Statement

Public consultation procedure on the EU Data Strategy

Transparency register number: 1771817758-48

Federation of German Industries (BDI)

Status: 29 May 2020

Table of contents

Executive Summary

- The BDI advocates an innovation-friendly data policy that provides additional incentives for companies to use the data and promotes the voluntary exchange of data within the framework of private sector contracts;
- The BDI supports the EU Commission's approach of establishing a comprehensive governance framework in order to create uniform framework conditions across Europe;
- Before additional horizontal regulation is introduced, a fundamental evaluation of the existing legal framework is urgently required in order to eliminate existing legal uncertainties, especially in antitrust and data protection law;
- Investments in trustworthy data infrastructures and cloud solutions are an important component for the success of the EU data strategy;
- The BDI supports the implementation of common European data spaces in strategic sectors. However, efforts must be made to achieve harmonisation within different data spaces and to ensure a high degree of interoperability.

Preliminary remark on the key actions of the EU Data Strategy

The BDI welcomes the initiative launched by the European Commission in the present data strategy to develop uniform and value-based European data spaces, in order to exploit the advantages of better data use in the interests of a data-driven society and economy to the full. The Commission's declared aim is to increase the use of data and data-based products and services and to stimulate demand. The COVID-19 outbreak has highlighted the importance of data and data exchange, especially in areas such as the health sector.

A large number of industrial companies are already working very successfully with their own and, where applicable, external data and are generating a high added value from this. Nevertheless, there is still enormous potential in this area, as there remains a discrepancy between the amount of data available and that which is actually used. The causes of this imbalance are manifold, ranging from technical, through economic to legal reasons. In this respect, supplementary political measures can be useful to further support and, if necessary, encourage the use and exchange of data by companies.

A coherent European data strategy is the necessary basis for further developing the European digital internal market and for better positioning the European data economy in global competition. Data-based business models and platforms are becoming increasingly important in the economy due to digital change. Exponential growth in data volumes and rapid technological advances in basic technologies, such as artificial intelligence (AI), are leading to an increasing use of data-based applications in industry. However, the EU Commission's data strategy is right to focus not only on purely quantitative, but also on the qualitative criteria of data.

The BDI is therefore very clearly in favour of an innovation-friendly data policy, which is essentially characterised by the self-determined handling of data and thus by the principle of voluntariness. The overriding objective must be to promote the exchange of data across industries and sectors, without violating the legitimate interests of the companies from whose sphere the data originates. We are convinced that the necessary prerequisite for efficient data management lies in particular in the promotion of free and fair competition between all market participants, in which companies - regardless of their size - can develop their own ideas and use data-based applications, and in which an appropriate balance is struck between the interests of the data producer and the data user. This also includes an expansion of the government's open data policy, whereby the state discloses (anonymised) data in a way that complies with data protection regulations.

However, the BDI rejects mandatory cross-sectoral data access rules. The innovative capacity of industrial companies should be strengthened by targeted incentives for the use and sharing of data, but not by horizontal

regulatory intervention. Moreover, it is hardly possible to specify such claims in concrete terms at an abstract and general level with regard to the regulatory object "data", especially since data and information held in companies will regularly be classified as business secrets or affect the interests of third parties worthy of protection.

The availability of trustworthy digital infrastructures is crucial for the realisation of a common EU internal market for data. It is therefore both important and right to provide appropriate investments in the framework of a "High Impact Project" for European data spaces and data infrastructures in order to strengthen Europe's digital sovereignty.

1. Cross-sectoral governance framework for data access and use

The first of four pillars of the EU data strategy deals with possible horizontal measures for data access and use. The aim is to counteract fragmentation within the EU through inconsistent approaches in the individual member states. With this comprehensive and cross-sectoral governance approach for a EU internal data market, the EU Commission is choosing the right approach. After all, only an increasingly uniform European legal framework can ensure that the current legal fragmentation in the individual EU member states is eliminated and that existing legal uncertainties in the use and sharing of data can be eliminated in the future.

The Commission proposes four key actions, which are described below.

