that do not involve the automated processing of data by algorithmic systems, it is immediately obvious to everyone that incorrect information is not only worthless, but also potentially harmful; as soon as automation comes into play, however, it is all too common for people to fall prey to **false objectivity** and show a foolhardy willingness to rely on the results of calculations that were carried out using incorrect or incomplete data, and are therefore also likely to share these characteristics ("garbage in, garbage out").

In the interests of everyone, therefore, responsible data governance in the data society must also include efforts to achieve a **standard of quality that is appropriate for the intended purpose** (→ Part C, section 2.1.1). The meaning of "appropriate" must always be determined on a **context-specific** basis when used in relation to data quality, however. For example, it is important to remember that data may reflect societal preconceptions, stereotypes and discrimination, which will, in turn, influence the functioning of any algorithmic system trained using these data (→ for further details, see Part F, section 2.6). Data that accurately reflect an existing deficit may therefore be unsuitable for use as a basis for other purposes, even if they are of a high statistical quality.

Another important factor in this connection is that data can be used across different sectors and for different purposes. The **FAIR principle** (*Findable, Accessible, Interoperable, Reusable*) may be relevant in this context, for example as regards data storage and encoding methods. According to this principle, data must be prepared and stored in such a way as to be findable and accessible, and must be coded in an interoperable format and in a way that makes the data reusable in different contexts by as many different players as possible.

In the case of personal data, the desire to achieve a high level of data quality is manifested in the **principle of accuracy** enshrined in the GDPR.

1.5 Risk-adequate level of information security

Data can be freely duplicated, and it is **almost impossible** to recover them once they have gone astray. The wide range of possibilities for **external attack**, many of which are invisible from outside, mean that data are also vulnerable to malicious attempts to falsify or destroy them. A high level of **information security** that is commensurate with the relevant risk potential is therefore, from a technical perspective, directly related to the principles of foresighted responsibility and respect for the rights of the parties involved. Appropriate information security, encompassing a broad spectrum of measures at different levels, is a vital prerequisite for mutual trust on the part of those involved in the data society.

In the case of personal data, the concept of information security is manifested in the **principle of integrity and confidentiality** enshrined in the GDPR.

1.6 Interest-oriented transparency

Since a party that uses and effectively controls data may gain influence and power as a result, this party must, in principle, be able and willing to **account** for its actions. One of the reasons for this is the protection of parties whose data rights might be affected or even violated. An **interest-oriented level of transparency** is required so that these parties (or entities enforcing data rights or data law for the benefit of others) can determine whether and to what extent data rights have, in fact, been affected or violated, and against whom they can lodge claims.

In the case of personal data, transparency – i. e. ensuring that data processing operations are easy **for data subjects to understand** – is a basic principle of the GDPR, and the same is also true for the **principle of accountability**. Many of the provisions of the GDPR, for example those relating to information, documentation and the right to request access, are designed to improve transparency.

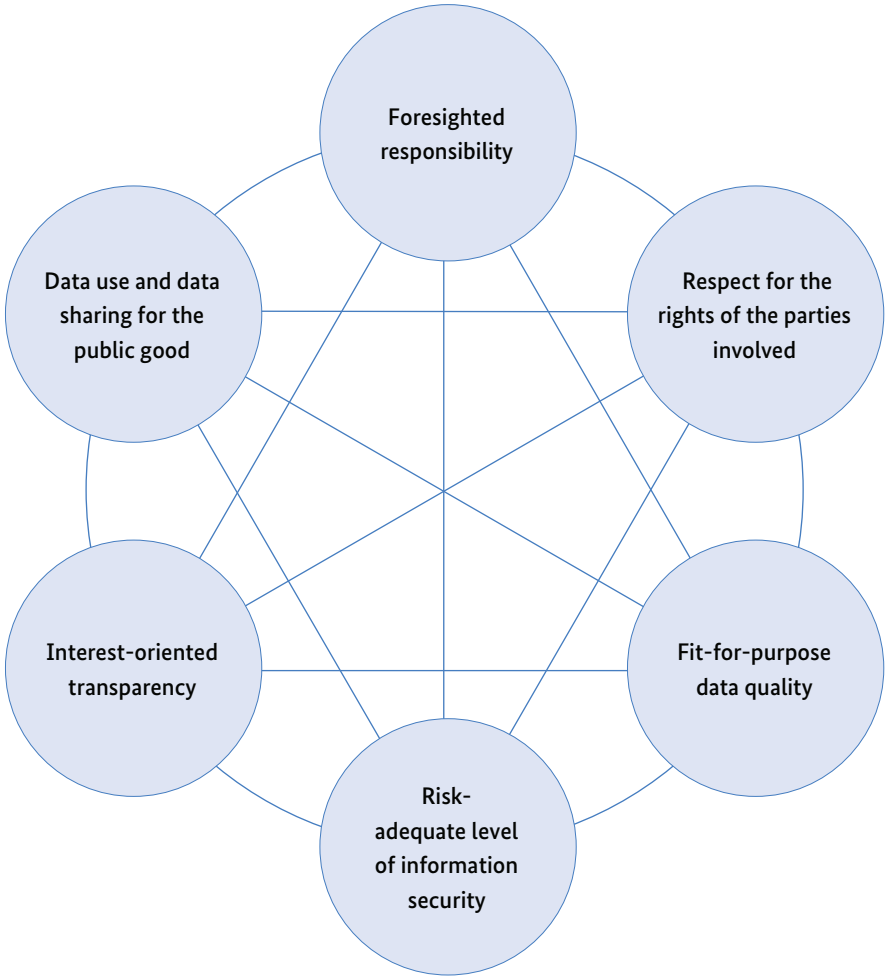


Figure 5: Standards for data governance

2. Data rights and corresponding obligations

According to the ethical principle of digital self-determination, individuals should not merely be perceived as being passive and in need of protection and as facing actual or potential threats, but rather as **self-determined actors in the data society**. Self-determined navigation of the data society by individuals requires that these individuals have certain rights that can be asserted against others. First and foremost among these rights are those which relate to an individual's **personal data**, which derive from the right to informational self-determination that is enshrined as a fundamental freedom, and which are guaranteed by the data protection law currently in force. Digital self-determination also encompasses the self-determined economic exploitation of one's data and the self-determined handling of **non-personal data**, for example the data generated by the operation of one's devices. The Data Ethics Commission takes the view that, in principle, a right to digital self-determination also applies to companies and **legal entities** and – at least to some extent – to groups of persons (collectives). In this context, the Data Ethics Commission believes that it is possible to identify general principles underpinning data rights and obligations that go beyond data protection alone.[1]

2.1 General principles of data rights and obligations

Complex data generation processes (understood in the broader sense, i.e. including various phases of data creation, enhancement and refinement) often involve interactions between different parties that may be pursuing different goals and playing different roles and that contribute, in their respective roles, to the generation of data in the process. A **contribution by a party** (i.e. a natural or legal person) **to the generation of data** may be relevant if any of the following are true:

a) the information stored in the data relates (in terms of meaning) to the party or to an object associated with this party (e.g. belonging to him or her);

b) the data were generated by an activity of that party or by the operation of an object (e.g. a sensor) that belongs to this party; or

c) the data were generated by software or another component (e.g. sensors) created by or invested in by this party.

Where the situation referred to in a), i.e. the situation that a party is the subject of the information stored in the data, relates to natural persons, this is of particular significance since this situation gives rise to the right to informational self-determination and data protection enshrined in constitutional law.

Given the specific characteristics of data and the inextricable link between personal data and personality rights, the Data Ethics Commission believes that a contribution to the generation of data should not give rise to exclusive ownership rights in said data, above and beyond the existing intellectual property rights (→ see sections 3.3.2 and 5.2.4). Instead, a contribution to the generation of data should entitle a party to specific data rights in the form of **co-determination and participation rights**; these rights in turn impose obligations on other actors. From an ethical perspective, this will result in a **dynamic and special relationship** between a party involved in the generation of data and the party controlling the data. The duration of this relationship may vary, as may its intensity. As far as personal data are concerned, the relationship will largely be determined by the applicable data protection law.

From an ethical perspective, the **recognition and design** of data rights, and corresponding data obligations, in dynamic environments depend on the following general factors, which are normally also the factors underlying relevant legal provisions where data rights and obligations have already been substantiated in the law:

a) the scope and nature of the **contribution to data generation** by the party asserting a data right;

1 Model of data rights and data obligations based on Preliminary Drafts no. 2 (February 2019) and no. 3 (October 2019) of the "Principles for a Data Economy" by the European Law Institute (ELI) and the American Law Institute (ALI), made available to the Data Ethics Commission. These preliminary drafts have not yet been adopted by either the ALI or the ELI and do not yet represent the official position of either of these organisations.

b) the **weight of that party's legitimate interest** in being granted said right (in particular the right to require desistance, access, rectification or an economic share);

c) the **weight of any possibly conflicting interests** on the part of the other party or of third parties, taking into account any potential compensation arrangements (e.g. protective measures, remuneration);

d) the **interests of the general public**;

e) the **balance of power** between the party asserting the data right and the other party.

These factors interact with one another in what can be described as a flexible system; if the public interest in data access is particularly high, for example, it may compensate for a relatively insignificant contribution to data generation. Consideration must always be given to the general principles outlined in Part B in order to avoid situations in which crucially important individual interests are undermined by a purported or actual public interest. These factors also determine how certain details (e.g. formats, deadlines, protective measures or financial compensation) should be **fleshed out and put into practice**. This includes the question of whether action should be taken only upon request by the party asserting the data right (e.g. data access claim) or also proactively (e.g. an obligation to publish data).

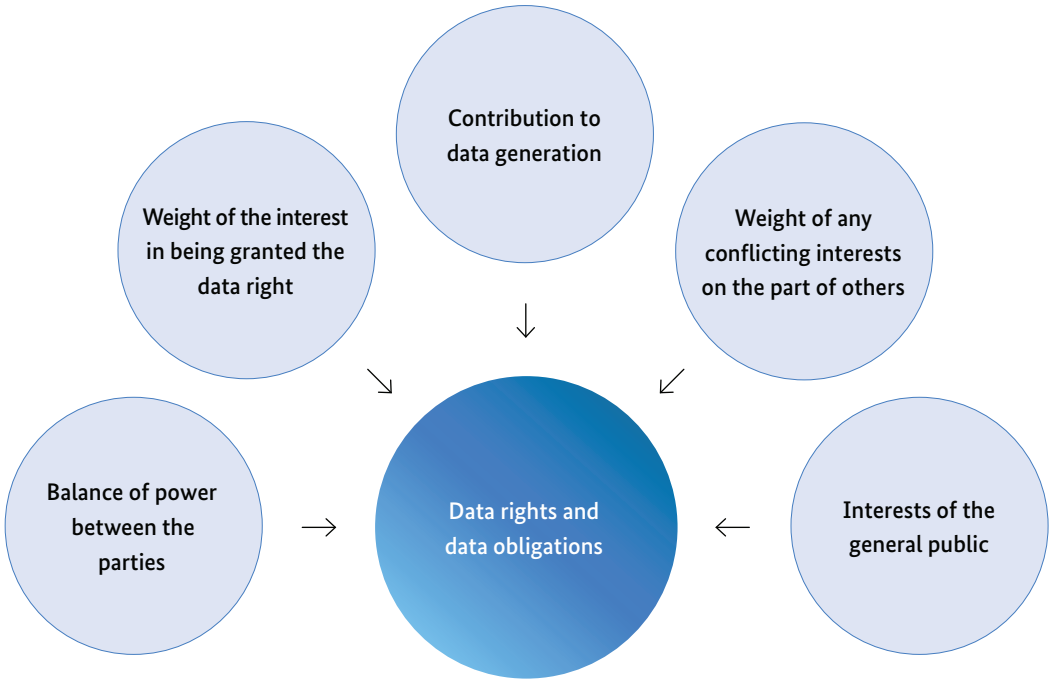


Figure 6: General factors for the shaping of data rights and the corresponding data obligations

The **rights granted to data subjects** by the GDPR are a particularly important manifestation of these principles, aimed specifically at protecting the natural persons to whom the information pertains; they are also to some extent a standardised manifestation given that they hinge on the qualification of data as personal data. The principles formulated here can also be applied to non-personal data, however, and relate not only to individuals, but also to legal entities and collectives.

2.2 Clarification of the general principles with reference to typical scenarios

Data rights may have a number of different **goals**; these include obliging another party to desist from using the data (up to requiring erasure of the data), gaining access to the data (e.g. disclosure, transfer, full portability), arranging for the data to be rectified, or claiming an economic share in the profits derived with the help of the data.

2.2.1 Scenarios involving desistance from use

Situations often occur in which a party requests another party to desist from using data in a certain way. The GDPR even works from the basic assumption that (personal) data should not be used unless there is a legal basis for doing so and a number of other requirements have been met.[2] In a general sense and beyond the scope of the GDPR, if a party has a significant legitimate interest in the controller desisting from data use, the outcome (from an ethical perspective) may be a **right to require said desistance**, potentially even including a right to erasure of the data, where the data processing operation:

a) might cause harm to that party or to a third party; and

b) is inconsistent with the circumstances under which that party contributed to generation of the data, in particular because

   (i) the contribution was made for another purpose, and the party could not reasonably have been expected to contribute to the generation of the data if it had foreseen the present data processing operation; or

   (ii) consent by that party would be invalid for overriding reasons.

Before any such right to require desistance from use can be affirmed, however, the party's legitimate interest in being granted the right must be weighed up against the other factors referred to above (→ in section 2.1). For example, such a right cannot be affirmed in cases where the processing of data is, by way of exception, justified by compelling other interests (e.g. the prosecution of criminal offences).

2 Article 6(1), Article 9(1) GDPR.

With regard to **non-personal data**, requests to desist from the use of data may become relevant, for example, in the context of value creation chains and customer relationships where non-personal data are often of enormous economic significance and a party involved may have a significant legitimate interest to assert such a right (→ section 5.3 below).

Example 1

The non-personal data collected by sensors in modern agricultural machinery (relating to soil quality, weather, etc.) are used by manufacturers as a basis for many of the services they provide (precision farming, predictive maintenance, etc.). If the manufacturers were to forward these data to potential investors or lessors of land, however, the latter would be given information that might prove harmful to an agricultural holding if negotiations over the land were to take place in the future. It can be assumed that the agricultural holding would not have helped to generate the data voluntarily had it known that they would be used for this purpose. When assessing a right to require desistance from an ethical perspective, consideration must be given to the balance of power between the parties in the case at hand, and also to the fact that the agricultural holding made an extremely significant contribution to generation of the data. Third-party rights deemed worthy of protection would include only the manufacturer's interest in maximising their profit and a general interest on the part of investors, lessors, etc. in obtaining accurate information.

From an ethical perspective, a **waiver of a data right** to require desistance is possible only under very limited circumstances. Such a waiver should automatically be ruled out in cases where consent to data use would be invalid for overriding reasons (within the meaning of requirement b) (ii)), for example because it is illegal or inconsistent with public policy; this is because, under our legal system and the fundamental values underpinning it, there exists no such thing as a liberty to do any kind of harm to oneself or to others. In other cases, a waiver may be possible, provided that stringent requirements are met (e.g. there is a separate agreement that is not linked to other services and does not involve the party being placed under pressure) to ensure the voluntary nature of the waiver, meaning that requirement b) (i) would no longer apply.

In Example 1, the agricultural holding could consent to the data being forwarded to third parties, e.g. on the basis of an individual agreement with appropriate remuneration; use of the tractor should not be dependent on the data being forwarded.

For **personal data**, obligations to desist from data use normally follow already from the provisions of data protection law, but the criteria outlined above can be used to determine whether **the substantive limits of consent** have been exceeded (→ section 3.2.1 below) or to guide the balancing of different legitimate interests, for example.

Example 2

Data relating to the activities of a social network user are used for extensive personality profiling; the profile contains the attributes "mentally unstable" and "esoteric tendencies". As a result, the user is shown advertisements by companies that offer personal horoscopes or energy healing services (at significant cost) on an almost daily basis and often immediately after he has posted content that signals stress or anxiety; he often makes purchases as a result. When he set up his user account, he clicked on a checkbox next to the following statement: "I am happy for my data to be evaluated so that my personal preferences and attributes can be identified more accurately and the services offered to me (including by third-party providers) can be personalised to my needs (profiling)." "Consent" of this kind does not make the subsequent data processing operations lawful. There are a number of different arguments for reaching this conclusion: one of them being that processing the data for this purpose may cause significant harm to the user, which would be inconsistent with the circumstances under which he generated the data (because he could not reasonably have been expected to do so had he known that data would be used for this purpose, and because the law does not allow the abuse of mental states of this kind, cf. Section 138 of the [German] Civil Code (Bürgerliches Gesetzbuch, BGB).

There are many circumstances under which an obligation to desist from the use of data cannot be mitigated by consent or a balancing of conflicting interests; in such cases, reference is often made to "red lines" or "**absolute limits**". There is no requirement for these limits to be data-specific, and most are not. For example, it is reasonable to prohibit election manipulation practices that are incompatible with the principle of democracy, regardless of whether said practices involve the use of data. In the view of the Data Ethics Commission, an example for data-specific absolute limits is the total surveillance of individuals.

Example 3

When entering into an employment contract, an employee signs an agreement stating that the location tracking functions on her smartwatch and mobile telephone, as well as a number of apps that collect data (e.g. by tracking sleeping behaviours and emotions), will be kept switched on at all times, even when she is not at work, and that she will hand the devices over to her employer when requested in order for the relevant data to be accessed. It is readily apparent that these arrangements, taken together, are equivalent to total (or almost total) surveillance, which is incompatible with human dignity, self-determination and privacy. This is true even if the employee gave consent to each of these measures, even if she decided of her own accord to enter into a contract with this employer, and even if there were other offers of employment available to her.

Conversely, the criteria that apply to scenarios involving desistance from use may also bear an indirect relevance to situations in which there is an ethical or even legal **obligation to use** data; such an obligation may arise where a party is under a general obligation to protect certain legally protected interests and has, at the same time, access to data that could be used to secure or improve the protection of these interests. In this kind of situation, an obligation to use data arises as the corollary of an obligation to protect certain legally protected interests unless a third party has a conflicting right to require desistance from data use.

Example 4

A hospital is experiencing an outbreak of a multi-resistant pathogen. It wants to analyse the health data of patients who have recently become infected in order to gain a better idea of why certain individuals are more likely to fall prey to the pathogen, as a basis for pinpointing the inpatients that might benefit most from a move to another hospital. Under these circumstances, the hospital has a general obligation to provide new patients with the best possible protection against infection by taking all available and reasonable precautions to this end. This includes the use of health data belonging to patients who have already been infected with the pathogen, provided that said use might protect new patients and there is no obligation emanating from the former group of patients to desist from use of their data.

2.2.2 Scenarios involving access to data

When it comes to scenarios involving a request for access to data, there will be many situations in which the party seeking access to data and the party who effectively controls the data will be able to reach an agreement on the action to be taken. **Voluntary arrangements** of this kind should be welcomed, provided that there are no conflicting and overriding third-party or public interests, and in particular provided that there are no parties with a right to require desistance from use based on the above criteria. Given the enormous potential for value creation inherent to data, however, in-depth discussions are also being held on the circumstances and conditions under which access to data should or even must be granted from an ethical viewpoint.[3]

This may apply in situations in which access to data is required (and perhaps even mandated by law) in order to enable a party to comply with a special **obligation or task** (e.g. prosecution of a criminal offence, public health concern). Any such data access right must be consistent with the rules that apply to this obligation or task; particular attention should be paid to the **principle of proportionality**, and any potential third-party rights to require desistance from use (→ see section 2.2.1 above) must be considered.

There may also be independent requests for access to data, for example within **existing value creation systems**. Such systems typically involve many different parties who contribute to the generation of data in different roles (e.g. as suppliers, manufacturers, retailers or end users), and who are, in principle, familiar with and have agreed to both their own roles and the roles of the other players involved (→ see section 5.3 below for further details). Legitimate interests that can be asserted by a party as a basis for an access request may, in particular, include cases in which the data are required for the following purposes:

3 By way of examples: European Commission: Building a European data economy, COM(2017) 9 final, 10 January 2017, pp. 11 et seqq. (available at: *https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-9-F1-EN-MAIN-PART-1.PDF*); European Commission: Towards a common European data space, COM(2018) 232 final, 25 April 2018, pp. 8 et seqq. (available at: *https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-232-F1-EN-MAIN-PART-1.PDF*).

a) to use an asset in line with its intended purpose within the value creation system (e.g. repair of a connected device by the end user);

b) monitoring and improving the quality of a service provided within the framework of the value creation system (e.g. by a supplier);

c) to ascertain the truth or provide evidence (e.g. in a legal dispute with third parties);

d) to avoid anti-competitive effects (e.g. lock-in effects); or

e) to create new value using the data (e.g. by developing a smart service).

Example 5

A supplier provides the engines for the agricultural machinery referred to in Example 1. It would be extremely useful for the supplier to have access to certain tractor data so that it can verify and constantly improve the quality of its engines. These data are stored in the manufacturer's cloud, however, and the latter is unwilling to allow the supplier to access them. In situations of this kind, it is important to remember that the supplier has made a significant contribution to the generation of the engine data, and that the data are urgently needed to improve the quality of a service provided within the framework of the same value creation system in which the manufacturer is also involved. Consideration must be given not only to the balance of power in the specific case at hand, but also to the fact that all parties involved – including the general public – have an interest in high-quality engines. There may, however, also be relevant economic interests on the manufacturer's side, in particular relating to confidentiality.

Access rights are also being discussed in situations where the party seeking access and the party that effectively controls the data are not yet part of the same value creation system, but where a **new value creation system** could originate in which they are both involved. The outcome of an assessment based on the general criteria will normally be different in situations of this kind, if only because the party seeking access has not typically contributed to the generation of the data, and the justifications that can be cited for granting an access right are rather **public interest considerations** or specific considerations, such as safeguarding **competition** (→ see section 5.5 below for further details).

Example 6

In Example 1, the manufacturer (which holds a dominant position in the tractor market) has been collecting soil and weather data for decades. A start-up recognises the potential of a database for investors using these data, and requests access to them. In this case, consideration must be given to the fact that the start-up itself has not made any contribution to the generation of the data. The existence of a public interest in data access (and the significance of this interest) depends on whether the manufacturer is abusing its market power and on how much the European economy would benefit from the breaking up of a small group of market-dominant companies (presuming that the start-up is based in Europe). In any case, potential harmful effects of data disclosure on trade secrets and other legitimate third-party interests, such as the interests of the manufacturer and the agricultural holdings in Example 1, must be taken into account.

The generally recognised principles of **open government data (OGD)**, which embody the idea that government data should be made available to the private sector, include "open by default" and re-use of data "by anyone for any purpose".[4] There have been calls from many quarters to expand these open data concepts to include data created by and effectively controlled by private entities. The move towards open data, however, also gives rise to complex ethical questions, for example the extent to which a generalised assessment that no longer looks at the individual case is acceptable.

Example 7

A municipality implements a large-scale project to collect mobility data using smartphone signals, with a view to facilitating traffic management (by adjusting the timing of public transport services, for example). Theoretically speaking, the data are "anonymised"; if the data sets are combined with other data sets and some additional knowledge, however, the owner can be identified with a confidence level of 95%. A number of different parties are interested in gaining access to these data; they include a researcher who wants to use them as a basis for identifying the optimal design of urban recreational areas, a start-up that wants to establish an online detective agency via which users can pay to access the mobility profile of their spouse, competitor, etc. and a research institute tasked by a foreign government with investigating the political activities of its citizens. Case-by-case assessments of these three access requests would deliver very different outcomes. It is therefore a difficult question whether the municipality may, or even must, make these data public with a view to the many possible uses of the data that would promote the public good.

The Data Ethics Commission wishes to emphasise, in this context, the importance of the (potential) rights of individual parties who have contributed to data generation, in particular the rights of data subjects, to require desistance from data use. It follows not only that all possible and reasonable protective measures (including anonymisation techniques, to be improved on an ongoing basis) should be taken after weighing up the potential for harm and the expected benefit for the public good, but also that – depending on the potential for harm – the granting of blanket access may be out of the question (→ see section 5.4 below for further details).

2.2.3 Scenarios involving rectification

Not all data are of a high quality. Problems that are particularly likely to arise include an unsuitable context, **inaccurate** encoding or **incomplete** data in the sense that any deductions obtained using the data are also **incorrect**. In circumstances of this kind, a party involved in the generation of data may have an ethically justified right to require rectification of the underlying data or of the deductions obtained using the data. The threshold for a right of this kind to be granted is relatively low, since in principle there is neither a protected individual interest nor a public interest in the processing of inaccurate or incomplete data. As a general rule, only the following requirements must be met:

a) the processing of inaccurate or incomplete data must be potentially harmful to a party (in particular the party to whom the information relates); and

b) the rectification must not be disproportionate, taking into account the severity and likelihood of harm on the one hand and the effort involved in rectifying the data on the other.

4 See Recital 16 of Directive (EU) 2019/1024 on open data and the re-use of public sector information (PSI Directive); Principles 1 and 3 of the G8 Open Data Charter signed at the G8 Summit on 18 June 2013; and Principle 1 of the International Open Data Charter signed in September 2015 at the Open Government Partnership Summit.

Example 8
A very high error rate has been detected in the engine data stored by the manufacturer in Example 5. This is problematic for the company that supplies these engines, not only because it deprives the company of the possibility to fulfil its quality assurance remit, but also because these engine-related data are pooled with engine-related data from other engine suppliers as a basis for evaluations, and poor performance metrics for the engines from the relevant supplier might reduce the latter's chances of securing orders from other manufacturers. In this case, the processing of inaccurate data causes harm to the supplier, and there are no indications that the effort involved in rectification would be disproportionate.

If the amount of effort involved in rectifying the data is excessive but the potential for harm is significant, a right to require desistance from use will frequently arise (→ see section 2.2.1 above).

2.2.4 Scenarios involving an economic share

Cases where a party uses data to create value after other parties have contributed to the generation of said data are an everyday occurrence, and a good thing in principle. Provided that no one is entitled to a right to require desistance from use (→ see section 2.2.1 above), such use of the data must normally be tolerated by the parties who contributed to their generation. Given the strong affinity which the data rights and obligations set out in this section have with **considerations of public good**, there are potent arguments against recognising a general right to remuneration for all parties who have contributed to the generation of data. Instead, such parties must content themselves with existing mechanisms of collective economic participation, in particular through the taxation of value creation.

In cases where there is no valid contract to back up a claim for remuneration, financial compensation should at most be considered as a mitigating measure, for example if the exercising of a data right without compensation appears disproportionate in the specific case at hand (→ see section 2.1 above, factor c). From an ethical perspective, and in the view of the Data Ethics Commission, a party who has contributed to the generation of data should be entitled to **independent remuneration** for their use by others only in very **exceptional cases**. Cases of this kind might arise if:

a) the party's contribution to the generation of data required an unusual amount of **effort** or was **particularly unique**, and it would hardly be possible (from an economic viewpoint) to replace it with contributions by other players; and

b) an exceptionally **large amount of value** has been created using the data; and

c) the circumstances under which the contribution to data generation was made mean that it would have been **impossible or unreasonable** for the party to engage in negotiations on any **remuneration**.

The amount of any remuneration paid in such exceptional cases must be adequate; in particular, basic incentives of using data to create value must not be removed. It must also be remembered that the party creating the value has typically incurred financial risks.

2.3 Collective aspects of data rights and data obligations

An answer must be found to the issue of whether (and if so to what extent) the above arguments concerning the right to require desistance from use, the right to access data, the right to rectification and the right to an economic share in profits derived with the help of the data can also be applied to **collectives** in the sense of defined groups of persons (e. g. indigenous peoples with regard to the use of their genetic data), i. e. whether collectives may be entitled to certain data rights in connection with the use of "their" data. For example,

thought must be given to the question of whether – ethically speaking – a population (of a nation state, or of the EU) which has generated data should have a right to an economic share in profits, such as in the form of taxes or transfer payments. The Data Ethics Commission believes that this question can, in principle, be answered in the affirmative.

Example 9

An Internet giant earns billions from the data generated when individuals all around the world use its services. Yet even though this megalith of a company generates 10-digit sums year on year using data from EU-based individuals, it pays virtually no taxes in the EU. The question arises whether the company should be obliged on ethical grounds to allow the general public in the EU to share (through taxation) in the value it creates. The issue raises fundamental questions about distributive and participatory justice, and about what a just economic system looks like. However, aspects such as market power and the unique nature of contributions (e.g. if audio data in a certain language is used to develop new voice-controlled services) may also have to be taken into account.

The **relational nature of many data types** makes it particularly important to include groups and collectives in any debate. This relational nature is apparent from the way that many digital services require users to disclose data about their contacts or "friends", for example. As far as data rights and the corresponding obligations are concerned, the "friends" may have the right to require desistance from use of the data and the right to gain access to the data, etc.; at the same time, their potential interests must always be taken into account when weighing up whether a data right should be granted (→ see section 2.1 above). However, there are also cases in which a party contributes to the generation of data, and these data then indirectly provide **information on other parties** – even if the latter played no role (not even in the broadest sense of the word) in their generation. This is particularly relevant in the sphere of genetic data, but also applies to other data types. There is still another, closely related group of cases, where individualised data (even in aggregated form) may have implications with potentially negative **third-party effects** that extend beyond the individual who supplied the data.

Example 10

A health insurance company offers reduced premiums as an incentive to sign up for health tracking schemes. While those who agree to disclose their data will benefit from lower premiums, those who refuse to do so may end up paying more.

Issues relating to the **representativeness of data** used to train algorithmic systems can also be interpreted as problems of relationality: the lack of any relationship between the parties who supply the training data and the parties to whom the trained systems are applied may result in systematic bias and potential discrimination (→ see Part F, section 2.6 for further details).

To overcome this hurdle, individualistic approaches to data rights in ethics, law and technology design must be expanded to include **relational concepts of data rights** (cf. also the debate on group privacy). Under certain circumstances, it may therefore be possible – at least when viewed through the lens of ethics – for one group member's contribution to data generation to be attributed to the other group members as well, potentially entitling these latter, in spite of the fact that they themselves made no individual contribution, to certain rights of their own (the right to request desistance from use or the right to gain access, for example).

3. Standards for the use of personal data

3.1 Personal data and data relating to legal entities

Any information relating to an **identified or identifiable natural person** is regarded as personal data. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person (Article 2(1) GDPR).

Even though the remainder of this section focuses on personal data in the legal sense of the term, the Data Ethics Commission wishes to stress that the **protection of companies and legal entities** is a valid concern that should not be relegated completely to the sidelines. The potential hazards confronting legal entities have been exacerbated yet further by the networking of all machines, the exchange of data between factory components, and the storage of all production data generated by Industry 4.0 plants in "digital twins". If individual sets of data (generated through the operation of devices, for example) are pooled together, the result may be an almost seamless overview of a company's internal operating procedures, which may – in the absence of appropriate protective mechanisms – easily fall into the hands of the wrong parties outside the company (competitors, negotiating partners, authorities, prospective buyers, etc.). The Data Ethics Commission believes that the risk posed not only to the digital self-determination of companies and legal entities but also to the **digital sovereignty of Germany and Europe** (since data flows predominantly involve third countries) is concerning from an ethical viewpoint, and that steps must be taken to mitigate against it.

A key legislative starting point for protecting enterprise data is the **protection of trade secrets**, in particular the [German] Act on the Protection of Trade Secrets (*Gesetz zum Schutz von Geschäftsgeheimnissen*, GeschGehG). When interpreting and applying this Act, efforts must be made to guarantee the comprehensive protection of sensitive business data, given the central importance of the latter in building a fair and competitive economic system as the basis for economic and social well-being. In many respects, however, Directive (EU) 2016/943 (the provisions of which were transposed into the Act on the Protection of Trade Secrets) is not adequately tailored to the reality of IoT and Industry 4.0. The Data Ethics Commission therefore calls on the Federal Government to **step up data-related protection of German and European companies**.

The recommendations for action relating to personal data put forward by the Data Ethics Commission in the remainder of this section, for example in relation to a risk-adequate interpretation of the applicable legal framework (→ section 3.2.2 below) or privacy-friendly design of products and services (→ section 3.6 below) also apply to the protection of data relating to companies and legal entities (in a modified or attenuated form where appropriate).

3.2 Digital self-determination: a challenge to be tackled by the legal system as a whole

3.2.1 Cooperative relationship between the applicable legal regimes

Our economy and society are heavily reliant on the use of personal data in a huge variety of different contexts, and yet there is always a degree of tension between this use of personal data and the fundamental rights of individuals. The constitutional right to informational self-determination (as part of the general right of personality) is essentially part of the protection of human dignity. **Data protection law**, in particular the GDPR, clarifies these benchmarks and has binding force on public and private bodies.

The GDPR is one of the great achievements of the EU legislator, and currently functions as a source of inspiration for other countries. It is important to temper our expectations of this piece of legislation, however; the GDPR is focused on data protection rather than on comprehensive promotion of individual welfare and the public good in the data economy. Taken in isolation, it is not a suitable tool for averting all the harm that an individual may suffer as a result of his or her personal data being processed, and cannot therefore be regarded as protecting his or her integrity in all respects. All of the different mechanisms provided by the legal system as a whole must be used to safeguard these legally protected interests, particularly those that are **not specifically addressed by the provisions of data protection law** (e.g. economic interests, the right to life and health, physical integrity and reputation). This applies even in situations where personal data are at play.

The **concept of consent** that is enshrined in **data protection law** is a vitally important mechanism for safeguarding informational self-determination in the digital and analogue spheres. Yet the concept of a right to self-determination that is not subject to substantive limitations and that includes the freedom to inflict any kind of harm on oneself or third parties would be an alien element in our legal system, and is ethically indefensible. The law should limit or even prohibit an individual's free and informed consent – as an expression of his or her general freedom of action, which is protected as a fundamental right – only in narrowly defined exceptional circumstances. However, consent under data protection law should be subject to substantive limitations, by way of analogy to the limitations to freedom of contract or to consent when it comes to intrusions on bodily integrity.

In the view of the Data Ethics Commission, it has become clear that the average individual is **systematically overwhelmed** by the number and complexity of the decisions that he or she is required to take in connection with consent under data protection law, and by the difficulty involved in estimating all the potential impacts of data processing. The Data Ethics Commission believes that inadequate use of consent by providers of digital services is one of several reasons for a general **loss of trust** in the digital society. As things stand, individuals can often no longer rely on the fact that the State and the legal system have put in place the framework conditions necessary for them to navigate the world in safety and (relatively speaking) free from care, without needing to worry about the possibility of suffering serious harm from other parties. For business-to-consumer transactions, contract law, and more specifically unfair contract terms, control has provided the basis for 'rational indifference' on the part of consumers and for far-reaching protection even in low-value cases. The same result should be achieved by way of applying the **fairness test to declarations of consent**.[5] In applying the fairness test, general values and principles underlying the legal system as a whole must be taken into account.

3.2.2 Risk-adequate interpretation of the applicable legal framework

The Data Ethics Commission wishes to stress that the existing legal framework must be interpreted and applied in such a way as to mitigate to the maximum the new hazards we are facing in connection with the widespread collection, use and analysis of personal data.

Notwithstanding the need to comply with the requirements of data protection law, data processing operations are also subject to a number of **absolute limits**. Wherever possible, any uses of data that go beyond these limits should be prevented by interpreting and applying the law in force[6] in a manner consistent with fundamental rights. In the view of the Data Ethics Commission, this is relevant, for example, for:

5 Cf. also Recital 42 of the GDPR.

6 This relates in particular to the fairness test applied to general terms and conditions of business (Sections 307 et seqq. of the [German] Civil Code (*Bürgerliches Gesetzbuch*, BGB)), the principles of public morals (Section 138 of the Civil Code), wilful immoral damage (Section 826 of the Civil Code) and contractual and quasi-contractual protection and fiduciary duties (Section 241 paragraph 2 of the Civil Code).

- **incursions into personal privacy and integrity** that are incompatible with fundamental rights and that result from profiling and/or scoring (e.g. certain methods of determining personality traits, emotions or expected behaviours);

- **total surveillance** that is incompatible with human dignity, *inter alia* through a "comprehensive surveillance footprint" or "super scoring";

- **immoral exploitation** of situations of urgent need or of medical conditions;

- **election manipulation practices** that run counter to the principle of democracy.

The legislation currently in force already categorises ethically reprehensible attempts to mislead or manipulate consumers in a commercial context – which should include business practices aimed at persuading the party to disclose his or her personal data – as **misleading or aggressive commercial practices** under the [German] Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*, UWG), regardless of whether the provisions of data protection law have been infringed; any such attempts will therefore trigger the appropriate legal consequences (e.g. rescission on grounds of fraud or threat, injunctive relief and compensation). The Data Ethics Commission wishes to cite the following as potential examples of such practices:

- **addictive designs**, i.e. technologies which exert undue influence on a user (in particular by means of mechanisms that promote addictive behaviour) and which are therefore liable to have a substantially adverse impact on his or her freedom to decide whether to use them (and stop using them);

- **dark patterns**, i.e. technologies (mainly user interfaces) that are designed in such a way as to deceive a user about certain facts and/or manipulate him or her into taking a certain decision (which may have financial implications).

Absolute limits must also be imposed on data processing in order to protect individuals against being placed at an **undue financial disadvantage**, and the existing legislation contains various provisions that can be used to enforce this protection.[7] In the view of the Data Ethics Commission, examples of unfair contract terms and violations of contractual or pre-contractual duties of a fiduciary nature include the following:

- preventing access to data that have been generated by a device and that are required for normal **use** of said device, including for the performance of repairs by an independent workshop, or making it unreasonably difficult to access these data (e.g. access only granted in accordance with Article 12 GDPR, i.e. only within one month or even three months);

- preventing access to the data needed to operate a **pre-owned** networked device, or making it unreasonably difficult to access these data (e.g. for an individual who has bought a house equipped with smart home technology);

- making it harder for individuals to switch provider by means of **data lock-in** (i.e. refusing to hand over data analyses for which the user has already paid from an economic perspective, and which are not protected trade secrets);

- processing user generated data by a manufacturer or another member of the supply chain and for a purpose that runs completely counter to the user's **economic interests** (e.g. price differentiation with the aim of extracting the maximum from each individual that he or she is willing to pay).

7 Cf. the instruments referred to in Footnote 6.

Social media monitoring

Social media monitoring is the systematic **oversight** of social media content on a particular topic. It has evolved into a data utilisation tool that takes advantage of the fact that social networks not only expand users' communication options but also allow their digital behaviour to be constantly monitored.

Companies frequently deploy data generated by social network users, e.g. for the purpose of market research or marketing. Although public-sector bodies have so far been slower to make use of the opportunities afforded by social media monitoring, it is by no means an unheard-of practice; for example, the tax authorities use web crawlers to trawl through content that is publicly available on the Internet as a way of pinpointing business sellers that are not paying VAT.

Algorithmic systems can be used to make information collated from social media monitoring **usable and exploitable** for more far-reaching and intrusive purposes (in particular the creation of personal profiles for commercial purposes). Provided that the weighing up of interests pursuant to Article 6(1)(f) GDPR supports such a use or exploitation or there is another legal basis for processing, this may be entirely consistent with the law. Pursuant to Recital 51 GDPR, the fact that the data subject has disclosed the data himself or herself does not, in itself, justify the further use and exploitation of the data.

The Data Ethics Commission takes the view that monitoring activities can, at any rate, be deemed to have crossed the boundary between lawful and unlawful when publicly available information is monitored and the scope of this monitoring could not have been gauged by the data subject when the information was disclosed (for example – generally speaking – statements made by minors without due consideration), or alternatively when the information is highly sensitive (for example suicidal ideation statements). Even if applicants for a job have willingly made data public, these data should not be used during the recruitment process if they represent too great an intrusion into personal integrity or if they are not clearly related to the applicant's job history (e.g. statements about his or her sexual orientation). The same applies to any other systematic evaluation of data originating from an individual's private life (e.g. tracking data).

Particularly when the modes of use and exploitation are more far-reaching and intrusive, a weighing up of interests may result in limits being placed on their admissibility (e.g. businesses that target advertisements on the basis of sexual orientation or exploit individuals known to be in an emotionally vulnerable state). Certain providers (in particular providers of social networking sites) are technically capable of carrying out in-depth evaluations of the communications that are exchanged via the central platforms they operate; even if general access to the content is prevented using end-to-end encryption, metadata provide them with the means to obtain highly instructive analytical findings. A legislative ban on the evaluation of communications between individuals or within closed groups should also be imposed on private providers in keeping with the principle of telecommunications secrecy. The Data Ethics Commission therefore recommends that the Federal Government should not delay in its efforts to secure the introduction of such a ban during the forthcoming negotiations on adoption of the ePrivacy Regulation.

3.2.3. The need to clarify and tighten up the applicable legal framework

As things currently stand, a level of protection of legally protected interests that is in line with constitutional requirements can be achieved, for many questions arising in a digital society, only through case-by-case interpretation of general legal concepts and blanket clauses by supervisory authorities and courts. The Data Ethics Commission believes that this situation is untenable. General legal concepts and blanket clauses offer the advantage of being flexible and keeping future options open, yet the authorities and courts often take years or even decades to develop established case law for new phenomena (digital phenomena in particular), which in the meantime results in a **structural enforcement gap** with regard to the law in force and in a **lack of legal certainty**. Given the extent to which this issue affects fundamental rights and the uncertainty as to whether and when solutions will emerge that meet constitutional requirements, the Data Ethics Commission believes that prompt action to establish a clear and binding regulatory framework falls squarely within the remit of the democratically legitimised legislator.

In view of the hazards posed to individuals by **personality-sensitive profiling** (sometimes resulting in **scoring**), the Data Ethics Commission believes that there is an urgent need to take effective action to tighten up the current legal framework in this particularly critical area, in order to effectively counter the risks of individuals being manipulated or suffering discrimination.

Profiling

"Profiling" is defined in **Article 4(4) GDPR** as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Profiling ultimately involves making **deductions** (drawing conclusions) on the basis of input data, in particular using certain statistical inference methods (→ Part C, section 2.2.2). These deductions may relate to the actual or purported "properties" of an individual (e.g. "mental stability", "reliability", "social acceptability") and/or take the form of predictions if they relate to an individual's future behaviour (e.g. a particular consumption pattern).

In addition to profiling, attempts are frequently made to assign users to a predefined **stereotype category** on the basis of their observed behaviour when interacting with digital systems, using "matching algorithms"; for example, someone who books a holiday might be classified as a sports fan, a culture enthusiast, a family man or woman, a keen hiker, a sales representative or a gourmet. The stereotype that is instantiated for an individual user is used to store typical preferences, goals and personality traits, which will be used in subsequent algorithmic processing operations.

Sometimes it is not the profiles themselves that are stored; instead, **ad-hoc deductions** (in particular behavioural predictions) are generated dynamically and in real time using raw data (e.g. "is now ready to purchase shoes").

Given that profiling makes it possible to personalise a wide range of digital products and services to a degree that many users perceive as convenient and helpful, a categorical ban on it would overshoot the mark. However, the Data Ethics Commission recommends that the Federal Government should speak out – during the forthcoming evaluation of the GDPR, for example – in favour of **expanding the GDPR to include specific rules on profiling** that go beyond the existing provisions of Article 22 GDPR on the permissibility of automated decision-making; alternatively, the Federal Government could lobby for a separate EU legislative act that would effectively counter the risks that profiling poses to the fundamental rights of individuals. If an adequately hard-hitting European solution proves unworkable in the foreseeable future, legislative rules should be put in place at national level (within the scope of what is permitted by EU law) to regulate profiling procedures that pose a potential risk to fundamental rights.