1.1. Legal framework for the governance of common European data spaces

The first priority for the Commission is to establish a legal framework for the governance of common European data spaces. The Commission intends to use governance structures to facilitate decisions on which data can be used and when. This should also facilitate cross-border data use and interoperability. Data access and data use are important factors through which the potential of a data economy can be optimally developed. In this respect, the EU Commission is taking up a very central concern, in which the BDI is convinced that the following fundamental aspects must be taken into account:

1.1.1. Designing an innovative data policy

Certain data held by a company may also be of high value to the public or other companies and vice versa. The BDI is convinced, however, that in addition to the endeavour to make data accessible to as many interested parties as possible, the legal and economic interests of the data producers must also be taken into account in the same way. After all, data generally originates from previous investments made by the company holding the data stock, which must be protected as a matter of principle.

An innovative data policy should therefore be designed in such a way that significantly more data can be shared voluntarily and, at the same time, fair data use is strengthened. There is still room for improvement here in many areas. The BDI therefore welcomes the principle of the EU Commission in the present data strategy to facilitate the voluntary exchange of data.[1] This takes into account the principle of contractual

[1] Cf. p. 16 of the EU Data Strategy.

freedom, according to which companies are free to decide with whom and under what conditions they share non-personal data they have collected themselves, whether through contractual agreements, private-sector data partnerships or a voluntary open data approach. It should also be taken into account that collaborative data processing between several companies is becoming increasingly common with the broad use of cloud services, machine learning and artificial intelligence. Such collaborations on a business-to-business level are defined by contractual agreements. Contract law has basically proven to be flexible enough to regulate the necessary economic allocation of rights of use of data between several partners in a practical manner.

On the other hand, regulatory projects that aim to establish a general legal right of access to company data must be strongly rejected. The BDI is firmly convinced that efficient and fair data use does not require a general legal obligation to grant data access and data sharing. Such legislative intervention would have the effect of thwarting existing contractual regulations, such as agreements about restrictions on use and confidentiality, and would prevent innovations from being made in future. Exceptions are only conceivable if access to necessary data is provided by state authorities or organisations acting on behalf of the state in narrowly defined areas, for example to avert danger or to protect life and limb.

The BDI is also convinced that there is no need for horizontal regulation, since data use can, in principle, be solved satisfactorily by individual contracts or sector-specific self-regulation (both association and company solutions) between the individual market players and competitors. There is no need or regulatory gap that would necessitate a general regulated access to private sector data.

Rather, the BDI believes that the legal and actual possibility of being able to decide on the transfer and use of data in a self-determined manner (the so-called principle of data sovereignty) must apply equally to private individuals and companies. In order to ensure functioning competition while maintaining the ability to innovate, legal regulation of data access should only be considered in the event of illegitimate market entry barriers or market failure. There are already legal possibilities in European competition law to impose data access obligations in order to ensure effective competition.[2] If, however, there is a structural market failure in individual areas, sector-specific access regulation, such as that introduced for the financial sector in the context of the implementation of the Second Payment Services Directive (PSD2), which specifically addresses market failures, is preferable to general horizontal regulation. Only in the case of such narrowly defined sector-specific approaches, will it be possible to specify the respective data or information to which a right of access is to refer with sufficient determination at the

[2] Cf. also Chapter A) III. 1. a).

legislative level, while at the same time protecting business secrets and any rights of third parties. Finally, the Union legislator has the task of carefully examining the proportionality of potential State intervention in the property rights of companies. In this context, the various legitimate interests of the actors involved, such as the protection of property and investment, must also be carefully balanced.

In addition, contractual arrangements can be flanked by data governance agreements and industry or market-specific data use and data access rules. Individual industries are developing data governance policies to agree on clear and fair data usage rules within their respective digital ecosystems. Furthermore, non-disclosure and usage restriction agreements in the industry have become increasingly standardised in terms of content over the last few decades and have become highly enforceable on the market.

1.1.2. Standardisation as a basis for interoperability and portability / Standardisation as a task for industry

For a data-driven economy, it is not only the quantity but also the quality of the data provided that matters. Data quality is measured by its accuracy, relevance, reliability, consistency and availability. Only through high data quality, can data analysis provide accurate results and a reliable basis for decisions. This requires a standardisation of the labeling and description of data in order to clearly define its content and semantics for further processing and linking. At the same time, high-quality data sets are an essential prerequisite for training AI algorithms, for example.

The companies of German industry are actively committed to competition. The ability to use data in parallel across different generation and application contexts can be achieved by supporting data portability through interoperable data formats and information models based on freely accessible standards. National examples of this can be seen in industrial production with the administration shell Industry 4.0 and ecl@ss, as well as in the health sector with HL7 and DICOM and IHE with reference to the respective standards. In this way, data exchange or data pooling between different providers is made possible, thus promoting competition.

However, standardisation is primarily a task for industry. According to the principle of the "New Legislative Framework", the Union legislator should refer to standards and prioritise them where necessary, but not define them itself. Here, however, it is important to reduce the current "traffic jam" in the examination and release for listing in the Official Journal of the EU through adequate and efficient processes. Nevertheless, support - especially for small and medium-sized enterprises (SMEs) - is needed to enable them to participate in international standardisation bodies. This is the only way to ensure that our European values and ethical principles are also reflected in the products and applications referring to these standards.

1.2. Adopt an implementing act on high quality data sets

The BDI expressly welcomes the efforts of the EU Commission to make more high-quality public sector data sets available for further use. With regard to the availability of public data, the EU must play a pioneering role, and at the same time, take into account coherence with regard to the open data portals of the Member States.

With regard to the availability of public sector data, it is important in principle that no data are made available which contain confidential information, business and trade secrets or personal data of economic operators or their employees, as is already partly regulated in Germany in Section 12a EGovG. The BDI welcomes the initiative of the EU Commission that data should increasingly be made available via the EU data portal in standardised, machine-readable form, taking into account the exceptions mentioned above. Support should also be given to the approach that the EU Commission wants to provide the high-quality data sets with open user programming interfaces (so-called API). It should be noted that the APIs are based on internationally recognized standards.

As much as the BDI welcomes the opening of data from government-to-business, the BDI believes that in the reverse "business-to-government" relationship, only voluntary cooperation is preferable to a legal obligation to access data "in the public interest".[3]

1.3. Presentation of a proposal for a legal act on data

In the third key action, the European Commission is considering certain legislative measures to create incentives for cross-sectoral data sharing. Firstly, it is to consider whether the sharing of data between companies and authorities should be promoted in the public interest. It is also considering various measures to support data sharing between companies.

1.3.1. Business-to-Government Data Sharing (B2G): No obligation to open company data

The BDI is critical of a regulatory framework for data exchange in the B2G sector. Even if the EU Commission is of the opinion that the public sector does not have sufficient data from the private sector to improve fact-based policy-making and public services such as mobility management, a mandatory opening of private data may only be considered very restrictively, if at all, due to the considerable interference with entrepreneurial freedom.

[3] For B2G data exchange, see Chapter A) III. 1.

The principle of freedom of contract must continue to have top priority in the B2G sector too.

Rather, the BDI also advocates a voluntary approach in B2G data exchange, which creates additional incentives for companies to exchange data. The establishment of appropriate platforms could be an important step towards B2G data sharing. Such platforms could, for example, contribute to improving urban mobility by making corresponding data available to various market participants and by offering the possibility of winning a contract or even developing a business model on the basis of this data. The expansion of such platforms could also promote cooperation between start-ups and experienced companies. Many creative scenarios seem conceivable in this respect. So-called data marketplaces, which are already widely offered by the industry, could also play an important role in this respect. Again, however, it is necessary to create data interoperability solutions (based on neutral standards) in order to link the various existing platforms in the market and thus prevent fragmentation. In addition, a large number of companies from a wide range of industries are already cooperating successfully with public authorities, for example, when it comes to intelligent traffic management through appropriate analysis and evaluation of location information. A structural market failure that would justify legislative intervention in the form of a horizontal access obligation has not yet been identified.