The Data Ethics Commission believes that there is a particularly urgent need for provisions (horizontal and/or sectoral) on profiling concerning the following matters, as far as solutions do not already follow from correct interpretation of the GDPR:

a) imposition of **absolute limits**, i. e. the prohibiting by law of certain **critical applications** (e. g. when selecting from a pool of job applicants, the use of profiles that have been generated on the basis of data originating from their private lives), of profiling procedures that involve **highly sensitive personal data**, for example in connection with emotion detection software and biometric data, and of data processing operations that entail an **unacceptable potential for harm** to the data subjects or society;

b) imposition of **admissibility requirements** for critical profiling procedures, including quality requirements in relation to the meaningfulness and accuracy of the profiles generated (→ see Part F, section 4.2.1 for further details), and a risk-adequate system of opt-ins and opt-outs (the latter being appropriate only if the level of risk is very low);

c) clarification of the **principle of proportionality**, *inter alia* as regards the requirements that apply to the nature and scope of the data used for profiling, the permitted level of detail in the conclusions drawn for profiling purposes, and in particular the purposes for which profiling may admissibly be used;

d) imposition of specific **labelling, disclosure and information obligations**, *inter alia* as regards the existence and purpose of algorithmic systems that may be used to carry out **ad-hoc deductions**, and any critical deductions that have already been carried out (instead of providing information only on automated decisions taken at a later stage in the process);

e) provision of feasible options for data subjects to **exert an influence** over the profiles that have been created about them, including the option to erase/rectify/verify them; this also includes the right to a "digital new start" involving the erasure of existing profiles (e. g. upon reaching the age of majority), as recently suggested by an EU High-Level Expert Group.[8]

8 High-Level Expert Group on Artificial Intelligence: Policy and Investment Recommendations for Trustworthy AI, 26 June 2019, pp. 14, 40 (available at: *https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence*).

Voice assistants

Voice assistants promise a great deal in terms of convenience and easier access to digital technologies (particularly for people with disabilities), yet they also harbour risks as far as self-determination by data subjects is concerned.

Voice assistants record ambient noise, often without the user having activated any related function. If these recordings include speech by the user or third parties, they are regarded as **biometric data** for the purpose of the GDPR. Speech recordings are analysed in real time so that a response can be given to spoken commands, and automated processes often log certain data types in a log file. The unique timbre of an individual's voice and his or her speech patterns can be analysed as a basis for **uniquely identifying** the individual or deciphering **speech emotions**. Profiling of this kind represents a particularly deep and invasive intrusion into the core area of personality rights, and entails the risk of further exacerbating the structural imbalances between the demand and supply side of the market. Enormous **potential for misuse** is also present given the possibility of recombining or digitally reconstructing the spoken word (deep fakes).

In reality, individual users often have only a vague idea of how data processing is carried out, and indeed of whether it is carried out at all. Particularly if a user is relatively inexperienced in technical matters, he or she may easily be persuaded to disclose additional sensitive personal data upon hearing an authentically **human-sounding voice**. In many cases, voice assistants are not limited simply to recording what is going on in their immediate vicinity, but instead – when networked with other virtual assistants and smart home products – act as the control centre and "technological heart" of modern homes.

The Data Ethics Commission believes that the creation of comprehensive profiles, based on the use of voice assistants and the integration of a wide range of software and hardware components, poses a critical risk. The ease, convenience and apparent benefits of connecting voice assistants to other devices may ultimately lead users into a "plug-and-play trap". In the view of the Data Ethics Commission, a range of measures should be taken to mitigate against the risks associated with voice assistants. These include not only bans on particularly critical profiling procedures and applications, but also the following:

a) binding technical requirements that implement the principles of data protection by design and by default (→ see also section 3.6 below), especially **the processing of speech files on an exclusively local basis** (as well as the option to erase these files locally), and restrictions stating that data may be forwarded to operators or third parties only in the form of commands that have already been translated into machine language (e. g. an order that has been placed);

b) binding technical requirements that include an option to **switch off** the microphone and Internet connection and a way of telling (i. e. a **visual indication**) whether the microphone is on or off (→ see also section 3.6 below);

c) **transparency obligations** which are designed in a manner appropriate to the medium (→ see Part F, section 4.1), i. e. which ensure that the most important information is also provided **acoustically**, either when a pertinent situation arises or at regular intervals.

In addition to special legislative measures of this kind aimed at protecting users, the Federal Government should examine the extent to which it would be possible to lobby for a new or expanded legislative framework to ensure appropriate data governance, preferably at European level but otherwise at national level; this framework should be entirely separate from the goals of data protection law (i. e. outside the scope of the GDPR). The Data Ethics Commission wishes to issue the following special recommendations in this connection (→ see section 3.2.2 above for further examples in each case):

a) blacklisting of data-specific **unfair contract terms** (Sections 308 and 309 of the [German] Civil Code (*Bürgerliches Gesetzbuch*, BGB)) and data-specific contractual and pre-contractual **duties of a fiduciary nature** (Section 241 paragraph 2 of the Civil Code);

b) specification of data-specific **torts** under the umbrella of the existing tort of intentional infliction of harm contrary to public policy (e. g. as a new Section 826a of the Civil Code);

c) blacklisting of data-specific misleading and aggressive **commercial practices**, such as addictive designs and dark patterns, by expanding the blacklist that already exists in the [German] Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*, UWG); the full harmonisation approach of the EU's Unfair Commercial Practices Directive means that this change would need to be initiated at EU level, however.

When profiling is carried out by **government agencies**, the potential for cumulative infringements of fundamental rights or for aggregated surveillance must be taken into account, as must potential side effects or "collateral damage". The Data Ethics Commission believes that there is particular potential for abuse if individual subsystems are connected, resulting in the pooling of data and analytical findings from very different areas and sectors, which significantly steps up the intensity of surveillance. Intelligent pattern recognition techniques (in particular facial recognition) make it easier to link up personal information across a variety of surveillance systems and to merge profiles; in view of this fact, the Data Ethics Commission recommends firstly that pattern recognition techniques of this kind should come into play only when their use is an **absolutely vital prerequisite** for the fulfilment of state obligations, and secondly that clear **legal limits** – beyond the separation rule concerning intelligence activities – must be imposed **on the exchange of information** and patterns between authorities. This may also encompass new legal provisions banning particular types of use and exploitation, particularly as regards the sharing of data between government agencies engaged in preventive and repressive measures.

3.2.4 Uniform market-related supervisory activities

The task of supervising compliance with data protection law by players in the German economy is shared between federal and *Land* authorities. Discrepancies can be observed in terms of the interpretation of data protection law and in the approach to enforcement; this raises certain challenges for the parties affected. Although the European Data Protection Board (EDPB) has been introduced by the EU Member States with the aim of ensuring uniform application of the GDPR, and this institution also has the power to adopt binding decisions in individual cases, the coexistence of different data protection authorities in the various German *Länder* within the framework of the federal system has, to date, prevented the emergence of any such **binding and uniform approach** at national level.

In the event that it proves impossible to strengthen and formalise cooperation between the German data protection authorities, thereby safeguarding the uniform and consistent application of data protection law, consideration should be given to the establishment of a new **data protection authority** at federal level for market-related data activities. Concentrating supervisory powers within a single body would make it possible to build up the specialist expertise required to enforce data protection law in an environment characterised by highly dynamic technological developments. The single authority – either acting alone or in close cooperation with other authorities – would also need to be able to safeguard the enforcement of **other data-related areas of law** that have close functional ties to data protection legislation (e. g. general private law and unfair commercial practices law). The establishment of a single body able to wield market supervisory powers in the field of data protection might also make Germany's voice louder within the European Data Protection Board, since all of the Member States are already represented on the EDPB by a data protection authority with national jurisdiction. Finally, the centralisation of official competencies should go hand in hand with the designation of a single court responsible for judicial control over market-related supervisory authorities in the field of data protection, so that this court can also build up the relevant expertise and set forth a consistent body of case law.

Various models are conceivable from the perspective of organisational law. Based on its powers to regulate economic law, the Federal Government could transfer supervisory competences for data protection in the economy (i. e. the private sector) to the Federal Commissioner for Data Protection and Freedom of Information, and provide the latter with the relevant resources. By setting up a number of different satellite offices, the Commissioner could ensure the nation-wide presence of data protection bodies, similar to the Federal Office for Migration and Refugees or the Bundesbank. Alternatively, the *Länder* could establish a joint facility on the basis of an interstate treaty, by way of analogy to similar projects in the broadcasting sector, for example, or the Central Offices of the *Länder* for Safety Engineering and Health Protection. The joint facility responsible for supervisory activities in the field of data protection would need to be an independent body, and this principle should be enshrined in the interstate treaty. Irrespective of the decisions taken in this connection, the authorities should be provided with better **human and material resources** to allow them to "punch at their weight".

For reasons of constitutional law, the **data protection authorities at *Land* level** should retain jurisdiction **for the public sector**.

3.3 Personal data as an asset

3.3.1 Commercialisation of personal data

The economic significance of personal data is hard to overestimate. It is generally acknowledged that the protection of personality rights as fundamental rights also encompasses the individual's right to decide whether certain **aspects of his or her personality** should be made **available for a fee** (e.g. the right to one's own image), or in other words whether they should be exploited for economic purposes.[9] In the same way that there is not a complete ban on the exploitation of data by individuals, however, there are no rules categorically stating that personal data may not be exploited for economic purposes on the initiative of third parties. Some people compare the situation to the trade in human organs, but this comparison is flawed in several respects: unlike human organs, data are a non-rivalrous resource, and so the mere fact that personal data are processed by someone else does not in and of itself necessarily cause harm to the data subject – harm is caused only by the processing of data in specific contexts or for specific purposes.

Interpreting the right to informational self-determination as a natural corollary of human dignity makes it clear that the **limits** imposed on the economic exploitation of personal data should generally coincide with the general limits placed on the processing of personal data (→ see sections 3.2.1 and 3.2.2 above), including the substantive limitations on consent. Against this backdrop, the economic exploitation of personal data is neither subject to more stringent rules in general, nor privileged in any way. Economic aspects frequently come into play when general data protection rules are applied, however (for example, consent may no longer be freely given if the data subject is exposed to economic pressure).

3.3.2. Data ownership and the issue of financial compensation

As things stand, the Data Ethics Commission does not believe that there are **adequate grounds** for introducing additional ownership-like rights of exploitation that would allow data subjects to request an economic share in the profits derived with the help of data (often referred to under the concepts of "**data ownership**" or "data producer right").[10] Both data protection law and general private law already provide the individual with a range of legal rights that are effective vis-à-vis third parties, and on the basis of these rights individuals could theoretically make their toleration of data activities dependent on payment of an appropriate fee. If the individual fails to negotiate a fee of this kind, this can be attributed to circumstances (e.g. lack of negotiating power and/or poorly functioning competition) that have nothing to do with the absence of any additional ownership-like right of exploitation.

In theory, the imbalance in negotiating power could be counter-balanced through the introduction of **collective societies** that collectively exercise ownership-like rights to exploit data. Extending the concept of personal data to include an ownership-like economic component would, however, potentially be **at odds with data protection**, in particular as regards the voluntary nature of consent, the ability to withdraw consent at any time and the right to request erasure. It would also create **questionable financial incentives** by encouraging the generation of a maximum of personal data, and would put pressure on individuals (in particular on vulnerable groups such as minors and low earners) to disclose as much data as possible. If industry passes the costs of any such remuneration on to the customers, **privacy-conscious individuals** might also be forced to shoulder a comparatively **greater burden** in financial terms.

9 See e.g. Section 22 of the [German] Act on the Protection of Copyright in Works of Art and Photographs (*Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie*, KunstUrhG).

10 By way of examples: European Commission: Building a European data economy, 10 January 2017, COM(2017) 9 final (available at: *https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-9-F1-EN-MAIN-PART-1.PDF*); Arbeitsgruppe "Digitaler Neustart" der Konferenz der Justizministerinnen und Justizminister der Länder [Working Group "Digital New Start" of the Conference of Ministers of Justice of the Länder]: Report of 15 May 2017, pp. 29 et seqq. (available at: *https://www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/zt_bericht_arbeitsgruppe/bericht_ag_dig_neustart.pdf*).

The above arguments do not hold water to the same extent when it comes to anonymised data. However, given the huge number of individuals that contribute to the generation and processing of data, the level of **complexity** of a fair remuneration system and the 24/7 monitoring that would be required to measure data flows would be out of all proportion to any potential gains in terms of justice. **Data quality** might also be negatively affected, since incentives would be created to generate data "artificially" (e.g. through the creation of fake profiles), ultimately producing a distorted picture of reality. The Data Ethics Commission therefore counsels against **introducing rights of exploitation** designed as exclusive rights, **either for anonymised data or for other data types**.

3.3.3. Data as counter-performance

A large number of digital content and service types (e.g. search engines, social networks, messenger services, online games) are offered to end users for no monetary consideration. They are financed in other ways, in particular through payments received from third parties in exchange for personalised advertising and other personalised information services targeted at users, or for user profiles and user scores. Personal data are therefore often referred to in shorthand terms as "counter-performance" for digital content or services, for example in the original draft of Article 3(1) of the Digital Content Directive (although the term was removed at a later point in the legislative procedure).[11] The extent to which the economic model described above is, in fact, compatible with the **prohibition under Article 7(4) GDPR of "tying" or "bundling" consent with the provision of a service**[12] must ultimately be clarified by the European Court of Justice.

The Data Ethics Commission argues that **data should not be referred to as "counter-performance" provided in exchange for a service**, even though the term sums up the issue in a nutshell and has helped to raise awareness among the general public. Firstly, personal data form an integral part of an individual's personality, and are protected under constitutional law. Secondly, their classification as a counter-performance might have unintended consequences. For example, it might be abused as an argument in favour of largely excluding data-related standard contract terms from unfairness control, or as a justification for triggering contractual sanctions against consumers who withdraw consent or exercise their right to erasure, etc.

In this connection, the German legislator should not – when implementing Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services – use the leeway available to Member States in any way that might prevent the individual from seeking legal remedies under data protection law. In particular, if an individual withdraws his or her consent to the processing of data, the provider may have a right to terminate provision of its service with immediate effect; however, it should not be possible for the provider to request **payment for services already provided**, and there should be no retrospective and **automatic reversion to a pay option**.

Pay options are increasingly being discussed as a way of avoiding the "tying" or "bundling" of consent with the provision of a service. Yet even the smallest of financial burdens represents a disadvantage, in particular for vulnerable population groups, and may dissuade data subjects and encourage them to disclose excessive amounts of personal data. It is also to be feared that the financial burden on privacy-conscious individuals would be disproportionate. **Commercial users** that have previously been able to use certain digital content or services for free (e.g. a company's page on a social networking site) should therefore be the **preferred source of funding**.

11 European Commission: Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, 9 December 2015, COM(2015) 634 final (available at: *https://ec.europa.eu/transparency/regdoc/rep/1/2015/EN/1-2015-634-EN-F1-1.PDF*).

12 European Data Protection Supervisor: Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 14 March 2017, p. 15 (available at: *https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf*).

Pay options may, however, increase consumer awareness of the financial value of their own data, and also create transparency. For these reasons, the Data Ethics Commission believes that **offering pay options as an alternative** may be an ethically acceptable way to ensure that consent given by users is genuinely free. At the same time, however, the price must not be abusive and exceed market prices; from the consumer's perspective, it must represent a realistic alternative to the disclosure of personal data. From an ethical viewpoint safeguards must be put in place to protect privacy-conscious users from having to "cross-subsidise" other users; equally, the needs of socially vulnerable groups must be taken into consideration, for example through government transfers.

3.3.4 Data as the basis for personalised risk assessments

Price-related predictions obtained using algorithmic systems for the purpose of **personalised risk assessment** (e.g. on a one-off basis when approving a loan or on an ongoing basis in the case of black box schemes operated by insurance companies) are characterised by a higher level of granularity. This is ultimately a sector-specific use case for a certain profiling technique and the associated scoring procedures (→ see section 3.2.3 above and Part F, section 4.2.2 below for further details of profiling in general). The processing of additional personal data for the purpose of personalised risk assessments regularly requires consent from the data subjects. Individuals who hope to gain economic advantages as a result are particularly likely to grant such consent, yet the granting of consent by one individual may have significant impacts on others, and give rise to chain reactions that are problematic from an ethical viewpoint (unravelling effects). This may put data subjects under disproportionate pressure, and jeopardise the voluntary nature of consent.

Example 11

Insured parties who are healthy are particularly likely to consent to the processing of their data by a health insurance company. As a result, others come under pressure to also grant consent in order to avoid arousing any suspicions regarding their state of health.

In cases where individual behaviour can influence the parameters, models of this kind can also have a significant **influence on how people lead their lives**. Another ethical consideration that is particularly relevant in the insurance sector is that the goal of increasingly granular risk assessments runs counter to the **basic principle of collective risk sharing** by the community of all insured persons. Taken to its extreme (i.e. if the insurer has access to "comprehensive" information and adjusts the price to the individual risk), the whole concept of insurance would be reduced to absurdity.

The Data Ethics Commission therefore believes that personalised risk assessments must comply with the following ethical requirements in particular:

a) data processing must not intrude into **the core of an individual's private life**; it must be restricted to areas where the individual is already in contact with the exterior world and must therefore expect conclusions to be drawn on the basis of his or her behaviour. This principle dictates that it would be ethically acceptable for a car insurance company (for example) to record the miles driven or traffic offences committed by a driver, but not purely private behaviour inside his or her vehicle, even if this behaviour might be relevant from a risk perspective (e.g. how often he or she yawns, whether he or she chats to passengers), or even the driver's state of health (e.g. heart problems) or other lifestyle factors (e.g. purchasing behaviour in relation to coffee or alcohol);

b) a **clear causal relationship** must exist between the data being processed and the risk to be determined, and any linking of data must avoid **discriminatory** repercussions (→ see Part F, section 2.6 below for further details);

c) the data must not allow conclusions to be drawn directly that have **implications for relatives or other third parties**;

d) full **transparency** is required as regards the specific parameters and their weighting, and the impacts on pricing or other conditions; the individual must also be provided with clear and comprehensible explanations of how to improve these conditions (→ see Part F, section 2.7);

e) in order to keep unwanted chain reactions in check, the difference between the "optimal" conditions and the conditions that apply if consent is refused must not exceed a certain ceiling (e.g. **maximum price difference**).

In the view of the Data Ethics Commission, most of the problems arising in connection with **price differentiation in the narrow sense** and measures of a similar ilk relate to the regulation of algorithmic systems (→ see Part F for further details). At the same time, however, price differentiation morphs into a data use problem as soon as consumers are led to believe that they can access prices that are lower overall by disclosing as much personal data as possible or by exhibiting certain behaviours tailored to the relevant criteria (e.g. making online purchases using a computer manufactured by a certain company), or conversely if it is suggested that consumers who refuse to consent to the processing of their data for the purpose of personalised pricing will always pay **higher prices on average**. The Data Ethics Commission believes that the latter would also pose an ethically questionable risk to the voluntary nature of consent.

3.3.5 Data as reputational capital

When coupled with **personalised economic conditions** (personalised prices, personalised ranking and personalised products and services), personal data, profiles and scores serve as reputational capital. Personalised behavioural rewards aimed at increasing **customer loyalty** (e.g. the granting of discounts depending on the quantity purchased in the previous month) incentivise consumers to consent to the processing of their personal data, and may be apt to influence the way they lead their lives. No evidence that the ethical limits outlined above (→ section 3.3.4) are currently being disregarded in the German economy in connection with customer loyalty programmes has come to the attention of the Data Ethics Commission, but developments should continue to be monitored.

True reputational data that are also visible to external third parties (e.g. "stars" indicating that someone with a profile on an online platform is a good person to do business with) are gaining ever more economic and non-material significance. To a certain extent, reputational data of this kind are covered by the new **Regulation (EU) 2019/1150 on promoting fairness and transparency** for business users of online intermediation services.[13] The regulatory approach chosen by the lawmakers who drafted this Regulation – based for the most part on transparency requirements and self-regulation – was cautious, and the Data Ethics Commission welcomes this approach in principle. However, it is worth noting that certain sectors are heavily dependent on true reputational data, and that this factor in particular might lead to significant lock-in effects that may jeopardise competition and cause problems if individuals are unable to take their data with them when switching to a different online intermediary platform.

13 Cf. Article 9 of this Regulation on data access and many general provisions, e.g. on general terms and conditions of business and ranking.

Example 12
A micro entrepreneur who offers taxi services via an online platform has been ranked highly by many of his former passengers, and now wishes to switch platform and take these rankings with him.

The Data Ethics Commission is aware of the problems that would arise if a general obligation to recognise ranking profiles built up on a different platform were to be enshrined in law. However, it recommends that the Federal Government should examine the conditions under which commercial users with profiles of this kind might nevertheless be granted a **right to portability**, with a view to lobbying for broader regulation at European level.[14]

By way of contrast, the rise in significance of **social reputation data** (number of "likes", "followers" or "friends") is part of a wider trend in our society, and – with the limited exception of "influencers" – can no longer be viewed predominantly through the lens of personal data as an economic asset, but must instead be discussed in relation to its systemic societal implications.

3.3.6 Data as tradeable items

A significant number of companies are already deriving financial gain (and, in some cases, earning a great deal of money) by compiling personal data, profiles and scores or personalised statistical evaluations (carried out using aggregated raw data) and then reselling them to third parties, or by enriching existing profiles with estimated data and then placing them on the market. In the following section, business models of this kind will be referred to as **"data trading"**.

The GDPR does not currently contain any provisions relating specifically to data trading; instead, business models of this kind are categorised merely as normal data processing operations that are subject to the general provisions of the GDPR. In many cases, closer examination of the applicable provisions leads to the inescapable conclusion that certain types of data trading infringe the provisions of the GDPR, and are therefore contrary to the law. Generally speaking, however, the field of data trading is characterised by a **significant enforcement gap**. The Data Ethics Commission therefore believes that urgent action should be taken by the data protection authorities in relation to this sector, and that the European Data Protection Board (EDPB), or alternatively the Conference of Independent Data Protection Authorities of the Federal Government and the *Länder (Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder)*, should develop – in keeping with the GDPR's risk-based approach – clearly delimitable categories for different types of lawful data trading. Greater clarity is needed regarding the instances of data trading where the data subject must grant consent to the forwarding of data, the instances where the data subject has a right only to object to the processing of data, and the instances where compelling reasons rule out even the right to object.

Having regard to the general principles governing data processing (Article 5 GDPR), the forwarding of data to third parties should be permitted only within closely prescribed limits in situations that are not covered by the existing provisions of data protection law. The Data Ethics Commission therefore recommends that the Federal Government should speak out at European level – in connection with the forthcoming evaluation of the GDPR, for example – in favour of **expanding the scope of the GDPR to include specific provisions on data trading**. The following **ethical considerations**, some of which are already enshrined in the GDPR, should be taken into account when drafting future legal provisions of this kind:

14 Cf. for example Articles 6 and 7 of the draft "Model Rules on Online Intermediary Platforms" by the European Law Institute, which were made available to the Data Ethics Commission.

a) The individual's right to informational self-determination should be the starting point for any balancing exercise, meaning that data trading in principle requires prior **consent** by the data subject, with due regard for the **substantive limitations** on consent (→ sections 3.2.1 and 3.2.2 above).

b) If data are processed on a legal basis other than consent (which is likely to occur only in isolated cases), the individual must have a straightforward opportunity to exercise his or her **right to object** in advance (e. g. by unchecking a checkbox immediately before the data are collected), and must not be forced to communicate his or her objection via separate communication channels.

c) Data trading models that deprive data subjects of any **choices** whatsoever should only rarely be considered, and only if and to the extent that the data need to be forwarded in order to further public interests that manifestly outweigh the countervailing interests. Comprehensive legislative clarification of this category is required.

d) The GDPR contains detailed provisions on the transfer of data to processors and on the forwarding of data to third countries. Given the content and rationale of the GDPR, it would be illogical to assume that the requirements that apply to transfers of data to third parties within the EU should be any less stringent than those that apply to transfers outside the EU, and certain other points can also be inferred from the general provisions, e. g. that these requirements should be regarded as "appropriate safeguards". Nevertheless, the Data Ethics Commission recommends that urgent action be taken to clarify (explicitly and by law) the obligations that apply when transferring data to third parties, e. g. control obligations, as well as the circumstances under which parties may be held liable.

e) Controllers should be obliged to document and disclose the specific source of the data they have collected or generated by the use of algorithmic systems, as well as the identity of the individual recipients of the data; the information must be provided in a standardised and machine-readable format, which allows e. g. automated data management using a privacy management tool/personal information management system (→ see section 4.3 below for further details). This would take due account of the fact that **data subjects** have largely been **left in the dark** as regards the existence of data traders, which means that a simple list of the different categories of sources or recipients would be of little use to them.

f) Given the large number of data traders in the market, data subjects will be able to **exercise their rights effectively** only if central mechanisms are established that facilitate this process or assume responsibility for it (e. g. data protection authorities, → see section 3.2.4 above, or privacy management tools/personal information management systems, see section 4.3 for further details).

g) Given that dispersion effects give rise to higher risks and the potential for loss of control, data traders should be subject to a **certification obligation under data protection law** that includes regular audits by the certification bodies. The Data Ethics Commission recommends that specific certification criteria should be adopted as appropriate by the independent data protection authorities of the Federal Government and the *Länder*, and that these criteria should take due account of the risks and recommendations it has outlined.

3.4 Data and digital inheritance

Modern communication technologies and data processing capacities make it possible to record every last detail of an individual's private activities for decades on end, and to evaluate these recordings using automated systems. Handing the data collected about a deceased individual over to his or her heirs or another third party adds a **whole new dimension of privacy risk**, both for the deceased person and, in particular, for the individuals with whom he or she communicated during his or her lifetime. These data are often compared to diaries and personal correspondence, but this comparison is flawed because many channels of digital communication (messenger services, chats, e-mails, etc.) serve as a functional replacement for the ephemeral spoken word rather than for letters.

3.4.1 Precedence of living wills

The Data Ethics Commission believes that, in the best-case scenario, a data subject should make intentional and informed dispositions during his or her lifetime. In many cases, however, people neglect to make any such dispositions for the sole reason that they are unaware of the legal and practical options or put off by the level of uncertainty. Against this backdrop, the Data Ethics Commission believes that there are justified grounds for **obliging service providers** to alert users to the option of making dispositions that provide for ongoing incapacity to provide consent (e.g. due to dementia) or for death, and to provide the technical means for making said dispositions, with the minimum of barriers (i.e. with the fewest possible changes of medium). Corresponding provisions could be added to the **[German] Telemedia Act (*Telemediengesetz*, TMG)**.[15]

In the view of the Data Ethics Commission, the situation following a data subject's death is merely an extreme example that should serve as a prompt for further reflection on the general design of digital modes of communication. The Data Ethics Commission therefore recommends that the Federal Government should examine the possibility of making it obligatory for messenger services to offer a **default option of erasing messages** after a certain period of time; if a user chose this option, a message would automatically be erased after expiry of the relevant period unless it had been manually archived by the recipient or the sender.

3.4.2 The role of intermediaries

Growing awareness of the topic of digital inheritance has allowed new business models to flourish, and a large number of companies are now offering services in this field (ranging from the central storage of account data and passwords through to comprehensive digital inheritance management). These services may provide useful guidance, but they are also associated with certain hazards, including inadequate provision for cases in which a company goes bankrupt or is otherwise liquidated, and shortcomings in information security (up to and including genuine fraud). The Data Ethics Commission believes that **quality assurance**, new **regulations** (characterised by a cautious approach) and **public awareness-raising** about the potential advantages and risks are required in order to protect citizens.

15 For a previous discussion of this topic, see Mario Martini, Juristenzeitung (JZ), 2012, p. 1154.

In addition, it recommends that the Federal Government, as part of its remit to provide services of general interest to the public, should set up a body that is (at the very least) subject to **state supervision** and that provides affordable basic digital inheritance protection and planning services to citizens; these services must reflect the latest developments in the field of information security technology. When a German citizen writes a will, he or she can choose to store it privately or with a notary or district court, and similar options (private or private-sector solutions or a government-run service) should also be available for an individual's digital inheritance.

3.4.3 Post-mortem data protection

The Data Ethics Commission does not recommend a wholesale rejection of the principles set forth by the German Federal Court of Justice[16] regarding the **transfer of estates to heirs**, since the potential advantages would be far outweighed by the effects (either undesirable and/or excessive) of a different default solution, e.g. a trust model imposed by law or a distinction between user account content that is regarded as an asset and content from the same user account that is regarded as highly personal. Conversely, inheritance law should not apply at all if the nature of a user account (e.g. an online account with an Alcoholics Anonymous group) renders all of the data within it financially worthless but highly sensitive. In cases where the **principle of telecommunications confidentiality** applies, *inter alia* to protect the deceased's communication partners, the legislator will, in any case, still have to reconcile this with the right to inheritance (which is enshrined as a fundamental right), for example through a corresponding reference in the part of the Civil Code devoted to inheritance law.

The principle set forth by the Federal Court of Justice – that an estate should be transferred to the deceased's heirs – is linked to the existence of a contractual relationship. If there is no contractual relationship, or if a transfer to the heirs cannot take place owing to the highly sensitive nature of the data, the heirs will have no right of legal recourse. Since **post-mortem data protection** is not provided by the GDPR, there are also no means of legal recourse for relatives under the current state of data protection law. Ethical concerns are raised by the fact that controllers have almost unlimited power to dispose of a deceased's personal data as a result, and the Data Ethics Commission therefore recommends that the Federal Government should follow in the footsteps of several other EU Member States and make use of the option provided by Recital 27 of the GDPR, by enacting provisions on **post-mortem data protection**. Even after the death of a data subject, the latter's relatives should be able to exercise his or her fundamental rights, such as the right to erasure and the right to rectification of incorrect data. At the same time, suitable measures should be taken to ensure compliance with dispositions made by the deceased during his or her lifetime, even if these dispositions are only implied (e.g. through a deliberate choice to publish a "life story").

16 Judgment by the German Federal Court of Justice of 12 July 2018, ref. III ZR 183/17.

3.5 Special groups of data subjects

3.5.1 Employees

The fact that employers collect employees' location data and performance data, which is a widespread phenomenon in certain modern workplaces, poses a significant risk to these employees' **right to informational self-determination and general rights of personality**; the same is true of the creation of biometric profiles which is a necessary precursor to certain forms of collaboration. Questions to be considered include not only the legal basis for data processing and for the granting of co-determination rights to employee representation bodies, but also obligations to provide employees with information (e. g. on the hazards posed by multi-sensor fusion) and, depending on the context, with opportunities to object, issues regarding data retention procedures, terms of data retention and the extent to which employees' data may be disclosed to third parties, the right to rectification of incorrect or obsolete data (in personal profiles, for example) and appropriate erasure procedures. Further points for consideration include framework conditions for (limited) control and surveillance of employees, restrictions on the tracking of employees' locations and a ban on comprehensive location profiles, restrictions on any obligation to share social media accounts or to allow an employer to access data in the context of "bring your own device" models, framework conditions for the use of biometric systems, and restrictions on psychological investigation methods.

The Data Ethics Commission recommends that the Federal Government should invite the social partners to work towards a common position on the legislative provisions that should be adopted with a view to **stepping up the protection of employee data**, based on examples of best practices from existing collective agreements. The concerns of individuals in non-standard forms of employment should also be taken into account during this process, and collective agreements and works council agreements should continue to play a significant part in employee data protection. Yet the foundational principles of employee data protection should not be regulated solely by collective agreements and works council agreements, firstly because not all employees are covered by these latter, and secondly because of the importance of these principles from a fundamental rights perspective. It is also worth noting that the legal uncertainty currently reigning over the scope of the GDPR provisions is having a negative impact on investment security.

With reference to the wider field of legal bases for the processing of employee data, the Data Ethics Commission believes that the traditional construct of **consent** under data protection law is not suitable in all contexts, since it is difficult to put in place the framework conditions necessary for consent to be given voluntarily in all employment situations, and impossible to find an appropriate balance in all cases between the employer's needs and the option for employees to revoke consent and request the erasure of data at any time. Employee data protection measures should therefore focus on **legal grounds of justification** that are specifically tailored to the employment context, and that guarantee a high level of protection and an appropriate weighing up of interests against fundamental rights. The outcomes may look very similar to consent in certain respects, while taking into account the power structures that typically exist in an employment context.

When deciding whether **interest groups should be granted co-determination rights**[17] in relation to the processing of data within companies, due regard must be given to the **asymmetry of knowledge** that exists between employers and employees as regards the operating principles and details of these data processing operations. There is a need for models that go further than the existing mechanisms by allowing interest groups to access external expertise, while at the same time ensuring not only the appropriate involvement of the company data protection officer, but also the protection of trade secrets. Given the constant advancement of data-processing systems within companies (software updates, self-learning elements, etc.), there should be a shift away from consent as a single, one-off event and towards **ongoing oversight of processes** by interest groups.

Progress in the field of employee data protection should not neglect the stages of **applying** for a job and **entering into an employment relationship**. For example, care must be taken to ensure that the provisions of applicable law that prohibit employers from asking certain questions during the application procedure or when recruiting an individual (e.g. asking whether a woman is pregnant) are not circumvented through the use of "human resources" algorithms or through a request to grant the employer access to social media accounts.

Steps must also be taken to ensure that persons in **non-standard forms of employment** are not excluded from progress in the field of employee data protection. The upsurge in these forms of employment in the platform economy means that many people no longer have access to the traditional employee rights and rights of co-determination. The imbalance of power that arises between the client or the platform operator on the one hand and the contractors or the platform workers on the other is often significant and may have implications in terms of data protection and informational self-determination. Appropriate legislative provisions should be adopted (ideally at EU level) and the institutional framework developed further (e.g. through an interest group) to mitigate against this risk.

3.5.2 Patients

In view of the benefits that could be gained from **digitalising healthcare**, as a basic principle the Data Ethics Commission recommends **swift expansion of digital infrastructures** in this sector and the introduction of **procedures for reviewing and assessing digital healthcare services**. Both the range and the quality of digitalised healthcare services should be improved to allow patients to exercise their rights to informational self-determination and become more health literate.[18]

Even as things stand today, the provision of healthcare services involves the processing of huge volumes of personal data. The data involved are typically health data and genetic data, or in other words special categories of personal data within the meaning of Article 9 GDPR. When designing a future health landscape that will be primarily digital in nature, comprehensive account must be taken of the need to provide **special protection for these data** at the same time as boosting the **right to self-determination** of patients and those with health insurance policies, *inter alia* in the field of research (→ see section 4.1 below).

17 For examples of current legislative provisions, see e.g. Section 87 (1) (6) of the [German] Works Constitution Act (*Betriebsverfassungsgesetz*, BetrVG) (in relation to works councils), or Section 75 (3) (17) of the [German] Federal Staff Representation Act (*Bundespersonalvertretungsgesetz*, BPersVG) (in relation to staff councils).

18 German Ethics Council (*Deutscher Ethikrat*), Big Data and Health, Opinion, 30 November 2017 (available at: *https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/englisch/opinion-big-data-and-health-summary.pdf*).

In this connection, the Data Ethics Commission emphasises the urgent need to introduce and roll out an **electronic health record** with a view to improving the quality, transparency and cost-effectiveness of medical care.[19] Given the vital role that an electronic health record would play in digitalising the healthcare sector, the Data Ethics Commission wishes to make it clear that greater attention should be paid to both information security and patient autonomy while implementing this system; the existing cryptosecurity concept (based on the decentralised management of keys (PINs) for insured parties) should continue to apply, for example. It should also be possible to use the electronic health record even if a patient is incapable of granting consent, based on the provisions concerning legal representation that otherwise apply and regardless of the type of health insurance policy held by the patient.

Digital health services and products that are not collectively financed **(consumer-funded health market)** are becoming ever more important, not least because the digital healthcare services offered by the statutory health insurance funds have been few and far between to date. It is important not to underestimate the relevance of these services – which include not only fitness, health and wellness apps, but in particular digital **self-monitoring** apps and the associated wearables – in the context of a digitalised healthcare sector. Yet these apps are often of questionable (and poorly verified) quality, meaning that the data they collect are of limited usefulness; this carries a risk to the health of the affected patients and users, which can, in some cases, be significant. It should furthermore not be assumed that patients are able to assess the quality of these products and services independently, in particular their compliance with the principles of data protection and information security; equally, access to digital healthcare services should not be dependent on individual financial wherewithal. With this in mind, the Data Ethics Commission welcomes the plans for the Federal Institute for Drugs and Medical Devices *(Bundesinstitut für Arzneimittel und Medizinprodukte)* to introduce a procedure for examining and assessing apps of this kind.

3.5.3 Minors

The Data Ethics Commission welcomes the efforts which have been undertaken – and which include both the adoption of legislation and voluntary self-regulation – to develop special **protective mechanisms** allowing minors to exercise their right to digital self-determination. The primary goal of these mechanisms should be to step up the level of data protection and the degree of protection against profiling, manipulation through dark patterns and addictive designs, etc.; their secondary goal should be to provide greater protection against content that is not age-appropriate (that glorifies violence, for example).

At the same time, however, the Data Ethics Commission wishes to make it clear that all such protective mechanisms will prove futile unless a reliable **identity management system** is in place, ensuring that the age of minors is detected and that they are treated appropriately. Relying on users to be honest about their age is without question the wrong approach. When viewed through the lens of ethics, however, it would also be problematic to ask providers to ascertain a user's age themselves by collecting personal data, some of which may be highly sensitive (e.g. facial recognition, with data transferred to the provider's cloud); at the same time, placing the entire burden on whoever holds parental authority may easily result in a situation where the latter feels that too much is being asked of him or her. The Data Ethics Commission therefore recommends that the Federal Government should promote the emergence of **family-friendly technologies** that allow minors to exercise their right to self-determined development while, at the same time, reliably guaranteeing their protection.

19 See in this respect the Data Ethics Commission's previous recommendation on participatory development of an electronic health record, dated 28 November 2018 (available at: *www.datenethikkommission.de*).

The Data Ethics Commission recommends that the Federal Government should lobby at European level for measures to enforce compliance with the principles of **data protection by design and by default** as enshrined in the GDPR, particularly in the case of mobile end devices, in order to protect the right to informational self-determination of minors and protect their privacy. The German and European data protection authorities, the competition authorities, the media regulators and the technical regulatory authorities should take action within their relevant remits and spheres of responsibility to force the manufacturers of operating systems for mobile end devices and the providers of digital services to adhere to all of the legislative requirements that apply to the age groups in question and to block services that are not age-appropriate. The parties responsible for procuring relevant systems with a view to their use in schools and kindergartens should also incorporate these requirements into the tendering procedures. A more detailed discussion of the need to force manufacturers to comply with the principle of data protection by design and by default can be found below (→ section 3.6.1).

As far as further action in this area is concerned, consideration should also be given to the introduction of an EU-wide obligation that forces manufacturers of child-friendly mobile end devices to program them from the outset as devices that are specifically intended for children, and to ensure that "jail breaking" or "rooting" is impossible (or possible only with a key). The devices programmed in this way should enforce compliance with all of the legislative provisions aimed at protecting children, and block services that are not age-appropriate. **If the relevant settings are enabled** on the device/operating system upon activation, minors should not be able to change these settings without their parents' consent. A solution of this kind would also offer clear advantages over parental control apps, firstly because these apps often pose data protection and information security problems in their own right, and secondly because they raise ethical questions in terms of the opportunities they afford for the total surveillance of private life.

3.5.4 Other vulnerable and care-dependent persons

In many cases, data belonging to vulnerable individuals are processed for the benefit of these individuals, e.g. in the care sector. Digital technologies can make it much safer for older people to remain in the environment to which they are accustomed, for example, and they may also help to alleviate some of the negative impacts of the skills shortage in the care sector and ensure better healthcare provision. In particular, **digital assistance systems** – when used correctly – can serve as a bridging technology, and adjust adaptively to the varying needs of different people.

The right to life, the right to bodily integrity and also the right to informational self-determination are fundamental rights that must be reconciled with each other in accordance with the principle of practical concordance. Particular consideration must be given to two questions in particular: whether **risks are posed to life or health**, and the extent to which the right to informational **self-determination** is encroached upon.

The Data Ethics Commission believes that **standards and guidelines** on surveillance by professionals in the care sector should be developed by the Conference of Independent Data Protection Authorities of the Federal Government and the *Länder*. In particular, these standards and guidelines should specify the legal provisions upon which the professionals can base their action in particular situations, and the cases in which (especially if **consent** has not been granted by the data subject or his or her caregiver) surveillance is either prohibited or possible on the basis of Article 6(1)(f) or (d) GDPR. They should also outline arrangements for the provision of information, whereby the Data Ethics Commission takes the position that differentiated information on digital surveillance options should be provided prior to their use in an institutional setting (e.g. care home, kindergarten or school), and that consent must also be obtained on a differentiated basis in cases where there is no legal basis for data processing. Standards and guidelines of this kind would also be an appropriate way both to provide more legal certainty for care home operators and care staff and to reduce liability risks. Section 1901a of the Civil Code should be amended accordingly to clarify the fact that **living wills** can also include dispositions in which the relevant data subject grants prior consent to the processing of data.

As a basic principle, a particularly high level of protection should also be accorded to people in their own homes, since they are likely to regard the space within their four walls as a safe haven of privacy. Once again, new technologies have opened up new and expanding **options for the surveillance of private individuals by other private individuals** (e.g. the surveillance of romantic partners, children or persons with disabilities), which range all the way through to the ethically alarming prospect of total private surveillance. Given that awareness of this topic is lacking in many quarters, the Data Ethics Commission recommends that **awareness-raising campaigns** in this area should be initiated both by the Federal Government and by the governments of the *Länder*, since the latter often hold jurisdiction in this field. Although it recommends that the Federal Government should continue monitoring developments, it does not believe that legislative measures (e.g. new criminal offences) are required at present.

3.6 Data protection by technical design

Citizens, companies, government agencies or other parties that are entitled to assert ethically justified data rights and that are obliged to comply with the corresponding data obligations must be in a position to do so in the first place. The necessary **technical framework** must be put in place, and enabling technologies must play a prominent role in this respect. Yet enabling technologies of this kind must not lead to a situation in which responsibility for the protection of fundamental rights and freedoms is offloaded onto individual users. Instead, the State must, as a matter of principle, adopt the **regulations** that are required to provide reliable protection for these fundamental rights and freedoms, without the need for action on the part of individuals.

3.6.1 Privacy-friendly design of products and services

As its heading suggests, Article 25 GDPR makes it mandatory for controllers to comply with the principles of **"data protection by design and by default"**. Designers of new technologies must therefore take due account of concerns relating to data protection (based on the interpretation of the term applied in Article 5 GDPR), while following a risk-adequate approach. The technical and organisational measures that must be implemented to this end may be required prior to processing (i.e. when the controller determines the means by which the data will be processed) as well as during the processing operation itself.

Data protection by design and by default

Data protection by design imposes conditions on the selection of technical and organisational measures (relating to the state of the art, implementation costs, processing and the risk posed to the rights and freedoms of natural persons, for example). **Data protection by default** imposes no such conditions, since this principle must be adhered to without exceptions. In practice, however, it is often the case that excessive amounts of personal data (e. g. identifiers) are processed, that inadequate restrictions are placed on processing, that retention periods are too long and that an inappropriately high number of people are able to access the data.

The field of **"privacy engineering"** has therefore emerged under the banner of additional protection-related goals such as non-linkability, transparency and intervenability; the standard data protection model (SDM) used by the German data protection authorities now incorporates these goals as "warranty objectives".[1] Like the IT Baseline Protection Catalogues published by the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, BSI), the SDM defines modules that can be used by controllers and designers of new technologies as a basis for choosing technical and organisational measures that are appropriate to their protection needs. Although only the first few modules are currently available, others are planned. The fact that many developers use the IT Baseline Protection Catalogues and the ISO 2700x series of standards as reference works means that these developers are familiar with the fundamental concept and able to take better account of the legal requirements when designing and implementing technical systems.

The choice between **centralisation and decentralisation** is another question that must be clarified on a case-by-case basis when designing technical systems. As a general rule, centralised systems allow operators to exercise a higher level of control and influence. This might be a good thing, for example if the underlying aim is to incorporate features that contribute to data protection or information security. Yet it can also be a bad thing, since the potential for misuse – either by malicious third parties wanting to steal data or sabotage data processing, or by the operators themselves exploiting the large volumes of data they have amassed for purposes other than those notified to the data subjects – is greater if data are stored centrally and the processing of these data is also controlled centrally. When designed appropriately, however, decentralised systems can help to decrease or prevent data linkability, and reduce disruptions to overall system availability.

1 Technology Working Group of the Conference of Independent Data Protection Authorities of the Federal Government and the *Länder*: Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele V.1.1 – Erprobungsfassung [The standard data protection model – a method for data protection consulting and assessment on the basis of uniform warranty objectives, V.1.1 – test version], 2018 (available at *https://www.datenschutzzentrum.de/sdm/*).

The design specifications of data protection law have a high level of practical relevance in relation to **end devices**. Some end devices are designed to be worn on the body (wearables, e. g. a smartwatch or smart textiles) or at least carried close to the body (e. g. a smartphone), while others are designed to be mobile by other means (e. g. a networked car) or immobile (e. g. smart home facilities). When designing software systems for end devices of this kind, the amount of time that should be spent reflecting on the ethical questions they raise depends on the likelihood that they will be used in close proximity to the body or in private and intimate spheres (e. g. bathrooms and bedrooms), on the probability that their use will affect particularly vulnerable persons (e. g.

children and young people, care-dependent persons, persons with disabilities), and on the extent to which they encroach upon an individual's personality. The high level of responsibility (or autonomy) granted to or demanded from the users who assemble, configure and operate these devices represents a particular challenge when attempting to design technologies that foster self-determination.

The Data Ethics Commission recommends that the Federal Government should step up its support for R&D efforts on **technical standards** for end devices. It also urges the Federal Government to lobby at European level for the introduction of **technical requirements** aimed at safeguarding self-determination and product safety in the private sphere, with particular reference to **end devices for consumers**. The Data Ethics Commission takes the view that the following principles should, as a minimum, be enshrined in any end device requirements that are adopted:

- Products must be protected against **cyber attacks and improper use** of data; the measures taken must be commensurate with the need for protection and comply with the state of the art, and suitable guarantees must be provided in particular for sensitive data (e.g. health data). A high level of cyber resilience must be achieved, and this is a joint task incumbent upon the State, industry and each individual.

- Users must be able at all times to identify the **functions that are currently enabled**; in particular, they must be able to see whether the camera, microphone, GPS or other sensors are switched on, whether the device is connected to the Internet, and whether their data are being transferred outside a closed local area.

- It must be easy to turn off **data transfers**, including transfers outside the local area, and data that are stored locally after this function is switched off must not be transferred without the user's consent when it is next switched on (and the same must also be true for individual applications, e.g. on smartphones or smart TVs).

- If **basic device functions** are technically possible **without data transfers of this kind**, the functions must remain available when data transfers are turned off (e.g. a smart fridge must continue to keep its contents cool).

- Devices should be supplied with **"user onboarding"** software; onboarding should take place automatically when the devices are first put into operation, and it should be possible to repeat the onboarding process as often as necessary, even for second users. The information provided to users should cover not only the mode of operation, but also the collection and further processing of user data.

- If end devices have a direct connection to the Internet (e.g. routers) and are secured using a password, it should not be possible to put them into operation without changing the factory password beforehand. On the system side, **passwords** should be allowed only if they comply with the state of the art.

Comprehensibility and transparency

Data protection by design also encompasses the comprehensibility and transparency of systems, including the applications, scripts, sources and elements for each point in time during the development procedure and the process itself. The Data Ethics Commission welcomes the ongoing efforts to develop best-practice models for good terms and conditions of business and "one-pagers" for consumers. As part of a multi-level approach, consumers should initially be provided with simple and "boiled-down" information on the most important data processing operations; if necessary, they should then be informed in detail about the general terms and conditions of business and data protection measures. On its own, however, this approach will not solve the underlying problem, which is that the information provided often fails to do its job, either because it is inadequate and/or because it exceeds the consumer's capabilities.

So that consumers can make informed purchase decisions, standardised, machine-readable and readily understandable graphical symbols **(icons)** should be introduced at European level, following broad consultations with industry and civil society. These icons should convey the key digital characteristics of products (including digital products such as apps) and services; "Basic functions available only with Internet connection", "Internet connection required for enhanced functions", "User data transfers" and "User tracking" are examples of possible characteristics. The icons could also be **colour coded**, which would be particularly useful in the case of product characteristics that apply to a greater or lesser degree. The Data Ethics Commission recommends that the Federal Government should lobby the European Commission to develop standardised icons of this kind, in keeping with Article 12(8) GDPR.

Increased transparency for consumers could also be achieved by supporting the development of certified **electronic shopping assistants**, which would identify a product in a brick-and-mortar or online shop and then serve up product information to the consumer in a format that he or she is likely to understand.

The way in which products, services and applications are designed has a huge influence on the extent to which controllers and processors are able to comply with the data protection obligations incumbent upon them, and yet manufacturers that are not directly responsible for processing personal data fall outside the scope of the GDPR. Controllers that cannot or do not want to use solutions they have developed themselves must therefore insist on "baked-in" data protection.[20] With this in mind, the Data Ethics Commission recommends that the Federal Government should either take steps itself or support action by other parties with the aim of **forcing manufacturers to shoulder a greater share of the responsibility**. Suitable measures might include the following:

- direct imposition by the legislator of **product design and product safety requirements**;
- new and **effective legal remedies** along the distribution chain that can be used to shift the burden of responsibility for inadequate data protection by design and by default onto manufacturers[21] (whereby a certain amount of progress has been made in the new Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods in terms of shifting the burden of responsibility from consumers onto retailers and along the distribution chain);

20 Cf. Recital 78 of the GDPR.

21 Christiane Wendehorst: Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge, Teil 2: Wissenschaftliches Rechtsgutachten [Consumer-oriented problems relating to possession and ownership structures in the Internet of Things, Part 2: Scientific legal opinion], Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen [Studies and opinions on behalf of the Advisory Council for Consumer Affairs], December 2016, p. 120 (available at: *http://www.svr-verbraucherfragen.de/wp-content/uploads/Wendehorst-Gutachten.pdf*).

- **calls for tenders** and guidelines for **public procurement measures** that are designed in such a way as to require evidence of all-round compliance with the GDPR, including the principles of data protection by design and by default;

- **incentives** that encourage compliance with particularly high standards of data protection by design and by default, for example requirements to this effect in government funding programmes.

3.6.2 Privacy-friendly product development

The importance of data protection by technical design must also be taken into account at the product development and enhancement stages. This applies, in particular, to the **development of algorithmic systems**, since these latter typically require data in bulk, for example to use as training data (→ see Part C, section 2.2 for further details).

Privacy-friendly training of algorithmic systems

Various options are available for complying with the principles of data protection enshrined in Article 5 GDPR while training algorithmic systems. In January 2018, for example, Datatilsynet (the Norwegian data protection authority) proposed privacy-friendly means and methods for the training of algorithmic systems:[1]

8. use of **data minimisation procedures** in relation to training data, e. g. through the use of synthetic data (using generative adversarial networks, for example), through federated learning or through the use of data-minimising variants such as those proposed for neural networks;
9. use of **encryption procedures** such as differential privacy, homomorphic encryption or other procedures that allow the retrieval of information without granting full access to the database;
10. use of **procedures that promote transparency** to achieve a higher level of comprehensibility and traceability.

The Data Ethics Commission believes that **research is still needed** in all of these areas, and this also applies to options for the privacy-friendly testing of algorithmic systems.

1 Datatilsynet: Artificial intelligence and privacy, Report, January 2018, pp. 27 et seq. (available at: *https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf*).

Summary of the most important recommendations for action

Standards for the use of personal data

1

The Data Ethics Commission recommends that **measures be taken against ethically indefensible uses of data**. Examples of these uses include total surveillance, profiling that poses a threat to personal integrity, the targeted exploitation of vulnerabilities, addictive designs and dark patterns, methods of influencing political elections that are incompatible with the principle of democracy, vendor lock-in and systematic consumer detriment, and many practices that involve trading in personal data.

2

Data protection law as well as other branches of the legal system (including general private law and unfair commercial practices law) already provide for a range of instruments that can be used to prevent such ethically indefensible uses of data. However, in spite of the widespread impact and enormous potential for harm, too little has been done to date in terms of harnessing the power of these instruments, particularly against the market giants. The various factors contributing to this **enforcement gap** must be tackled systematically.

3

As well as steps to make front-line players (e.g. supervisory authorities) more aware of the existing options, there is an urgent need for the **legislative framework in force to be fleshed out more clearly and strengthened in certain areas**. Examples of recommended measures include the blacklisting of data-specific unfair contract terms, the fleshing out of data-specific contractual duties of a fiduciary nature, new data-specific torts, the blacklisting of certain data-specific unfair commercial practices and the introduction of a much more detailed legislative framework for profiling, scoring and data trading.

4

In order to allow supervisory authorities to take action more effectively, these authorities need significantly better human and material resources. Attempts should be made to strengthen and formalise cooperation between the different data protection authorities in Germany, thereby ensuring the uniform and coherent application of data protection law. If these attempts fail, consideration should be given to the **centralisation of market-related supervisory activities** within a federal-level authority that is granted a broad mandate and that cooperates closely with other specialist supervisory authorities. The authorities at *Land* level should remain responsible for supervisory activities relating to the public sector, however.

5

The Data Ethics Commission believes that **"data ownership"** (i. e. exclusive rights in data modelled on the ownership of tangible assets or on intellectual property) would not solve any of the problems we are currently facing, but would create new problems instead, and **recommends refraining from their recognition**. It also advises against granting to data subjects copyright-like rights of economic exploitation in respect of their personal data (which might then be managed by collective societies).

6

The Data Ethics Commission also argues that **data should not be referred to as "counter-performance"** provided in exchange for a service, even though the term sums up the issue in a nutshell and has helped to raise awareness among the general public. Regardless of the position that data protection authorities and the European Court of Justice will ultimately take with regard to the prohibition under the GDPR of "tying" or "bundling" consent with the provision of a service, the Data Ethics Commission believes that consumers must be offered **reasonable alternatives** to releasing their data for commercial use (e. g. appropriately designed **pay options**).

7

Stringent requirements and limitations should be imposed on the use of data for **personalised risk assessment** (e. g. the "black box" premiums in certain insurance schemes). In particular, the processing of data may not intrude on intimate areas of private life, there must be a clear causal relationship between the data and the risk, and the difference between individual prices charged on the basis of personalised and non-personalised risk assessments should not exceed certain percentages (to be determined). There should also be stringent requirements in respect of transparency, non-discrimination and the protection of third parties.

8

The Data Ethics Commission advises the Federal Government not to consider the issues falling under the heading of **"digital inheritance"** as having been settled by the Federal Court of Justice's 2018 ruling. The ephemeral spoken word is being replaced in many situations by digital communications that are recorded more or less in their entirety, and the possibility that these records will be handed over to a deceased's heirs adds a whole new dimension of privacy risk. A range of mitigating measures should be taken, including the imposition of new obligations on service providers, quality assurance standards for digital estate planning services and national regulations on post-mortem data protection.

9

The Data Ethics Commission recommends that the Federal Government should invite the social partners to work towards a common position on the legislative provisions that should be adopted with a view to **stepping up the protection of employee data**, based on examples of best practices from existing collective agreements. The concerns of individuals in non-standard forms of employment should also be taken into account during this process.

10

In view of the benefits that could be gained from **digitalising healthcare**, the Data Ethics Commission recommends swift expansion of digital infrastructures in this sector. The expansion of both the range and the quality of digitalised healthcare services should include measures to better allow patients to exercise their rights to informational self-determination. Measures that could be taken in this respect include the introduction and roll-out of an electronic health record, building on a participatory process that involves the relevant stakeholders, and the further development of procedures for reviewing and assessing digital medical apps in the insurer-funded and consumer-funded health markets.

11

The Data Ethics Commission calls for action against the significant enforcement gap that exists with regard to statutory **protection of children and young people** in the digital sphere. Particular attention should be paid to the development and mandatory provision of technologies (including effective identity management) and default settings that not only guarantee reliable protection of children and young people but that are also family-friendly, i. e. that neither demand too much of parents or guardians nor allow or even encourage excessive surveillance in the home environment.

12

Standards and guidelines on the handling of the personal data of **vulnerable and care-dependent persons** should be introduced to provide greater legal certainty for professionals in the care sector. At the same time, consideration should be given to clarifying in the relevant legal provisions on living wills that these may also include dispositions with regard to the future processing of personal data as far as such processing will require the care-dependent person's consent (e. g. for dementia patients who will not be in a position to provide legally valid consent).

13

The Data Ethics Commission believes that a number of binding requirements should be introduced to ensure the **privacy-friendly design of products and services**, so that the principles of privacy by design and privacy by default (which the GDPR imposes on controllers) will already be put into practice upstream, by manufacturers and service providers themselves. Such requirements would be particularly important with regard to consumer equipment. In this context, standardised icons should also be introduced so that consumers are able to take informed purchase decisions.

14

Action must also be taken at a number of different levels to provide manufacturers with adequate **incentives to implement features of privacy-friendly design**. This includes effective legal remedies that can be pursued against parties along the entire distribution chain to ensure that also manufacturers can be held accountable for inadequate application of the principles of privacy by design and privacy by default. Consideration should also be given, in particular, to requirements built into tender specifications, procurement guidelines for public bodies and conditions for funding programmes. The same applies to **privacy-friendly product development**, including the training of algorithmic systems.

15

While debates on data protection tend (quite rightly) to centre around natural persons, it is important not to ignore the fact that **companies and legal persons must also be granted protection**. The almost limitless ability to pool together individual pieces of data can be used as a means of obtaining a comprehensive picture of a company's internal operating procedures, and this information can be passed on to competitors, negotiating partners, parties interested in a takeover bid and so on. This poses a variety of threats – *inter alia* to the digital sovereignty of both Germany and Europe – in view of the significant volumes of data that flow to third countries. Many of the Data Ethics Commission's recommendations for action therefore also apply on a *mutatis mutandis* basis to the data of legal persons. The Data Ethics Commission believes that action must be taken by the Federal Government to **step up the level of data-related protection afforded to companies**.

4. Improving controlled access to personal data

All types of data (both personal and non-personal) represent a **key resource** within the data economy and serve as a vital ingredient in many applications that foster the public good. The breakneck speed of development of digital technologies – some of which benefit each and every one of us enormously – can be attributed in part to the ability to evaluate data generated by billions of users. Although data protection must always remain the central priority for applications involving personal data, more and more people are asking whether general improvements in the area of controlled access to personal data might be ethically tenable or even desirable, in keeping with the principle of data use and data sharing for the public good (→ section 1.3 above) and within the framework prescribed by data protection law.

4.1 Enabling research that uses personal data

4.1.1 Preliminary considerations

Research serves as the basis for almost all our technical achievements, and the current onslaught of digitalisation means that data-based research is becoming **increasingly important**. Its significance has already been recognised by the GDPR, backed up in certain cases by national law (i.e. the [German] Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG) and the data protection acts of the *Länder*). The Data Ethics Commission wishes to emphasise the fact that data processing operations involving genetic, biometric and other **health data** are of enormous value in terms of furthering research goals, promoting preventive methods and developing new diagnostic and therapeutic approaches. The use of artificial intelligence holds the promise of significant progress in certain areas, but – depending on the problem being tackled – may rely on large pools of data. The issue of releasing health data for research purposes (referred to as **"data donation"**) is a recurrent topic of debate. This term "data donation" is **misleading**, however, because data that have been donated – unlike organs or money – can be reused as often as necessary and in parallel, even by the data donor himself or herself.

Provided that the research can, for the most part, be described as a public-good activity in terms of the way that it uses data (e.g. for providing healthcare services, developing sustainable mobility concepts or improving living conditions in the broader sense), the Data Ethics Commission recommends that full use should be made of the existing **privileges under data protection law**, and that research should be viewed as a particularly valuable good when weighing it up against competing interests.[22] It additionally recommends that the *Länder* should exercise the regulatory powers they already hold (for example in the area of higher education law or within the framework of data protection law) in such a way as to foster innovation and in keeping with the aforementioned notion of special privileges for research. A broad interpretation should be placed on the term "scientific research" in this context, *inter alia* with reference to consistent past decisions by the Federal Constitutional Court, and it should be irrelevant whether the research in question is being carried out by government-funded or private institutions.

The Data Ethics Commission wishes to point out that – challenging though the task may be – an **appropriate balance** must be sought between the researchers' fundamental rights and the data subjects' right to informational self-determination. When carrying out the weighing up of interests required by law, special priority should be accorded to the **protection of sensitive data** and the associated rights of data subjects such as patients and insured parties. For example, the duty of confidentiality imposed on certain individuals (such as doctors) who are subject to a code of professional secrecy (cf. Section 203 of the [German] Criminal Code (*Strafgesetzbuch*, StGB)) may also apply to the work of research institutions if these latter use data collected or stored by the individuals in question. The procedural precautions imposed by law with a view to protecting the right to informational self-determination would then need to be observed.

22 Cf. Conference of the Independent Data Protection Authorities of the Federal Government and the *Länder*: Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien [Guidance by the supervisory authorities for telemedia providers], March 2019, p. 14 (available at: *https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf*).

4.1.2 Legal clarity and certainty

Although the law as it currently stands permits and promotes data-based research, **questions of interpretation** arise in relation to certain details, and these questions require further clarification by the supervisory authorities and courts. For example, it has yet to be definitively clarified whether the **further processing** of data that have already been lawfully collected for one purpose (e.g. healthcare provision) can – on the basis of Article 5(1)(b) GDPR and, in the light of Recital 50, with "appropriate safeguards" within the meaning of Article 89 GDPR – automatically be deemed lawful if they are processed for research purposes, or whether the requirement for a separate legal basis pursuant to Article 6(1)–(3) or Article 9 GDPR applies just as it did when the data were first collected (for example, Section 27 of the Federal Data Protection Act states that health-related data can be processed only if express consent has been provided or if the research interests "substantially outweigh" the data subject's interests). It has also been suggested in certain quarters that the right to process the data further can only be invoked by the party that collected the data in the first place; similar uncertainty reigns over the scope of the term "research" as regards **product development and enhancement**.

Even though a legal framework exists for data-based research in Germany, *inter alia* in relation to health-related data and other special categories of data, the finer details of this regulatory framework lack uniformity, if only because the country's federal structure means that both the Federal Government and the *Länder* hold constitutionally enshrined legislative powers. From a research perspective, the resulting **legal uncertainty** is exacerbated yet further by an ongoing lack of reliable guidance, in particular as regards the criteria that must be met in order for consent to be deemed valid and in order for the data subject's interests to be "substantially outweighed" by research interests within the meaning of Section 27 of the Federal Data Protection Act. This legal uncertainty could prove a stumbling block for data-based research in Germany. The Data Ethics Commission believes that **recommendations for action and interpretative criteria** should therefore be developed – perhaps by the Conference of Independent Data Protection Authorities of the Federal Government and the *Länder*, with the involvement of relevant stakeholders from politics, the healthcare industry and civil society – so that the relevant rules can be applied in a feasible and legally compliant way (for further information on pseudonymisation and anonymisation standards, → see section 4.2 below).

With a view to **further harmonisation** aimed at overcoming regulatory discrepancies in the field of research (different regulatory approaches by the Member States, division of regulatory scope between the Federal Data Protection Act and the data protection acts of the *Länder*, special regulations for specific subjects), the Data Ethics Commission recommends that the Federal Government should:

a) push for synchronisation of the research-specific **legal bases** in the Federal Data Protection Act, in the data protection acts of the *Länder* and in subject-specific acts;

b) drive forward projects at **European level** aimed at greater harmonisation of the regulatory frameworks put in place by the Member States in respect of research data protection; and

c) lobby for a **duty of notification** incumbent upon Member States when adopting national laws in this area, and for the establishment of a European **clearing house** for cross-border research projects.

4.1.3 Consent processes for sensitive data

Voluntary, informed and explicit consent by the data subject is a critically important means of protecting individuals (test subjects) participating in research projects, particularly in the case of clinical research and research involving health data and other particularly sensitive categories of data, because it provides the test subject with an opportunity to exercise his or her right to **informational self-determination**. Since it necessitates the provision of easy-to-understand information about the research project, it also ensures that the test subject will not discover at a later date that his or her **values or preferences** prevent him or her from participating in the study. As a protective instrument enshrined in law, it improves the transparency of research and therefore increases people's level of confidence in it. Not least among its benefits is the fact that it also promotes the integrity of research and researchers.

Yet researchers who act as controllers face considerable challenges when it comes to obtaining informed consent, particularly when the project involves sensitive data. For example, if researchers want to embark on a new project using health data already available in a database, the data subjects must be contacted so that consent can be obtained again (unless the data subjects originally consented to the reuse of their data in future, or provided – to use the term preferred within ethics discourse – **broad consent**). Researchers wishing to use health data collected in the course of routine medical care for research purposes must first contact patients and ask them to grant informed consent, which is a task fraught with huge practical obstacles. With this in mind, the Data Ethics Commission recommends that appropriate **model procedures for the obtaining of consent** should be designed and developed with a view to making it easier to process data for research purposes.

With explicit reference to the link that exists between consent and a data subject's fundamental rights, the Data Ethics Commission also calls for the development of **innovative consent models** in the research sector. **Dynamic consent** models that involve tailoring declarations of consent to the individual context are already being trialled, for example. In this connection, it must be ensured that the consenting party remains able to control his or her data even after granting consent; in order to ensure that this is the case, the Data Ethics Commission recommends that more emphasis be placed on the development and design of privacy management tools (PMT) and personal information management systems (PIMS) (→ see section 4.3 below) for the research sector, such as **digital consent assistants** or data agents. Consent assistants of this kind may make it significantly easier for data subjects to keep track of the data processing operations to which they have granted consent, even after these operations have commenced; equally, they may make it possible to go back and ask data subjects for consent again if circumstances change, and to provide data subjects with a straightforward way of revoking their consent.

Calls are being heard increasingly often – particularly in connection with research using health data – for **blanket consent** models that involve a data subject granting consent to a wide range of data uses in the field of research, without reference to a specific course of treatment or other event. Although the research sector can advance compelling reasons for models of this kind, there are a number of concerns and obstacles that must be overcome before they are adopted (in particular the need for consent to be informed and for it to be linked to a specific purpose). They would make it impossible to take a consenting party's preferences and values into account on a differentiated basis, even if far-reaching legal safeguards were provided against misuse of his or her data and encroachments upon his or her privacy.

Against this backdrop, the Data Ethics Commission recommends further discussion of the innovative model known as **"meta consent"**.[23] After being appropriately informed – and without being in a situation where consent is specifically required – the data subject decides on the type of research projects and research contexts for which he or she wishes to grant consent and the type of consent involved (specific or broad). Consent may be limited on the basis of considerations such as the following:

- research context (e.g. private or public research, commercial or non-commercial research, national, European or international research);
- data sources (e.g. electronic health record, human tissue, health data, lifestyle data from wearables);
- type of research (e.g. preventive research, research into cancers or neurodegenerative disorders, any kind of health research).

If researchers later wish to use the data for a specific research project, the data subject is **informed** in advance and given the opportunity to **object** to this use of his or her data.

Each real-life implementation of this model should be under the **oversight** of a data trust scheme, an ethics commission or another responsible body tasked with ensuring that the consenting party's preferences are, in fact, taken into account. It should also be possible for the data subject to amend the terms of his or her meta consent at any time, and the technical and regulatory framework required to do so must be in place.

Example 13

Example 13 A data subject specifies that the data from his electronic health record may be used for public and commercial research. He also specifies that his blood and tissue samples may be used for public and commercial research into degenerative diseases. He consents to the processing of data from his electronic health record provided that the data are not transferred out of Europe. A company from Spain would like to use data from his electronic health record as well as data from his tissue samples for dementia research. The data subject is informed of their intention to do so, and told that he has four weeks to object to his data being used in this way.

23 Thomas Ploug / Søren Holm: Bioethics, 2016 (30:9), pp. 721 et seqq.

When deliberating on and designing a model of this kind, care must be taken to ensure that any constraints placed on the **freedom of research** and the research privilege for secondary use of data are equivalent in scope to the restrictions imposed under the current legal system. Preference should be given to meta consent models that emphasise the ability of data subjects to express their **values and preferences** regarding the use of their health data for research purposes; this would also increase public confidence in health data governance.

Another ethical question that must be considered is that of accountability – not only in relation to the use of data, but also in relation to their non-use, since this may block potential progress in vital areas and result in discrimination against certain groups as a result of their **exclusion from progress**. For example, methodological reasons mean that clinical studies involving older people suffering from several different chronic diseases and taking several different kinds of medication at the same time must necessarily be very limited in scope. If high-quality procedures can be used to evaluate their health data, however, key findings might be obtained on the interactions between these different medications and their actions under everyday conditions; these findings could then be used as a productive basis for more extensive research and the treatment of these patients going forwards.

With the above in mind, and given the significance of the European healthcare sector from both a medical and economic perspective, the Data Ethics Commission recommends proactive **support for a "learning healthcare system"** in which healthcare provision is continuously improved by making systematic and quality-oriented use of the health data generated on a day-to-day basis, in keeping with the principles of evidence-based medicine. A learning healthcare system imposes high requirements in terms of multi-level governance and requires a cross-disciplinary approach to healthcare provision that puts the insured party or patient front and centre.

4.1.4 Legal protection against discrimination

At the same time, however, the Data Ethics Commission wishes to emphasise that all parties involved in developing and designing new health-related research projects must take due account of the significant **potential for discrimination** that is opened up through the availability of sensitive data (e.g. when a data subject looks for a job or takes out an insurance policy). Technical progress has made it possible to sequence and decode the human genome, and data scientists are now able to analyse biometric and behavioural data collected in the course of daily life; this means that it is also possible to profile an individual's risk of falling ill in the future, typically based on the likelihood that he or she will suffer from this or that disease – and when genetic data come into play, his or her relatives may also be affected.

With this in mind, the Federal Government should examine the possibility of **including new grounds for action under the [German] General Act on Equal Treatment (*Allgemeine Gleichbehandlungsgesetz*, AGG)**, as well as specific **bans** on using information about a person's health (by way of analogy to the corresponding provisions on genetic data in the [German] Genetic Diagnostics Act (*Gendiagnostikgesetz*, GenDG)).

4.2 Anonymisation, pseudonymisation and synthetic data

Operations that involve accessing personal data must always comply with the applicable provisions of data protection law, and abide by the rules on data processing laid out in these provisions – from the purpose limitation principle right through to appropriate protective measures. Under certain circumstances, therefore, it may be vitally important for businesses or other users to know for certain that their operations either fall outside the scope of data protection law or are compliant with data protection law. The Data Ethics Commission believes that there is a lack of **legal certainty** in a number of different areas, for example concerning the anonymisation and pseudonymisation of data, the identification and consideration of a link between individuals and (allegedly anonymised) data sets, and synthetic data.

Anonymised and pseudonymised data

Anonymisation involves processing a set of personal data in such a way that any link to the data subject is broken irrevocably. A distinction is made between randomisation and generalisation; both are different ways of approaching the task of anonymisation, and they can be used individually or in combination. **Randomisation** involves modifying data in such a way that the anonymised data can no longer be matched up with the data subject. This can be achieved by falsifying individual data sets, for example. Appropriately designed randomisation methods ensure that the statistical properties of the original data set are retained, for example by swapping values rather than changing them. **Generalisation** involves aggregating pieces of [less] detailed information, such as age categories instead of dates of birth, names of regions instead of postcodes, or periods of time instead of time stamps that are accurate to the nearest second.

Three main strategies are used to identify natural persons in a data set:

a) **singling out:** a method of pinpointing data sets relating to specific individuals from a larger pool of data, for example by using unique characteristics that make it possible to identify these individuals;

b) **linkability:** a method that involves linking up at least two data sets that relate to the same individual or group of individuals on the basis of matching values that appear in both data sets, such as identifiers, spatial coordinates or times. Even a small amount of data available on an individual can be augmented using this linking strategy, allowing him or her to be identified;

c) **inference:** a method that involves deriving the highly probable value of a characteristic from the values of a number of other characteristics, again allowing the data relating to an individual to be augmented and increasing the likelihood that he or she will be identified.

Anonymised data sets make it impossible to recreate the links that once existed between the data and the individuals to whom the data relate, or to create such links for the first time, given the technological means that are reasonably likely to be used and that are available or being developed at the time of the processing (cf. Recital 26 GDPR); an attacker wishing to identify one or all of the data subjects (through de-anonymisation) would find the task impossible.

Modifications to a set of data – in particular the artificial addition of fuzziness (also referred to as noise or blurring, depending on the context) – ensure that it is impossible to pull out data that belong to a specific individual, that linkable data are not used and that inferences cannot be drawn; these modifications typically also place constraints on the utility of the data. If the user is aware of the evaluations that will later be carried out using the data set, the anonymisation procedures can be optimised with this in mind, for example by retaining the necessary level of detail for the relevant characteristics wherever possible. The same applies to comparisons of different data sets (interoperability); if the user knows which comparisons will be carried out, appropriate anonymisation methods can be designed by categorising the data into identical groups as required, and taking into account the increase in risk that may occur as a result of incorporating information from other data sets.

Pseudonymisation involves processing data in such a way that they can no longer be assigned to a specific data subject without additional information, which may take the form of mapping tables or cryptographic hash methods, for example. Pseudonymisation differs from anonymisation in that a reference to a person (in the legal sense of the term) is retained. The controller must prevent (unauthorised) access to the additional information whenever the pseudonymised data are processed in future, since otherwise it would be possible to map the data to the data subjects. The GDPR refers to pseudonymisation several times as a technical and organisational measure for reducing the risk to the rights and freedoms of natural persons.

Both anonymisation and pseudonymisation involve processing a set of data that is already available, and must be distinguished from **pseudonyms**, which are deployed on the user side. Users may choose their own pseudonymised identifiers (e. g. user names for online services or e-mail addresses), or use identifiers provided automatically by a technological system, for example the online ID function of an electronic ID card or attribute-based authorisation certificates designed with data protection concerns in mind. In the vast majority of cases, the use of pseudonyms provides little in the way of protection against identification of the data subject, particularly if they are used across contexts and communication partners, which allows the data in a user-specific profile to be linked to other data and augmented. Conversely, constantly changing "transaction pseudonyms" are restricted to a specific context, making it much harder to identify the individual in question.

Internet-based procedures aimed at **concealing the link** between a data subject and the data relating to that data subject cannot generally be regarded as anonymisation in the strict sense of the term, but may nevertheless provide some level of protection against identification and observation. Simple web proxies make it possible to surf the Internet using the identifier (i. e. the IP address) of an intermediary server; multiple users (whose identifiers are known to the proxy server) may therefore have the same identifier as far as the destination web servers are concerned, provided that they avoid identifying themselves through the use of cookies, etc. Further steps to prevent identification can be taken by arranging multiple intermediary servers one behind another, for example in mix networks such as Tor or in mix cascades such as JonDo. Once again, noise can be added by sending artificially created "dummy traffic", as an additional obstacle in the path of anyone attempting to observe the human users.

4.2.1 Procedures, standards and presumption rules

It is often not possible to **anonymise** data – i.e. completely break the link between data and the data subject to whom they belong in such a way that it cannot be recreated – without losing any of the data's utility. At the same time, however, perfect anonymisation is often not required, firstly because many goals can (upon closer examination) be achieved using data with a somewhat lower level of utility, and secondly because the GDPR already contains exemptions for data processing operations that serve the public good (e.g. in the research sector), meaning that even personal data can be processed without obtaining consent from the data subjects. Nevertheless, efforts aimed at developing effective **anonymisation technologies and procedures** should be stepped up with a view to allowing data to be processed wholly outside the scope of the GDPR.

Ultimately, legal certainty can be achieved only by developing **standardised technologies and procedures**, which must always take due account of the whirlwind pace of technological development. The Data Ethics Commission therefore recommends that the Federal Government should lobby – in particular at EU level – for easy-to-use **anonymisation standards** that would benefit both data subjects and users, and for **pseudonymisation measures** that are commensurate with the level of risk faced by data subjects in their private lives (as featured on the agenda of the Federal Government's Digital Summit).

In particular, anonymisation standards should be combined with clear rules imposing a rebuttable legal **presumption**, which would provide legal certainty for users, who could rely on their data processing operations falling outside the scope of the GDPR where the standard has been met. In this context, it is important to remember that restrictions may need to be imposed in these presumption rules, for example on the period of validity (by way of analogy to cryptographic procedures),[24] or on the authorised methods of processing (for example stating that data may not be published or made accessible to an unspecified number of people). As long as there is no legal basis for rebuttable presumption rules, the Federal Government should support the development of technical **best practices** and industry-specific **codes of conduct**, with a view to building up experience in these fields.

In certain fields, the standardisation of anonymisation and pseudonymisation procedures may also impose rules on the way in which the link between a data subject and the data relating to him or her should be broken, making it possible to compare different data sets and improving **interoperability**. At least in areas where improved interoperability is a sought-after outcome, the Data Ethics Commission recommends that context-specific rules should be developed for preferred groupings (e.g. value ranges of age categories, postcodes or IP addresses). A similar approach is already followed by Germany's statistical offices when handling data, for example.

24 Federal Office for Information Security: Technical Guidelines BSI TR-02102 Cryptographic Mechanisms: Recommendations and Key Lengths, last updated in February 2019 (available at: *https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=9*).

Anonymisation and pseudonymisation procedures are carried out on repositories of data that are known to (or at least suspected to) contain personal data. These differ from repositories of data that are not thought to contain personal data, but could be used as a means or at least a starting point (either on their own or in combination) for creating a link between purportedly anonymous data and the data subject to whom these data belong. Once again, the Data Ethics Commission recommends the development and binding implementation of **standardised methods for checking whether data subjects can be identified from a set of data**; these methods must allow the user to conclude with a reasonable degree of certitude that the data are either personal or non-personal.

4.2.2 Ban on de-anonymisation

Presumption rules should also be accompanied by appropriate **bans on de-anonymisation**, and any infringement of these bans (i. e. cases where it proves possible to identify a data subject using formerly anonymous data, for example as a result of technological developments) should be subject to a **penalty**. The bans would need to be designed in such a way as to avoid placing roadblocks in the way of research into the detection and removal of links between data and data subjects in repositories of data, since any options for de-anonymisation that are available must be investigated further with a view to developing appropriate anonymisation standards and verifying their effectiveness. In addition, the introduction of bans on de-anonymisation and penalties for their infringement must not be misused as a pretext for downgrading the standards that apply to anonymisation or diluting the meaning of the term "personal data" as used in the GDPR, since companies involved in vitally important efforts to drive forward the technology of anonymisation using technical means would otherwise be placed at a competitive disadvantage. The same applies to the reversal of pseudonymisation in the absence of justified reasons (a list of which should be drawn up).

4.2.3 Synthetic data

A distinction should be made between genuine data and **synthetic data**, i. e. data that are generated artificially rather than being collected directly in the real world. Synthetic data boast several advantages over real-world data;[25] firstly, they can be produced in any quantity, which is particularly important when dealing with simulations for which real-world data cannot be generated. Secondly, steps can be taken when synthetic data are created to ensure that the entire range of values is mapped as comprehensively as possible, e. g. in order to test how a technical system would behave when confronted with unusual data combinations. Thirdly, the quality of synthetic data can be measured, and if necessary it can be guaranteed in individual cases that the properties of a set of real-world reference data are retained; alternatively, distortions occurring in sets of real-world data can be pinpointed and removed in order to avoid discrimination. If the set of synthetic data contains no references to persons, it is anonymous and does not fall within the scope of the GDPR.

The Data Ethics Commission recommends that the Federal Government should support **research in the field of synthetic data** on a number of different issues, including the question of whether, to what extent and in which contexts synthetic data might replace real-world data in processing operations, and how closely the synthetic data should resemble the real-world data in terms of their properties. The Data Ethics Commission recommends further investigations into the creation and use of synthetic data, with a particular emphasis on topics including data quality and the avoidance of bias and discrimination.

25 Jörg Drechsler / Nicola Jentzsch: Synthetische Daten: Innovationspotenzial und gesellschaftliche Herausforderungen [Synthetic data: potential for innovation and societal challenges], Stiftung Neue Verantwortung, May 2018 (available at: *https://www.stiftung-nv.de/sites/default/files/synthetische_daten.pdf*).

4.3 Controlled data access through data management and data trust schemes

4.3.1 Privacy management tools (PMT) and personal information management systems (PIMS)

In an ever more complex environment, one of the major challenges faced by individuals in exercising their data rights is a **lack of oversight over personal data** – data subjects typically have no records documenting the times when they have granted consent, for example. Sharing of data by the original data controller can also result in the "scattering" of data, with a significant decrease in transparency and a corresponding increase in data protection risks for the data subjects (→ see section 3.3.6 above regarding the problem of data trading). There are currently not enough standards and software tools that data subjects can use to track and control, on an ongoing basis, who has been granted access and to whom data have been transferred, which would be necessary for them to exercise their data rights effectively.

An increasing number of technical and institutional measures are being proposed in response to this problem. **Privacy management tools (PMT)** range from applications that make consent management easier for users (dashboards, etc.) through to AI tools that automatically implement individual user preferences ("data agents"). Where the focus is not so much on the provision of technical applications but rather on the service end, it is more common to use the term **personal information management systems (PIMS)**. Such services range from single sign-on services, local data safes and online storage systems through to offers (both comprehensive and less so) for third-party management of user data (data trust models). When designed as data trust models, PIMS may support digital self-determination by shouldering some of the responsibility for exercising the data subject's rights under data protection law, such as granting and withdrawing consent and exercising the right to information, the right to rectify data, the right to erase data, the right to data portability and the right to object. The Data Ethics Commission recommends that the Federal Government should promote innovation and standardisation in relation to software tools and services of this kind.

4.3.2 Need for regulation of PMT/PIMS

The above notwithstanding, privacy management tools/personal information management systems may pose **risks** if they fail to comply with certain requirements, some of which go beyond the scope of the GDPR. If these tools or systems fail to be properly designed, for example, there is a risk that data subjects will not be empowered to exercise true self-determination, but will instead unwittingly find themselves on a path of **external determination**. In particular, privacy management tools/personal information management systems that are designed in such a way that data subjects "write a blank cheque" by handing over the majority of decisions to the operators of these tools/systems, or that result in data subjects taking decisions contrary to their own interests under the influence of these tools/systems, would ultimately be inconsistent with the ethical value of self-determination. Privacy management tools/personal information management systems must be available as aids for data subjects, but they must not usurp the power of these latter to take self-determined decisions, and they must certainly not manipulate them using dark patterns et al. (→ see section 3.2.2. above).

Given the significant risks that these systems and tools may pose to fundamental rights and the lack of options for data subjects to carry out quality assurance measures themselves, the Data Ethics Commission recommends that the Federal Government should develop **quality standards for privacy management tools/personal information management systems and introduce a certification and monitoring system**. The latter should apply in particular to systems that act on behalf of or in place of a data subject, or that – as a result of their technical design – play a major role in steering and channelling the data subject's decisions. In cases where data are stored directly by the operators of these tools/systems (i. e. if they are not stored on a decentralised basis and simply managed, which is also possible), provision must also be made for the company's insolvency or liquidation.

Privacy management tools/personal information management systems can operate reliably only if cooperation on the part of all relevant controllers is guaranteed. The only possibility to achieve the wide-ranging coverage required is by imposing a **legal obligation** that applies (under appropriate conditions) to controllers within the meaning of the GDPR, with a view to ensuring that any access to personal data can be monitored by the tool/system and that any information that is relevant in terms of data protection reaches the tool/system so that the tool/system can effectively protect the data subject's interests in relation to all of his or her personal data. A **sector-specific approach** – for social networks, for example – might be a realistic option to start with.

In the view of the Data Ethics Commission, systems of this kind could either be operated on a non-profit basis and without any involvement of commercially motivated actors – such as by charitable **foundations** and similar independent bodies – or organised as **private-sector enterprises** provided that the operator derives profits from managing rather than from using the data. In either case, the fiduciary duties that are owed to the data subject must be precisely defined in legislation, the involvement of parties with conflicting interests must be ruled out, and appropriate opportunities for oversight must be built into the system as a whole (such as to minimise bias and discrimination). If the private-sector option is chosen, it will also be necessary to ensure that the operator's commercial motivations do not undermine the role it plays as custodian of the data subject's interests, and that operators that have access to personal data are based in the European Union.

The Data Ethics Commission recommends that the Federal Government should lobby for appropriate **amendments to the GDPR** in the form of a clearer and legally secure framework for privacy management tools/personal information management systems. Steps should also be taken (in addition to action on legal matters relating to mandates, etc.) to prevent excessive centralised storage of personal data, since arrangements of this kind increase the level of risk for data subjects in the event of cyber attacks or similar incidents. Machine-interpretable formats and communication protocols must be standardised for the automated execution of services.

4.3.3 PMT/PIMS as a potential interface with the data economy

Provided that the appropriate regulations are adopted, privacy management tools/personal information management systems could also serve a dual function. On the one hand, these tools/systems might help individuals to exercise their right to informational self-determination effectively and to verify compliance with any limitations on use that have been imposed; on the other hand, however, they could also be used to release data from the confines of "data silos" and allow them to be used within the European data economy (in particular by exercising the right to data portability granted by Article 20 GDPR). The main idea underlying privacy management tools/personal information management systems is to improve an individual's control over his or her personal data, which does not in and of itself promote third-party data access. An indirect data access function might, however, be compatible with the **principle underpinning data trust schemes** if third parties were allowed to access the data only to pursue certain purposes approved by the data subject (→ in connection with research, for example; see section 4.1.3 above), or if the economic exploitation of the data served the data subject's interests and took place with his or her express consent (→ see section 3.3 above for a discussion of the problems raised by treating personal data as an economic asset).

The Data Ethics Commission believes that – if it is decided that privacy management tools/personal information management systems should play a dual role and also serve as a platform for legally secure data access by companies – it must be ensured that these qualified dual-function tools/systems do not ultimately subvert the goal of protecting data subjects' rights. Strict compliance with the principles of privacy and ethics by design must be enforced; in particular, the objective pursued must not be the broadest possible exploitation (and "scattering") of data. The Data Ethics Commission wishes to emphasise the fact that privacy management tools/personal information management systems must continue to serve as dedicated custodians of data subjects' interests, and that **conflicts of interest must be ruled out**.

4.4 Data access through data portability

4.4.1 Promotion of data portability

The **right to data portability** granted by Article 20 GDPR is a tool that a data subject can use to determine whether companies should gain access to his or her personal data which another company has already collected, and if so, which companies. It includes the right to receive the data provided in a "structured, commonly used and machine-readable format" or to have them transmitted directly to another controller. The right to data portability has two main implications:

a) It prevents unwanted lock-in effects if data subjects switch providers, thereby protecting both the individual data subjects' right to economic self-determination and free competition.

b) Even if data subjects do not switch providers, it allows them to ask the controller to make the data available either to them or to other companies. This provides the other companies with an option for gaining access to data that might otherwise not have been available to them, bearing in mind that they need a separate legal basis for data processing under data protection law (e.g. consent or a contract).[26]

Despite the fact that providing data in a "structured, commonly used and machine-readable format" is a basic prerequisite that must be met in order for data subjects to exercise the right to data portability effectively, to date this requirement has been subject to an enormous range of varying interpretations in practice. The Data Ethics Commission therefore recommends that the Federal Government and the data protection authorities – in implementation of Recital 68 of the GDPR – should support the development of **industry-specific codes of conduct and standards** at European level so that the right to data portability can be realised uniformly and effectively in practice, to the benefit of all parties involved.