Compulsory disclosure of company data could only be considered as the *ultima ratio* in clearly defined individual cases, if voluntary disclosure to the public sector is not appropriate, within the framework of data protection requirements. In any case, however, it must be ensured that access to private sector data pays for a pre and narrowly defined public objective in order to guarantee legal certainty for companies. This also means that public authorities should not become competitors in relation to existing commercial initiatives in the market (e.g. in the field of Smart City, mobility). At the same time, long-term sustainable cooperation between industrial companies and public administration can only be achieved by means of an adequate compensation mechanism that appropriately acknowledges the, often costly, data preparation and analysis on the company side.

1.3.2. Possible actions of the data (B2B) legal instrument

In the view of the BDI, the current obstacles within the European data industry are due to a large number of existing uncertainties with regard to the current legal framework. Especially in the age of digitisation and Industry 4.0, business co-operations and new forms of co-operation play an important role. The markets have changed considerably in recent years and have become fast-moving due to increasing digitisation. This requires companies to act more flexibly and collaborate more frequently in order to create innovative digital solutions for customers, ensure interoperability and create

new technological standards for the benefit of customers. For example, data pooling offers companies a larger database for analytical purposes and enables them to improve their solutions and create innovative solutions for their customers' benefit. Industrial companies are faced with considerable doubts, especially when it comes to planned data cooperation with competitors, as to whether the planned project complies with existing data protection and antitrust laws.

Before additional regulatory approaches are considered, the BDI therefore considers it imperative to first carry out a comprehensive analysis of the existing legal framework in order to provide companies with greater incentives for increased data use and data exchange.

The BDI considers that there is a need for action in the following areas in particular:

1.3.2.1. Antitrust Law

1.3.2.1.1. Promoting business cooperation through practicable guidelines

European companies must enter into cooperation, be part of ecosystems and participate in creative formats, such as hackathons, to promote innovation. This is all the more necessary if they want to catch up in global competition in the digital field.

Antitrust law currently puts obstacles in the way of such cooperation projects between competitors. The grey areas are large and the legal uncertainty among companies is considerable. This already applies to cooperations outside of Industry 4.0, but even more so with regard to new digital issues (e.g. cooperations for the generation and use of data and data pooling), for which there has so far been little case and decision practice. Here the Commission should make improvements and offer more legal certainty to companies wishing to develop new digital projects or enter into data cooperations. For example, within the framework of a platform, including the possibility of informal preliminary discussions with DG Competition, official decisions stating that "there is no reason to act" and additions, explanatory notes and case studies in the Horizontal Guidelines. The BDI had already[4] listed concrete case studies and possible solutions at the beginning of last year in its statement "Shaping competition policy in the era of digitisation". These will continue to be highly relevant.

In addition, the EU Commission should emphasise much more strongly that data cooperation is typically pro-competitive. Here, a general statement would be very helpful for companies to reduce the aforementioned factual

[4] BDI Position Paper (Translation), available at: https://ec.europa.eu/competition/information/digitisation_2018/contributions/bdi.pdf

obstacles. The BDI has also set out its concerns about horizontal co-operation in its detailed statement about the horizontal block exemption regulations and the horizontal guidelines, to which we refer.[5] The Horizontal Guidelines should take into account these new market dynamics and new forms of co-operation. As companies which fear that they may end up infringing the antitrust rules may be reluctant to participate in such cooperation or joint initiatives, the Horizontal Guidelines should be revised in order to increase legal certainty, for example by

- Introduction of de minimis rules/safe harbor, especially for digital markets and more targeted damage theories. Current discussions on antitrust law in digital business often focus on very large and powerful companies, but there are several co-operations between smaller companies and companies with small to moderate market shares that are pro-competitive and should not be subject to the same restrictive rules. The size of the company is not an indication of the size of the market shares.
- Creation of a general safe harbor/exception for emerging digital markets, e.g. for a period of five years