In the absence of new intermediaries (→ see section 4.3 above), the stimulus to exercise the right to data portability often stems from a company that has gained a new customer. Companies that offer a convenient and automated process for data subjects to exercise their right to data portability are likely to be particularly successful (e.g. a provider of a map service that allows data to be ported from a mobility service provider at the click of a button). There are also grounds for assuming – in view of the potential for network effects and effects of scale – that the companies likely to benefit most from the right to data portability, at least in the medium term, will be those that already hold a dominant position in the market and have accumulated huge amounts of data. The Data Ethics Commission therefore recommends that the Federal Government should **observe developments closely** and, in so far as it judges necessary, lobby at European level for measures that specifically encourage and facilitate the porting of data from market-dominant and data-rich companies to other market participants, including start-ups.

26 For an example of the debates on the requirement for a separate legal basis of this kind under data protection law, see Article 29 Data Protection Working Party: Guidelines on the right to data portability, WP 242, rev. 01, last revised and adopted on 5 April 2017, p. 7 (available at: *http://ec.europa.eu/newsroom/document.cfm?doc_id=44099*).

4.4.2 Should the scope of the right to data portability be extended?

Debates are ongoing on whether the scope of the right to data portability should be extended in various ways, in particular by expanding it to cover data other than the (raw) data provided to a controller (e.g. certain forms of processed or derived data), or by widening it to include a right to dynamic real-time portability (e.g. real-time streaming of data flows). As things currently stand, and further to the above recommendation, the Data Ethics Commission proposes that the Federal Government should not lobby for amendments to the GDPR aimed at extending the scope of the current right to portability; given that the GDPR has been in force for such a short period of time, a "wait and see" approach should instead be adopted until more clarity has been gained on its practical application, supervisory practice by the data protection authorities and interpretation by the courts.

4.4.3 From portability to interoperability and interconnectivity

Network effects (e.g. in the case of messenger services) mean that data portability alone will not be sufficient to mitigate the risks posed by existing and future data and service oligopolies, or to lower the barriers to market entry for new competitors to the extent that they represent a serious challenge to the market-dominant providers. The Data Ethics Commission therefore recommends that the Federal Government should push for the introduction of **sector-specific interoperability obligations**, of the sort that have previously been imposed for postal services and mobile telephony, for example. At the same time, measures must be taken to ensure that interoperability features comply with data protection principles, such as privacy-friendly default settings; examples include an option to use different and changing identifiers instead of a single universal identifier, a reduction in the use of central components to collect large volumes of data, and other suitable examples of interoperable technical interaction at different levels.

Asymmetric interoperability obligations could be imposed on **powerful companies and new market entrants** respectively (for example, a market-dominant provider of messenger services might be obliged to allow customers of smaller providers to send messages directly to its own customers and to allow its own customers to send messages directly to the customers of smaller providers); at the same time, however, it must be ensured that interoperability requirements are not abused for the purpose of increasing yet further the flow of personal data towards data-rich and powerful companies. If this risk can reliably be averted, it would be useful to impose certain **interconnectivity obligations, e.g. for short messaging services and social networks**, with a view to counteracting the concentration effects of these networks and promoting the aims of data portability more effectively (i.e. healthier competition and easier access for new market entrants to a data-intensive economy). A model of this kind is also a prerequisite for building up or strengthening certain basic services of an information society in Europe, thereby promoting the digital sovereignty of both Germany and Europe.

4.5 Crowdsensing for the public good

Crowdsensing has also been hailed as a way of opening up new data resources for the data society and data economy; in order to do so, it deploys users' technical devices in the form of "sensors" that collect data (in a certain locality, for example) and forward them to a higher-level instance that analyses the collected data. The Data Ethics Commission acknowledges the potential inherent to this technology, especially if it is **put to use for the public good**. For example, crowdsensing can be used in a smart city for real-time analysis of traffic conditions, the state of repair of infrastructure, air quality and so on. At the same time, however, the Data Ethics Commission believes that achieving an ethically appropriate design will be a significant challenge. An analysis carried out using crowdsensing techniques will typically have an extremely high level of granularity, meaning that the data involved may fall under the category of "sensitive" not only from the perspective of the individuals that generated them, but under certain circumstances also from the perspective of anyone in their vicinity. Efforts must therefore be stepped up to introduce **standards for anonymisation and pseudonymisation** (→ see section 4.2 above) with a view to preventing not only situations in which data can be traced back to (non-consenting) users or potentially to other persons affected, but also other forms of misuse. Crowdsensing-related data transfers may also overstrain the resources of users' devices and raise security issues.

Consideration must be given to these points even if users participate voluntarily and intentionally in crowdsensing programmes ("participatory sensing"), and thought must therefore be given to the **substantive limitations to consent** that exist in this connection (→ see section 3.2 above). Even when data are used for purposes that serve the public good, it must always be ensured that the requirements outlined in legislation – in particular data protection law and consumer protection law – are complied with in full. In this case, it should also be remembered that decisions and measures taken by government agencies must not be based solely or customarily on data collected using participatory sensing techniques, since these data are necessarily **incomplete** owing to the voluntary nature of participation, and it is likely that they will also exhibit **bias**.

The Data Ethics Commission believes that any discussion of whether crowdsensed personal data should be collected, forwarded and compiled without the user's knowledge ("opportunistic sensing") ignores the potential for such measures to violate the fundamental principles of data protection. It believes that decisions must be taken on a case-by-case basis as to whether a **legal obligation** can justifiably be imposed to force data subjects to make available technical devices so that the data from these devices can be collected and forwarded automatically, if and to the extent that the analysis of these data promotes vital public interests.

Summary of the most important recommendations for action

Improving controlled access to personal data

16

The Data Ethics Commission identifies enormous potential in the use of data for research purposes that serve a public interest (e.g. to improve healthcare provision). Data protection law as it currently stands acknowledges this potential, in principle, by granting far-reaching privileges for the processing of personal data for research purposes. Uncertainty persists, however, in particular as regards the scope of the so-called research privilege for secondary use of data, and the scope of what counts as "research" in the context of product development. The Data Ethics Commission believes that appropriate **clarifications in the law** are necessary to rectify this situation.

17

The fragmentation of research-specific data protection law, both within Germany itself and among the EU Member States, represents a potential obstacle to data-driven research. The Data Ethics Commission therefore recommends that **research-specific regulations should be harmonised**, both between federal and *Land* level and between the different legal systems within the EU. Introducing a notification requirement for research-specific national law could also bring some improvement, as could the establishment of a European clearing house for cross-border research projects.

18

In the case of research involving particularly sensitive categories of personal data (e.g. health data), **guidelines** should be produced with information for researchers on how to obtain consent in a legally compliant manner, and **innovative consent models should be promoted and explicitly recognised by the law**. Potential options include the development and roll-out of digital consent assistants or the recognition of so-called meta consent, alongside further endeavours to clarify the scope of the research privilege for secondary use of data.

19

The Data Ethics Commission supports, in principle, the move towards a **"learning healthcare system"**, in which healthcare provision is continuously improved by making systematic and quality-oriented use of the health data generated on a day-to-day basis, in keeping with the principles of evidence-based medicine. If further progress is made in this direction, however, greater efforts must be made at the same time to protect data subjects against the significant potential for discrimination that exists when sensitive categories of data are used; this might involve **prohibiting the exploitation of such data** beyond the defined range of purposes.

20

The development of procedures and standards for data **anonymisation** and **pseudonymisation** is central to any efforts to improve controlled access to (formerly) personal data. A legal presumption that, if compliance with the standard has been achieved, data no longer qualify as personal, or that "appropriate safeguards" have been provided in respect of the data subject's rights, would improve legal certainty by a long way. These measures should be accompanied by rules that – on pain of criminal penalty – prohibit the de-anonymisation of anonymised data (e.g. because new technology becomes available that would allow the re-identification of data subjects) or the reversal of pseudonymisation, both in the absence of narrowly defined grounds for doing so. Also research in the field of **synthetic data** shows enormous promise, and more funding should be funnelled into this area.

21

Fundamentally speaking, the Data Ethics Commission believes that **innovative data management and data trust schemes** hold great potential, provided that these systems are designed to be robust, suited to real-life applications and compliant with data protection law. A broad spectrum of models falls under this heading, ranging from dashboards that perform a purely technical function (**privacy management tools**, PMT) right through to comprehensive data and consent management services (**personal information management services**, PIMS). The underlying aim is to empower individuals to take control over their personal data, while not overburdening them with decisions that are beyond their capabilities. The Data Ethics Commission recommends that research and development in the field of data management and data trust schemes should be identified as a funding priority, but also wishes to make it clear that adequate protection of the rights and legitimate interests of all parties involved will require additional **regulatory measures at EU level**. These regulatory measures would need to secure central functions without which operators cannot be active, since their scope for action would otherwise be very limited. On the other hand, it is also necessary to protect individuals against parties that they assume to be acting in their interests, but that, in reality, are prioritising their own financial aims or the interests of others. In the event that a feasible method of protection can be found, data trust schemes could serve as vitally important mediators between data protection interests and data economy interests.

22

As far as the right to **data portability** enshrined in Article 20 GDPR is concerned, the Data Ethics Commission recommends that industry-specific codes of conduct and standards on data formats should be adopted. Given that the underlying purpose of Article 20 GDPR is not only to make it more straightforward to change provider, but also to allow other providers to access data more easily, it is important to evaluate carefully the market impact of the existing right to portability and to analyse potential mechanisms by which it can be prevented that a small number of providers increase yet further their market power. Until the findings of this evaluation are available, expansion of the scope of this right (for example to cover data other than data provided by the data subject, or real-time porting of data) would seem premature and not advisable.

23

In certain sectors, for example messenger services and social networks, **interoperability or interconnectivity obligations** might help to reduce the market entry barriers for new providers. Such obligations should be designed on an asymmetric basis, i.e. the stringency of the regulation should increase in step with the company's market share. Interoperability and interconnectivity obligations would also be a prerequisite for building up or strengthening, within and for Europe, certain basic services of an information society.

5. Debates around access to non-personal data

The data economy will play a key role in the future competitiveness of German and European companies; the growing penetration of the Internet of Things (IoT) and the Internet of Services (IoS) means that data which are collected automatically by sensors and which can potentially serve as a basis for developing new business models and innovations are acquiring ever-greater industrial significance. **Germany is at the cutting edge of developments** as far as many IoT/IoS-related technologies are concerned (e.g. sensor technology, mechanical engineering and embedded systems), and also plays a leading role in the broader field of industrial production and the digital services that cater for this sector; given the increasingly cut-throat nature of international competition, it must build on this head start in order to safeguard the country's future prosperity. A differentiated and robust research landscape, a diversified economic structure and a reputation as a global leader in key technological segments such as Industry 4.0 put Germany in the perfect position to leverage the potential associated with the data economy as a basis for creating future value.

5.1 Appropriate data access as a macroeconomic asset

The Data Ethics Commission believes that providing appropriate access to data for German and European companies and decreasing the current level of dependency on a small number of data oligarchs would go a long way towards building a market-oriented data economy that serves the public good, and towards strengthening the digital sovereignty of both Germany and Europe. In this connection, data access in the narrower sense firstly relates to the extent to which the data required for a particular business model or other project can be **used on a *de jure* and *de facto* basis**. In order to benefit from **access to data** in this narrower sense, however, stakeholders must have a sufficient **degree of data-awareness** and have the **data skills** that are necessary to make use of the data. Also, access to data proves to be disproportionately advantageous to stakeholders that have already built up the **largest reserves of data** and that have the best **data infrastructures** at hand. The Data Ethics Commission therefore wishes to stress that the factors referred to should always receive due attention when discussing whether and how to improve access, in keeping with the **ASISA principle** *(Awareness – Skills – Infrastructures – Stocks – Access)*.

The discussions in this section focus on non-personal data. **Genuinely non-personal data** hold enormous potential for science, the economy and society, and yet this potential is often underestimated. Most scientific data can be categorised as non-personal; these include data originating from the technical sciences (e.g. engineering and materials science), data from the fields of physics (e.g. data from particle accelerators), biology (e.g. data from the plant and animal kingdoms), geology and chemistry, environmental data, weather data and ocean data right through to economic data (e.g. data from the financial markets). If they can be analysed (using big data methods, for example) and used (to develop AI applications, for example), these non-personal data hold enormous value for science, the economy and society; focused support must therefore be provided to researchers using these data, and systematic efforts must be undertaken to make data access an easier task.

The broad nature of the GDPR's definition of "personal data" means that it can safely be assumed that a substantial proportion of data repositories are mixed in nature (i.e. contain both non-personal data and data that are or could become personal); at the same time, the processing of personal data is a vital prerequisite for certain activities that fall under the heading of the data economy and that provide benefits for both individuals and the general public. Any discussion of data access that concentrates solely on non-personal data would therefore appear counter-productive. A more appropriate approach would be to work towards **general data access arrangements** that are **superseded by data protection law** only in cases where personal data are processed (meaning that activities falling under the heading of the data economy would need to comply with the provisions of the GDPR). Equally, it should not be forgotten that the GDPR already allows the economic exploitation of personal data in many circumstances; in addition to consent, for example (Article 6(1)(a) GDPR), there are five additional justifying grounds (Article 6(1)(b)–(f)), some of which are explicitly tailored to economic interests and needs.

5.2 Creation of the necessary framework conditions

5.2.1 Awareness raising and data skills

The use of data to create value presupposes that operators (whether they belong to the private sector or serve a public interest) are adequately well-informed about the relevant options and risks, and also have the data skills required (which may involve drawing on technical, economic, ethical and legal knowledge; (→ see Part D, section 3. above). In certain areas of the German **economy**, companies have still not tapped into the potential that exists to make more productive use of their data flows and repositories (in some cases for the benefit of the public). The Data Ethics Commission welcomes the steps that have been taken to raise awareness and build digital skills by various stakeholders (e. g. chambers of industry and commerce, associations or vocational institutions). A value-based approach to improving data skills across the board is, however, required, for example in the form of **initial and continuing training courses**. A further objective of these courses must always be to raise awareness of the risks posed to individuals and society from the viewpoint of data protection law and ethics.

Government bodies have been slow to recognise the import and implications of the huge volumes of data they have already generated (for statistical purposes, for example), and the advantages and risks entailed by models in which they share data with businesses (government-to-business (G2B) data sharing) or in which the businesses share operating data with them (business-to-government (B2G) data sharing). The current reticence on the part of public authorities to utilise these opportunities means that a large-scale shift in mindset is required, modelled on forerunners in the field of e-governance such as the Scandinavian countries or Estonia. The Data Ethics Commission also recommends that the Federal Government should support work in this area by the relevant research institutions.

5.2.2 Building the infrastructures needed for a data-based economy

Although Germany continues to occupy a leading position in the field of science and technology research, the tech companies providing vital data and analysis infrastructures for the new digital economy primarily hail from the USA (and increasingly from China). This means that a great deal of European data – consumer data, enterprise data and research data – is stored outside Europe and analysed in third countries using software belonging to non-European companies. This makes it crucially important for Germany to develop a data-based economy using **home-grown infrastructures**.

The Data Ethics Commission recommends that the Federal Government should support the following **measures at European level**, which have been initiated by the European Commission:

a) establishment and expansion of the Support Centre for data sharing;

b) development of model contracts for the data economy;

c) support for forums and consortiums tasked with developing open standards for legally compliant data exchanges, in particular formats and programming interfaces (APIs) that are tailored to data exchanges and that increase the traceability of data flows;

d) promotion of European platforms for legally compliant data exchanges; and

e) establishment of a European Open Science Cloud (EOSC).

Key precursors to the achievement of digital sovereignty by Germany include **access control** for sensitive data and the option to carry out appropriate **audits** on critical data analysis software, which would require manufacturers to disclose their source code and design criteria, for example. Given the ethically problematic nature of these analyses, they should, wherever possible, be carried out within the geographical purview of the German legal system.

The Data Ethics Commission **expressly welcomes a number of initiatives** by the Federal Government and other stakeholders aimed at creating secure international data spaces (spearheaded by Germany) for different application domains, allowing companies and organisations of all sizes and from all sectors of industry to retain sovereignty over their data and exchange data securely with each other.

The Data Ethics Commission also recommends the setting up of an **ombudsman's office** at federal level to provide assistance and support in relation to the negotiation of problematic data access agreements and dispute settlement. The competent data protection authorities should be consulted on cases involving personal data, and decision-making power must ultimately rest with the aforementioned authorities in order to avoid conflicting decisions.

Establishment of data infrastructures

The **Federal Government's initiatives** aimed at establishing data infrastructures include the following:

f) Efforts by the German Research Foundation *(Deutsche Forschungsgemeinschaft)* to establish a national research data infrastructure, the aim of which is to implement a science-driven process that systematically opens up data repositories and provides long-term data storage, backup and accessibility across the boundaries of different disciplines and *Länder*.

g) The open International Data Spaces Consortium (IDS, formerly Industrial Data Space) promoted by the Federal Ministry of Education and Research, the aim of which is to provide the companies and organisations taking part with a standardised interface to a platform for exchanging data, based on a federal architecture concept.

h) An initiative to develop a comprehensive network of big data and AI centres, with nodes distributed throughout Germany, as part of a national and generally accessible ecosystem. The aim is for this network not only to provide access to a large amount and variety of data on a 24/7 basis, but at the same time for it to offer easy-to-use tools along the entire data value creation chain (preparation, analysis, visualisation, exploitation) and develop them further on the basis of user feedback.

In addition to these technical platforms, other interesting developments include platforms developed by the Federal Government in collaboration with associations with a view to promoting coordinated research and development and the standardisation and practical implementation of data-hungry applications in the form of socially and economically innovative future projects, such as Industry 4.0, Smart Service World and Learning Systems.

At European level, the **European Commission** is implementing similar projects (e.g. the future-oriented FIWARE project), and is currently developing a freely available toolbox of open-source software components that can be used to configure innovative Internet services in a short space of time. The Big Data Value Public-Private Partnership (organised by the European Commission and the Big Data Value Association, BDVA) has developed an interoperable data-driven ecosystem at European level as a launchpad for new business models using big data, which has already delivered an impressive number of flagship projects. Lastly, the European Institute of Innovation and Technology (EIT Digital) has fostered the emergence of a Europe-wide technical and economic ecosystem involving 180 companies and research institutions.

5.2.3 Sustainable and strategic economic policy

As far as the data economy is concerned, the biggest challenges facing Europe include the lack of **sustainable** funding that is so often a problem for research projects, and a paucity of **venture capital** (the latter being required to make ideas that have already been developed market-ready and inject capital at the appropriate points so that start-ups can reach a competitive size). One of the reasons why the USA has been so successful in the field of digital products and services is because of the country's many "angels" willing not only to invest billions into high-risk projects, but, in many cases, to forfeit those investments. Another trend worth noting is that innovative companies are often **bought out** by foreign companies or forced by international investors to move their headquarters to other countries outside Europe.

Thinking outside the box of the "European path" explicitly endorsed by the Data Ethics Commission (→ see Part G, below), German start-ups must be given access to a larger **pool of funding** and better **tax incentives** so that Germany can continue to attract the brightest and the best and remain at the cutting edge.

Sectors such as education, public administration and medicine are characterised by a high level of public interest and the existence of mandatory values (as expressed through the legal system and professional ethics). At the same time, there is enormous potential to achieve efficiency gains through digitalisation and AI in these sectors, and global platforms have not yet gained a stranglehold over the market to the same extent as in other areas. The Data Ethics Commission therefore recommends that public funding should be channelled into these three areas in particular, and that it should be used to incentivise the **development of platforms** in Germany that reflect our values and are also internationally scalable.

5.2.4 Improved industrial property protection

Also from the perspective of the data economy, the Data Ethics Commission does not see any benefit in introducing **new exclusive rights** to data (often discussed using the terms "data ownership" or "data producer right", → see section 3.3.2 above). Rights of this kind, which would need to be incorporated into (and aligned with) the existing provisions of data protection law or intellectual property law or the rules on the right of personality, trade secrets, ownership rights to storage media, etc., would do nothing but increase the (already significant) level of complexity and legal uncertainty, without any clear indication that rights of this kind would be necessary or even particularly helpful in making data more marketable.

The Data Ethics Commission does, nevertheless, believe that the calls made by industry and government bodies to afford **limited third-party effects** to contractual agreements (e.g. to restrictions on data utilisation and onward transfer of data by a recipient) are justified. Under the legal situation as it currently stands, third-party effects of this kind are at most afforded in extreme situations (unless protection under intellectual property rights law applies, including the "sui generis" protection of databases). Consideration should be given to extending the scope of recognition of third-party effects, along the lines of the model provided by Article 4(4) of the Trade Secrets Directive (Directive (EU) 2016/943);[27] according to this approach, the acquisition, use or disclosure of data would also be considered unlawful whenever a person, at the time of the acquisition, use or disclosure, knew or ought, under the circumstances, to have known that the data had been obtained directly or indirectly from another person who was using or disclosing the data unlawfully. This approach would further the interests of the data economy and also fit seamlessly into the existing (primarily contract-focused) model.

27 This solution is endorsed in Preliminary Drafts no. 2 (February 2019) and no. 3 (October 2019) of the ALI-ELI Principles for a Data Economy (see footnote 1 above), for example.

5.2.5 Data partnerships

The Data Ethics Commission believes that cautious development of the current legal framework would also be appropriate in the field of **anti-trust law**. The breakneck pace of developments in the data economy poses fresh challenges for this field of law; in return, the provisions of anti-trust law pose fresh challenges for digital companies. The Data Ethics Commission recommends that the Federal Government should pay particularly close attention to the opportunities and risks entailed by **data partnerships**; consideration should be given to the introduction of a mandatory but confidential procedure for notifying data partnerships to the anti-trust authorities and to the supervisory authorities under data protection law (in the case of personal data). Mention should also be made of the proposals presented by the Commission of Experts on Competition Law 4.0 under the headings of "data exchange" and "data pooling".

5.3 Data access in existing value creation systems

5.3.1 Context

Fair and efficient data access plays a significant role in modern value creation systems. The area of law most suitable for regulating fairly and efficiently the ability of various stakeholders to access data in a commercial context is **contract law**, since this is the branch of the legal system where the autonomy of private entities ("private autonomy") is expressed most explicitly. At the same time, there is a general presumption that freely negotiated agreements – except in cases of market failure – achieve an efficient allocation of resources and thus increase the general level of prosperity.

Unfair and inefficient contractual arrangements may arise, however, as a result of imbalances of power and information asymmetry; for example, certain issues relating to data access are typically underestimated during the negotiation process, with the result that they are skimmed over or omitted entirely. Given the dynamic nature of data-specific interests and the correspondingly dynamic assessment of data rights and data obligations (→ see section 2.1 above), it is often difficult for parties to determine what exactly a data access regime should look like in order for it to remain fair and efficient for the entire term of the contract. In a not insignificant number of cases, it is accordingly found at a later date – after the contract has been put to the test in the real world – that the balance of interests has shifted in unpredictable ways to benefit one or the other party, with a major impact on the equilibrium of rights and obligations that was originally agreed. Since one of the parties typically stands to benefit from the new state of affairs, contracts are often not renegotiated, and so there is no opportunity to regulate data access properly and efficiently.

Particularly in complex value creation systems, there is frequently **no direct contractual relationship** between the party requesting access and the party that effectively controls the data (because there is an interposing link in the distribution chain, for example); in the interests of fairness and efficiency, however, data access arrangements would be desirable. In the B2B sector, incursions into freedom of contract in the form of an obligation to contract currently result almost exclusively from the provisions of anti-trust law, as well as a small number of general provisions of law in the case of essential commodities and monopoly positions; generally speaking, however, they are restricted to a small number of extreme situations.

5.3.2 Presence of a contractual relationship

In the estimation of the Data Ethics Commission, the steps that should initially be taken with a view to ensuring fair and efficient data access arrangements include **raising awareness and promoting digital skills** (→ see section 5.2.1 above), practical support in the form of **model contracts** that provide for a fair distribution of data access, and **infrastructures and intermediaries** that facilitate shared data use while ensuring protection of trade secrets, for example (→ see section 5.2.2 above).

In cases where a contractual relationship already exists, the principles of fair data access can be enforced primarily through **contract interpretation** (including by way of gap-filling by the courts), for example by assuming the existence of appropriate contractual ancillary obligations, and through **standard contract terms control** pursuant to Section 307 of the Civil Code ("fairness test"). However, one of the problems inherent to substantive fairness tests is the virtual absence of default provisions that can be used as a benchmark for these tests. Specific abusive contractual practices could therefore be spelt out explicitly as **blacklisted contract terms** (→ see section 3.2.3 above for corresponding recommendations for B2C contracts). If significant changes occur since the conclusion of the contract it may be possible for a party to invoke the provisions on **frustration of contract** (Section 313 of the Civil Code).

In this connection, the Data Ethics Commission wishes to reiterate the **general basic principles governing business-to-government (B2G) data sharing** as formulated by the **European Commission** in its communication of April 2018 entitled "Towards a common European data space".[28] These basic principles provide for the following:

a) transparency regarding access rights and the purposes for using the data;

b) recognition that several parties have contributed to shared value creation;

c) respect for each other's commercial interests;

d) undistorted competition; and

e) minimised data lock-in.

Particularly with regard to repositories that potentially include personal data as well as non-personal data, consideration could also be given to expanding these principles to include a right to informational self-determination for data subjects and the principle of "do no harm".

28 European Commission: Towards a common European data space, COM(2018) 232 final, 25 April 2018, p. 10 (available at: *https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-232-F1-EN-MAIN-PART-1.PDF*).

5.3.3 Absence of a contractual relationship

Where there is no contractual relationship at all between participants in a value creation system, despite any support provided, neither the rules on the interpretation of contracts nor the substantive fairness tests for standard contract terms apply, and it is also impossible to rely on frustration. In the view of the Data Ethics Commission, however, the simple fact that the party requesting access has contributed to generation of the data means that a special legal relationship exists between this party and the party that effectively controls the data (→ see section 2.1 above); this is all the more true if the relationship exists within a value creation system that is primarily shaped by contracts. This special legal relationship may give rise to certain duties of a fiduciary nature, including a **duty to enter into negotiations about fair and efficient data access arrangements**. The future legal framework should make explicit reference to this fact.

The Data Ethics Commission therefore recommends **amending Section 311 of the Civil Code** to include a new subparagraph mentioning the special relationship that exists between participants in a value creation system (e.g. as suppliers, manufacturers, brokers or end users), which would entail certain relevant duties, including with regard to data. The enormous significance of data for general legal and economic relations means that there are justified grounds for inserting a subparagraph in the law rather than subsuming such relations under the general heading of "similar business contacts". This would neither constitute a separate legal basis for the processing of personal data, nor would it restrict data protection law in any way.

Beyond this, consideration could be given to introducing **data-specific rules in the law of obligations** based on the principles referred to above (→ in section 2), aimed at judicial "gap-filling" and for use as a benchmark when carrying out substantive fairness tests on standard contract terms.[29] In particular, provisions for data contracts of this kind might define the conditions under which parties are entitled to access data and/or to request desistance from data access or data use and/or to request the rectification of data. However, the Data Ethics Commission was also concerned that, if such rules were specifically spelt out in the law (albeit as default rules only) this might give rise to additional disputes.

5.3.4 Sector-specific data access rights

If a need is identified for more extensive data access rights within existing value creation systems, priority should be given to sector-specific solutions. The Data Ethics Commission therefore recommends that the Federal Government should pay greater attention to data access issues when adopting and/or revising sector-specific regulations.

29 For a discussion of personal data, see Louisa Specht: Datenrechte – Eine Rechts- und Sozialwissenschaftliche Analyse im Vergleich Deutschland – USA, Teil 1: Rechtsvergleichende Analyse des zivilrechtlichen Umgangs mit Daten in den Rechtsordnungen Deutschlands und der USA, ABIDA-Gutachten [Data rights, an analysis from the perspective of the legal and social sciences based on a comparison between Germany and the USA, Part 1: Comparative law analysis of data governance under civil law within the framework of the German and US legal systems], 2017, pp. 89 et seqq. (available at: *http://www.abida.de/sites/default/files/ABIDA_Gutachten_Datenrechte.pdf*); for a discussion of non-personal data, see ALI-ELI Principles for a Data Economy (above, footnote 1).

5.4 Open data in the public sector

5.4.1 Preliminary considerations

The recently revised Directive (EU) 2019/1024 on open data and the re-use of public sector information (PSI Directive) and (at national level) the [German] Information Reuse Act (*Informationsweiterverwendungsgesetz*, IWG), the [German] E-Government Act (*E-Government-Gesetz*, EGovG) and additional special acts provide a sound legislative basis for the disclosure of public-sector data on the basis of OGD concepts. The premise underlying the concept of open government data is that citizens and companies have already subsidised the generation of the data **through the taxes they pay**, and should therefore be allowed to share in the associated benefits rather than incurring a double financial burden. Making public-sector data available for reuse by the private sector also benefits the European data economy; since open government data often hold **enormous potential for private-sector value creation**, companies can use them to develop new and innovative products and services, helping to increase the general level of prosperity in the process.

Looking beyond the economy, access to government data is also vitally important for **democracy and an open debate involving all of society**, since it increases administrative transparency, facilitates participation and allows oversight and fact-based discussions. Open government data can also be used in many different shapes and forms for social initiatives and innovations (for social or ecological purposes, for example).

As a basic principle, therefore, the Data Ethics Commission supports the **Open Data Charter** adopted at the G8 Summit in 2013, which defines the following as central principles for the governance of administrative data:

a) open by default (the expectation that administrative data will be made public without compromising the right to privacy);

b) quality and quantity (high-quality, timely and fully described open data);

c) usable by anyone (as much data as possible, in as many open formats as possible);

d) improved governance through open data (transparency and sharing of expertise regarding data collection, standards and publication procedures);

e) innovation (user consultations and support for future generations of creative minds).

Ethically speaking, if a government body decided to provide commercial operators with free-of-charge access to its data instead of selling them for a profit or otherwise exploiting them for economic purposes, this decision would need to be justified (on an approximated basis) by corresponding **increases in prosperity** at the macrosocial level.

The Data Ethics Commission also wishes to draw attention to a degree of tension between calls for privacy by default on the one hand and open by default on the other, and – in a broader sense – between the **debate on data protection** and the **debate on open government data**. If personal data are made public in a legally compliant manner on the basis of open-data concepts, there is no guarantee that the security mechanisms put in place to protect the right to informational self-determination (in the form of explicit or implicit restrictions on reuse or in the form of technical and organisational protection measures) will continue to be applied. The general provisions of data protection law concerning reuse can also be an issue. Furthermore, since Article 30 GDPR requires only the "categories of recipients" to be documented, and government bodies are almost never in a position to monitor compliance with the "appropriate safeguards" required pursuant to Article 89 GDPR, the disclosure of data that are, or might at some point become, personal data can be regarded as a potentially high-risk measure for data subjects.

When applying OGD concepts in this area, the right to informational self-determination that is protected as a fundamental right must always be weighed up carefully against the public-good interests pursued under the OGD banner, the right to freedom of information (which is also protected as a fundamental right), and the freedom of OGD recipients to exercise a trade or profession. The Data Ethics Commission submits that, in cases of doubt, priority should be given to the **State's duty of protection**. Compliance with this duty is all the more important because individuals may not be able to decide freely which data they entrust to government bodies, or may be **particularly apt to believe** that government bodies will refrain from forwarding personal data to third parties.

5.4.2 Legal framework and infrastructures

The Data Ethics Commission welcomes the Federal Government's National Action Plan to implement the G8 Open Data Charter and the efforts on the part of the Federal Government and the governments of the *Länder* to include OGD concepts when digitalising their administrations. It recommends that the Federal Government should take action to ensure across-the-board implementation of an **obligation to publish structured unprocessed data (open by default)** and to allow these data to be used without limitations and, in principle, free of charge, which already applies to the direct federal administration (Section 12a(1) E-Government Act). Given the aforementioned tension between open government data and data protection, the obligations imposed by Section 12a of the E-Government Act should only apply in relation to certain types of data (in particular those that have undergone effective anonymisation procedures).

The Data Ethics Commission welcomes the legislator's attempts to change the data governance culture within the administration, and acknowledges that this is a task made significantly more challenging by the **highly fragmented nature of the current legal situation**. It is often difficult – both for authorities and for potential OGD users – to forge a path through a tangled regulatory thicket made up of different legal regimes that set out general and specialised rules on access to data, reuse of data and e-governance at both Federal Government and *Land* level. A further complicating factor is the interplay between these regulations, data protection law and intellectual property rights (in particular copyright law), which is often fiendishly complex in practice. In this connection, the Data Ethics Commission recommends **merging** and **synchronising** the various legal bases that exist in Germany, as well as **clarifying** the demarcation lines between the various legal arrangements.

Another obstacle that stands in the way of the culture change that needs to take place is the fact that it is currently all but impossible to verify reliably whether the authorities are, in fact, complying with the data provision obligations already in force. For example, Section 12a(1) of the E-Government Act imposes an obligation on the direct federal administrative authorities to provide public access to data, but explicitly states that parties requesting access have **no enforceable right** to the data being made publicly available. Companies that wish to access data are therefore deprived of effective avenues for forcing the authorities to comply with the statutory obligation of making data open by default. In the view of the Data Ethics Commission, the introduction of a **right to request publication of data** might encourage a more proactive approach to the provision of open data on the part of the administrative authorities, within the limits placed on their obligation to do so by the E-Government Act and the Information Reuse Act.

The **quality standards** that must be achieved in respect of the data provided by government bodies are another question that is left open under the current legal situation. In particular, the E-Government Act states that the obligation to provide access to data can be met by handing over unprocessed data, but data can be reused easily and in a manner that complies with the OGD objectives only if a high level of data quality is guaranteed.

Aside from the legal framework, establishment or expansion of an **infrastructure framework** (e. g. open government data portals such as GovData) is also essential, particularly at local level (e. g. in the form of municipal platforms), and the same applies to investments in appropriate quality assurance tools.

5.4.3 The State's duty of protection

Keeping in mind the State's duty to protect all of the data entrusted to it, **appropriate precautions** must be taken to ensure that central interests of private individuals (e. g. those relating to personal data, operating and trade secrets or other sensitive data, such as confidential information relating to public procurement procedures) are given the same comprehensive level of protection as key public interests (e. g. security interests or interests relating to national sovereignty). The ethical premise underpinning the OGD concept – that citizens and companies have already paid for the data through their tax contributions – places certain **constraints on reuse**. In particular, care must be taken to ensure that data are not used by the private sector to develop services and products that may ultimately restrict the freedom of citizens and businesses and/or be available only to them under unfair conditions.

The Data Ethics Commission therefore recommends that the Federal Government should make use of the opportunity afforded by Article 8 of the recast PSI Directive by developing **model conditions** for standard licences, including restricted-use agreements and conditions for the transfer of data to third parties; alternatively, it should lobby for such conditions to be introduced at European level. It may even be advisable to make these model conditions **mandatory**, at least on a sector-specific basis, and they should be based on a number of key considerations, including the following:

a) pursuant to Article 8(1) of the PSI Directive, the conditions must be objective, proportionate, non-discriminatory and justified on grounds of a public interest objective; they shall not unnecessarily restrict possibilities for re-use and shall not be used to restrict competition;

b) the rules imposed on companies should contain clearly defined safeguards for the rights of affected third-parties, and mechanisms that allow compliance with these rules to be verified;

c) any intellectual property developed using the data must not be used to disallow activities carried out by government bodies in the fulfilment of their public remit or to make these activities subject to payment of a licence fee;

d) any product or service developed using the data should be offered to government bodies under preferential conditions;

e) companies with a large market share should be subject to a reciprocal obligation to make data generated by their operations available (under identical conditions);

f) the data should be used only for business activities that take place in the EU (or at a minimum for product or service development processes that take place in the EU).

As a basic principle, compliance with the agreed safeguards and restrictions on use can no longer be reliably verified once data have been transferred and once the copies of the data sent to the recipient have been stored on infrastructure controlled by the latter. Given the duty incumbent upon government bodies to protect data that may be used to harm third parties or the public (even if such harm would be possible only after de-anonymisation of the data or linking of the data with other data sets), special consideration must be given to a model under which government bodies allow only supervised data access and **supervised processing** of data on infrastructures that they control. Any costs incurred in this connection should be passed on to the companies seeking access.

5.5 Open data in the private sector

5.5.1 Platforms and data use

Operating data are generated by companies at all levels of the German economy in the course of their everyday business, and these data are enormously valuable for innovation, particularly when combined with data generated by other participants in the value creation chain. The German economy has already established sector-specific platforms for the express purpose of linking these different types of data.

Examples of different platform models include: (1) merger of several different companies into a GmbH (limited liability company); (2) in-house operation by a single company with the involvement of partners; (3) proprietary platform operated as a service for third parties.

The various sectors of the economy are increasingly coming around to the idea not only of shared platforms, but also of common regulatory approaches to data use.

The Data Ethics Commission believes that it is reasonable to assume that data use within value creation systems will continue to be organised by industrial players themselves on a sector-specific basis, and that new market entrants and start-ups will continue to find opportunities to innovate within this landscape, since market participants themselves stand to benefit from working together with trailblazing start-ups to develop disruptive digital innovations, and from sharing their data to this end. The trend for companies to club together to establish platforms modelled along various lines should be welcomed, as it allows them to build on the industrial know-how that already exists in Europe and fosters higher-quality data use (including higher standards of data protection and information security). The Data Ethics Commission proposes that the Federal Government should lend its support to the emergence of an increasing number of **private-sector platforms**, with a view to achieving the necessary market size and effects of scale and allowing German businesses to harness their shared strength to compete on the international stage.

5.5.2 Additional incentives for voluntary data sharing

There is already a large number of business models based on private providers voluntarily allowing the public to access their data.

Example 14

Example 14 One case in point is the geoinformation industries, which take basic geodata (in some cases from official sources) and enrich them with other information, allowing users to access specialist geodata for a wide range of purposes. Examples include both map services such as OpenStreetMap or Google Maps, which feature not only purely topographical and administrative information but also a wide range of other interesting details, and also tailored offerings such as weather forecasts or traffic predictions.

The Data Ethics Commission recommends that voluntary data access arrangements of this kind should be supported; in addition to the **practical support measures** recommended in → section 5.2 above, consideration should therefore be given to **additional incentives** for voluntary data sharing. For example, data transfers or releases and open access strategies should be favourably viewed:

- under tax legislation;
- under procurement law;
- when making grant awards (either inside or outside the research sector); or
- when carrying out authorisation procedures.

Voluntary data sharing, data transfers or releases and open access strategies should, however, be envisaged in the fields referred to above only if there is no risk of infringing confidentiality requirements under procurement law, operating and trade secrets, or the provisions of data protection law as a result.

5.5.3 Statutory data access rights

By way of contrast to the debate on voluntary data sharing, the main idea underpinning the discussion on statutory data access rights is that a society should "get something back" from the large repositories of data that many members of that society have helped to build up (in the case of social networks, for example). When viewed in conjunction with the fundamental value of social solidarity and the public-good interests that may be relevant in specific cases, this concept could serve as a basis for granting more extensive rights in respect of **data access and disclosure obligation**s on the part of private individuals.[30]

One potential measure that is often discussed in the context of improving general access to privately held data repositories is the introduction of a **general right to portability** for non-personal data, modelled along the lines of Article 20 GDPR. This would mean that a business that has supplied raw data to a controller would have a right to request the controller to make the data available to the business in a commonly used and machine-readable format, or to ask the controller to forward them directly to a third party. For reasons that are essentially similar to those cited in its arguments against an extension to the scope of Article 20 GDPR (→ section 4.4.2 above), the Data Ethics Commission recommends that the Federal Government should initially adopt a **"wait-and-see" approach** to developments relating to the **use and interpretation of Article 20 GDPR**. The complexity of this issue is exacerbated yet further by the fact that the issue of proper allocation of the portability right (i.e. who is the equivalent to the "data subject" with regard to non-personal data) would raise its head again.

A range of other measures that are ultimately synonymous with statutory data access rights are also being discussed with a view to improving general access to privately held data repositories. **Potential options** in this respect include a statutory obligation to publish reports containing internal data analytics, access rights for private individuals (e.g. mandatory licensing that complies with the FRAND[31] principles and/or incorporates the three-factor or four-factor test under copyright law[32]), or the disclosure of data to the general public (open access) based on either a general model or a market-share model.

The Data Ethics Commission believes that at least the following factors should be taken into account during an initial examination of these options:

30 For further details, see Viktor Mayer-Schönberger / Thomas Ramge: Das Digital [english title: Reinventing Capitalism in the Age of Big Data], pp. 195 et seqq.
31 FRAND = Fair, Reasonable and Non-Discriminatory.
32 The "three-factor test" features in several international agreements as a basis for assessing whether an exemption (i.e. a limitation on copyright) represents an acceptable encroachment on the copyright holder's rights. According to the test, exemptions of this kind are subject to three conditions: (i) they may apply only to certain special cases; (ii) they may not be in conflict with normal exploitation; and (iii) they may not unreasonably prejudice the legitimate interests of the right holder. Calls are increasingly being made for the test to include (iv) mandatory consideration of third-party interests and general interests.

a) the need to protect the personal data or the operating and trade secrets to which access may be given or which may be disclosed;

b) the need to ensure that any encroachment on the fundamental rights of private entities affected by a data access or disclosure obligation is proportionate; this relates in particular to the freedom to exercise a trade or profession;

c) the need to avoid any negative impacts on competition resulting from access to data or the disclosure of data, for example owing to strategic use by competitors that may not themselves be obliged to disclose data in return;

d) the need to ensure that incentives still exist to invest in business models for the data economy; and

e) the need to protect the strategic interests of German or European companies in the face of global competition; in particular, consideration must be given to whether these companies would still be able to compete effectively on the international stage if they were forced to provide access to their data repositories and the digital giants – which already stand head and shoulders over other companies in terms of their data proficiency, their data infrastructures and (in particular) the volumes of data they hold – were to exploit this open-door policy.

Having regard to the above, the Data Ethics Commission recommends that preference should be given to a **sector-specific approach**. As far as spatial information is concerned, the INSPIRE Directive and the provisions transposing it into national law already set out sector-specific data access rules; these rules apply only to government bodies, however. One of the first private-enterprise applications of an sector-specific data access right can be found in the payment services industry, and the Data Ethics Commission proposes that steps should be taken to identify the level of demand and implementation options in a number of other selected industries, for example the **media, mobility or energy sectors**.

5.5.4 Role of competition law

Although the framework of competition law that is currently in place contains almost no provisions relating to data, its general thrust also applies to the data economy. For example, the **essential facilities doctrine** (EFD) can be used (in a slightly modified form if necessary) if a market-dominant company holds exclusive control over a resource (e.g. a network/infrastructure) that is crucially important for competition on a neighbouring market. The **aftermarket doctrine** relates to cases in which lock-in effects mean that consumers of a primary product are unable to exercise in full their freedom to choose on a secondary market (e.g. market for repairs/spare parts), or in which a third-party provider on a secondary market of this kind faces anti-competitive barriers.[33] Yet the uncertain legal situation, the stringent requirements that apply, and the amount of time and money involved in the relevant procedures means that supervisory efforts to prevent abuse cannot currently be regarded as a fix-all solution to data access problems. The applicable provisions of competition law (either individually or in their entirety) could, however, act as a central building block in a new framework of **digital economic law**, one of the crucial components in which should be a range of solutions to data access problems. The findings of the Commission of Experts on Competition Law 4.0 should be taken into account in this respect.[34]

33 Jacques Crémer / Yves-Alexandre de Montjoye / Heike Schweitzer: Competition policy for the digital era, Special Advisers' Report for the European Commission, pp. 87 et seqq. (available at: *https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf*).

34 A New Competition Framework for the Digital Economy, Report by the Commission 'Competition Law 4.0', September 2019 (available at: *https://www.wettbewerbsrecht-40.de/KW40/Redaktion/DE/Downloads/a-new-competition-framework-for-the-digital-economy_.pdf?__blob=publicationFile&v=3*).

5.6 Data access for public-sector (B2G) and public-interest purposes

Thought should be given to whether controllers should be subject to an obligation to grant access to specific subsets of data in order to allow their use either by **public-sector bodies** or for certain **public-good purposes**, and the scope of any such obligation. Rights to access data belonging to private entities or obligations to disclose data might be particularly relevant in the **research** sector, and easier access to data might lead to general advances in science, provided that the access arrangements are designed appropriately and take due account of data subjects' rights. Corresponding access rights to private-sector data might also make it easier for NGOs, the media and similar institutions to deliver on their social remit, thereby helping to protect the **democratic polity**. Particularly priority must also be given at all times to the **averting of risks** (e. g. issuing storm warnings).

In the view of the Data Ethics Commission, preference should again be given to a **sector-specific approach** that tailors the design of data access and disclosure obligations to the specific requirements of constitutional law that come into play on the one hand, and to the practical circumstances that characterise the relevant sphere of activity on the other. The **health sector**, the **mobility sector** and the **energy sector** should be regarded as particular priorities for action in this respect. The Data Ethics Commission also calls for a broad-based, society-wide debate as a precursor to decisions on more general obligations to provide access to data, e. g. in connection with research projects that serve the public good.

The Data Ethics Commission wishes to reiterate the **basic principles governing business-to-government (B2G) data sharing** set out by the European Commission in its communication of 25 April 2018 entitled "Towards a common European data space":[35]

a) proportionality (i. e. justified by clear and demonstrable public interest and proportionate in terms of details, relevance and data protection);

b) purpose limitation (i. e. clearly limited for one or several purposes and assurances that the data obtained will not be used for unrelated administrative or judicial procedures);

c) "do no harm" (i. e. respect for legitimate interests such as data subjects' right to informational self-determination, trade secrets, commercially sensitive information and exploitation interests);

d) acknowledgement of the public interest goal when agreeing on conditions for data reuse (preferential treatment for government bodies, non-discriminatory conditions for government bodies, reduction in the overall burden on citizens and companies);

e) data quality management (an obligation to offer reasonable and proportionate support to help assess the quality of the data for the stated purposes, but no general obligation to improve the quality of the data);

f) transparency and societal participation in respect of parties to the agreement, their objectives, insights and best practices.

These basic principles may serve as a **good starting point** not only when drafting the provisions of freely negotiated contracts on data exchanges, but also when designing more extensive sector-specific statutory measures to improve data access.

35 European Commission: Towards a common European data space, COM(2018) 232 final, 25 April 2018, pp. 13 et seq. (available at: *https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-232-F1-EN-MAIN-PART-1.PDF*).

Summary of the most important recommendations for action

Debates around access to non-personal data

24

Access by European companies to appropriate non-personal data of appropriate quality is a key factor for the growth of the European data economy. In order to benefit from enhanced **access to data**, however, stakeholders must have a sufficient degree of data-awareness and have the data skills that are necessary to make use of the data. Also, access to data proves to be disproportionately advantageous to stakeholders that have already built up the largest reserves of data and that have the best data infrastructures at hand. The Data Ethics Commission therefore wishes to stress that the factors referred to should always receive due attention when discussing whether and how to improve data access, in keeping with the **ASISA principle** *(Awareness – Skills – Infrastructures – Stocks – Access)*.

25

The Data Ethics Commission therefore supports the efforts already initiated at European level to promote and improve **data infrastructures** in the broadest sense of the term (e.g. platforms, standards for application programming interfaces and other elements, model contracts, EU Support Centre), and recommends to the Federal Government that these efforts should continue to be matched by corresponding efforts at national level. It would also be advisable to set up an ombudsman's office at federal level to provide assistance and support in relation to the negotiation of data access agreements and dispute settlement.

26

The Data Ethics Commission ascribes enormous importance to a holistically conceived, sustainable and strategic **economic policy** that outlines effective methods of preventing not only the exodus of innovative European companies or their acquisition by third-country companies, but also an excessive dependence on third-country infrastructures (e.g. server capacities). A balance must be struck in this context between much-needed international cooperation and networking on the one hand, and on the other a resolute assumption of responsibility for sustainable security and prosperity in Europe against the backdrop of an ever-evolving global power dynamic.

27

Also from the perspective of boosting the European data economy, the Data Ethics Commission does not see any benefit in introducing new exclusive rights ("data ownership", "data producer right"). Instead, it recommends affording **limited third-party effects to contractual agreements** (e.g. to restrictions on data utilisation and onward transfer of data by a recipient). These third-party effects could be modelled on the new European regime for the protection of trade secrets. The Data Ethics Commission also recommends the adoption of legislative solutions enabling European companies to cooperate in their use of data, for example by using data trust schemes, without running afoul of anti-trust law (**"data partnerships"**).

28

The data accumulated in existing value creation systems (e.g. production and distribution chains) are often of enormous commercial significance, both inside and outside that value creation system. In many cases, however, the provisions on data access that appear in the contractual agreements concluded within a value creation system are unfair and/or inefficient, or lacking entirely; in certain cases, there is no contractual agreement at all. Efforts must therefore be made to **raise awareness among businesses** in sectors far outside what is commonly perceived as the "data economy", and to provide practical guidance and support (e.g. model contracts).

29

The Data Ethics Commission furthermore recommends cautious **adaptations of the current legislative framework**. The first stage in this process should be to make explicit reference in Section 311 of the [German] Civil Code (*Bürgerliches Gesetzbuch*, BGB) to the special relationship that exists between a party that has contributed to the generation of data in a value creation system and the controller of the data, clarifying that such parties may have certain quasi-contractual duties of a fiduciary nature. These duties should normally include a duty to enter into negotiations about fair and efficient data access arrangements. Consideration should also be given to whether additional steps should be taken, which could range from blacklisting particular contract terms also for B2B transactions, to formulating default provisions for data contracts, to introducing sector-specific data access rights.

30

The Data Ethics Commission believes that **open government data (OGD) concepts** hold enormous potential, and recommends that these concepts should be built on and promoted. It also recommends a series of measures to promote a **shift in mindset among public authorities** (something that has not yet fully taken place) and to make it easier in practice to share data on the basis of OGD concepts. These measures include not only the establishment of the relevant **infrastructures** (e.g. platforms), but also harmonisation and improvement of the existing **legal framework** that is currently fragmented and sometimes inconsistent.

31

Nevertheless, the Data Ethics Commission identifies a degree of tension between efforts to promote OGD (relying on principles such as "open by default" and "open for all purposes"), and efforts to enhance data protection and the protection of trade secrets (with legally enshrined concepts such as "privacy by default"). The Data Ethics Commission submits that, in cases of doubt, **priority should be given to the duty of protecting** individuals and companies who have entrusted their data to the State (often without being given any choice in the matter, e.g. tax information). The State must deliver on this duty by implementing a range of different measures, which may include technical as well as legal safeguards against misuse of data.

32

In particular, it would be beneficial to develop **standard licences and model terms and conditions** for public-sector data sharing arrangements, and to make their use mandatory (at least on a sector-specific basis). These standard licenses and model terms and conditions should include clearly defined safeguards for the rights of third parties who are affected by a data access arrangement. Provision should also be made against data being used in a way that ultimately harms public interests, and also against still greater accumulation of data and market power on the part of the big players (which would be likely to undermine competition) and against the taxpayer having to pay twice.

33

As regards **open-data concepts in the private sector**, priority should be given to **promoting and supporting voluntary data-sharing arrangements**. Consideration must be given not only to the improvement of infrastructures (e.g. data platforms), but also to a broad range of potential incentives; these might include certain privileges in the context of tax breaks, public procurement, funding programmes or licensing procedures. Statutory data access rights and corresponding obligations to grant access should be considered as fall-back options if the above measures fail to deliver the desired outcomes.

34

Generally speaking, the Data Ethics Commission believes that a cautious approach should be taken to the introduction of statutory data access rights; ideally such rights should be developed only on a **sector-by-sector basis**. Sectors in which the level of demand should be analysed include the media, mobility or energy sectors. In any case, before a statutory data access right or even a disclosure obligation is introduced, a full impact assessment needs to be carried out, examining and weighing up against each other all possible implications; these include implications for data protection and the protection of trade secrets, for investment decisions and the distribution of market power, as well as for the strategic interests of German and European companies compared to those of companies in third countries.

35

The Data Ethics Commission recommends considering enhanced obligations of private enterprises to grant access to data **for public interest and public-sector purposes** (business-to-government, B2G). A cautious and sector-specific approach is, however, recommended in this respect as well.

Part F

Algorithmic systems

1. Characteristics of algorithmic systems

Numerous products and applications these days, from voice assistants and automated lending right through to "autonomous" (driverless) cars, are based on more or less "smart" algorithms. Due to the many different forms that these types of technical systems can take, it seemed advisable to the Data Ethics Commission to base the considerations on the **general concept of "algorithmic systems"**. (→ see Part C, section 2.2.5 above). The key questions presented by the Federal Government regarding the topics of "algorithmic prognosis and decision-making processes" as well as "artificial intelligence" will therefore be discussed below together as questions concerning the use of algorithmic systems.

However, the **following distinctions** in particular must be taken into account as part of any ethical and legal **assessment of individual algorithmic systems**:

- From a **technical perspective**, different algorithmic systems have different characteristics. The spectrum ranges from systems which operate on a completely deterministic basis right through to systems which use machine learning to develop action plans independently in order to achieve the goal specified by the operator of the algorithmic system.

- Where algorithmic systems are used as social informatics systems, ethically and legally relevant processes can be established at **different system levels**, i. e. from the level of the pool of data used or the algorithm in the technical sense right through to the level of human individuals involved in the development, implementation, assessment or correction of the system.

- **The purpose and consequences** of using algorithmic systems can vary considerably. Where algorithmic systems support or replace human decision-making and prognoses, they often have a direct impact on individuals' rights and interests. Examples include automated lending and automated administrative acts. However, algorithmic systems are also used where such a link to human decision-making can, at most, be indirectly established. This is the case, for example, with various processes which constitute "autonomous" driving or with predictive maintenance in mechanical engineering.

- Algorithmic systems affect different **ethical and legal principles** depending on the context in which they are used. As such, the externally visible and discernible "action" of "autonomous" cyber-physical systems, for example, typically raises questions. This is a key aspect, for example, in the debate surrounding the use of robotics in healthcare. Principles such as that of human-centred design are essential for the assessment of such systems. Where algorithmic systems are not "physically embodied" in a similar way, it is conversely often the system's externally invisible method for making the "decision" that is the focus of attention. Discussions may, for example, centre on the system's transparency or the principle that the final decision should be made by a human in accordance with Article 22 GDPR. An example of this is automated credit checks. However, the distinction between "action"-oriented and "decision"-oriented perspectives becomes relative upon closer inspection, because every visible "action" by a system is, at some point, preceded by a human "decision", for example in the construction of the system, and every "decision" has an impact because another system component (including a human) will base its "action" on it.

The Data Ethics Commission believes that **further distinctions** should be made in particular where algorithmic systems are closely involved in human **decision-making processes**. An algorithm itself cannot make a decision in an ethically substantial sense, since it has no value-based preferences of its own accord. Three different levels of the involvement of algorithmic systems in human decision-making can be distinguished based on the specific distribution of tasks between humans and machine:

- **Algorithm-*based*** decisions are human decisions based either in whole or in part on information obtained using algorithmic calculations. Examples include clinical decision support systems which provide a doctor with treatment recommendations using patient data from electronic medical records and based on an assessment of scientific literature. Taking this recommendation into consideration, the doctor then makes the decision together with the patient as to which treatment option should ultimately be selected. Algorithm-based decisions can nevertheless subtly yet significantly influence human decisions, for example if the algorithmic system collates information on humans/objects/procedures which contain a value judgment of which the user may not necessarily be aware.

- **Algorithm-*driven*** decisions are human decisions shaped by the outputs of algorithmic systems in such a way that the human's decision-making abilities and capacity for self-determination are effectively restricted, in particular because the decision can be made only within algorithmically determined and prescribed paths. One such example is an Industry 4.0 application whereby, as part of human-machine interaction, a robotic system provides the human involved in the production process with only limited room for manoeuvre.

- **Algorithm-*determined* and hence fully automated** decisions are, prima facie, made independently of a human. In fact, the outputs of an algorithmic system trigger consequences automatically; no provision is made for an explicit human decision. Examples of applications range from price differentiations in e-commerce and fully automated administrative acts up to what are known as autonomous weapons systems. Human decisions are nevertheless involved in the sense that a human must have decided to use the algorithmic system for such a purpose and in such a way.

Example 1

The differences can be illustrated by an algorithmic system being used in the process of selecting candidates for a job: if an algorithmic system simply collates information on the individual candidates for the employer in question on the basis of which the employer will then make their decisions, this constitutes an algorithm-based decision-making process. The system will lead to algorithm-driven decisions if the information provided to the employer contains an evaluation of the individual candidates (for example a ranking), as this could significantly influence the likelihood of the individual candidates being selected. The actual restriction of the employer's ability to make decisions becomes even more apparent if the system already screens the candidates in advance, meaning that the employer no longer even sees some of the applications. In the case of an algorithm-determined selection process, each notification regarding the acceptance or rejection of an application would be automatically provided by the algorithmic system without a human ever checking the selection.

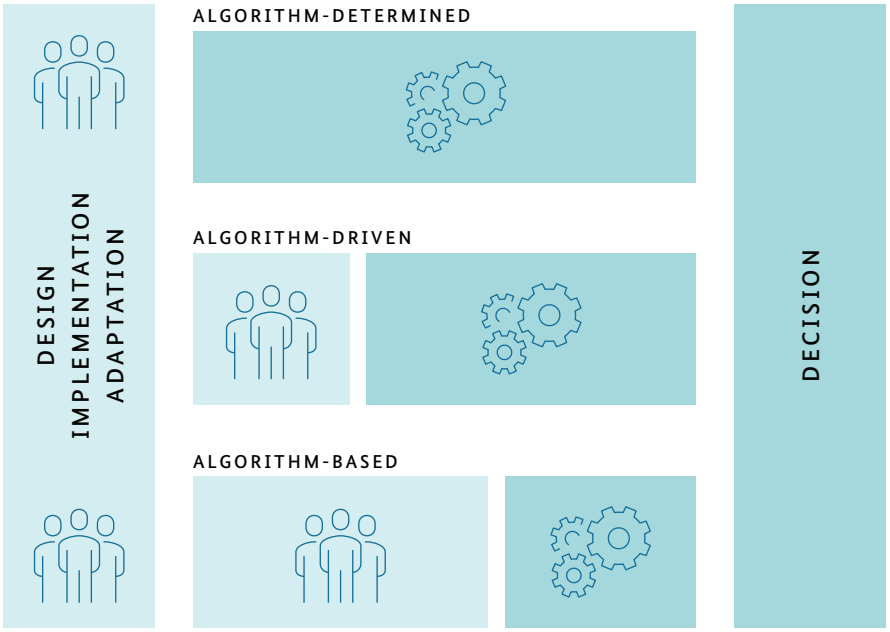


Figure 7:
Characteristics of algorithmic systems

Classifying an algorithmic system as one of these three types is often difficult, and **hybrids** are possible within complex software architecture. The level of determination for humans at the same point can also be different depending on the way the system works: in the example above, a decision-making process in which an algorithmic system filters out individual candidates in advance and rejects them is algorithm-determined from the point of view of the candidates who were filtered out but algorithm-driven for all the remaining candidates.

There can be **overlaps** in the practical operation of the systems on account of what are known as **automation bias and default effects**. Even in the case of algorithm-based decisions where humans have full decision-making authority, they may tend to simply go with the algorithmic system's recommendation without carrying out a sufficiently critical check, as otherwise they would feel an uncomfortable need to justify their decision and would get the impression that the risk of being blamed for any wrong decision would increase. Nevertheless, the fundamental distinction is relevant for assigning responsibility for a risk assessment and therefore also for regulation.

2. General standards for algorithmic systems

General ethical and legal principles, primarily human dignity (→ see Part B, section 3 above), constitute the benchmark for the design and use of algorithmic systems. In terms of the **principle of prospective responsibility**, the intentional and unintentional effects on the users and the individuals affected by the use of an algorithmic system must be taken into consideration as part of the assessment of specific algorithmic systems. It is also necessary to think about and plan for social consequences depending on the intended purpose and context of their use, especially with regard to network effects, effects of scale and effects of scope. These consequences range from the positive effects of social innovations right through to the (sometimes subtle) negative effects, for example on diversity and the culture of social debate as an essential condition for a functioning democracy. On that basis, the Data Ethics Commission believes that the following key requirements for the design and use of algorithmic systems can be set out which, in terms of the **governance perspective** taken up here, must be met in the interplay of, especially, developers, companies, users and state bodies.

2.1 Human-centred design

At the centre is the requirement to strive for algorithmic systems with a **human-centred and value-oriented design** which takes fundamental rights and freedoms into consideration. The Data Ethics Commission believes that the human-centred approach must permeate the entire design process. It must be ensured by means of a wide range of different measures, which may also and in particular involve i**nclusion and participation in the development** of algorithmic systems.

Human-centred design requires in particular taking into account changes in self-perception and self-design resulting from the individual's confrontation with algorithmic systems. Gains and losses in expertise in using the systems, effects on people's own lifestyles and the formation of opinions as well as on physical well-being must be taken into consideration as early as in the system development stage.

Attention should also be paid to the **emotional state** of the affected individuals which may differ (in both directions) depending on whether humans and conventional technology or algorithmic systems are used. This is significant not only for the individual affected by a decision but also for the user. Consideration should be given for example to the fact that direct interpersonal interaction fulfils a variety of functions which go far beyond "good decision-making".

Example 2
Where medical diagnoses are supported by algorithmic systems, the accuracy of diagnosis can be identified first and foremost as the intended purpose. However, the need for human care and contact in consultations concerning treatment (with corresponding significance for the success of the treatment) can be strong and must not be disregarded, nor should the need for doctors to be able to contribute their own medical experience. Conversely, in certain situations, for example in case of embarrassing symptoms, they may find it more comfortable not to have to confide primarily in another human person.

These functions include, for example, the satisfaction of a basic human need for **communication**, the feeling, in principle, of being able to assess the other person's line of thinking and reactions and to be understood by the other person, the opportunity to convince the other person of one's own point of view, as well as the certain control effect arising from the fact that the other human being is directly confronted with the reaction of the individual affected by the decision.

Example 3
Emotional aspects also play a major role where algorithmic systems are used in human-machine interaction. For example, the use of a system which is intrinsically intended to support employees may be perceived by the employees to be invasive or patronising, since the system analyses employees' behaviour, takes certain tasks off their hands which they have actually come to enjoy or makes them think that their own performance is inferior to that of their "robotic colleague".

The well-being of all individuals affected by technology, including for example in the use of robotics in nursing, is a central guiding value which absolutely must be taken into consideration as part of an ethical approach to technology design. It is important to note here that well-being is extremely subjective and not static but can change depending on the context and over time and therefore needs to be **constantly reassessed**.

2.2 Compatibility with core societal values

Depending on their area of application, the impacts of algorithmic systems may be relevant for society as a whole: for example they may affect the **democratic process**, **citizen-centred state action**, **competition**, the **future of work** and also the **digital sovereignty** of Germany and Europe.

Example 4
In the development of smart systems, providers which are able to build their business model on large amounts of data have a privileged starting position, since many applications of algorithmic systems depend on such amounts of data. The more data that can be analysed, the more likely correlations and findings are to be generated. Taken together with the network effects, effects of scale and effects of scope which are typical for platform markets, the market power of companies begins to strengthen and monopolies are formed, once a certain threshold is reached. This ultimately enables companies to prevent new players from entering the market and to interfere with the market-regulating forces of competition. Depending on the area of application, companies can then control social opinion-forming processes and market behaviour. In order to counteract that and create framework conditions for fair competition, the competition law control mechanisms must be readjusted and, where necessary, subsequently tightened.

The Data Ethics Commission is of the view that these supra-individual consequences often cannot be handled by state bodies or with legislative measures alone. Instead, they need to be taken into consideration in all phases of the design and use of algorithmic systems. **To that extent, developers, companies and users have a (shared) social responsibility.** In particular where corresponding consequences seem likely, for example in the case of algorithmic systems which affect communication between people which is relevant to democracy, it is necessary already in the design process to thoroughly assess the purposes and the unintended indirect consequences of the system in question and to examine the extent to which the system can affect democracy, fundamental rights, secondary law and the basic principles of the rule of law. As far as possible, a culture of "incorporating" the basic principles of democracy, the rule of law and fundamental rights into the system architecture should be established for the process of designing technology.

Many aspects of the interplay between technology and society are admittedly still unclear. The Data Ethics Commission believes that more research is therefore necessary to shed light on the social impacts of algorithmic systems and develop corresponding strategies to limit any negative effects.

2.3 Sustainability in the design and use of algorithmic systems

Any assessment of the personal and social effects of algorithmic systems must also be global in nature and not limited with regard to time. For this reason, when deciding on the use and design of algorithmic systems, **sustainability** and **human skills retention** in particular must also be taken into consideration. These are important for remaining human control functions (e.g. the "human-in-the-loop" principle), for the failure of algorithmic systems in exceptional circumstances (e.g. in the event of a disaster or cyber attacks) and for ensuring the innovative prowess of future generations (e.g. development of new digital technologies). It is, first and foremost, a question of basic and advanced training, as well as education in the sense of lifelong learning, ensuring that future generations also have the necessary general skills and not limiting training only to the user's perspective.

Teaching and developing digital skills also promotes **social sustainability**. Social framework conditions, for example in institutions and procedures, must be organised in such a way as to ensure the promotion of the participatory and inclusive design of algorithmic systems and their use to serve the public interest.

Sustainable development also includes the **ecological dimension**. Irrespective of the positive contribution which algorithmic systems can make to environmental protection, a key ethical requirement is reducing the need for electricity and for certain resources such as "rare earths" and using them efficiently.

Economic sustainability requires a perspective which looks beyond exclusively short-term economic profits and also takes the long-term effects into consideration. Short-term commercial success can have long-term disastrous consequences, as demonstrated by the global financial crisis several years ago. This should not limit the freedom of economic activity but should focus attention on the responsibility associated with economic activity within the context of a social market economy.

The principle of prospective responsibility as well as considerations of fairness and solidarity must, with regard to sustainability, be specifically taken into consideration in the design and use of algorithmic systems. As is the case with the handling of data, the **risk assessment** is of crucial importance for ecological, economic and social sustainability in the design and use of algorithmic systems.

2.4 High level of quality and performance

Algorithmic systems must work well and reliably in order to achieve the goals pursued with their help. If the systems are also used to promote ethical aims, then technical and legal specifications, designed to **improve, further develop and safeguard the state of the art**, will take on an ethical quality. Where such systems support or replace human activities, they are deemed, irrespective of the intrinsic value of human activity, to be implementing ethical principles better than previously.

Example 5

Any ethically sound use of algorithmic systems in the healthcare sector firstly requires the technology to have the necessary medical quality, i.e. the accuracy of the assessment of findings, the accuracy of the diagnosis, the probability that the recommended treatment will be successful or the success rate of a medical intervention, etc. must, when the system is used, be at least as good as and (in view of the sensitive usage context) ideally better than if conventional technology and humans were used.

Quality and performance can be improved through a wide range of different measures. These include, for example, appropriate risk models, the, as inclusive and participatory as possible, development of standards, systemic management and control approaches, and process design which is aimed at the continuous improvement of the entire system. The role of humans who are part of an algorithmic system understood as a social-informatic ensemble (→ see section 1 above) must always be taken into consideration in this context. After all, a number of algorithmic systems still rely on input from critical experts to perform optimally. Quality-oriented system design therefore also includes mechanisms which help **enhance human capabilities** and prevent or counteract any reduction in skills and any critical ability and readiness to reflect, for example in connection with automation bias. Examples of productive interaction between humans and machines which is also designed to ensure skill retention can be found in algorithm-supported diagnostic imaging in the healthcare sector.

2.5 Guarantee of robustness and security

Algorithmic systems must be robust and secure, otherwise the legitimate goals they are used to pursue will not be achieved or will be achieved only at the expense of potential harm to ethically and legally protected rights and interests. From an ethical perspective, it can be said that robust and secure system design and appropriate system usage therefore affect the respective purposes of a system and the need to protect the data used by the system. As a result, the robustness and security requirements are not identical for all systems. The specific requirements can differ based on the **specific need for protection and the usage context**.

Example 6

Systems which are not robust or secure which are used in control systems can pose an immediate threat to people or the environment, for example if they control the emission of pollutants from industrial plants, control robots or steer autonomous (driverless) cars in traffic. A failure here could even cause harm to important legally protected rights such as life and limb. In order to prevent this, processes should be put in place to define the current state of the art, legal rules and regulations should be enacted which make it mandatory to follow the state of the art, and measures should be implemented which guarantee the effective enforcement of standards.

Robust and secure system design involves not only **securing the system** against external threats (e. g. by means of encryption or anonymisation, etc.), but also **protecting humans and the environment against any negative influences from the system** (in particular through a systematic risk management approach, e. g. on the basis of a risk assessment). It must also incorporate all phases of data processing and all technical and organisational components. Risks can arise not only in the technical design but also as a result of errors caused by human decisions taken when using algorithmic systems. As algorithmic systems and the way they are incorporated in an organisation's other information technology are not static, a **management system** is also required which checks and ensures the effectiveness of the measures in view of changing conditions, for example newly discovered risks.

2.6 Minimising bias and discrimination as a prerequisite for fair decisions

A key aim in regulating algorithmic systems is to ensure that the decision-making patterns upon which the algorithmic systems are based do not have any systematic distortions (bias) leading to discriminatory and unfair decisions. It should, first of all, be noted that biased, discriminatory and unfair decisions can also be found where conventional technology and humans are used. Conversely to prejudiced decisions of individual humans, algorithmic systems however bear the danger that using the system on a large scale will have a broad impact which individual human decision-makers could never cause. With that in mind, the discussion surrounding bias and discrimination by algorithmic systems should, in the view of the Data Ethics Commission, **also be seen as an opportunity** to detect existing problems in existing decision-making contexts and, in general, achieve better decision-making processes.

Example 7

An algorithmic system used to detect skin cancer was trained predominantly on patients with white skin, and so the probability of its correctly detecting skin cancer is therefore significantly higher in the case of patients with white skin than in the case of patients with different coloured skin. As a medical device, such a system would be permitted for use only on patients with white skin. The same effect would admittedly also be noted if a dermatologist did their training and practised as a clinical professional exclusively in a specific cultural environment. Ultimately, in both cases, steps would need to be taken to ensure that all patients, irrespective of their skin colour, receive proper medical care.

Even in cases where there is no direct intention to discriminate when developing algorithmic systems, discriminatory decisions may still be made, i. e. decisions which systematically put certain groups at an unfair disadvantage. In particular in the case of machine learning, the problem is rather that the systems learn models by using available data. The resulting predictions and recommendations **extrapolate the past into the future**, whereby existing social injustices can be obscured through incorporation into seemingly neutral technology, and potentially amplified.

Example 8

An algorithmic system used to assess applications for a managerial position was trained with data of managers who had proven themselves at the relevant company over the past few decades. Since predominantly male managers had been employed over the past few decades, the system, which was trained with this data set, consistently assesses male candidates as being better than equally qualified female candidates.

The keyword **bias** covers a **range of different types of systematic distortions** with a range of different causes. In the case of human decision-makers, both cognitive bias and social preconceptions, prejudices or stereotypes can negatively affect the decision-making process. In the case of algorithmic systems, bias can refer to the technical reproduction of those social preconceptions, prejudices or stereotypes. This reproduction can take place at various points primarily within the context of machine learning. Often, an insufficient level of representation or a low number of cases of a social group in the training data leads to distortions whereby the specific characteristics of this group are not sufficiently recognised during the development process and are therefore not taken into account. In addition to the training data used, other technical and methodological decisions, e.g. regarding the target variables or labels, can also lead to discriminatory models and therefore to unfair decisions. Lastly, problems may not arise until the systems are actively used in practice for example if algorithmic systems are used in changing social framework conditions or in unforeseen usage contexts.

Algorithmic systems which **directly** use categories of data which are legally explicitly recognized to be **highly sensitive**, such as gender or origin, are particularly critical from the point of view of discrimination. Direct use of sensitive information may, depending on the area of application, be important for correct data processing and is also often permissible within legal limits.

Example 9
Many systems for diagnosing diseases know the patient's gender and age and take them into account. Sensitive characteristics may also be used within the context of a business decision for implementing business strategies, for example where a business is expanding into a specific age group, occupational group or region, if the characteristics define a customer segment, for example, for which simplified acceptance criteria apply.

The use of information which **indirectly** codes sensitive categories can, however, also be problematic.

Example 10
Household income is used as information in creditworthiness assessments. In Germany, the average income varies between genders. As a result, an algorithmic system which uses household income may incorrectly assess the creditworthiness of the men and women involved in terms of the distribution between them.

Fully preventing discrimination even in terms of legally recognised categories such as gender or origin is difficult within the context of algorithmic systems. Furthermore, the use of algorithmic systems can lead to **totally new groups being thrown together based on coindicing characteristics** being excluded from socially protected rights due to a certain classification system and without any just cause, or being confronted with other negative consequences. In the light of this, all those involved in the development and use of such a system must be made aware of the complex conditional discriminatory effects so that they can prevent or counteract them as far as possible (→ see section 4.2.4 below).

However, technical measures designed to minimise discrimination have their limitations even where continuous improvement processes are used, partly because different technical fairness targets cannot be achieved simultaneously. Which criteria for non-discrimination and fairness are appropriate in which context is not a technical but a social and political question. Accordingly, as such, these decisions must not be entrusted to technology developers alone. Instead, they should be part of a future regulation of algorithmic systems and be included in the operational obligations of data controllers. The prerequisite for that is that the **criteria must be decided on specifically based on context as well as democratically**.

Algorithmic systems are difficult to analyse precisely. In order to be able to detect and prevent discrimination, the data controllers and oversight bodies must have the opportunity to gain an idea of any undesirable discrimination effects that occur within an algorithmic system, both within the context of its development and its productive deployment. Such effects can be identified through processes such as **risk assessments and output analyses**.

There is a tension between specifications to limit the collection and storage of discriminatory characteristics and the concern to retain the possibility to detect any discriminatory effects or be able to prove non-discrimination. These different requirements must be balanced on a case-by-case basis, which may have an influence on tests in different phases of the system development lifecycle; standard collation of all potentially discriminatory and therefore sensitive information for the sole purpose of proving that, as a result, no discrimination is taking place would not be justified. Greater efforts are needed here to produce **practical concordance between anti-discrimination law and data protection law**.

2.7 Transparent, explainable and comprehensible systems

In order to be able to carry out a reliable ethical and legal assessment of an algorithmic system, it is essential that enough information be available about its scope, functionality, pool of data and data analysis. **Only a truly transparent system can be examined to determine whether it is pursuing a legitimate purpose.** The transparency principle can have further key functions depending on the type and addressee of possible transparency obligations. With regard to the public, sufficient transparency must be created so that sufficient information is available for socio-political discourse on algorithmic systems. Supervisory authorities or other oversight bodies must be able to decide whether the legal and technical specifications are being or have been met where algorithmic systems are being used. Individual citizens must be able to take informed and confident decisions regarding the use of algorithmic systems and, in the event of negative effects on their freedoms and rights, be able to assess whether and to what extent they wish to exercise their rights. That too is a consequence of the ethical principle of digital self-determination.

In view of the increasing complexity of systems, the demand for transparency is, in practice, confronted with the fact that even experts are hardly able to go through all the individual components of a system fully, look at how they interact and **comprehend** everything within a reasonable amount of time. In particular in the case of individual machine learning methods, it is difficult, with today's state-of-the-art science and technology, to state which input led to a specific output of the system. There is also the fact that even technically simple algorithmic systems are often incorporated into complex social informatics ecosystems, i. e. information and work-sharing processes in which numerous manufacturers and operators are involved.

Example 11
The visual display of a personalised online advert is the result of complex processes in which the advert is delivered and paid for on the basis of behaviour-based analysis and segmentation. In particular, analytics services are used which are deployed by site owners across websites by incorporating the corresponding program code (such as JavaScript code for tracking). The components of such systems are also not fixed but can change, for example if manufacturers provide new versions or if they are adaptive and/or self-learning systems.

Legal aspects can also **limit** certain forms of information disclosure via algorithmic systems. Source codes and hardware designs are often protected as trade secrets. Operators also often have a legitimate interest in preventing their systems from being manipulated. Where algorithmic systems process personal data, data protection law can also limit the interest of the public or other affected citizens in information. However, where the transparency requirement regarding the system concerns the disclosure of the source code, which as such does not contain any personal data, data protection law does not stand in the way of disclosure.

However, the ever-present complexity cannot refute the goal of designing algorithmic systems to be transparent, nor can it justify any lack of transparency. Just like the aforementioned legal grounds, these aspects must nevertheless be taken into account in the drafting of any information rights and transparency obligations, which must be based on what is legally and actually possible. **The principle of transparency** also requires continuously developing technology to make the disclosure of information easier (for example through the use of open-source software and open hardware) and developing approaches which reduce complexity. Research is also required here. Under the banner of "explainable AI", researchers are working with increasing success on producing meaningful findings on the internal processes of algorithmic systems.

The demand for transparency must always take the **different levels of expertise** of the parties potentially interested in transparency into account. For example, the disclosure of the computer code to supervisory authorities carrying out necessary checks, may make it much easier for them to understand the system. Conversely, laypersons often need clearly and comprehensibly prepared information on a system's basic characteristics which enables them to carry out a risk assessment suitable for everyday purposes. At the same time, their interest is seldom limited to the system "itself". In order to prevent any negative decisions in the future, an **explanation** is rather also required as to how the decision specifically concerning them came about and which factors had what weighting. The specific drafting of the specifications on transparency and explainability should be based on the affected individuals' level of understanding and always be **comprehensible** for them. In that sense, rules on transparency and explainability will safeguard citizens' capacity to act and their self-determination.

2.8 Clear accountability structures

Just as having control over data implies the obligation to be accountable for such power, the opportunity to control algorithmic systems must also be accompanied by willingness **to answer for one's own actions**, i. e. to **be liable** where necessary.

Again, it is the complexity of algorithmic systems which, in practice, can make it difficult to assign responsibility. Hardware or software manufacturers, data providers, algorithm developers, operators of individual components, clients and users (either as the organisation or its individual employees) contribute to the system. Components are often used which can change without the knowledge or control of the user, for example as a result of important updates required for information security purposes. Those involved are often also located in different parts of the world. Efforts are required at all levels in order to prevent any diffusion of responsibility and **establish accountability structures**, starting with the technical design of the systems right through to legal specifications, for example in the form of the concept under data protection law of "joint control" (Article 26 GDPR).

2.9 Result: responsibility-guided consideration

Assessing the ethical aspects of algorithmic systems is, **in practice, extremely complex**. This is due to the large number of factors which need to be taken into account as well as the fact that, in a specific area of application, different individuals may be put in a "better" or "worse" position. The same can be said of social consequences and sustainability aspects which can rarely be unequivocally classified as either "positive" or "negative". However, this does not mean that humans can surrender all judgment. In cases where it is difficult to weigh everything up, everyone is required to take particular care with their assessments and decisions. Where algorithmic applications may potentially develop such phenomenally impressive performance and scope that questions are raised concerning the future of mankind, weighted assessments of the opportunities and risks will increasingly reach their limits, and more fundamental anthropological and ethical discussions will be required. This is precisely where the principle of prospective responsibility is of fundamental importance.

With regard to all this, the **democratic process** provides ways and means for balancing conflicting convictions, ideally supported by special **deliberative processes and institutions** through which society can ensure, in as inclusive and participatory a way as possible, that the challenges presented by algorithmic systems are addressed.

It should only rarely be the case that human activity and the use of an algorithmic system do not need to be weighed up against each other because the latter, in all ethically relevant respects, achieves a "better" result than humans using conventional technology. Where this is the case however, the Data Ethics Commission believes that the use of algorithmic systems is **ethically commanded**, because a general ethical preference for human activity over the use of machines at the expense of the protection of important legally protected rights is not justified in the view of the Data Ethics Commission. However, with regard to the question as to whether human or machine activity is preferable (→ see Part B, section 1 above), other factors will routinely need to be taken into consideration, such as the emotional well-being of people, human skills retention and sustainable development, which ultimately requires weighing up the options. This may go against or in favour of the algorithmic system.

Example 12

If the use of a diagnostic algorithmic system in a specific clinical area leads to just 2% of patients dying, whereas 10% of all patients would die as the result of human misdiagnoses, the use of the system would, depending on the circumstances of the specific case, be ethically advisable even if, as a result, minor but tolerable reductions in patients' emotional well-being occurred and additional measures would have to be taken to ensure human skills retention.

However, if, taking all circumstances into account, the use of an algorithmic system, at the expense of important legally protected rights, leads to an inferior result than the use of conventional technology and humans (for example because more wrong decisions are made) and there is only an increase in efficiency or convenience, the use of algorithmic systems must, in principle, be **rejected for ethical reasons**. However, ethically defensible exceptions could be made in this case based on economic considerations if there would be only a minimal impairment but an exceptionally high potential saving which would benefit the public good.

3. Recommendation for a risk-adapted regulatory approach

From a regulatory point of view, the fact that algorithmic systems need to be assessed very differently from an ethical perspective, depending on their intended purpose, performance, robustness and security as well as in terms of their impacts, suggests that a **risk-adapted regulatory approach**[1] is required. It follows the principle that the **greater the potential** of algorithmic systems **to cause harm**, **the more stringent the requirements and the more far-reaching the intervention** by means of regulatory instruments. The risk spectrum of algorithmic systems therefore ranges from systems, the application of which involves low risk, right through to systems which could lead to irreversible harm for individuals and society. Causes of risks can, for example, be inadequate models, an unsuitable pool of data, in particular in the case of self-learning systems, or inappropriate basic assumptions and weighting (→ see sections 2.3 and 2.6 above).

Potential **harm** caused by algorithmic systems can vary in nature and can include financial loss, non-material damage and physical harm. For example, individual applications can cause potentially serious financial loss (for example lending or insurance terms), affect opportunities for participation (for example discrimination in hiring) and involve violations of fundamental rights and risks to the life and health of consumers (for example in the case of robotic nurses or mobility applications).

The overarching objective of regulating the use of algorithmic systems is to prevent detrimental effects at the individual and supra-individual level. In particular where algorithmic systems affect matters which are sensitive in terms of fundamental rights, legal provisions concerning the design of the systems are also needed. Regulation should strive to intervene as much as necessary and as little as possible in order not to hamper innovation and creativity while at the same time ensuring the protection of fundamental rights, freedoms and values. **Efficient and proper regulation** can help increase public trust in the use of algorithmic systems: The public perception of self-learning systems in particular is that they are not controllable, which adds to corresponding scepticism towards technology.[2]

The Data Ethics Commission takes the view that the primary addressees of regulation should be the **manufacturers** and **operators** of algorithmic systems. Due to the State's direct obligation to uphold fundamental rights, it is necessary to differentiate, however, between **private and state use** of algorithmic systems (→ see section 7 below in particular) when the regulation is drawn up in more detail. Given the model and role model character of state action, the Federal Government is advised to exercise particular care when using algorithmic systems for state purposes.

3.1 System criticality and system requirements

A risk-adapted regulatory approach can be made more concrete by orienting it towards the criticality model of an algorithmic system. **System criticality** is based on the system's potential to cause harm, which is determined based on the likelihood that harm will occur and on the severity of that harm.

1 Compare in particular Tobias Krafft / Katharina Zweig: Transparenz und Nachvollziehbarkeit algorithmenbasierter Entscheidungsprozesse [Transparency and traceability of algorithm-based decision processes], Studie im Auftrag des Verbraucherzentrale Bundesverband e. V. (vzbv) [Study commissioned by the Federation of German Consumer Organisations (vzbv)], 22 January 2019, pp. 18 et seqq. (available at: *https://www.vzbv.de/sites/default/files/downloads/2019/05/02/19-01-22_zweig_krafft_transparenz_adm-neu.pdf*).

2 Sarah Fischer / Thomas Petersen: Was Deutschland über Algorithmen weiß und denkt – Ergebnisse einer repräsentativen Bevölkerungsumfrage [What Germany knows and thinks about algorithms – results of a representative population survey], Bertelsmann Stiftung, 2018 (available at: *https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/was-deutschland-ueber-algorithmen-weiss-und-denkt/*).

The **severity** of harm that could potentially result, for example from a faulty decision, depends among other things on the significance of the legally protected rights and interests affected (in particular, for example, the right to determine the use of one's personal data, to freedom of expression, the fundamental right to life and physical integrity, as well as to equal treatment) and the extent of the potential harm resulting from an infringement. Furthermore, the assessment of the severity of the potential harm must take into account the specific sensitivity of the data used, the level of potential harm for individuals or groups (including non-material harm or loss of utility that are hard to calculate in monetary terms), the number of individuals affected, the total figure for the potential damage and the harm to society as a whole, which may go well beyond a straightforward summation of the harm suffered by individuals. The consequences of using an algorithmic system should, based on its area of application, be considered in terms of its ecological, social, psychological, cultural, economic and legal dimensions. The general ethical values and principles (→ see Part B above) set the standard with regard to the assigned value.

The **likelihood** that harm will occur is also influenced by the following system properties, and factors:

- the role of algorithmic calculations in the decision-making process (from the mere inspiration of humans without any claim to accuracy up to algorithm-determined decisions, → see section 1 above);
- the complexity of the decision to be made (from a simple deterministic depiction of reality or a probabilistic appraisal of reality up to the multifactorial and non-determinate prediction of a future reality);
- the effects of the decision (from a purely abstractly conceivable context of action or a specific context of action up to direct implementation); and
- the reversibility of the effects (from full reversibility up to irreversibility).

The likelihood of the potential harm and the severity of that harm may also depend on whether it is a **state or private** party taking action and, particularly in economic contexts, on the **market power** of the party using the algorithmic system. This is due to the fact that the state or private nature of the action and market power are not only relevant in terms of the obligation to uphold fundamental rights and potential harm to society as a whole. They also determine possible alternative options for those affected. Where **affected persons depend** on an algorithmic system, for example in terms of access to markets, goods and services, the criticality increases. The limitation of options can be due to various different causes, for example network effects, effects of scale and effects of scope which can, in turn, be reflected in market power and (a lack of) equivalent alternatives.

The greater the system criticality, the stricter the **requirements** that have to be imposed on the system from a regulatory perspective. These requirements are being formed out, in particular, by

a) corrective and oversight mechanisms;

b) specifications regarding the transparency of algorithmic systems and the explainability and comprehensibility of the results; and

c) rules on the assignment of responsibility and liability within the context of the development and use of algorithmic systems (→ see sections 4, 5 and 8 below).

The variety, complexity and dynamics of algorithmic systems pose major challenges for regulation which cannot be based on a limited toolbox but must, depending on the system's criticality, implement **very different corrective and control instruments at different regulatory levels** in order to achieve the objectives of regulation and ensure that the risks involved in the systems are manageable. The spectrum of possible instruments ranges from forgoing special legal provisions and "soft" incentives for self-regulation, giving authorities the right to monitor, and requiring any final decision to be taken by a human, up to banning certain intended purposes and contexts for using algorithmic systems.

Provisions regarding the **transparency** of systems and the **explainability** and **comprehensibility** of their results (→ see section 2.7 above) are key components of a corrective and control regime for algorithmic systems. Also, to that extent, the criticality of a system determines the scope of any rights to information and obligations to provide information. How the information requested can be comprehensibly communicated varies depending on the addressees of the system and hence also the intended purpose and usage context.

From an ethical and legal perspective, it is crucial, for all dealings with algorithmic systems, that **responsibility** for their impacts can be clearly assigned to human decision-makers at all times. Rules on **liability** are, in particular, also of key importance here, while the question of the proper organisation of a liability regime for certain digital products, content and/or services must also be addressed with a view to the criticality of the system (→ see section 8 below).

In terms of the governance perspective adopted by the Data Ethics Commission, **all relevant stakeholders** (the State, companies, developers and the public) must participate in **specifying and drawing up** these differentiated **regulatory requirements**. The Data Ethics Commission points out that, even without any special regulation, the use of algorithmic systems must be measured against general legal norms. These include in particular civil liability law, which fundamentally states that compensation is mandatory in the event of action which infringes legally protected interests. The provisions of existing regulation against unfair competition also apply, for example in the event that consumers are misled, as well as criminal law if crimes are committed with the help of algorithmic systems. When examining the conditions of these norms, the criticality of the systems and the resulting system requirements also have legal significance in accordance with general standards.

Algorithmic systems are used in order to fulfil specific functions. In order to assess system criticality, the **ethical assessment of the intended purpose** is therefore also of crucial importance. If the intended purpose is ethically indefensible, for example because it infringes fundamental rights and freedoms or breaches the free democratic basic order, then there are "red lines" and "absolute limits" – both for algorithmic systems and for humans. For example, an algorithmic system used for political manipulation, fraud or collusive price-fixing must be seen per se as ethically objectionable.

The intended purposes are often multifaceted, and individual facets, in particular regarding secondary purposes, may each need to be assessed differently from an ethical perspective. Identifying an intended purpose which is decisive for the assessment often, in that sense, requires difficult **value judgments**. Assessing the intended purpose of algorithmic systems is further complicated in the case of digital products because the development and market launch phases increasingly overlap; the intended purpose of a product may also change after it has been launched on the market due to updates or deployment in other usage contexts.

Complex intended purposes in the case of media intermediaries

A number of media intermediaries, such as search engines, are essential in the Internet age because they provide access to information online, channel the flood of information and actually enable individuals to use the Internet in the first place. To that extent, their purposes are desirable and unproblematic in ethical terms. However, media intermediaries can be ethically problematic in terms of their specific design. Their systems provide users with a personalised selection of information which leads to selection of the displayed content. However, since as a result the overwhelming majority of content is not displayed or is only displayed with a lower priority, the individual's spectrum of perception is narrowed. As such, the intermediary decides, through programming, over the user's head as to what the user sees. As far as the business models of media intermediaries are driven by advertising, as is the case with major social networks, there is a risk that operators will have an economic interest in disseminating also ethically questionable or even extremist content because it promises to keep users on the platform longer, thus increasing advertising revenue. Due to the interplay of the sorting and narrowing of what is seen and the additional danger of influencing the user through non-transparent third-party interests, there is the possibility that influence will be non-transparently exerted, for example over the political decision-making process, and could even result in political manipulation. This is a significant danger for the free formation of opinions as a basic foundation of democracy.

3.2 Criticality pyramid

The Data Ethics Commission recommends consistently determining the degree of criticality of algorithmic systems using **an overarching model**. The degree of criticality should guide legislators and society when seeking suitable regulatory thresholds and instruments, but can also provide developers and operators with guidance for assessing their products and systems themselves and finally also be used in basic, advanced and further training to educate and **increase awareness amongst** various stakeholders. To that extent, with regard to the potential of algorithmic systems to cause harm, the Data Ethics Commission differentiates, both for private and for state operators, between **five levels of criticality**:

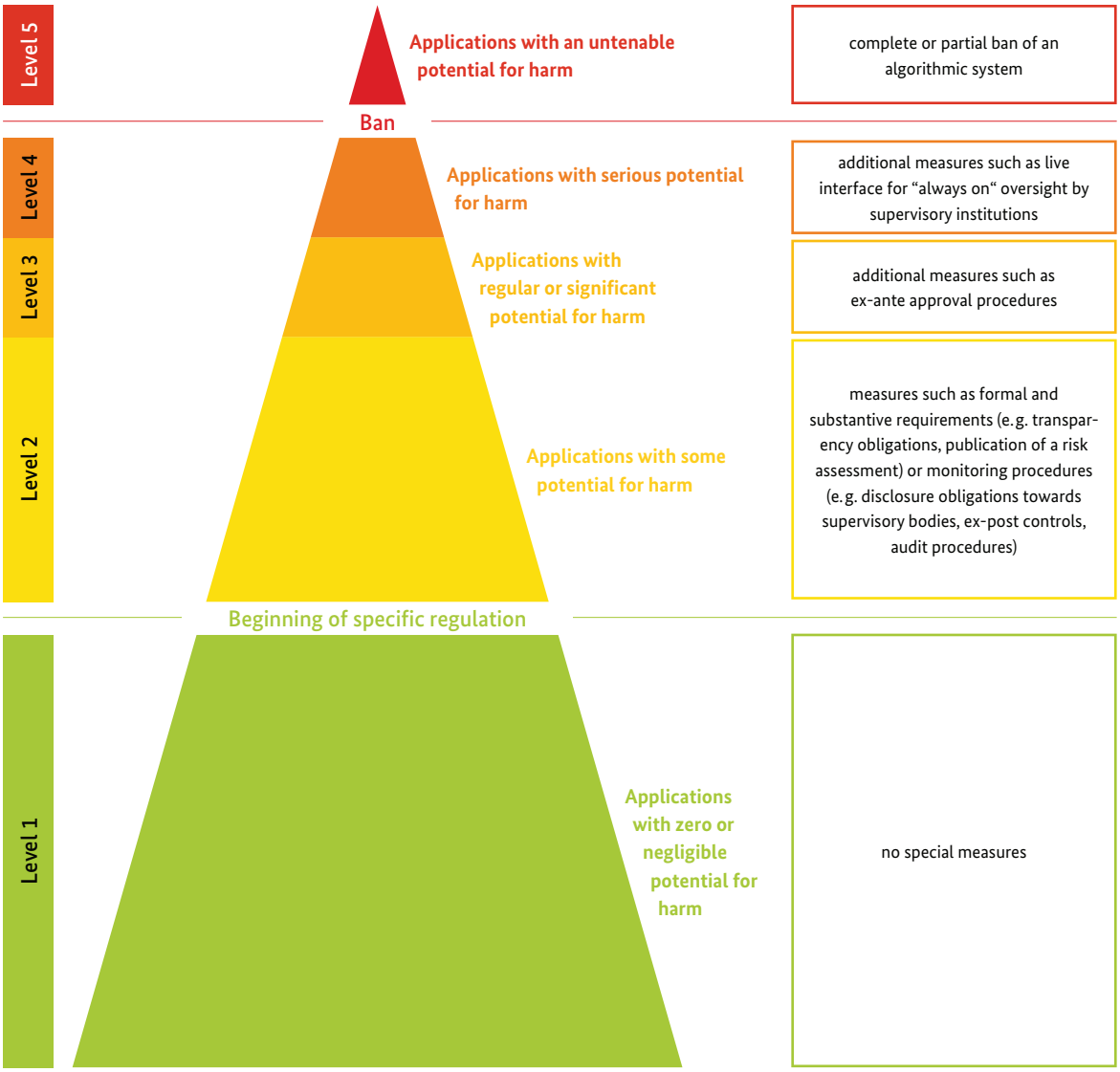


Figure 8:
Criticality pyramid and risk-adapted regulatory system for the use of algorithmic systems

In unproblematic usage contexts, it will normally not be necessary to require developers, clients or operators to go through specific ethical and legal oversight procedures. For the many **applications with zero or only negligible potential for harm**, i. e. on the lowest level (Level 1) of the criticality pyramid, the Data Ethics Commission sees no need for special oversight which would go beyond the general quality requirements which apply even to products without algorithmic elements.

Example 13
The algorithms used in a drinks vending machine do have a certain potential for harm, since a user could, for example, not receive any goods and lose his or her money. However, this potential for harm does not exceed the threshold for specific potential for harm within the algorithm context. It is sufficient here to rely on the general mechanisms which oblige contractual partners to fulfil their contractually undertaken performance obligations or manufacturers to produce devices which function properly.

In the case of **applications with some potential for harm** (i. e. on Level 2 of the criticality pyramid), regulation can and should be implemented. However, the scope of the necessary measures is limited here. In view of the low level of criticality, any excessive burden on manufacturers and operators should specifically be avoided here in order not to excessively hinder technological or social innovations or market development. Measures which could be offered at Level 2 include for example ad-hoc ex-post controls (for example in the form of an input-output control), if there is reason to suspect that the system is malfunctioning. Furthermore, there should be an obligation to produce and publish an appropriate risk assessment (→ see section 4.1.3 below). In addition, on a sector-specific basis, obligations to disclose information to supervisory institutions (including establishing an interface for a supervisory institution to carry out input-output controls), increased transparency obligations as well as access rights for individuals affected (→ see section 4.1 below for more details) may be useful. Codes of conduct should also be considered which would be developed specifically for each industry and then approved by the competent supervisory authorities. Compliance would then need to be tested by the supervisory authorities using spot checks as well as on an ad-hoc basis (→ see section 5.2 below).

Criticality in the case of smart mobility applications

A provider of smart mobility applications has access to a data pool generated using all vehicle and mobility data. If these data are used exclusively for predicting traffic jams, the level of criticality should be classified as negligible. However, the flow of traffic can also be controlled using smart mobility. If algorithms can, for example, identify which route is the optimum route for travelling from A to B based on the overall usage of the mobility system consisting of road, rail, water and air transport determined in real time using the vehicle data, a corresponding route can be suggested to the user based on the user's preference (e. g. fastest/most environmentally friendly/cheapest, etc. route). However, there is also the question as to whether the State can stipulate certain routes for the user in consideration of state-prescribed criteria. Here, in view of the changed potential for harm, the level of criticality would be higher and would therefore require stricter regulation as appropriate.

Example 14
Dynamic pricing (for example based on the criteria of supply and demand) in e-commerce, which however does not involve any personalised pricing, has a potential for harm that is generally low but still exceeding the threshold of relevance, for example concerning covert discrimination.

Example 15
Price algorithms for setting personalised prices (i. e. setting a price based on criteria which are tailored to the individual customer and usually estimate their maximum personal willingness to pay) involve appreciable potential for harm, for example concerning discrimination against particularly vulnerable groups. At best, it should be possible to use them only after they have undergone a licensing procedure.

In the case of **applications with regular or tangible potential for harm** at Level 3 on the criticality pyramid, in specific cases, in addition to the mechanisms already required for Level 2, an ex-ante control in the form of a licensing procedure may be justified (→ see section 4.2.5 below). On account of the fact that many algorithmic systems are highly dynamic, a regular review will be required in the event that a licence is granted.

The same must apply for **applications with significant potential for harm** at Level 4 as applies for Levels 2 and 3. However, here, additional oversight and transparency obligations, which may extend all the way through to the further publication of information on the factors that influence the algorithmic calculations and their relative weighting, the pool of data used and the algorithmic decision-making model in a comprehensible format, should be required or even “always-on” oversight via a live interface should be provided for. Further protective measures to prevent harm are also necessary.

Differentiated criticality in the case of media intermediaries

With the help of their algorithmic filtering systems, media intermediaries process and communicate both content relevant for the formation of opinions, which is relevant for the democratic decision-making process, and content used for advertising, purchase recommendations or entertainment. They therefore represent the perfect example of situations in which the use of the same algorithmic system has differing potential for harm. In the case of user interaction in the consumer goods sector (in particular advertising or purchase recommendations), depending on the personalisation model used, there will be a low to high potential for harm. As soon as balanced variety must be produced (in particular in the case of topics relevant to the formation of opinions) on account of overarching interests in maintaining the free democratic basic order, the potential for harm is already higher right from the outset due to the content. As a result, the regulatory requirements change simultaneously. In the case of consumption and entertainment offerings, depending on the personalisation criteria used, the usage contexts or the welfare effects to be expected, more or less stringent regulation must ensue.

Example 16
Algorithmic systems, for example of players with huge market share, which are used to determine the creditworthiness of an individual consumer or company must be classified as Level 4. Whether a person receives a loan or not can have a decisive bearing on that person's fate. The high level of system criticality is also justified by the market concentration with few providers and the tendency for a lender to rely on the judgment of a particular player.

With regard to the system criticality criteria, it may ultimately be worth considering a complete or partial ex-ante **ban** on the use of an algorithmic system for **applications with untenable potential for harm** (Level 5). An ex-post ban may also be used as a consequence for breaches of applicable law or non-fulfilment of the system requirements set out for the specific system criticality.

Example 17
Lethal autonomous weapons systems are often seen as a "red line", as machines should not be allowed to kill people. However, that can apply only on the basis that they are algorithm-determined killings. Where lethal autonomous weapons simply provide human soldiers with support in recognising objects or are merely used to keep a missile on track in the face of crosswinds, an ethical "red line" is not being crossed.

The classification of an algorithmic system in the criticality pyramid must, where necessary, be **regularly reviewed** in the light of the dynamic nature of these systems.

3.3 EU regulation on algorithmic systems enshrining horizontal requirements and formed out in sectoral instruments

Algorithmic systems are infiltrating more and more areas of our personal and social lives. The purposes of algorithmic systems and the areas in which they could potentially be used are therefore not set in stone. For example, a facial recognition system developed for use with private photos could also be used by state investigative authorities for law enforcement purposes or to prevent threats. This suggests addressing the challenges posed by algorithmic systems following the example of data protection law in the form of **horizontal regulation**, i. e. through a legal instrument, the material scope of which covers algorithmic systems in general, and which applies to **private and public players** alike. In addition to the considerable symbolic power, another point in favour of horizontal regulation is the fact that gaps in protection would be eliminated and dangerous situations which currently cannot be foreseen would be covered. One of the main arguments in favour of such overarching regulation which sets out basic principles for all algorithmic systems is also the fact that citizens would, as a result, have a clear idea of what to expect in all areas, and (European) legislators could complete this task within a reasonable period of time.

As a result, **the Data Ethics Commission recommends** that the Federal Government should work towards drawing up horizontal basic regulation at the European level in the form of an **EU Regulation on Algorithmic Systems (EU-ASR)**. In addition to the key basic principles for algorithmic systems developed here as requirements for algorithmic systems, the horizontal legal instrument should group together general substantive rules – informed by the concept of system criticality – on the admissibility and design of algorithmic systems, transparency, the rights of individuals affected, organisational and technical safeguards and supervisory institutions and structures.

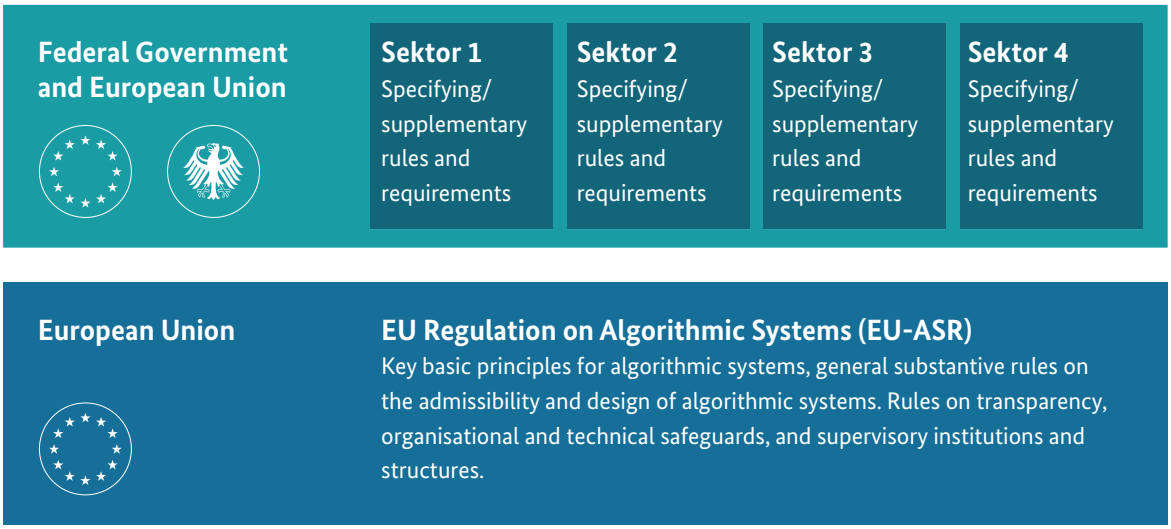


Figure 9:
EU regulation on algorithmic systems enshrining horizontal requirements and specified in sectoral instruments

At the same time, the Data Ethics Commission recommends that the Federal Government should also advocate sectoral rules on the European level and, outside the competences of the EU itself and within its own legislative and administrative competences, enact appropriate sectoral legal acts which are oriented towards system criticality. (Fig. 9).

An **overarching EU-ASR** will have to be limited to few **basic principles**, as otherwise European legislatory powers would be overburdened. Legislators would, if rules were too detailed, in particular face the issue of how to deal, in a general legal instrument, with the wide variety of systems of which it is now almost impossible to keep track and the highly dynamic development of technology. From the perspective of those affected, general legal instruments also carry the risk that the administrative obligations will also apply in cases where there is not sufficient potential for harm, because a horizontal legal instrument cannot distinguish between risky and less risky operational aims (as well as potential exceptional configurations) with the same level of detail that they have in reality. With regard to both points, the **supplementary** recourse to **sector-specific legislation** which would be limited in terms of scope but would therefore be easier to form out would relieve some of the burden. Any supplementary sector-specific approach would also have to take into consideration the legislative and administrative powers distributed in accordance with applicable law between the EU, the Federal level and the States *(Bundesländer)*. An additional fact is that, with regard to the official oversight and supervisory institutions and structures, for various reasons there could be no question of consolidating and assigning the "overall task" to one single authority (→ see section 5.1 below).

Therefore, in addition to the EU-ASR it will be necessary to enact several **legal instruments with specific provisions for individual sectors or potentially harmful situations**. In the view of the Data Ethics Commission, combining a general basic regulation with further sector-specific legal instruments has the major advantage of enabling differentiation between the different needs for protection involved for individual systems and usage contexts. This is in line with the basic concept behind risk-adapted regulation, according to which the regulatory requirements for algorithmic systems should be determined based on the specific system criticality.

Even in data protection law, in the public sector, there are numerous special laws which supplement the general provisions of the GDPR for different sectors. The basic idea behind data protection law is that, in the case of automated data processing, there is no longer such a thing as "inconsequential" data, which is why it is hardly possible any more to differentiate meaningfully between personal data on the basis of worthiness of protection or criticality in the absence of common basic rules. Nonetheless it is also true that a variety of special provisions ensures an increased level of protection in the wide range of areas of state activity. Similarly, there is an according need for supplementary sectoral provisions for algorithmic systems. The application of such regulation also does not have to fall short as a result of the fact that their purpose and usage context could change. After all, firstly, such a change would be, especially in more complex systems, inherently limited. Secondly, the issue could be addressed from a regulatory perspective by the fact that the legal instruments would not be materially linked to the original purpose or original usage context but the **current functionality of the system or the new intended purpose** of the system. In this way, any changes in purpose and context would, if necessary, result in the application of a differentiated regulatory framework.

However, these primarily pragmatic considerations in no way affect the requirement for the standard-setting body or bodies to ensure the greatest possible **coherence between legal instruments** in their respective undertakings. This will apply not only to the regulatory approaches developed here, i. e. in particular the notion of system criticality, and the rights of data subjects; regulatory infrastructures and processes should also be designed as uniformly as possible.

Summary of the most important recommendations for action

Risk-adapted regulatory approach

36

The Data Ethics Commission recommends adopting a **risk-adapted regulatory approach** to algorithmic systems. The principle underlying this approach should be as follows: the greater the potential for harm, the more stringent the requirements and the more far-reaching the intervention by means of regulatory instruments. When assessing this potential for harm, the **sociotechnical system as a whole** must be considered, or in other words all the components of an algorithmic application, including all the people involved, from the development phase – for example the training data used – right through to its implementation in an application environment and any evaluation and adjustment measures.

37

The Data Ethics Commission recommends that the potential of algorithmic systems to harm individuals and/or society should be determined uniformly on the basis of a **universally applicable model**. For this purpose, the legislator should develop a **criteria-based assessment scheme** as a tool for determining the criticality of algorithmic systems. This scheme should be based on the general ethical and legal principles presented by the Data Ethics Commission.

38

Among other things, the **regulatory instruments and the requirements that apply to algorithmic systems** should include corrective and oversight mechanisms, specifications of transparency, explainability and comprehensibility of the systems' results, and rules on the allocation of responsibility and liability for using the systems.

39

The Data Ethics Commission believes that a useful first stage in determining the potential for harm of algorithmic systems is to distinguish between **five levels of criticality**. Applications that fall under the lowest of these levels (Level 1) are associated with zero or negligible potential for harm, and it is unnecessary to carry out special oversight of them or impose requirements other than the general quality requirements that apply to products irrespective of whether they incorporate algorithmic systems.

40

Applications that fall under Level 2 are associated with **some potential for harm**, and can and should be regulated on an as-needs basis; regulatory instruments used in this connection may include ex-post controls, an obligation to produce and publish an appropriate risk assessment, an obligation to disclose information to supervisory bodies or also enhanced transparency obligations and access rights for individuals affected.

41

In addition, the introduction of licensing procedures may be justified for applications that fall under Level 3, which are associated with **regular** or **significant potential for harm**. Applications that fall under Level 4 are associated with **serious potential for harm**; the Data Ethics Commission believes that these applications should be subject to enhanced oversight and transparency obligations. These may extend all the way through to the publication of information on the factors that influence the algorithmic calculations and their relative weightings, the pool of data used and the algorithmic decision-making model; an option for "always-on" regulatory oversight via a live interface with the system may also be required.

42

Finally, a complete or partial ban should be imposed on **applications with an untenable potential for harm** (Level 5).

43

The Data Ethics Commission believes that the measures it has proposed should be implemented in a new EU Regulation on algorithmic systems enshrining general **horizontal requirements (Regulation on Algorithmic Systems, EU-ASR)**. This horizontal regulation should incorporate the fundamental requirements for algorithmic sytems that the Data Ethics Commission developed. In particular, it should group together general substantive rules – informed by the concept of system criticality – on the admissibility and design of algorithmic systems, transparency, the rights of individuals affected, organisational and technical safeguards and supervisory institutions and structures. This horizontal instrument should be fleshed out in **sectoral instruments** at EU and Member State level, with the concept of system criticality once again serving as a guiding framework.

44

The process of drafting the EU-ASR (as recommended above) should incorporate a debate on how best to demarcate the respective scopes of this Regulation and the **GDPR**. A number of factors should be taken into account in this respect; firstly, algorithmic systems may pose specific risks to individuals and groups even if they do not involve the processing of personal data, and these risks may relate to assets, ownership, bodily integrity or discrimination. Secondly, the regulatory framework introduced for the future horizontal regulation of algorithmic systems may need to be more flexible and risk-adapted than the current data protection regime.

4. Instruments: obligations of data controllers and rights of data subjects

In order to provide individuals and groups with effective protection against the dangers of algorithmic systems, the Data Ethics Commission believes that both transparency requirements (→ see section 4.1 below) and further specifications for algorithmic systems with a view to effective protection against substantively inappropriate decisions and unfair decisions (→ section 4.2.) are advisable.

4.1 Transparency requirements

4.1.1 Mandatory labelling ("if")

A key tool for creating transparency is **mandatory labelling**. Because a mandatory labelling scheme requires little detailed information, infringements of the fundamental rights of system operators, in particular with regard to their business secrets, are also less serious than in the case of access rights. The Data Ethics Commission believes that this justifies establishing labelling in the case of critical systems (as from Level 2) as a blanket obligation for system operators and not as a request-based right for the individuals affected.

Due to the comparatively narrow scope of Article 22 GDPR (relating to a decision based solely on automated processing), to which the duties to provide information refer, the Data Ethics Commission believes that the existing labelling obligations of the GDPR[3] are **insufficient**. In particular, significant impacts for affected individuals can arise even below the threshold of Article 22 GDPR. That applies for algorithm-based and algorithm-driven decisions, i.e. situations in which the humans taking the decisions run the risk of accepting algorithmic information and proposed decisions without reflection and by default (in particular in areas where human assessment is expected) or only following algorithmically determined and prescribed paths.

Because the Data Ethics Commission sees the authenticity of interpersonal communication as a fundamental condition for trustworthy interaction within society, a mandatory labelling scheme should always apply if there is any **risk of confusion** between human and machine and should therefore apply irrespective of system criticality. This applies, for example, to digital voice assistants and chatbots which these days are sometimes hard to identify as such. Labelling may, in the case of voice assistants for example, be carried out both by means of a regular reminder of the assistant's mechanical nature (even during ongoing communication) and also through the use of a mechanical-sounding voice. Conversely, the Data Ethics Commission considers that there is no risk of confusion (and therefore also no need for a mandatory labelling scheme) in areas where the nature of the information is irrelevant or the recipient expects a mechanical voice anyway, such as in the case of loudspeaker announcements at railway stations.

4.1.2 Duties to provide information, duties to provide an explanation and access to information ("how" and "what")

Whilst mandatory labelling schemes require system operators to ensure transparency regarding as to whether and the extent to which algorithmic systems are used ("if"), duties to provide information and **rights of access** are regularly focused on more detailed information regarding the decision-making mechanism ("how") and the data used ("what") by the algorithmic system.

3 Article 13(2)(f), Article 14(2)(g) and Article 15(1)(h) in conjunction with Article 22 GDPR.

Duties to provide information and rights of access regarding the behaviour of algorithmic systems and the way that decisions are made inside the systems are important from the perspective of citizens for them to be able to understand decisions and review them and/or have them reviewed individually. Only with their help can data subjects exercise their rights and challenge a decision on an informed basis. The following transparency requirements apply equally to private and state operators of algorithmic systems. Special requirements with regard to the transparency of systems used by the State will be covered in more detail in section 7 below.

4.1.2.1 Duties to provide information and rights of access

Articles 13, 14 and 15 GDPR already set out duties to provide information and rights of access where personal data are processed. In the event of automated decision-making within the meaning of Article 22 GDPR, the GDPR grants the data subject a right to "meaningful" information about the "logic involved", as well as the "significance" and the "envisaged consequences" of the processing.[4]

The Data Ethics Commission takes the view that, just as in the case of the mandatory labelling scheme (→ see section 4.1.1 above), the legal concept behind these norms should also apply outside of the narrow scope of Article 22(1) GDPR and be an integral part of the EU-ASR suggested here (→ see section 3.3 above). The extent of such a duty to provide information will depend on the **criticality of the system**. In the case of applications with negligible potential for harm, brief statements on the logic behind decisions will suffice, for example on the pool of data used or the general weighting of certain factors with regard to the result. The more risk a system involves, the more extensive the duties to disclose information will essentially be.

The more sensitive a decision is in terms of personality, the more detailed information relating to the individual case is needed. However, it should also be borne in mind that providing detailed information regarding the factors and their weighting could also have potentially ethically questionable influence on the private lifestyle of the data subject. Furthermore, the data subject could also use the acquired information to undermine an algorithmic system which performs an important function.

The **technical and organisational requirements** which must be met in order to be able to fulfil these extensive duties to provide information must be incorporated in the design of algorithmic systems right from the outset, as it will be possible to ensure that the systems are operated lawfully only if the corresponding necessary "meaningful" information can also be provided when the system is used.

When defining duties to provide information and rights of access in order to increase the transparency of algorithmic systems, care should be taken to ensure that no special technical skills or knowledge are required of consumers. Whenever rights of access are expanded, it should be borne in mind that, from the perspective of data subjects, this will increase transparency only if the information is prepared **in a way which is suitable for the recipient**.

4 Article 13(2)(f), Article 14(2)(g) and Article 15(1)(h) GDPR.

4.1.2.2 Duties to provide an explanation

At least in certain areas of complex algorithmic systems, it may be appropriate, in addition to the general explanation regarding the system's logic and significance, to require an explanation of the specific reasons why the system made a recommendation or decision. Such a specific explanation is required above all if the decision concerns areas which are sensitive in terms of personality or otherwise is of particular significance in terms of fundamental rights or socioeconomics. It is important, in such cases, for data subjects to be informed in a comprehensible, relevant and clear manner. The Data Ethics Commission therefore welcomes the technical efforts to improve the explainability of algorithmic (in particular self-learning) systems (explainable or explicable AI), and encourages the Federal Government to promote such projects.

The Data Ethics Commission believes that, in certain situations, it is worth considering an entitlement to **"counterfactual explanations"** as is sometimes discussed in the literature.[5] In such cases, data subjects are informed of the factors in the decision-making process which, in the case of a (negative) decision for them, would have made the positive difference, i. e. would have actually led to the desired outcome. In a case where an application for a loan has been rejected based on the use of an algorithmic system, the data subject would, for example, be entitled to learn from the system operator which of the factors taken into consideration by the system would have had to have been different, and in what way, for the application to have had a positive outcome. However, the Data Ethics Commission points out that this approach quickly reaches its limits in the case of more complex systems, as the data subject would have to be provided with a whole host of different "counterfactual" scenarios here in order to be given a reasonably complete picture; otherwise there would be a danger of misinformation, questionable steering or even manipulation by focusing on certain aspects for strategic or educational reasons.

In the view of the Data Ethics Commission, given the current state of technical development, the concept of "counterfactual explanation" is therefore not suitable for use as a general component of any regulation of algorithmic systems; however, it could be considered for special processing situations.

4.1.2.3 Access to information for not directly affected persons

In addition, the Data Ethics Commission considers that, in certain sectors in which not only individual but also social interests are affected to a significant extent, it is advisable even for individuals not directly affected to be granted a right of access to information regarding the algorithmic systems. This would apply, in particular, if their use were **relevant for public opinion-forming** or had major **welfare effects** for the population. Such rights would, first and foremost, be worth considering for journalistic and research purposes and would also have to be accompanied with adequate protective measures for any affected interests of system operators.

Under certain circumstances, in particular in the event of the State's use of systems with significant potential for harm, **unconditional rights of access to information** and **publication requirements** are also conceivable in the view of the Data Ethics Commission.

5 Sandra Wachter / Brent Mittelstadt / Chris Russel: Harvard Journal of Law & Technology 2018 (31), pp. 841 et seqq.

4.1.2.4 Requirements for defining duties and rights, in particular in consideration of system operators' rights

When defining duties to provide information and explanations and rights of access, it must always be borne in mind that these may also affect the **legally protected interests of the operators** of algorithmic systems, as well as of those who use their outputs. This includes, most notably, the protection of business secrets and the interest in preventing any manipulation of the systems and manipulative use of the systems. Private system operators can, in principle, invoke the fact that they define their own free-will decisions and contractual decisions based on the outputs of an algorithmic system. However, that does not release them from monitoring required to check whether they are acting in accordance with the law, as the fundamental right to freedom of action is restricted by bans on discrimination (in particular the General Act on Equal Treatment), the fundamental rights of the data subjects or third parties and, in general, the provisions (and specific contractual provisions) of the legal system. Furthermore, transparency rights must always be balanced with the provisions of data protection law relating to the protection of the personal data of third parties stored in the system.

The Data Ethics Commission therefore believes that it is appropriate for legislators to accompany transparency obligations with rules which, at the initiative of the system operators or also possibly affected third parties, enable **the conflicting rights and interests to be weighed** against the transparency interests of the data subjects or other private individuals entitled to claim rights. However, in the view of the Data Ethics Commission, **rigid rules of priority**, for example a general preference for the protection of business secrets over transparency interests, are **not appropriate for the matter concerned**, despite the increase in legal certainty they might bring. Where system operators or third parties invoke conflicting interests, meticulous checks must be carried out to see whether such interests cannot be taken into account with specific protective measures before a transparency obligation is completely rejected. If private individuals have rights of access to information, the requirements regarding the protective measures and the demonstration of their existence must be devised so that they do not act as a barrier preventing vulnerable consumers and/or citizens from acquiring information. Interests of third parties must be protected for example by means of anonymisation.

4.1.3 Risk impact assessment

The impact assessment within the meaning of Article 35(1) GDPR concerns only information on the impacts for the protection of *personal data*; however, it does not include a comprehensive risk analysis of an algorithmic system. In the case of algorithmic systems, as from a certain level of potential for harm, it is, however, appropriate and reasonable legally to require the provider/user to produce and publish an appropriate risk impact assessment in order to assess the risk involved with the system. The more critical the system is, the more comprehensive the risk impact assessment must be. It should also cover an assessment of the **risks relating to self-determination, privacy, bodily integrity and personal integrity, as well as assets, property and non-discrimination**, and also include methods for gauging the quality and fairness of the data and the model accuracy, for example the bias or the rates of (statistical) error (overall or for certain sub-groups) exhibited by a system during forecasting/category formation.

Use Case: Personalised prices I – transparency requirements

The increasing use of pricing algorithms in e-commerce presents challenges not only for consumer protection law but also for competition law: pricing algorithms can review the market in order to adjust prices in line with demand and competitors' offers in real time.

In e-commerce, providers can therefore apply personalised prices (for individual users or groups) directly or via individual discounts. Algorithmic systems can, for example, be used specifically to cash in on consumers' maximum willingness to pay or encourage users not to abort a purchase transaction. This personalisation is based on scoring processes, for example using real-time analyses of users' surfing habits or data collected in another way. The underlying algorithmic systems are usually "black boxes", meaning that the pool of data used and logic behind the decisions on pricing are not comprehensible to outsiders. There is therefore a risk of price discrimination, for example relating to protected population groups within the meaning of the General Act on Equal Treatment.

The potential for harm to be caused by the implementation of higher personalised prices for individual consumers can vary greatly. Nevertheless, even small price increases for individual goods and services can, when added together, lead to significant welfare losses for the individuals and population groups affected. In particular, learning systems, which may, for example, use signalling, can also lead to quasi-collusive high market prices. If competitors deviously collude on prices or conditions via algorithms, this has a negative effect on competition, the innovative prowess of the economy and ultimately consumers; this applies both to the intentional use of algorithms to influence prices and also where parallel behaviour and high prices (tacit collusion) occur by means of learning algorithms without such specific intention and where no direct price-fixing was undertaken by humans.

It would not suffice for this overall high level of criticality to merely trigger transparency requirements and labelling obligations for pricing systems. A comprehensive impact assessment could also help to identify the discrimination risks of an algorithmic pricing system: if the pool of data being used to calculate personalised prices is known, independent experts should be able to check whether they correlate with protected population groups (known as proxies), i. e. whether, for example, women or certain religious groups have to pay higher prices. If consumers are also made aware, via labelling obligations, that prices and/or discounts are personalised, the affected parties could exercise rights of access to check the data used for "their" price for accuracy or potential discriminatory factors.

Transparency regarding price-relevant factors is also important in order to observe the steering effects of personalised pricing on the behaviour of individual consumers, as they may be of a scale which is relevant for freedom.

4.1.4 Duty to draw up documentation and keep logs

The more complex, dynamic and dispersed the process is by which individual IT systems convert an input into an output, the more important it is, from a regulatory perspective, to make the specific causes of a particular decision comprehensible. Only then can errors be detected and infringements of rights be penalised effectively. One approach to better understand how software-based processes work is to record individual program steps digitally and use them for test purposes. This may be required for personal data processing in accordance with data protection law in order to fulfil the accountability requirement.

Firstly, such a requirement to document and log the data sets and models used, the level of granularity, the retention periods and the intended purposes should be specified in data protection law so as to provide controllers and processors with greater legal clarity. Secondly, systems which have a significant potential for harm (Level 4) should be required to document and log program processes. The data sets and models used should be described in such a way that they are comprehensible to the supervisory institutions carrying out oversight measures (as regards the origin of the data sets or the way in which they are prepared, for example, or the optimisation goals pursued using the models).

4.2 Other requirements for algorithmic systems

4.2.1 General quality requirements for algorithmic systems

System operators should be required by standards to **guarantee a minimum level of quality, from both a technical and a mathematical-procedural perspective**. The procedural criteria imposed must ensure that algorithmically derived results are obtained in a correct and lawful manner. For this purpose, quality criteria can be imposed, in particular as regards the mathematical model, specific processing methods, corrective and control mechanisms or data quality and system security. To strike a balance between the conflicting fundamental rights of the software operator and the subjects of decisions, the requirements for the validity of mathematical models and the relevance of the underlying data should become stricter as **the potential of algorithmic systems to cause harm increases**.

In the case of algorithm-based and algorithm-driven decisions, **skill sensitivity** should also be built into the **design**, for example by deliberately mandating the completion of certain **training modules**. In situations where decision assistants are used, for example, it has proven particularly helpful to introduce system-imposed **role changes** at certain intervals, or in other words to assign the user the task of making the initial decision before he or she sees the algorithmically derived proposal. **Attention tests** are another option, albeit one which the individual user may perceive as more onerous; they require him or her to detect incorrect decisions which the computer has deliberately interspersed among correct ones – and therefore also require the true nature of the proposals in question to be identified in good time before anyone suffers harm.

Steps should also be taken to ensure that improvement processes are carried out fairly and with regard to the interests of everyone affected; particular attention should be paid to ensuring that suitable **feedback loops** take the interests of the data subjects and not just of the system operators into account. With regard to data quality, it would also be advisable to specify the extent to which the use of estimated or "proxy" data (→ see Part C, section 2.2.2 et seq. above) should be permitted or forbidden for certain areas of application.

In addition to the requirements placed on the algorithmic system by the actual processing purpose, the **security** requirements should also be fulfilled at the design stage. The individual requirements of all parties involved should be taken into consideration in order to ensure that appropriate design-related decisions are taken as part of conceptualisation, implementation and operation. Although the system operator usually has the main responsibility for the risk assessment, the system operator can fulfil this responsibility only with access to sufficient documentation, e.g. the manufacturer's risk impact assessment. There also needs to be clarity as to who is responsible for which area. For areas identified as critical, the Data Ethics Commission recommends setting out legal specifications relating to

- minimum standards for the required security and the measures to be taken;
- specific details regarding how and under what conditions manufacturers or system operators must design and conduct test procedures (for example to identify bias and/or discriminatory distortion);
- legal consequences in the case of security gaps or other errors;
- duties to draw up documentation on functionality and on tests which users receive in order to be able to assess risks;
- obligations to carry out system updates within a specified time frame and to report on them.

4.2.2 Special protective measures in the use of algorithmic systems in the context of human decision-making

Humans must not become an object of technology. This key principle for the regulation of algorithmic systems is particularly pertinent where algorithmic systems are used in order to support human decisions or automate decision-making processes, i.e. replace human decision-making with technical processes.

Article 22 GDPR codifies this principle in applicable existing law for certain algorithmic systems which fall within the scope of the GDPR: no one can be subject to a decision based solely on automated processing, including profiling, which produces legal or other significant effects concerning him or her – unless it is necessary for entering into, or performance of, a contract, is based on the data subject's explicit consent or is authorised by law. Where such a fully automated decision is permitted, the data controller must implement protective measures in order to safeguard the data subject's rights and interests[6] Stricter duties to provide information and rights of access also apply.[7]

6 Cf. Article 22(3) GDPR.
7 Cf. Article 13(2)(f) GDPR, Article 14(2)(g) GDPR and Article 15(1)(h) GDPR.

The Data Ethics Commission believes that various aspects of these rules currently **require further clarification**. The duties to provide information and rights of access connected with Article 22 GDPR ("including profiling") should refer to automated **profiling as such**. Individual credit reference agencies, for example, do not consider themselves subject to these rules, claiming that they apparently simply conduct profiling, while the "decisions" are made by the companies which, for example, request a credit score. The Data Ethics Commission believes this argument does not sufficiently take the intention of the GDPR into account, as the long-term effects on the data subjects of such profiling could, firstly, be significant, and secondly, the GDPR particularly emphasises profiling. Where the data protection authorities and the courts are able to apply the applicable law to the appropriate extent by means of an interpretation based on the protective purpose of the GDPR, this is to be welcomed. However, at the same time, given how sensitive this issue is in terms of fundamental rights, the democratically legitimised legislator is called upon to further specify the legal framework conditions soon in order to create legal certainty as quickly as possible. The Data Ethics Commission recommends that the Federal Government should advocate for this as part of the evaluation of the GDPR.

Clarification and specification is also needed regarding the question as to when a decision pursuant to **Article 22 GDPR** is "based solely" on automated processing of personal data and the scope of the term "similar effect" and of the protection rights under Article 22(3) GDPR. The Data Ethics Commission recommends that the Federal Government should advocate, in the evaluation of the GDPR, for the scope of Article 22 GDPR to be fleshed out. The potential for harm caused by the algorithm-determined decision-making systems, which was the original guiding principle of Article 22 GDPR, does not, in particular, categorically differ from that of many algorithm-driven decision-making systems. In particular, the tendency of the humans involved simply to accept the recommendations of algorithmic systems and not exercise discretion plays a role.

In view of the fact that the potential for harm of algorithm-based systems varies heavily in the detail, the Data Ethics Commission does not believe that it would be appropriate to generally broaden the prohibitory principle of Article 22 GDPR. In particular, the principle of human final decision-making pursuant to Article 22(3) GDPR is not suitable for all algorithmic systems in equal measure. As such, for algorithmic systems where no "decision" is taken by the system within the meaning of the current wording of Article 22(1) GDPR, a right to having the final decision made by a human would often not be very practical and also often not desirable. Instead, the Data Ethics Commission recommends a risk-adapted regulatory regime which provides individuals with appropriate safeguards (in particular against profiling) and opportunities to defend themselves if mistakes are made or if their rights are jeopardised.

The legal notion that humans must not become a mere object of technical systems should also form a **central legislative anchor point** within the horizontal EU legal instrument of a EU-ASR (→ see section 3.3 above) on the risk-adapted regulation of algorithmic systems, which the Data Ethics Commission recommends, and within the accompanying sectoral legal instruments. These legal instruments should therefore include provisions which also set out specifications for algorithm-based decision-making systems outside of the scope of Article 22 GDPR. In so far as the new layer of regulation also covers algorithmic systems which also fall within the scope of Article 22 GDPR (which may have been modified in light of the recommendations made here), the **regulatory systems** must be precisely **synchronised**.

4.2.3 Right to appropriate algorithmic inferences?

The Data Ethics Commission believes that the processes involved in the data-based generation of **algorithmic inferences** on the supposed interests, tendencies and character traits of individuals, in particular consumers, deserve maximum social and political attention. The digital economy is awash with such inferences. They are very characteristic of many digital business models which are geared towards the detailed personalisation of certain offers or services. Many consumers appreciate the convenience of such offers and services; however, they can also lead to risks if inferences are made based on an incorrect pool of data or if results with inappropriate contents are obtained on account of the inadequacy of other system components.

In order to prevent the risks which could be posed by certain algorithmic inferences, many want to grant data subjects a legal "right to appropriate inferences".[8] That proposal sets out a comprehensive package of measures which would give each data subject an effective tool for monitoring the inferences concerning them generated by operators of algorithmic systems. In addition to a substantive right to be subject to appropriate inferences, it sets out an obligation on the part of the system operator, without having to be requested for the information, to inform the individual concerned that the inferences drawn were "appropriate" and the reasons why that is the case.

The Data Ethics Commission welcomes the debate which the proposal of such a "right to appropriate inferences" has triggered. However, it points out that such a right could affect constitutionally protected interests of operators of algorithmic systems. In the view of the Data Ethics Commission, any regulatory development of the proposal should take these protection aspects into consideration, for example by limiting the scope to systems which have a high level of criticality due to their relevance in terms of participation and fundamental rights.

4.2.4 Legal protection against discrimination

One of the main aims of the regulation of algorithm-based, algorithm-driven and algorithm-determined decision-making systems is to prevent discrimination against an individual based on a characteristic set out in Article 3(3) of the Basic Law for the Federal Republic of Germany and/or Article 21(1) of the Charter of Fundamental Rights of the European Union, as well as any objectively unjustified discrimination, and to protect the personal integrity of individuals concerned. Whilst state bodies have a direct **obligation to uphold fundamental rights** when undertaking any kind of state activity and are therefore subject to a comprehensive prohibition on discrimination, a sub-constitutional basis is required for private actors. The technical legal starting point for this is essentially the **German General Act on Equal Treatment**, also serving to incorporate according EU directives into German law, alongside general clauses in German private law, for example on unconscionable contracts.

For discrimination between private individuals to fall under the General Act on Equal Treatment, firstly the discrimination must be on the grounds of a **sensitive characteristic** (race, ethnic origin, gender, religion, disability, age or sexual orientation); secondly, the **situational scope** must be open (employment context or access to goods and services, including housing, which are available to the public).

8 Omer Tene / Jules Polonetsky: Northwestern Journal of Technology and Intellectual Property, 2013 (11:5), pp. 279 et seq.; Sandra Wachter / Brent Mittelstadt: Columbia Business Law Review, 2019 (2), p. 1, et seqq. The proposal consists of a material component and a procedural component.

In principle, the provisions of the General Act on Equal Treatment already cover discrimination by algorithmic systems in accordance with applicable law. However, not all matters susceptible to discrimination are included in the scope of the General Act on Equal Treatment, and that Act does not cover all sensitive situations where algorithmically established results trigger or facilitate discrimination (e.g. in the case of a mortgage offer based on an individual risk assessment). It is therefore worth considering to, for example, broaden the **situational scope of the General Act on Equal Treatment** to include all automated decision-making processes or additionally incorporating individual areas relating to algorithmic inferences which are particularly sensitive in terms of personality.[9] This primarily concerns areas which could have a long-lasting negative effect on a person's way of life, such as consumer contracts drawn up based on scoring or on high-risk procedures, facial recognition methods or price discrimination in certain areas of life such as healthcare. The contractual partner's general freedom of action which is equally constitutionally protected must also be properly taken into consideration.

It is also necessary to discuss whether, in the context of algorithmic systems, legislators should remove the restrictive reference to specific grounds for discrimination. The discriminatory effects of algorithmic systems only sometimes reflect bias which exists within society with regard to **classic grounds for discrimination**, for example in so far as the bias is in the training data or in the model used. This would, for example, be the case if a system which is used to select candidates was trained using the data of successful managers from the past who were overwhelmingly male. However, the potential for algorithmic systems to discriminate extends far beyond this, for example if a disadvantage is systematically associated with group attributes against which discrimination is not prohibited by law (e.g. home address in a specific district) or with correlations determined by means of pattern recognition but which are really more random. To some extent, these situations can already be managed in the form of **indirect discrimination**. In that respect, a suitable relaxation of the rules relating to the burden of proof may also possibly be required. To some extent, however, entirely new issues of fairness also arise. These concern not only the distribution of opportunities to the detriment of traditionally marginalised communities but also the exclusion of groups which have been thrown together based on more or less coincidental attributes: the specific characteristics of machine learning are creating **new grounds for discrimination** which, however, could have enormous widespread impacts on account of the fact that trained algorithms are also used in other areas of application.

9 Mario Martini, Juristenzeitung (JZ), 2017, p. 2021.

It is therefore appropriate to consider broadening protection to include every systematic and objectively unjustified type of discrimination based on a group attribute. The Data Ethics Commission recommends that the Federal Government should also **examine appropriately adjusting the General Act on Equal Treatment or alternatively anchoring protection in any future specific algorithm legislation**. A particular regulatory problem is that there is a (fundamentally ever-growing) plethora of group attributes which could lead to such algorithmic discrimination, and hence the systematic nature would be the sole criterion for differentiating between prejudices which are relevant and irrelevant in terms of discrimination law. Any corresponding regulation for substantive protection against discrimination would therefore, in any case, have to be accompanied, on the one hand, by corresponding duties of disclosure and duties to state reasons and, on the other, by various internal and external oversight mechanisms for which the new regulation would provide the substantive examination criteria. The consequences of such regulation on all the parties involved would, in any case, have to be meticulously assessed and weighed up.

Irrespective of the issue of broadening the definition of the offence, thought should be given to whether the **rules on the burden of proof** already sufficiently reflect the characteristics of algorithmic systems. Ascertaining indirect discrimination requires neither proof of any intent to discriminate nor any unambiguous proof of causality. In fact, all the injured party has to prove is a correlation between the decisions and sensitive criteria. Where algorithmic systems are used, however, this proof is generally difficult for the affected parties to provide.

The Data Ethics Commission therefore recommends that legislators should enact legislation clarifying the requirements for providing proof of discrimination by operators of algorithmic systems and lower such requirements further for affected parties as needed. For this reason, the General Act on Equal Treatment should always be considered together with **rights of access and duties to state reasons** (→ see section 4.1.2) without which the injured party would often be unable to exercise his or her rights. The protection interests of third parties and of system users affected as a result must be given sufficient consideration.

4.2.5 Preventive official licensing procedures for high-risk algorithmic systems

In the case of algorithmic systems with regular or appreciable (Level 3) or even significant potential for harm (Level 4), in addition to existing regulations, it would make sense to establish licensing procedures or preliminary checks carried out by supervisory institutions in order to prevent harm to data subjects, certain sections of the population or society as a whole.

Summary of the most important recommendations for action

Instruments

45

The Data Ethics Commission recommends the introduction of a **mandatory labelling scheme** for algorithmic systems of enhanced criticality (Level 2 upwards). A mandatory scheme of this kind would oblige operators to make it clear whether (i.e. when and to what extent) algorithmic systems are being used. Regardless of system criticality, operators should always be obliged to comply with a mandatory labelling scheme if there is a risk of confusion between human and machine that might prove problematic from an ethical point of view.

46

An individual affected by a decision should be able to exercise his or her right to "meaningful **information** about the logic involved, as well as the scope and intended consequences" of an algorithmic system (cf. GDPR) not only in respect of fully automated systems, but also in situations that involve any kind of **profiling**, regardless of whether a decision is taken on this basis later down the line. The right should also be expanded in the future to apply to the algorithm-based decisions themselves, with differing levels of access to these decisions according to system criticality. These measures may require the clarification of certain legislative provisions or a widening of regulatory scope at European level.

47

It certain cases, it may be appropriate to ask the operator of an algorithmic system to provide an **individual explanation** of the decision taken, in addition to a general explanation of the logic (procedure) and scope of the system. The main objective should be to provide individuals who are affected by a decision with comprehensible, relevant and concrete information. The Data Ethics Commission therefore welcomes the work being carried out under the banner of "Explainable AI" (efforts to improve the explainability of algorithmic systems, in particular self-learning systems), and recommends that the Federal Government should fund further research and development in this area.

48

In view of the fact that, in certain sectors, society as a whole may be affected as well as its individual members, also particular **parties who are not individually affected** by an algorithmic system should be entitled to access certain types of information about it. It is likely that rights of this kind would be granted primarily for journalistic and research purposes; in order to take due account of the operator's interests, they would need to be accompanied by adequate protective measures. The Data Ethics Commission believes that consideration should also be given to the granting of unconditional rights to access information in certain circumstances, in particular when algorithmic systems with serious potential for harm (Level 4) are used by the State.

49

It is appropriate and reasonable to impose a legal requirement for the operators of algorithmic systems with at least some potential for harm (Level 2 upwards) to produce and publish a proper **risk assessment**; an assessment of this kind should also cover the processing of non-personal data, as well as risks that do not fall under the heading of data protection. In particular, it should appraise the risks posed in respect of self-determination, privacy, bodily integrity, personal integrity, assets, ownership and discrimination. It should encompass not only the underlying data and logic of the model, but also methods for gauging the quality and fairness of the data and the model accuracy, for example the bias or the rates of (statistical) error (overall or for certain sub-groups) exhibited by a system during forecasting/category formation.

50

To provide controllers and processors with greater legal clarity, further work must be done in terms of fleshing out the requirements to **document and log** the data sets and models used, the level of granularity, the retention periods and the intended purposes. In addition, operators of sensitive applications should be obliged in future to document and log the program runs of software that may cause lasting harm. The data sets and models used should be described in such a way that they are comprehensible to the employees of supervisory institutions carrying out oversight measures (as regards the origin of the data sets or the way in which they are pre-processed, for example, or the optimisation goals pursued using the models).

51

System operators should be required by the standard-setting body to guarantee a minimum level of **quality, from both a technical and a mathematical-procedural perspective**. The procedural criteria imposed must ensure that algorithmically derived results are obtained in a correct and lawful manner. For this purpose, quality criteria could be imposed, in particular as regards corrective and control mechanisms, data quality and system security. For example, it would be appropriate to impose quality criteria on the relationship between algorithmic data processing outcomes and the data used to obtain these outcomes.

52

The Data Ethics Commission believes that a necessary first step is to clarify and flesh out in greater detail the scope and legal consequences of Article 22 GDPR in relation to the use of algorithmic systems in the context of human decision-making. As a second step, the Data Ethics Commission recommends the introduction of additional **protective mechanisms for algorithm-based and algorithm-driven decision-making systems**, since the influence of these systems in real-life settings may be almost as significant as that of algorithm-determined applications. The prohibitory principle followed to date by Article 22 GDPR should be replaced by a more flexible and risk-adapted regulatory framework that provides adequate guarantees as regards the protection of individuals (in particular where profiling is concerned) and options for these individuals to take action if mistakes are made or if their rights are jeopardised.

53

Consideration should be given to expanding the **scope of anti-discrimination legislation** to cover specific situations in which an individual is discriminated against on the basis of automated data analysis or an automated decision-making procedure. In addition, the legislator should take effective steps to prevent **discrimination on the basis of group characteristics** which do not in themselves qualify as protected characteristics under law, and where the discrimination often does not currently qualify as indirect discrimination on the basis of a protected characteristic.

54

In the case of algorithmic systems with regular or significant (Level 3) or even serious potential for harm (Level 4), it would be useful – as a supplement to the existing regulations – for these systems to be covered by **licensing procedures or preliminary checks** carried out by supervisory institutions, in the interests of preventing harm to individuals who are affected, certain sections of the population or society as a whole.

5. Institutions

The Data Ethics Commission takes the view that the burden of responsibility for the ethically justified and lawful use of algorithmic systems must be shared and rest on several sets of shoulders. The institutions and supervisory structures which currently exist are not sufficiently prepared to effectively oversee monitoring of algorithmic systems at various levels. The Data Ethics Commission therefore urges the Federal Government to expand and reorient the competences of existing supervisory institutions and structures and set up new institutions and structures where necessary.

5.1 Regulatory powers and specialist expertise

5.1.1 Distribution of supervisory tasks within the sectoral network of oversight authorities

The Data Ethics Commission recommends that the Federal Government should in principle entrust regulatory supervisory tasks and oversight powers in each case to authorities which already have **sector-specific expertise**. In the view of the Data Ethics Commission, the same should apply to matters which fall within the administrative competence of States (*Bundesländer*).

Specifically, the Data Ethics Commission believes that it would make sense to entrust oversight of the use of algorithmic systems by private parties in the sectors of the digital economy in which authorities with sector-specific responsibility already exist to those **existing authorities**. As examples, authorities such as the Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht*, BaFin), the Federal Network Agency (*Bundesnetzagentur*, BNetzA), the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, BSI) and the Federal Motor Transport Authority (*Kraftfahrtbundesamt*, KBA) come into mind. Furthermore, the Federal Cartel Office (*Bundeskartellamt*, BKartA) and the data protection supervisory authorities would have special status, as they both have horizontal responsibilities, i.e. responsibilities which span the various different sectors of the economy.

The Data Ethics Commission believes that a national and EU-level **"oversight network for critical algorithmic systems"** should be set up in order to coordinate the activities of the authorities entrusted with algorithm supervisory tasks. In particular, rules on the distribution of responsibilities within the network, the exchange of information, the organisation of administrative procedures carried out by the network and legal protection would be appropriate for such purposes.

In order to prevent any gaps in supervision, the Data Ethics Commission urges the Federation and the *Länder* to identify areas where there is **currently no sector-specific authority with sufficient expertise** to which oversight tasks could be assigned for monitoring critical algorithmic systems. In the view of the Data Ethics Commission, in such cases, it will often be appropriate, in the event of a corresponding need for oversight, to entrust matters to one of the existing authorities with horizontal responsibility. In the case of algorithmic systems which process sensitive personal data, the data protection authorities, for example, may have the adequate expertise. However, the Data Ethics Commission believes that, in particular cases, it may be necessary to create completely new regulatory control structures. In the light of ever-changing technical developments, the Federation and the *Länder* should regularly review the situation.

Authorities are faced with a structural challenge in effectively executing their algorithmic system oversight tasks: the object which is the focus of their oversight work is technically highly complex and is subject to dynamic change. The Data Ethics Commission therefore believes that **providing the authorities with practical skills** will be particularly important. It firmly recommends that the Federal Government should provide the federal authorities with the financial, human and technical resources required. The draft Salary Structure Modernisation Act (*Besoldungsstrukturenmodernisierungsgesetz*), which is expected to increase the salaries and bonuses of public-sector IT professionals and establish new regulations for them as from 2020, is without doubt a welcome first step. However, in the light of how difficult it is to attract well-trained professionals to the public sector, further measures will soon be required.

The Data Ethics Commission also recommends that the Federal Government should set up an official unit in the form of a **competence centre for algorithmic systems** to provide the sectoral authorities with support in monitoring algorithmic systems. The responsibility of such a body should not only acquire, analyse, further develop and impart the technical methodological knowledge required for supervising critical algorithmic systems. It should (in coordination with and at the request of the sector-specific authorities) also primarily support the sector-specific supervisory authorities in building up the expertise needed to carry out their tasks and assess the criticality of algorithmic systems. This will extend in particular to the centre's task of further developing **criteria, processes and tools** for the oversight of algorithmic systems. This will also include **standards for assessing criticality** and checking the compliance of critical algorithmic systems. Such a centre of competence will also have an important **intermediary advisory role**: as far as possible, it will advise not only bodies of the Federation, the *Länder* and municipalities, but also manufacturers, system operators, system users and data subjects with regard to the use and development of algorithmic systems. It will also be involved in international and European initiatives designed to build up sufficient oversight expertise including standardisation procedures. However, the competence centre should not have its own supervisory powers. These remain with the sectoral supervisory authorities. The service unit should either be created as a new, autonomous federal authority or be attached to an existing cross-sectional authority, such as the Federal Office for Information Security.

The Data Ethics Commission considers that it would also make sense to establish a corresponding body at **European Union level** in the future, for example in the form of an agency, and the Federal Government should work towards achieving this.

In principle, the Data Ethics Commission sees no reason why state bodies should not be able to make use of the **expertise of private individuals or entities** in carrying out their tasks and in building up their own in-house expertise or to involve private individuals or entities in the execution of their tasks, as long as such cooperation complies with the general constitutional and administrative specifications applicable to such cooperation. Conversely, corresponding cooperation, for example also by entrustment, may be used in order to deal with the current lack of qualified specialists and expertise in the public sector.

5.1.2 Definition of oversight powers according to the tasks involved

The regulating body should, **by law**, clearly **assign** the relevant competent authorities the **powers of intervention**, including rights to information and rights of inspection and access, required for the supervision of algorithmic systems. Blueprints for such regulatory powers for content control can be found in various areas of the law.[10]

The competent supervisory authorities must, at all times, be able to **examine** algorithmic systems in sensitive areas of application or those with a high potential for harm. The audit and test procedures used in doing so must, in particular, cover systems where there is interaction with the user. This may, for example, take place via standardised interfaces. Such access can be used to carry out what are known as input-output tests, which check, for example, whether an algorithmic system systematically discriminates against groups. This is particularly useful in the case of learning systems which adapt their internal rules over time. Steps must be taken here to ensure that any testing of learning systems does not lead to a change in the system of rules whereby the system learns from the test data during the test.

10 For example, Article 58 GDPR governs the investigative powers relating to data protection supervision and Section 32e of the [German] Act against Restraints of Competition (*Gesetz gegen Wettbewerbsbeschränkungen*, GWB) governs sector inquiries by the Federal Cartel Office. Oversight of high-frequency trade by financial supervisory authorities is based on Section 6(4) of the [German] Securities Trading Act (*Gesetz über den Wertpapierhandel*, WpHG) and Section 3(4)(4)(5) of the [German] Stock Exchange Act (*Börsengesetz*, BörsG) amended version in conjunction with Section 7(3) of the Stock Exchange Act.

When assigning legal authority, steps must be taken to ensure that the supervisory authorities have the power, in the event of a proven breach of the law, to force operators of algorithmic systems to configure systems in compliance with the law (for example by adapting the pool of data used) and, where necessary, apply **penalties**. Provided that it is commensurate with the case in question, the supervisory authorities should also be able to impose official **bans** on the use of unlawful algorithmic systems (or their components).

5.1.3 Criticality-adapted extent of oversight

All elements of an algorithmic system must be taken into account in order for its behaviour to be effectively audited. An audit conducted by authorities may, and potentially must, extend to the training data and learning processes used, the final rule-based model as well as the input and output data underlying the decisions. Quality indicators regarding the pool of data used and model accuracy (training model, final decision model) can also be taken into consideration in order to identify a system's bias or rates of (statistical) error (overall or for certain sub-groups). From a methodological perspective, a test may be carried out by analysing large amounts of data, reviewing the weighting of factors in complex multidimensional systems and analysing input-throughput-output.

Due to the complex nature of the subject matter and amounts of data involved, the use of control algorithms can significantly increase the efficiency and effectiveness of the audit. They can systematically look for conspicuous patterns in the pool of data used and the results of an algorithmic system which can, for example, shed light on a case of discrimination.

The extent of oversight required in each specific case should be determined based on the area of application and system criticality. In the case of systems which have only some potential for harm (Level 2), it may suffice for legislators to limit regulatory oversight to an inspection of the results in the event of a system's documented failure. However, in areas with a high potential for harm, it may be necessary to stipulate that system operators must use a standardised interface.

In the view of the Data Ethics Commission, the question as to whether regulatory oversight affects system operators' trade and **business secrets** or third parties' **privacy rights** is not an issue at any level of the criticality pyramid. As supervisory authorities are obliged to treat all information obtained as part of their oversight work as confidential due to professional secrecy, these aspects do not represent any legal obstacle to far-reaching powers for full and detailed audits.

The proper interpretation of test results is, from a technical perspective, anything but trivial. In particular, it is not always clear whether they really unearth an error by an algorithmic system. This restricts their ability to provide evidence. The quality and informative value of the different test procedures and audits therefore also need to be agreed on – in particular with regard to their probative value in court proceedings in order to enforce the rights of the parties affected. The Data Ethics Commission therefore recommends that the Federal Government should support initiatives to **develop statistical technical standards for test procedures and audits**, where necessary differentiated by areas of application. The competence centre for algorithmic systems (→ see section 5.1.1) should take a leading role in such endeavours.

Use case: Personalised prices II – ex-post controls by supervisory institutions

Supervisory institutions could check whether algorithmic pricing systems used in e-commerce comply with the law or discriminate, for example, against protected population groups (within the meaning of the General Act on Equal Treatment). Supervisory authorities could look for conspicuous patterns in the pool of data used and the issued prices, which may shed light on a possible case of discrimination.

To do so, those carrying out the supervision do not have to comprehend the (potentially highly complex) rules of the underlying algorithm by analysing the code. Effective oversight can be carried out with the help of statistical tests which analyse how, all other things being equal, issued prices change depending on input data which are associated with certain population groups. If, for example, the system issues higher prices for consumers when only the gender is changed from "male" to "female" in the input data or if the issued prices correlate with attributes, protected under equality legislation, of individual population groups (for example via proxies), this can be mathematically statistically determined.[11]

11 Cf. Gesellschaft für Informatik: Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren. Gutachten der Fachgruppe Rechtsinformatik der Gesellschaft für Informatik e.V. im Auftrag des Sachverständigenrats für Verbraucherfragen [Gesellschaft für Informatik: Technical and legal considerations regarding algorithmic decision-making processes. Report by the Legal Informatics expert group of Gesellschaft für Informatik e.V. at the request of the Advisory Council for Consumer Affairs], Berlin, pp. 63 et seqq. (available at: *www.svr-verbraucherfragen.de/wp-content/uploads/GI_Studie_Algorithmenregulierung.pdf*).

5.2 Corporate self-regulation and co-regulation

It is neither possible nor necessary for the legislator to implement blanket regulations covering all algorithmic systems. Instead, various models of self-regulation and co-regulation could also essentially provide sufficient responses for certain situations. Co-regulation involves regulatory approaches which navigate between state regulation and private self-regulation and is characterised by the combination of a public/state component and a private/institutional component.

5.2.1 Self-regulation and self-certification

The Data Ethics Commission recommends self-regulation in the form of an internal audit conducted by the manufacturer or operator of the algorithmic system for the lowest level of the criticality pyramid. This could be supported by self-certification of manufacturers and operators on the basis of specific standards for algorithmic systems. The particular advantage of such a system would be that the self-certification bodies would have the necessary know-how on account of their **close connection to the specific topics**. As a result, experts, even from the companies in question, could take the legal standards and monitoring of compliance therewith into consideration, including at the development stage, and, where necessary, also incorporate their corporate expertise into the regulatory mechanisms institutionally. Admittedly, purely internal and voluntary self-regulation would not constitute an independent monitoring and, in the event of breaches, would not ensure any effective implementation of penalties.

The self-regulation architecture could be supplemented with a model involving regulated self-monitoring, which would set out external standards for quality and risk management of self-monitoring which could also be externally monitored. A similar system is set out in the GDPR, in which Article 40 establishes the option to specify general clauses of the GDPR and make them applicable to specific real-life circumstances which are significant to the parties subject to the codes of conduct as well as set minimum standards specific to the sector in question. In order to be able to guarantee that the regulation would be as effective as intended, effective monitoring must ensure actual compliance with the approved codes of conduct pursuant to Article 40 GDPR. Not only would the codes of conduct themselves have to be drawn up, but the procedural rules relating to monitoring, control and the implementation of penalties for cases of non-compliance would also have to be set out.

Where a provider signs up for voluntary self-monitoring and verifiably demonstrates compliance with the agreed procedures, the standard-setting body may grant privileges in terms of supervisory measures. Such an approach would be based on the condition that, in exercising their corporate responsibility and in cooperation with a private self-monitoring body, providers would have to develop procedural standards which would be recognised by the supervisory authority. The involvement of civil society organisations in the preparatory work would be essential in order to be able properly to represent the interests of citizens and consumers and take them into consideration.

5.2.2 Creation of a code of conduct

For the concept of regulated self-regulation, it would be worth considering including an **Algorithmic Accountability Code**, adopting a "comply or explain" approach which is well-established in other parts of the legal system. It could oblige parties subject to regulation to state whether or not and the extent to which they are following the recommendations of the code.[12] False statements would be subject to sanctions. As such, a code to be drawn up could be binding in nature by holding companies and authorities responsible for the consequences of the use of algorithmic systems. It could, for example, be developed based on corporate digital responsibility guidelines (→ see Part D, section 2 above) or conversely also help to shape such guidelines. What level of granular detail for codes and guidelines is practical and/or the sector-specific ethical challenges for which a specific code would be useful will become clear.

The quality of the defined requirements and the framework conditions, i. e. the opportunities for independent external parties to carry out checks and the ability to impose penalties in the event of breaches, would be essential in ensuring that a code had a control function. Responsibility for developing such a code should be assigned to an independent commission with equal representation of manufacturers, operators, the scientific community and civil society. It remains to be seen whether the Government Commission on the German Corporate Governance Code *(Regierungskommission Deutscher Corporate Governance Kodex)* (*www.dcgk.de*) could be a model for this.

In addition or alternatively, binding statements by and between manufacturers and operators of algorithmic systems could be considered.

12 Mario Martini, Juristenzeitung (JZ), 2017, p. 1022 et seq.

5.2.3 Quality seals for algorithmic systems

Establishing quality seals for algorithmic systems are sensible in order to support effective algorithm regulation. They could take the form of voluntary or mandatory evidence of protective measures which would make the extent to which an algorithmic system meets certain requirements clear to users. It would be important to clarify who would define the requirements of a quality seal and who would specifically be responsible for fulfilling the requirements connected with the quality seal and the extent to which breaches would be subject to penalties. As in the case of an Algorithmic Accountability Code, responsibility for defining the requirements of a quality seal should be entrusted to an independent commission with equal representation of operators of algorithmic systems, the scientific community and civil society.

5.2.4 Contact persons for algorithmic systems in companies and authorities

Companies and authorities which work with critical algorithmic systems (as from Level 2) should (at least starting at a certain size of company or authority) appoint a contact person responsible for communications with authorities and cooperation. In all cases, it must be ensured that such a contact person has **specific expertise**. He or she will monitor the use of algorithmic systems internally and provide the company's or authority's management team with advice and will be functionally independent. As is the case with data protection officers, the contact person could act as a link between the supervisory authority, operators of algorithmic systems and affected groups of people. This would also help to ensure proper awareness of problems within companies and authorities and increase oversight pressure from inside.

5.2.5 Involvement of civil society stakeholders

In order to ensure that the interests of civil society and affected companies are properly taken into account as part of audits of algorithmic systems, **advisory boards** should be set up within sector-specific competent authorities, and civil society stakeholders should also, for example, be involved in connection with a code. Such advisory boards should feature a balance of representatives of civil society organisations and individuals appointed by companies in order to ensure that both the interests of affected individuals and groups and the interests of affected companies are properly taken into account as part of audits.

5.3 Technical standardisation

In the view of the Data Ethics Commission, standardisation organisations such as ISO/IEC, IEEE, IETF, ITU, ETSI, W3C, CEN and DIN, which set technical standards for information and communications technologies, could significantly help with forming out sector-specific requirements for algorithmic systems. Technical standards which take ethical and legal requirements into consideration could provide legal certainty for companies which develop and use algorithmic systems. They could also easily translate the requirements for the legality of algorithmic systems into specific guidelines in individual sectors.

The Data Ethics Commission believes that technical standards would essentially be useful tools to bridge the gap between "classic" state regulation and purely private self-regulation. It therefore recommends that the Federal Government should suitably work to develop and adopt technical standards designed to prevent the risks posed by algorithmic systems.

However, in the view of the Data Ethics Commission, the Federal Government should also not lose sight of the fact that **technical standards have their limitations** (→ see Part D, section 6 above). Technical standards are no substitute for defining clear legal requirements for algorithmic systems or for regulatory supervision of the use of such systems. For constitutional reasons, the principle that the more citizens' fundamental rights are affected, the more detailed legal provisions should be, must be upheld. In practice, this means that legislators must, first of all, define the legal framework – not technical standard-setting committees. This will not least ensure that the integrity of decision-making will be protected, as the active participation of representatives of sectors and/or affected companies will ensure that, in addition to impressive technical expertise, the interests of such companies and/or sectors are, of course, also often taken into consideration first hand when the technical standards are drawn up.

5.4 Institutional legal protection (in particular rights of associations to file an action)

The system of granting competitors, competition associations and consumer associations the right to file an action has been an important feature of the German legal landscape for many years, and could play a key role in **civil society oversight** of the use of algorithmic systems. In particular, private rights of this kind allow civil society players with a legitimate mandate to enforce compliance with legislative provisions in the area of contract law and fair trading law without needing to rely on the authorities to take action and without needing to wait for individuals to authorise them. This civil law approach has particularly strong market focus and is characterised by swift responses and is therefore, by international standards, very successful. Associations are essentially politically and administratively independent and can therefore advocate, on their own authority and in the common interest of consumers and companies, for competition regulations and consumer rights to be efficiently protected against unfair business practices which are also damaging for consumers.

Anyone who does not comply with regulatory provisions will potentially benefit from an unfair competitive advantage. In order to prevent any competitive edge being gained by breaking the law, competition associations and consumer associations should be able to stop such legal infringements.

Summary of the most important recommendations for action

Institutions

55

The Data Ethics Commission recommends that the Federal Government should expand and realign the competencies of existing supervisory institutions and structures and, where necessary, set up new ones. Official supervisory tasks and powers should primarily be entrusted to the **sectoral supervisory authorities** that have already built up a wealth of expert knowledge in the relevant sector. Ensuring that the competent authorities have the financial, human and technical **resources** they need is a particularly important factor in this respect.

56

The Data Ethics Commission also recommends that the Federal Government should set up a **national centre of competence for algorithmic systems**; this centre should act as a repository of technical and regulatory expertise and assist the sectoral supervisory authorities in their task of monitoring algorithmic systems to ensure compliance with the law.

57

The Data Ethics Commission believes that initiatives involving the development of technical and statistical **quality standards for test procedures and audits** (differentiated according to critical application areas if necessary) are worthy of support. Test procedures of this kind – provided that they are designed to be adequately meaningful, reliable and secure – may make a vital contribution to the future auditability of algorithmic systems.

58

In the opinion of the Data Ethics Commission, particular attention should be paid to innovative forms of **co-regulation and self-regulation**, alongside and as a complement to forms of state regulation. It recommends that the Federal Government should examine various models of co-regulation and self-regulation as a potentially useful solution in certain situations.

59

The Data Ethics Commission believes that an option worth considering might be to require operators by law (inspired by the "comply or explain" regulatory model) to sign a declaration confirming their willingness to comply with an **Algorithmic Accountability Code**. An independent commission with equal representation – which must be free of state influence – could be set up to develop a code of this kind, which would apply on a binding basis to the operators of algorithmic systems. Appropriate involvement of civil society representatives in the drafting of this code must be guaranteed.

60

Voluntary or mandatory evidence of protective measures in the form of a specific **quality seal** may also serve as a guarantee to consumers that the algorithmic system in question is reliable, while at the same time providing an incentive for developers and operators to develop and use reliable systems.

61

The Data Ethics Commission takes the view that companies and authorities operating critical algorithmic systems should be obliged in future to appoint a **contact person**, in the same way that companies of a specific size are currently obliged to appoint a data protection officer. Communications with the authorities should be routed through this contact person, and he or she should also be subject to a duty of cooperation.

62

To ensure that official audits of algorithmic systems take due account of the interests of civil society and any companies affected, suitable **advisory boards should be set up within the sectoral supervisory authorities**.

63

In the opinion of the Data Ethics Commission, technical standards adopted by **accredited standardisation organisations** are a generally useful measure, occupying an intermediate position between state regulation and purely private self-regulation. It therefore recommends that the Federal Government should engage in appropriate efforts towards the development and adoption of such standards.

64

The system of granting **competitors, competition associations or consumer associations the right to file an action** has been an important feature of the German legal landscape for many years, and could play a key role in civil society oversight of the use of algorithmic systems. In particular, private rights of this kind could allow civil society players with a legitimate mandate to enforce compliance with legal provisions in the area of contract law, fair trading law or anti-discrimination law, without needing to rely on the authorities to take action and without needing to wait for individuals to authorise them.

6. Special topic: algorithmic systems used by media intermediaries

6.1 Relevance for the democratic process: the example of social networks

For many people, it would be impossible to imagine life these days without social networks, search engines and the like: they enable users to keep up to date on the latest news from around the world and from their circle of friends in real time, are platforms through which people can portray their lifestyles and communicate with each other, and can also be used for entertainment purposes and for business activity, including advertising.

On the whole, they are becoming increasingly important for private and public opinion-forming. In order to manage the wealth of information available, providers of such services use algorithmic systems which are designed, amongst other things, to identify the interests, tendencies and convictions of users, identify posts which are of potential relevance to them, present them with similar posts in order to encourage them to interact with the network, and filter out illegal or offensive posts. The economic aim is primarily to generate high advertising revenue.

Depending on their reach and content, media intermediaries can have a profound impact on the democratic process. More and more people are also using social networks to keep abreast of politics and world affairs. Social networks therefore offer users new opportunities to participate in the information society and, in that sense, constitute **media and factors for the exchange of information and opinions**.

At the same time, the fact that public debate is concentrated on only a few private platforms also poses a challenge for democracy. After all, as economic stakeholders, private operators of social networks have a vested interest in directing traffic to their networks and gearing activity on them primarily towards economic aspects rather than focusing on social interests in having a multi-faceted opinion-forming process for the benefit of the public good. The use of algorithmic systems which are **predominantly oriented on economic criteria** can have negative consequences for the diversity of opinions on social networks.

The use of services can also lead to the manipulation of opinions. On the one hand, this can happen unintentionally due to certain characteristics of underlying software, such as for example recommender systems. On the other hand, these systems can be used intentionally by various actors for manipulative purposes. Up to now, operators of social networks have not sufficiently guarded against such activities which threaten the foundations of democracy. What is more, a regulatory framework and social oversight are needed, in particular in view of their **high level of criticality**.

The Data Ethics Commission believes that, in the future, media intermediaries which have a gatekeeper role can ultimately develop a high potential for harm to our democracy and that there is a resulting **need for regulation**. The Data Ethics Commission believes that it is essential for legislators to create an appropriate regulatory framework for the use of algorithmic systems by media intermediaries. The Data Ethics Commission is of the opinion that, first of all, the operators of such platforms and providers of such services should themselves define and implement basic rules to ensure fairness in the opinion-forming process. However, this "digital domiciliary right" has its limitations, in particular where the integrity of the democratic process is affected. Depending on the market share and gatekeeper role of such platforms and services, operators have fundamental-rights-based obligations on account of the indirect third-party effect.[13] In the view of the Data Ethics Commission, these obligations should be specified more precisely in sub-constitutional law, in particular also with regard to the use of algorithmic systems by and on platforms and by and in services with a significant market share and a gatekeeper role. This is also relevant for the EU-ASR recommended by the Data Ethics Commission (→ see section 3.3 above).

Regulation is also needed to ensure regulatory fairness in comparison to broadcasters. The Data Ethics Commission recommends that the Federal Government should examine how risks posed by providers which have a particular power to influence opinions can be countered. A whole range of measures are possible, from greater transparency right through to ex-ante controls in the form of a licensing procedure for algorithmic systems which are relevant in terms of democracy.

6.2 Diversity and media intermediaries: the example of social networks

The wide variety of roles played by social networks and the predominantly high level of criticality of the algorithmic systems they use present particular challenges for the Data Ethics Commission's suggested approach of risk-adapted regulation of algorithmic systems. The Data Ethics Commission believes that positive legal provisions for social networks which, for example, increase the **transparency and range of discussions held there** and bolster the **rights of users** would be particularly constructive.

In any case, where social networks have dominant market share, the Data Ethics Commission calls for further measures to **safeguard diversity**, as defensive measures alone will not suffice. Algorithmic systems which operate in these types of networks and have impacts on the freedom and diversity of opinion-forming which are constitutive of democracy have an extremely high level of criticality on account of their reach alone. The Data Ethics Commission believes that legislators are therefore under an ethical and constitutional obligation to establish a **binding normative framework** for the regulation of media intermediaries in order to protect democracy. This may require transforming the regulatory framework governing the media.

Legislators must take suitable measures to ensure that the total range on offer reflects the variety of opinions that exist and guarantees **balance, neutrality and freedom from bias in the information society**.[14] This applies in particular to media intermediaries with a gatekeeper role and power to influence opinions. According to the Federal Constitutional Court, to safeguard pluralistic diversity, substantive, organisational and procedural regulations are needed which are focused on creating freedom of communication and are therefore suitable for producing the desired effects of Article 5(1) of the Basic Law for the Federal Republic of Germany.

13 Decisions of the Federal Constitutional Court 128, p. 249 (FRAPORT); 148, p. 267 et seqq., margin no. 32 et seqq. (Stadionverbot).
14 Cf. decisions of the Federal Constitutional Court 136, 9, 28 with further references.

In the light of this, the legislators in the *Länder*, which are responsible for media law, are obliged to implement the aforementioned provisions. The same applies to the legislators of an EU Regulation on Algorithmic Systems (EU-ASR (→ see section 3.3 above). As media intermediaries, video-sharing platforms (VSPs) are already subject to the Audiovisual Media Services Directive[15] because they provide user-generated content for the general public. The draft Interstate Media Services Agreement also covers media intermediaries. The Data Ethics Commission once again welcomes, in that respect, the provisions for the transparency of social networks set out in the draft **Interstate Media Agreement (Medienstaatsvertrag, MStV-E)** as an initial step in this direction.

The **legislators for the *Länder*** have plenty of scope and freedom for drawing up the provisions. However, they must decide on the regulation model themselves and must not leave it to private individuals to agree on. The Data Ethics Commission is of the view that plurality obligations for media intermediaries should, in any case, include the obligation to use algorithmic systems which, at least as an additional option, also provide access to an unbiased and balanced selection of posts and information which reflect a diverse range of different opinions.[16]

Based on these considerations, the Data Ethics Commission also recommends that the Federal Government should investigate whether there are other areas where, irrespective of the situation relevant to democracy discussed here, a corresponding obligation to establish requirements for neutrality and provisions on diversity seems necessary. **Protecting minors** from being influenced by and on social networks, for example, is one such consideration.

6.3 Labelling obligation for social bots

The democratic process is, in essence, based on people's freedom to form their own opinions and make their own decisions. However, bots, i. e. software programs which **give the impression that they are human users**, are used on various platforms. In the view of the Data Ethics Commission, it is highly problematic if such bots are used to manipulate individual users and/or public debate or guide the result of a vote one way or the other where political decisions are to be made. Firstly, the simulation of human traits falsely suggests that the statements made are the result of independent thought and of the independent formation of political opinions. Secondly, automation can massively increase the number and frequency of expressions of opinion, making it harder or even impossible to assess actual majorities of opinions. The Data Ethics Commission believes that regulatory intervention is required here.

On that basis, the Data Ethics Commission recommends implementing a **measure to enhance transparency** in the form of a labelling obligation for social bots on social networks. Based on general considerations, the Data Ethics Commission recommends that such a labelling obligation should be implemented anywhere where there is a risk that social bots could be mistaken for human interlocutors (→ see section 4.1.1 above). Given the particular potential to jeopardise the democratic process, the Data Ethics Commission furthermore believes, in any case, that a labelling obligation for social bots which have an impact on political opinion-forming processes is essential, even irrespective of any real risk of confusion.

15 Directive 2010/13/EU of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive).
16 Rolf Schwartmann / Maximilian Hermann / Robin Mühlenbeck, Multimedia und Recht (MMR), 2019 (8), p. 498 et seqq.

6.4 Measures to combat fake news

A labelling obligation for social bots could help to combat the automated spread of fake news. However, the Data Ethics Commission also believes that the concept of fake news is **not suitable as a starting point for any regulation relating to media legislation**. The presentation of a legal definition of fake news, which draws an objective and distinct line between an exaggerated or satirical expression of opinion and an intentional misrepresentation of news is impossible due to the complexity of human communications. Disinformation and the manipulation of public opinion-forming, typically associated with the term "fake news", can also result from true facts being presented selectively.

The Data Ethics Commission also, in particular, recommends to legislators that operators of social networks should grant their users an easy-to-exercise **right of reply** requiring the network to post the correction of a statement proven to be false (e. g. an invented quote) on the timeline or newsfeed, etc. of all users whom the network, using available data, can trace back to have been shown the false statement.

The Data Ethics Commission emphasises that the State must not create any incentives for collateral censorship through social networks. To provide protection from "overblocking", the Data Ethics Commission therefore believes it is necessary, in parallel to the obligations imposed on the operators, to grant the affected individuals prompt and efficient procedural protection mechanisms. The Data Ethics Commission believes that these should include in particular a **right to an effective process to reinstate deleted posts** provided that they do not break any laws; any invocation by networks of their own rules alone cannot suffice as grounds for permanent deletion/blocking. In the view of the Data Ethics Commission, such rights must apply to users with respect to all social networks.

6.5 Transparency obligations for news aggregators

Where social networks use algorithmic systems which also aggregate, select and present journalistic/editorial content of third parties in a generally accessible way, they should have to allow users and interested third parties enough insight into the technical procedure they use to select and prioritise news to make clear how a recommendation is arrived at in an individual case. The democratic information interest would essentially take precedence over any business secrets of media intermediaries. In the interests of a fair opinion-forming process and a fair exchange of opinions, such duties to disclose information should also stretch to any economic ties. For that reason as well, the Data Ethics Commission welcomes the current thoughts on reforming the Interstate Media Agreement (Medienstaatsvertrag, MStV-E) which call for corresponding transparency obligations for media intermediaries as soon as they have a certain reach.

Summary of the most important recommendations for action

Special topic: algorithmic systems used by media intermediaries

65

Given the specific risks posed by media intermediaries that act as **gatekeepers to democracy**, the Data Ethics Commission recommends that options should be examined for countering these risks, also with regard to influencing EU legislation (→ see Recommendation 43 above). A whole gamut of risk mitigation measures should be considered, extending through to ex-ante controls (e.g. in the form of a licensing procedure).

66

The national legislator is under a constitutional obligation to protect the democratic system from the dangers to the free, democratic and pluralistic formation of opinions that may be created by providers that act as gatekeepers by establishing a binding normative framework for **media**. The Data Ethics Commission believes that the small number of operators concerned should be obliged to use algorithmic systems that allow users (at least as an additional option) to access an unbiased and balanced selection of posts and information that embodies pluralism of opinion.

67

The Federal Government should consider measures that take due account of the risks typically encountered in the media sector in respect of all media intermediaries and also in respect of providers that do not act as gatekeepers or whose systems are associated with a lower potential for harm. These measures might include mechanisms for **enhancing transparency** (for example by ensuring that information is available about the technical procedures used to select and rank news stories, **introducing labelling obligations for social bots**) and establishing a right to post countering responses on timelines.

7. Use of algorithmic systems by state bodies

7.1 Opportunities and risks involved in the use of algorithmic systems by state bodies

Citizens will rightly expect their State to **use the best technology available** to carry out its duties. Depending on the type of duties, this will also include algorithmic systems. Systems already exist which can relieve state bodies of repetitive tasks (thereby expediting processes and freeing up human resources for complex cases) and which, in certain set-ups, improve the consistency and quality of state activity or, in the form of chatbots or voice assistants, for example, can facilitate citizens' access to justice.

At the same time, when using algorithmic systems, state bodies must uphold particularly high standards: firstly, they have a direct obligation to uphold fundamental rights as public authorities and secondly, state activity is, in general, expected to **set an example** for the whole of society. The institutional capacity and expertise, which the State must build up in order to ensure sufficient oversight of algorithmic systems used by private parties, must therefore also be used in order to guide and oversee the work carried out by state bodies themselves. In particular, the competence centre for algorithmic systems called for by the Data Ethics Commission is likely to play a key role in this context.

The use of algorithmic systems by state bodies must be treated **in principle as particularly sensitive** within the meaning of the criticality pyramid (at least Level 3). Therefore, in the view of the Data Ethics Commission, a comprehensive risk impact assessment must be carried out as a mandatory requirement for any ethically sound use of algorithmic systems. Furthermore, depending on the criticality of the systems used by the State, where necessary, other instruments discussed above and designed to ensure that citizens are protected should be put in place for such algorithmic systems used by the State. Farther-reaching legal data protection requirements will remain unaffected, as will other constitutional and administrative specifications for the design of the systems. Additionally, in the view of the Data Ethics Commission, in certain sectors where the use of algorithmic systems conflicts with constitutionally protected rights of overriding importance, the use of algorithmic systems should, irrespective of the protective measures taken in the case in question, be permitted only under very restrictive conditions or prohibited. This in particular concerns the use of algorithmic systems for the purposes of law-making and jurisprudence.

7.2 Algorithmic systems in law-making

The use of algorithmic systems within the government context of law-making is subject to restrictions. The Data Ethics Commission sees the democratic process, in the sense of people being able to form their own opinions and make their own decisions as freely as possible, as essentially sacrosanct. Automated support in law-making is therefore acceptable **at most for low-level ancillary tasks** (e.g. detecting inconsistent use of terms) and/or **legal instruments which are far removed from the democratic decision-making process** (e.g. catalogues of technical specifications in subsequent regulations). In both cases, the systems must meet extremely strict requirements for quality and security.

In this context, the Data Ethics Commission also, in particular, opposes any demand that newly enacted legal instruments should already be formulated with a view to possible future automated application; **in that regard, technology must follow the law and not the reverse**. Only if, in accordance with conventional criteria for the assessment of legislation (compliance with fundamental rights and other higher-ranking law, impact assessment, etc.), two equivalent versions are conceivable may the argument that one version is easier to algorithmise tip the scales in its favour.

7.3 Algorithmic systems in the dispensation of justice

The Data Ethics Commission is of the view that the use of algorithmic systems in the dispensation of justice is permissible **only for peripheral tasks**. Justice is administered "in the name of the people", and that means, at least in contentious proceedings as well as in administrative court proceedings and criminal proceedings, always administered by human judges. The pacification effect of court proceedings is achieved not only through the judgment itself (fairness of the finding) but also through the hearing and weighing up of conflicting interests by humans and, in particular, the structural processing of the facts and legal consequences (procedural fairness), in contrast to an opaque black-box decision.

Due to the often high level of trust placed in the supposed "infallibility" of technical systems (automation bias) as well as the low level of willingness to make divergent decisions, in particular if this is associated with an additional burden of reasoning and proof and the risk of a "miscarriage of justice" (default effects), **even legally non-binding proposals for decisions** for judgments by algorithmic systems are generally **highly problematic** from the perspective of the parties concerned.

However, algorithmic systems can, provided that there are strict quality control and high security standards in place, be useful for **preparatory work** which does not directly affect the judicial decision (e.g. file management and document control).

Lastly, the use of systems which **retrospectively analyse judicial decisions**, are available only for voluntary use by judges and are protected against access by third parties with high-level security measures, is also conceivable. Such systems could, for example, work out whether decisions were influenced by external factors and, if so, which ones in order to provide judges in future with ways to prevent such distortions themselves and thus contribute to better and more consistent dispensation of justice. Researchers may also have a legitimate interest in access to such systems, though sufficient safeguards would be required here in individual cases. The use of systems for the purpose of monitoring the path of judicial decision-making or of checking the dispensation work of judges against external targets (e.g. average processing time for a case) is, however, in view of objective judicial independence, not permissible.

In the **pre-litigation domain** (for example, exercising of air passenger rights) or also in a dunning procedure or similar, in the view of the Data Ethics Commission, fully automated handling of legal claims is permissible provided that procedural rights of the individual parties concerned are safeguarded as a result. However, this is not the case if algorithmic systems create correlations which do not follow the legal provisions and procedural steps set out. With the current state of the art, only systems based on classic deterministic algorithms can therefore generally be considered which, for example, make decisions by meeting formal criteria (which are not open to assessment). From a systemic point of view, impending losses of expertise are compensated for here by the freeing up of human resources for complex individual cases.

7.4 Algorithmic systems in public administration

There is a potentially greater scope for the use of algorithmic systems in public administration. The increased **automation of authorities' routine cases**, which can be included subject to precisely defined conditions regarding facts and legal consequences, may be advisable in the interest of efficiency (Section 10(2) of the Administrative Procedures Act) in order to carry out administrative procedures as appropriately and swiftly as possible. Here in particular, it relieving administrative staff of routine tasks frees up human resources which can then be deployed to handle procedures which cannot be automated.

There is potential, in particular, in the **provision of services and benefits**. The Data Ethics Commission believes that algorithmic systems can and should be used here to expand proactive procedure management whereby, where all the required data are available for the authorities, services and benefits will be increasingly provided without the need for applications. Educationally disadvantaged individuals and the needy in particular could benefit from this (cf. family allowance in Austria provided when a child is born without the need to apply for it).

However, in the case of **intervention by authorities**, the use of algorithmic systems must be dealt with carefully because fundamental rights are particularly affected. As with judicial use, this applies not only to algorithm-determined administrative decisions but also where the use of the systems limits the authorities' scope for decision-making. In general, in assessing whether to permit the use of the systems, the extent of the resulting intervention and the reversibility of the decisions need to be taken into consideration. Essentially, in designing the systems, technology must be used which is most easily accessible to oversight. Therefore, in sensitive areas, public administration will often be allowed to use only systems which are based on classic deterministic algorithms. The use of proprietary software should be avoided for the same reason.

In the case of **discretionary decisions** by the executive and decisions with a margin of discretion which have an external legal effect, the Data Ethics Commission believes that it is currently necessary for humans to make the final decision where the decision has more than mere beneficial impacts. However, by forming groups of cases and through further specification, it is conceivable that discretion could be reduced to such an extent that, from the view of the algorithmic system, there is only one option in terms of the decision. The Data Ethics Commission is of the view that Section 35a of the German Administrative Procedures Act does not sufficiently reproduce the range of different possible types of cases and is too schematic. Taking into account the safeguards required by constitutional law and based on Article 22 GDPR, legislators should **carefully expand the scope of Section 35a of the Administrative Procedures Act** and/or set out provisions, differentiated in terms of specific legislation, for administrative acts supported partially or fully by automation. Regulations on the partial and full automation of administrative procedures should be further developed as part of the horizontal and sectoral regulations for algorithmic systems recommended by the Data Ethics Commission (→ see section 3.3 above).

7.5 Algorithmic systems in public security law

The public discussion is especially critical of the use of algorithmic systems by security authorities. As administrative measures in this area can have a particularly profound effect on fundamental rights, the use of algorithmic should generally be **restricted**.

If algorithmic systems are used to predict crimes or threat situations **(predictive policing)**, consideration must be given to the fact that even systems which do not use any personal data can directly have effects relevant to fundamental rights. This is the case in particular if a reference to a person can be (re-)created by means of especially detailed location information. In addition, "location-related risk prognoses" can lead to excessive police checks in certain neighbourhoods identified as hotspots and therefore to the ethnic or social profiling of population groups living there. Such measures can also trigger crime relocation and displacement effects. The Data Ethics Commission therefore recommends making the security authorities of such effects and incorporating randomisations into the prediction systems in order to reduce corresponding effects and other system-based distortions; steps must also be taken to ensure that the security authorities can still always carry out a human review of more cases other than the risk cases selected by the system (cf. Section 88 of the Fiscal Code of Germany (*Abgabenordnung*, AO)). Nor should the security authorities be allowed to order further discretionary intervention measures solely on the basis of location-related forecasts.

Where **risk forecasts relating to individuals** are allowed by law in the area of security, such forecasts must not be created fully automatically where doing so could have negative legal consequences for the parties concerned. On account of the risk of automation bias, even in the case of algorithm-based decisions, support for human decision-makers from algorithmic systems in such profiling may, if at all, only be permissible within very strict limits.

7.6 Transparency requirements for the use of algorithmic systems by state actors

State decisions made using algorithmic systems must remain **transparent and justifiable**. This is, generally speaking, even more important than in the private sector due to the obligation to uphold fundamental rights and the need for democratic accountability of all authority and power in the public sector. Therefore, not only do the general transparency requirements (→ see section 4.1 above) apply to state bodies, but state bodies must also strive particularly hard to ensure openness.

The Data Ethics Commission points out that, in many cases, algorithmic systems used by state actors already fall within the scope of existing freedom of information and/or transparency laws. The Data Ethics Commission also welcomes the position paper "Transparency in Public Administration in the Use of Algorithms" ("*Transparenz der Verwaltung beim Einsatz von Algorithmen*") adopted during the 36th Conference of Freedom of Information Officers (*Konferenz der Informationsfreiheitsbeauftragten*) in Germany. According to this paper, state bodies must have meaningful, comprehensive and generally comprehensible information regarding their own data processing and, where legally possible, should publish it, including information (i) on the data categories of the procedure's input and output data; (ii) on the logic involved, in particular on the calculation formulae used including the weighting of the input data, on the underlying expertise and on the individual configuration deployed by the users; and (iii) on the scope of the resulting decisions and on the possible consequences of the procedures.[17]

17 Position paper as part of the 36th Conference of Freedom of Information Officers in Germany – "Transparenz der Verwaltung beim Einsatz von Algorithmen für gelebten Grundrechtsschutz unabdingbar" ["Transparency Public Administration in the Use of Algorithms as Essential for the Protection of Fundamental Rights"], Ulm, 16 October 2018 (available at: *https://www.datenschutzzentrum.de/uploads/informationsfreiheit/2018_Positionspapier-Transparenz-von-Algorithmen.pdf*).

With regard to specifying the corresponding transparency obligations and/or duties to provide access to information, the Data Ethics Commission also points out that insufficient provisions on transparency can lead to a lack of trust in the systems, which can lead to greater numbers of appeals, thereby counteracting any efficiency gains intended with the use of algorithmic systems. For that reason, the Data Ethics Commission ultimately believes that it is justifiable in no more than very few cases to rule out access to information regarding public algorithmic systems across the board by citing a risk of manipulation or the protection of business secrets. As a rule, therefore, the particular interests must be weighed against each other.

The disclosure of information on a system's general functionality will not be sufficient in every case where algorithmic systems are used by public authorities. Often, decisions made by public authorities must also be justified to the parties affected, i. e. the **"main factual and legal reasons"** which led to the decision in the particular case must be provided (cf. Section 39(1)(2) of the Administrative Procedures Act). Where such an individual explanation is required under constitutional or sub-constitutional law but, due to the technical complexity of the system, is not possible or is not possible in a way which, in the course of an official complaint procedure or before the court, enables an effective review of the viability of the reasoning, the use of algorithmic systems must be prohibited. Apart from that, the Data Ethics Commission believes that the State is required to build up sufficient **expertise** within administration and the courts to be able to ensure the necessary oversight of the system-internal decision-making processes.

The Data Ethics Commission points out that the transparency of state activity can also be negatively affected if the State uses proprietary software (closed-source software) of private providers in carrying out its duties. Generally speaking, proprietary software makes it difficult for users to make changes and adaptations, which results in a dependent relationship. In addition, the use of proprietary software leads to a lack of transparency and can therefore threaten public acceptance of the systems. Especially in areas which are sensitive in terms of fundamental rights, such as public security law, the use of proprietary software should therefore be avoided if possible. Instead, state bodies should rely on **open-source solutions** or develop their own systems ideally through interdisciplinary teams of developers. Where this is not practical, the Data Ethics Commission recommends that the Federal Government should consider amending public procurement law to minimise the aforementioned negative effects of proprietary software. Where there is no need to fear that the effectiveness of the system will suffer as a result of transparency, i. e. exploitation effects can be ruled out, the software should be developed in an open and consultative process with the inclusion of civil society stakeholders.

7.7 The risk involved in automated total enforcement

The Data Ethics Commission refuses, from an ethical point of view, to acknowledge any general right to non-compliance with rules and regulations. However, an automated total enforcement of the law raises a number of ethical concerns. For example, citizens might feel that full enforcement in practice places everyone under suspicion, which in turn, reduces their general willingness to obey rules and regulations. Furthermore, with automated enforcement, there is the danger that the complexity of real-life situations will not be sufficiently portrayed and, in particular, that unforeseen exceptional situations (for example, speeding in a private vehicle taking a seriously injured individual to the hospital) will not be sufficiently taken into consideration. Finally, many laws were not originally enacted for total enforcement. As a general rule, therefore, systems should be designed in such a way that a human can override technical enforcement in a specific case. In addition, each law enforcement measure constitutes state intervention and, as such, must be based on the **principle of proportionality**.

Summary of the most important recommendations for action

Use of algorithmic systems by state bodies

68

The State must, in the interests of its citizens, make use of the best available technologies, including algorithmic systems, but must also exercise particular prudence in all of its actions in view of its obligation to preserve fundamental rights and act as a role model. As a general rule, therefore, the use of algorithmic systems by public authorities should be assessed on the basis of the criticality model as **particularly sensitive**, entailing at the very least a comprehensive risk assessment.

69

In the areas of **law-making** and the **dispensation of justice**, algorithmic systems may at most be used for peripheral tasks. In particular, algorithmic systems must not be used to undermine the functional independence of the courts or the democratic process. By way of contrast, enormous potential exists for the use of algorithmic systems in connection with **administrative** tasks, in particular those relating to the provision of services and benefits. The legislator should take due account of this fact by giving the green light to a greater number of partially and fully automated administrative procedures. Cautious consideration should therefore be given to expanding the scope of both Section 35a of the German Administrative Procedures Act (*Verwaltungsverfahrensgesetz*, VwVfG) (which is couched in overly restrictive terms) and the corresponding provisions of statutory law. All of these measures must be accompanied by adequate steps to protect citizens.

70

Decisions taken by the State on the basis of algorithmic systems must still be **transparent**, and it must still be possible to provide **justifications** for them. It may be necessary to clarify or expand the existing legislation on freedom of information and transparency in order to achieve these goals. Furthermore, the use of algorithmic systems does not negate the principle that decisions made by public authorities must generally be justified individually; on the contrary, this principle may impose limits on the use of overly complex algorithmic systems. Finally, greater priority should be accorded to open-source solutions, since the latter may significantly enhance the transparency of government actions.

71

From an ethical point of view, there is no general right to non-compliance with rules and regulations. At the same time, however, automated "total" enforcement of the law raises a number of different ethical concerns. As a general rule, therefore, systems should be designed in such a way that a human can override **technical enforcement** in a specific case. The balance struck between the potential transgression and the automated (and perhaps preventive) enforcement measure must at all times meet the requirements of the proportionality principle.

8. Liability for algorithmic systems

8.1 Significance

Criminal responsibility, administrative sanctions and liability for damages are vital components of any ethically sound regulatory framework, especially for algorithmic systems and other digital technologies. From an ethical perspective, the Data Ethics Commission also highlights, in particular, the role of tort law, which serves both for compensation for and prevention of damage and therefore very significantly contributes to **the protection of legally protected interests in line with fundamental rights**.

From an ethical perspective, the following requirements, *inter alia*, must be set out for a liability system which needs to keep up with new digital technologies:

a) sufficient **compensation** for victims, in particular in the case of legally protected interests which are highly relevant in terms of fundamental rights and where compensation in a comparable situation involving humans or conventional technology would be owed;

b) provision of the right **behavioural incentives**, whereby damage is paid for by the actors who caused the damage through avoidable and undesirable behaviour or out of whose sphere the risk in question resulted;

c) **fairness**, whereby the actors liable to pay damages are those who, for example, placed the system on the market or who exercise control over the system and benefit from its use;

d) **efficiency**, whereby costs are covered (internalised) by the actors who can avoid or insure such costs with the least amount of effort.

8.2 Harm caused by the use of algorithmic systems

8.2.1 Liability of the "electronic person"?

The Data Ethics Commission **expressly advises against** granting robots or autonomous systems legal personality (often discussed using the keyword **"e-person"**) with the intention of making the systems liable themselves (e.g. a self-driving car with no registered owner, which "operates itself" as a mobility service). Such a measure would not achieve allocation of responsibility and liability for harm to those who are responsible for the use of the system and ultimately benefit economically from such use. In fact, the measure could, conversely, be used to evade responsibility. The legal personality of machines as a new type of legal entity would not enable any desirable outcome to be achieved which could not be achieved more freely and easily another way (for example with the help of company law). Treating autonomous machines even in analogy to natural persons would be a dangerous mistake.

8.2.2 Vicarious liability for "autonomous" systems

The Data Ethics Commission believes, however, that harm caused by autonomous systems should be attributed to those operating the systems according to the same rules of **vicarious** liability as would apply in the case of human auxiliaries (cf. in particular Section 278 of the [German] Civil Code). An actor which uses such a system in order to broaden its range of activities (for example a hospital which uses a surgical robot) should, in the event of a malfunction, not be able to release itself from liability because an actor which uses a human vicarious agent (for example a human surgeon) will be liable for any culpable misconduct of the vicarious agent, which is treated as behaviour on the part of the actor. This becomes particularly important in the case of **liability for an algorithmic system**, where otherwise liability loopholes will easily occur if no breach of duty of care by the person behind it can be proven in the use and monitoring of the algorithmic system.

Example 18
A surgical robot at a hospital makes an operational incision which is too long and causes complications. Or: an algorithmic system incorrectly derives the score for the creditworthiness of a bank's customer, which is why the customer cannot take up a one-off attractive offer relating to a property.

It may occasionally be difficult to establish an adequate equivalent to "standard of care" for autonomous systems, in particular as soon as the abilities of a machine exceed those of a human. In the majority of cases, however, malfunctions will be distinguishable from normal functions, and therefore this cannot, in general, be cited against the operator's liability. The standard must then be defined based on comparable systems available on the market, whereby the question as to the use of which technology could be expected of the operator must be decided on based on general principles (e.g. in that respect, the question as to what quality of surgical robot was to be used does not differ from the question as to what quality of X-ray device was to be used).

8.2.3 Strict liability

It is essentially a well-known fact that the rules relating to classic fault-based liability are not always sufficient for resolving the legal issues which arise in the case of dangerous products. The legal system has so far come up with a range of different answers to this challenge. In particular, these include:

- **modification of fault-based liability** (for example through adaptations of the standard of care and various ways of easing the burden of proof right through to the reversal of the burden of proof);

- various bases of **strict liability** (i.e. for facilities and activities which typically cause harm but which, on account of their benefit for society as a whole, should not be prohibited); and

- **product liability** in accordance with the [German] Act on Liability for Defective Products (*Gesetz über die Haftung für fehlerhafte Produkte*, ProdHaftG); it acts as a special form of liability regardless of fault which differs from strict liability on account of the fact that it requires, *inter alia*, a product defect and therefore comes fairly close to fault-based liability.

Steps must be taken to ensure that these answers lead to legally watertight solutions in terms of compensation for harm caused by dangerous digital applications.

The operation of digital applications currently involves **legal uncertainties and liability loopholes**, which primarily result from the unpredictability of harmful events, including when the applications are placed on the market (and hence possibly a failure of classic fault-based liability). They also result from the fact that, when various different actors and applications interact, generally speaking, it is almost impossible to prove where an error occurred and/or what the cause of the error was. The open and dynamic nature of digital ecosystems and the close functional interplay of products, digital contents and digital services also present a challenge. These legal uncertainties are, from the perspective of both companies and consumers, **obstacles to innovation and to the acceptance of new technologies**. If harmful events cannot routinely be assigned in terms of liability and compensated for, the impact on the market intended to be achieved through liability provisions cannot be achieved. In order to create an appropriate balance of interests, the legislator must provide for transparency and responsibility. Only if the responsibilities are clarified will it be possible to insure against harm or damage in practice.

The Data Ethics Commission cannot solve at this point the complex technical legal questions that arise, and cannot pin down the right solutions in terms of liability law, especially as, in some instances, the chances of finding a solution at European level should be explored first. From an ethical perspective, it is crucial that **legal clarity and legal certainty, in particular with regard to the liability principles described above**, be created. However, as the debate currently stands, it appears highly likely that, in addition to appropriate amendments to the Product Liability Directive (→ see section 8.2.4 below), certain changes may need to be made to the rules relating to fault-based liability and/or new bases of strict liability may need to be introduced.

In the legislative process, it will firstly be necessary to determine the liability regime that is most appropriate **for particular types of products, digital content and digital services**, and the exact shape that this regime should take, depending, once again, on the criticality (→ see section 3.1 above) of the relevant system, but also on other criteria which are specifically relevant within the context of liability. As such, strict liability (for example based on the model involving the car owner's liability) could be most appropriate in cases regarding devices where the operational risk is similarly uncontrollable and could end up leading to harm to life and limb. As part of this, the question of insurability and/or possible compulsory insurance must always play a role. A decision must also always be taken on **which type of harm** should be the subject of the liability (e.g. personal injury and damage to property, data loss, pure financial losses and non-material damage).

Ultimately, in each case, a decision will need to be taken as to who, taking into consideration the liability principles described above, is the right **party to which liability should be assigned**. There will, in particular, be three possible parties to which liability could be assigned, of which two could possibly also be jointly and severally liable:

- the individual **registered owner** of the system (i.e. the owner or person who, in a similar position, uses the system for their own purposes);
- the **manufacturer** of the system;
- the **operator** of the system (i.e. whoever exercises greater control over the system's operation, the individual registered owner as the front-end operator or a back-end operator who may also be the manufacturer but does not have to be).[18]

Determination of that party and of the type of liability will always depend on the specific type of networked or autonomous system and the identification of the specific spheres of liability.

8.2.4 Product security and product liability

Overall, it is currently important to highlight a paradigm shift from a situation whereby products were simply placed on the market to a situation whereby products are placed on the market but additional services continue to be provided for the products thereafter. As such, ongoing **product monitoring** and **product maintenance** are becoming more and more important. IT security and data protection standards not only have to be fulfilled when a product leaves the production plant but also must continue to be met as part of subsequent software updates. Conversely, in the event that security gaps subsequently appear, the manufacturer should (in accordance with the provisions of the directives on digital content and digital services and trade in goods) be subject to a duty to provide **security updates** in line with consumers' reasonable expectations regarding service life.

18 For the liability concept of such differentiated liability of the operator in digital ecosystems, see the report entitled "Liability for Artificial Intelligence and other emerging digital technologies" by the European Commission's Expert Group on Liability and New Technologies (New Technologies Formation), September 2019, no. [11], p. 40 et seqq.

Example 19
No security updates are provided for a smart home system and, as a result, following a cyber-attack, the house is broken into.

The Product Liability Directive from the 1980s is no longer able to cover the features of networked, hybrid or autonomous products. The Data Ethics Commission recommends that, as part of the **evaluation and revision of the Product Liability Directive** at European level, the Federal Government should push for watertight and clear legal provisions, in particular for the following aspects:

a) inclusion of digital content and digital services, including algorithmic systems, under the term "product";

b) liability for product defects which do not appear until after the product has been placed on the market and are the result of self-modifying software, of provision of updates or a failure to provide them, or of product-specific data feeds;

c) liability for breaches of the product monitoring obligation;

d) inclusion of legally protected interests typically affected by digital product safety, in particular the right to informational self-determination, in compensation regimes;

e) adaptation of the development risk defence.

8.3 Need for a reassessment of liability law

Digital ecosystems throw up a variety of other issues in connection with liability and responsibility. For example, there is, to some extent, a liability loophole in current tort law in cases of **damage to data and digital products**, provided that neither a recognised 'absolute right' has been infringed (e.g. ownership of the storage medium), nor a statute that is intended to protect another person breached (e.g. provisions of criminal law), nor the conditions of intentional damage contrary to public policy met. New digital technologies often also involve the **opportunistic use of other people's infrastructures** (e.g. the systematic collation and use by third parties of sensor data generated by private IoT devices or the direct use of computing capacity or transmission functions), which can create complicated liability issues. In contexts with a stronger focus on contract law, major harm or damage (in particular at the expense of consumers) can be caused on account of the fact that the **usability of high-value goods** (real property, machines, cars, etc.) is becoming increasingly dependent on the long-term provision of digital services (software updates, user accounts, etc.) and the provision of such services is not guaranteed and/or can even be specifically suspended in order to put individuals under pressure **(electronic repossession)**.

Digital ecosystems are also, to some extent, characterised by the interaction of numerous components and operators, whereby it is often disproportionately difficult for the injured party to prove **which of several potential tortfeasors** (e.g. hardware supplier, suppliers of various software components, data feed provider or network operator) caused the harm. On the other hand, digital technologies not only create a new lack of transparency with regard to the cause of harm or damage but can, conversely, also help in documenting the course of causal events in an unprecedented way. The question therefore arises as to which actor is obliged to contribute to providing clarification on the cause of the harm by already **logging data** ex-ante and to whom the data actually recorded via logging should be disclosed in the event of harm.

The Data Ethics Commission therefore recommends overall that the Federal Government should investigate the extent to which current liability law has kept up with the **challenges of digital ecosystems** or needs to be reworked. Priority must be given to striving to achieve a solution at European level. The Data Ethics Commission advises in this context against any tendency towards a one-sided focus on specific technological features, in particular the feature of machine learning. Whilst machine learning creates certain additional dangers and involves certain additional issues regarding the assignment of liability, most challenges for liability law are attributable to other factors (e.g. intangibility, interaction of numerous components, networking and decentralisation).

Summary of the most important recommendations for action

Liability for algorithmic systems

72

Liability for damages, alongside criminal responsibility and administrative sanctions, is a vital component of any ethically sound regulatory framework for algorithmic systems. It is already apparent today that algorithmic systems pose challenges to liability law as it currently stands, *inter alia* because of the complexity and dynamism of these systems and their growing "autonomy". The Data Ethics Commission therefore recommends that the current provisions of liability law should undergo in-depth checks and (where necessary) revisions. The scope of these checks and revisions should not be restricted on the basis of too narrowly defined technological features, such as machine learning or artificial intelligence.

73

The proposal for a future system under which legal personality would be granted to high-autonomy algorithmic systems, and the systems themselves would be liable for damages (**"electronic person"**), should **not be pursued further**. As far as this concept is, by some protagonists, based on a purported equivalence between human and machine it is ethically indefensible. And as far as it boils down to introducing a new type of company under company law it does not, in fact, solve any of the pertinent problems.

74

By way of contrast, if harm is caused by autonomous technology used in a way functionally equivalent to the employment of human auxiliaries, the operator's liability for making use of the technology should correspond to the otherwise existing vicarious **liability regime of a principal for such auxiliaries** (cf. in particular Section 278 of the German Civil Code). For example, a bank that uses an autonomous system to check the creditworthiness of its customers should be liable towards them to at least the same extent that it would be had it used a human employee to perform this task.

75

As the debate currently stands, it appears highly likely that appropriate amendments will need to be made to the **Product Liability Directive** (which dates back to the 1980s), and a connection established to new product safety standards; in addition, certain changes may need to be made to the rules relating to **fault-based liability** and/or new bases of **strict liability** may need to be introduced. In each case, it will be necessary to determine the liability regime that is most appropriate for particular types of products, digital content and digital services, and the exact shape that this regime should take (once again depending on the criticality of the relevant algorithmic system). Consideration should also be given to innovative liability concepts currently being developed at European level.

Part G

A European path

The Data Ethics Commission has examined a great many different questions, and discussions on these questions have raised new ones in turn; this alone should indicate that this Opinion can serve only as one out of many building blocks in the larger edifice of a broad-based **debate on the future of ethics, law and technology** that we must return to again and again. This debate must be interdisciplinary from the outset, and encompass a broad range of sciences and a diverse mix of representatives from the worlds of the economy, civil society and politics. In view of the immense economic pressure and the fast-paced nature of technological change, the findings that emerge from this debate must be integrated on an ongoing basis into the activities of the parties involved at all levels, so that we can shape a technological future that is founded on values.

Data transfers and the use of algorithmic systems transcend national boundaries, which means that a forward-looking discussion of the ethical and legal issues arising in connection with data and algorithmic systems must not be restricted to the national level. We need to view problems from a **global perspective**, and accordingly strive to present our findings and perspectives more than before on a pan-European debate as well. Lessons learned from implementing the GDPR have shown that the economic clout of the European Economic Area and its significance as a market for the operators and providers of algorithmic systems may ultimately mean that these latter are prompted by economic interests to comply with the EU's basic requirements when developing and implementing their products and services. These European requirements are also being used by ever more non-European governments as a reference point when drafting their own regulatory frameworks.

The debate that needs to take place should therefore be a priority topic on the agendas of international forums (EU, OECD, Council of Europe, United Nations, G7 and G20). With this in mind, the Data Ethics Commission recommends that the Federal Government should make its voice heard within these international bodies. In particular, the **German Presidency of the EU Council** in the second half of 2020 should be utilised as an opportunity to promote the measures to deal with data governance and algorithmic systems as proposed in this opinion on the European level. The Data Ethics Commission also believes that the Federal Government should be actively involved (both in the early stages of the process and on an ongoing basis) in the establishment of an International Panel on Artificial Intelligence (IPAI) as initiated on the level of the G7.

In the global contest for future technologies, Germany and Europe are being confronted with value systems, models of society and cultures that differ widely from our own. This has prompted a debate whether Germany and Europe are to adapt to one or the other non-European models in order to remain competitive. The Data Ethics Commission supports the **"European path"** which has been followed to date. It is often referred to in debates as a "third way" that strikes a balance between the US and Chinese positions, and which asserts that the defining feature of European technologies should be their consistent alignment with European values and fundamental rights, in particular those enshrined in the European Union's Charter of Fundamental Rights and the Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms.

In order to remain actively involved in the future debate on the interplay between ethics, law and technology, the digital sovereignty of Germany and Europe must be preserved to the greatest extent possible. When used in reference to nation states or organisations, the term "digital sovereignty" encompasses every aspect of data processing, i.e. control over the storage, transfer and use of the sensitive data held by these bodies, and autonomous decisions on who can access them.

A globalised world in which people, states and companies co-exist side by side requires cross-border flows of data, and the Internet – which serves as the conduit for these flows – is a global "network of networks"; this distributed global structure, which embraces very different legal and societal systems, renders complete sovereignty an impossible task. The debate on digital sovereignty must therefore tackle vital questions relating to technical infrastructure, including hardware, networks, control components such as routers or address servers, and data centres. With a view to preserving the digital sovereignty of Germany and Europe, and given the huge extent to which we are reliant on foreign products, the Data Ethics Commission believes that there is an urgent need to take action at German and European level through **investments into developing and safeguarding appropriate technologies and infrastructures**.

Virtually all of the most important and basic Internet infrastructure components that are used in Germany (and indeed in Europe as a whole) can be procured only from other continents at present, and so efforts to preserve sovereignty must be restricted for now to the two main avenues open to us; the first of these is the critical analysis and assessment of the basic components being used, and the second is the application of the highest possible security standards when operating them in order to minimise the risk of misuse by foreign states and organisations. Looking to the future, however, the Data Ethics Commission believes that it is important for Germany and Europe as a whole to develop a **higher level of digital sovereignty**, right down to the level of **technical infrastructure**. Support should be available for R&D work on systems that comply with the highest possible standards of security. Work of this kind would include both the design of new components to replace previous systems, and attempts to engineer integrated solutions that use existing components and that achieve the required level of protection in spite of known or suspected inadequacies or security risks.

The digital sovereignty of a nation state should be viewed not only in relation to other nation states, but also in relation to non-state actors that wield significant amounts of power. As the data economy grows, there is a trend for **economic power to be concentrated** in the hands of a few, and the emergence of **new power imbalances** is apparent. To an ever greater extent, R&D work on algorithmic systems and other digital technologies is being carried out within a framework established by a small group of digital giants; what is more, these companies often act as an important source of public research funding and therefore have a say in this research. Over the past few decades, intermediaries have played an increasingly important role in forming opinions, and therefore in influencing the sociopolitical discourse; this means that the associated risk of abuse has also increased. Given the importance of ethical and legal fundamental values and freedoms and to preserve the digital sovereignty of Germany and Europe, the Data Ethics Commission believes that there is an urgent need to closely monitor the shifts in power structures, as those are vital for the functioning of a democratic State and a social market economy, and to efficiently regulate the according areas wherever needed.

Excessive dependence on others turns a nation into a rule taker rather than a rule maker, resulting in the citizens of this nation being subject to requirements imposed by players elsewhere in the world. Embarking on **efforts to safeguard digital sovereignty in the long term** is therefore not only a politically far-sighted necessity, but also an expression of ethical responsibility.

Appendix

1. The Federal Government's key questions to the Data Ethics Commission

Coalition Agreement:

"We will set up a data ethics commission that within the next year will provide the government and parliament with proposals on how to develop data policy and deal with algorithms, artificial intelligence and digital innovation. Clarification of data ethics questions can add impetus to the process of digital development and can help define an approach towards resolving social conflicts within the area of data policy."

Key questions for the Data Ethics Commission:

Digitisation is fundamentally changing our society. New data-based technologies can be beneficial for people's everyday lives as well as for industry, the environment, science and society as a whole. Their potential is enormous.

At the same time, digitisation also clearly brings certain risks. Numerous ethical and legal questions are raised, particularly concerning the effects of these developments and the desired role of new technologies. If digital change is to benefit the whole of society, we need to examine the possible consequences of new technologies and establish ethical safeguards.

One challenge is to develop 21st-century law in a way that protects human dignity ("a human being must not become a mere object") and guarantees fundamental and human rights such as the general right of personality, the right to privacy, the right to informational self-determination, freedom from discrimination, freedom of science, freedom to conduct a business, and freedom of expression and information – bringing all of these rights into equilibrium with one another.

There are complex tensions between the principles of the common good, progress, innovation and solidarity.

The task of this Commission – having identified the current state of discussion and legislation at the European and international level, ascertained the possibilities for positive action at the national level, and given special consideration to sensitive areas – is to develop ethical standards and guidelines for the protection of individuals, the preservation of social cohesion and the safeguarding and promotion of prosperity in the information age. The Commission is also tasked with providing the Federal Government with recommendations and regulatory proposals on how ethical guidelines can be developed, respected, implemented and monitored. These proposals should also include a description of the underlying concepts used, as well as assessments of the possible consequences and side effects.

The public is to be appropriately involved in the work of the Commission.

In order to help the Data Ethics Commission carry out its work, the Federal Government has provided it with the following key questions in three areas:

I. Algorithmic decision-making (ADM)

Advanced automation systems are increasingly shaping economic and social realities and people's everyday lives. Data collection and analysis enable the development of innovative interpretation models, which are also used to make or prepare algorithm-based decisions. Algorithms make it possible, for example, to recognise patterns and differences in the behaviour of different groups. Whether it is a matter of setting individual prices in e-commerce, assessing creditworthiness or selecting candidates in recruitment procedures, people are being evaluated by technical processes in more and more areas of life. Data evaluation and predictions about individual behaviour can offer opportunities (e.g. aiding research, strengthening innovation within industry, increasing the efficiency of data processing processes), but they also harbour risks (e.g. for individual freedom and self-determination, for participation and equal opportunities among certain individuals and social groups). Social inequality and discrimination against individuals or groups of individuals can be perpetuated if biases are incorporated into the programming of an algorithm or its training data. These risks are particularly acute in participation-relevant and personality-sensitive ADM processes. Against this background, the following questions arise, especially with regard to consumer protection:

- What are the ethical limits to using ADM processes? Or what ethical limits should there be?
- Can it be ethically necessary to use ADM processes?
- Are there characteristics, criteria or certain kinds of data that should not be incorporated into ADM processes – due to their age or origin, for example?
- How can we determine which prejudices and distortions in which areas are ethically undesirable? What effects can the use of ADM processes have on social groups?
- What regulatory approaches could be used to prevent manipulation, unequal treatment and discrimination?
- Is it advisable to have a graduated regulatory framework based on the risk to social participation or the potential for discrimination?
- How can the reliability, reproducibility and scrutiny of ADM be guaranteed?
- Are there limits to the use of ADM if its use and criteria cannot be explained to the people affected?
- Are there test methods that can make self-learning ADM open to scrutiny?

II. Artificial Intelligence (AI)

With the development of AI, industrial and administrative environments are deploying more and more highly automated systems that use AI methods and have the ability to "learn" through the use of training data. In addition, work is being done on simulating the cognitive functions of the human brain. The developments in the field of artificial intelligence raise the question of how the dignity, autonomy and self-determination of the individual can be safeguarded and fostered. This leads to questions such as the following:

- What fundamental ethical principles must be observed when developing, programming and using AI?
- Where do the ethical boundaries lie for using AI and robots, especially in special areas of life such as care/assistance and dealing with particularly vulnerable groups (children, the elderly, people with disabilities)? Can it be ethically necessary to use AI?
- Is "ethics by design" possible for AI? If so, how could it be implemented and monitored?
- How can it be ensured that machines working on an AI basis can be controlled?

- To whom are the creations/inventions generated by AI to be ascribed? Who should bear the responsibility for malfunctioning systems? How can the responsibility of the actors involved in the development and use of AI systems (programmers, data scientists, clients, etc.) be made transparent?

- What else will be necessary in the future to sustainably guarantee the freedoms and fundamental rights upon which our society is based?

III. Data

Digitisation is characterised by an increase in the volume of data (big data), by a vast accumulation of data by individual actors, by the high speed of data processing (real time), by connectivity (internet, complex networks of actors, Internet of Things), by the increasing ubiquity and permanence of data, and by the further development of various methods of data analysis. As the amount of available data increases, so too does the ability to undertake more granular analyses. Data is used to develop new business models and change value-added chains and work processes. By some, data is regarded as a commodity that enables value creation ("data economy").

At both the national and European level, there are current laws (e.g. the General Data Protection Regulation, open data legislation) and numerous legislative initiatives that concern the handling of data (e.g. the ePrivacy Regulation, legislative proposals regarding the free flow of data). On the one hand, these are intended to safeguard fundamental rights such as the right to informational self-determination, while on the other hand they are intended to enable useful and innovative data processing. Further proposals are discussed as to whether and how access to data, use of data, trade in data, and rights to data could be regulated for the first time or be better regulated.

In the process, the following questions may arise regarding the handling of data in general, data access and the use of data:

- What are the ethical limits to the economization of data?

- Who should be permitted to derive economic benefit from data?

- Should there be an obligation to offer payment models?

- Is it advisable to have uniform rules that apply equally to all data? Or should preference be given to rules that apply to specific areas (e.g. for brain data)? What should be the connecting factor for rules that apply to specific areas?

- What consequences do existing access and exclusivity rights to data have for competition and innovation? And what consequences would additional access and exclusivity rights to data have?

- Is there a need for the state to offer support as part of its provision of general public services so that citizens can navigate the internet and social networks in a responsible, competent and confident manner and learn how to handle data? Can the provision of data, in particular open data, become part of the provision of public services by the state?

- How much transparency is necessary and appropriate to safeguard the right to informational self-determination and to enable citizens to participate in economic life in a self-determined manner?

- Do particular life circumstances require special protection concepts for specific user groups?

- Are the existing institutions in sensitive areas sufficient to ensure data is used ethically? How can adequate stakeholder representation be ensured in the long term?

- What effects can extensive data collections have on the functioning of the market economy (e.g. competitiveness, information asymmetry between suppliers and consumers, the possibility of developing innovative products) and democracy (e.g. recording and analysing behaviour in social networks)? If necessary, how can action be taken against data power/data silos (especially intermediaries)?

- Should data or access to data be declared a public good in certain cases? In which cases and under which ethical criteria?

- The use of non-personal data can have collective effects. For example, individuals or certain population groups may be placed at a disadvantage because data analysis shows that payment habits are worse in a particular neighbourhood. What regulatory instruments would be needed for this? In which sectors?

- Are statutory regulations on improving access to data possible, necessary and advisable?

- Should data processing be prohibited in certain cases for ethical reasons, for example in cases involving certain types of data (e.g. political views; brain data) or certain areas of use (e.g. profiling for political purposes or for use in elections)?

- Under what circumstances can there be an ethical obligation to use data?

- Does the legal system sufficiently recognise the possible benefits that data processing can have for the common good? If not, how can this be achieved?

- Is it possible and advisable to create experimentation clauses for testing new applications or new regulatory instruments?

- Does it make sense to invest in data infrastructures? If so, in which ones?

- How can the constitutionally protected interests of individuals, enterprises, science and art be reconciled with the public interest in the use of data?

2. Members of the Data Ethics Commission

Co-Spokespersons

Prof. Dr Christiane Wendehorst

- Professor of Civil Law at the University of Vienna
- Co-Head of the Department of Innovation and Digitalisation in Law at the University of Vienna
- President of the European Law Institute (ELI)

Prof. Dr Christiane Woopen

- Professor for Ethics and Theory of Medicine and Head of the Research Unit Ethics at the University Clinic of Cologne
- Executive Director of the Cologne Center for Ethics, Rights, Economics, and Social Sciences of Health (ceres) at the University of Cologne
- Chair of the European Group on Ethics in Science and New Technologies (EGE)

Members

Prof. Dr Johanna Haberer

- Professor of Christian Media Studies at Friedrich Alexander University Erlangen Nuremberg (FAU)
- Director of the Institute for Practical Theology at Friedrich Alexander University Erlangen Nuremberg (FAU)

Prof. Dr Dirk Heckmann

- Full Professor of Law and Security of Digitization at the Technical University of Munich (TUM)
- Director at the Bavarian Research Institute for Digital Transformation
- Judge at the Bavarian Constitutional Court

Marit Hansen

- Data Protection Commissioner of Land Schleswig-Holstein
- Head of Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Independent Centre for Privacy Protection Schleswig-Holstein)

Prof. Ulrich Kelber

- Federal Commissioner for Data Protection and Freedom of Information
- Honorary Professor at Bonn-Rhein-Sieg University of Applied Sciences (H-BRS)

Prof. Dieter Kempf

- President of the Federation of German Industries (BDI)
- Honorary Professor at Friedrich Alexander University Erlangen Nuremberg (FAU)

Prof. Dr Mario Martini

- Professor of Public Administration, Public Law, Administrative Law and European Law at the German University of Administrative Sciences Speyer (DUV Speyer)
- Head of the Programme Area "Transformation of the State in the Digital Age" and Deputy Director of the German Research Institute for Public Administration (FÖV)

Klaus Müller

- Executive Director of the Federation of German Consumer Organisations (vzbv)
- Lecturer at Heinrich Heine University Düsseldorf (HHU)

Paul Nemitz

- Principle Advisor at the European Commission, Directorate-General for Justice and Consumers

Prof. Dr Sabine Sachweh

- Professor for Applied Software Engineering at Dortmund University of Applied Sciences and Arts (FH Dortmund)
- Spokesperson and Board Member of the Institute for the Digital Transformation of Application and Living Domains (IDiAL) at Dortmund University of Applied Sciences and Arts (FH Dortmund)
- Co-Spokesperson of the "Digitalisation and Education for the Elderly" Advisory Council at the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth

Christin Schäfer

- Founder and Managing Director of the company acs plus, a data science boutique
- Advisor of the Big Data Analytics Research Group at the German Economic Institute in Cologne (IW Köln)

Prof. Dr Rolf Schwartmann

- Professor of Civil Law and Economic Law at Cologne University of Applied Sciences (TH Köln)
- Head of the Research Centre for Media Law at Cologne University of Applied Sciences (TH Köln)
- Chairman of the German Association for Data Protection and Data Security (GDD)

Prof. Dr Judith Simon

- Professor for Ethics in Information Technology at the University of Hamburg (UHH)

Prof. Dr Wolfgang Wahlster

- Professor of Computer Science, Chair for Artificial Intelligence, Saarland University
- CEO/CEA of the German Research Center for Artificial Intelligence (DFKI)
- Head of the Steering Committee for the AI Standardisation Roadmap at the German Institute for Standardization (DIN)

Prof. Dr Thomas Wischmeyer

- Assistant Professor (Tenure Track) for Public Law and Information Law at the University of Bielefeld

Current as of: 10 October 2019

Imprint

Berlin, December 2019

Opinion of the Data Ethics Commission

Publisher
Data Ethics Commission of the Federal Government
Federal Ministry of the Interior, Building and Community
Alt-Moabit 140, 10557 Berlin
Federal Ministry of Justice and Consumer Protection
Mohrenstraße 37, 10117 Berlin

E-mail
datenethikkommission_gs@bmi.bund.de
datenethikkommission_gs@bmjv.bund.de

Website
www.datenethikkommission.de

Design
Atelier Hauer + Dörfler GmbH, Berlin

Photo credits
p. 53: shutterstock.com
p. 234: BMI (group photo), Studio Wilke (Christiane Wendehorst), Reiner Zensen (Christiane Woopen), BPA/Kugler (Ulrich Kelber)
p. 235: Christian Kruppa (Dieter Kempf), vzbv/Gert Baumbach (Klaus Müller), Markus Mielek (Sabine Sachweh), TH Köln/Schmülgen (Rolf Schwartmann), UHH/Nicolai (Judith Simon), Jim Rakete (Wolfgang Wahlster)

Printing
Brandenburgische Universitätsdruckerei und Verlags-gesellschaft Potsdam mbH (bud)