1.3.2.1.2. Create legal certainty in the exchange of information

There is also a need for increased legal certainty in the area of information exchange. For example, the final report on the e-commerce sector inquiry has raised questions about data exchange between manufacturers with their own distribution, and their retailers. The Commission takes a rather critical view of this. Often, however, such exchanges can also have pro-competitive effects, as information on sales, for example, can improve production and product range planning at the manufacturer. In this respect, it would be desirable to further elaborate on the circumstances under which such exchanges do not give rise to competition concerns. The uncertainty on the part of companies as to the type of information they can exchange will be even greater when considering these new models of cooperation in digital ecosystems. Companies currently lack clear guidance on the limits of what information can be exchanged in such collaborations. With regard to ecosystems in particular, it should be made clear that exchange and cooperation within the ecosystem (intra-ecosystem), e.g. platforms initiated by several companies, can potentially only harm competition if there is insufficient competition from other ecosystems (inter-ecosystem). The underlying idea is that through appropriate cooperation between companies, both belonging to the same sector and across sectors, new European players

[5] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/11886-Evaluation-of-EU-competition-rules-on-horizontal-agreements/public-consultation, under “Documents annexed to Contributions”.

emerge, which form a countervailing force to the non-European digital champions.

The Commission should also review the market share thresholds. SMEs in particular are dependent on the synergy effects of cooperation. Nonetheless, SMEs will often not benefit from the exemption regulations, as their market share, despite their small company size, is in any case above the thresholds if they operate in niche markets. Cooperation between large companies and SMEs is also often excluded from the scope of the exemptions from the outset, even though this is exactly where there is a need. However, it is precisely for the benefit of these companies that the opportunities for cooperation should be expanded. The Commission should consider raising and standardising the thresholds for horizontal cooperation. The market share criterion should therefore no longer be the decisive criterion for a block exemption. Cooperation (e.g. in the data field) between large companies and SMEs would then be excluded from the benefits of the block exemption from the outset, even though there is a need for such cooperation. The existing BERs are therefore not suitable for forms of cooperation that may institutionally challenge dominant technology companies. It is suggested that the thresholds for horizontal cooperation should be harmonised and raised to at least 30%. In this way, the uncertainties in determining the relevant market shares could be reduced, at least slightly. It would also be helpful if the Commission were to provide more concrete guidance to companies in determining the relevant market. The Commission's 1997 notice on the definition of the relevant market is, in our view, too abstract and hardly helps companies in practice.

1.3.2.1.3. Not creating general competition law data access claims

As already made clear elsewhere, the BDI rejects the introduction of general data access claims, as long as no structural market failure can be identified that cannot be remedied in any other way. This also applies to cartel law. The BDI supports the premise underlying the Commission's approach to data access rights, which, at the same time, refers to the existing competition law means of granting data access claims:

"A right of access to data should always be sector-specific and should only be granted where a market failure is identified or foreseeable in the sector and cannot be remedied by competition law alone[6]".

What often speaks against a general data access claim, for example within the framework of the *"essential-facilities-doctrine"*, is that the relevant data are usually replicable and have been provided by the user free of charge and voluntarily. The EU Commission, for example, considers a right of access to be non-existent if the access petitioner can use or develop an alternative

[6] Communication from the Commission - COM(2020) 66 final of 19.02.20 - A European Data Strategy, p. 16, footnote 39.

technology. Moreover, in contrast to the classical cases of access to critical physical infrastructure, granting a data access right within the framework of the *"essential-facilities-doctrine"* would increase the risk of abuse, since it cannot be ruled out that the access petitioner duplicates the data inappropriately, in order to compete on the "market of the data set" with the owner of the data set to which access has been granted.

Against this background, the BDI is also critical of individual elements of the planned reform of competition law in Germany, such as the establishment of general data access rights in cartel law. The supervision of abuse under cartel law is primarily aimed at preventing certain harmful behaviour by dominant companies. A reinterpretation into a "duty to promote innovation", with the obligation towards companies to make their own data stocks accessible to third parties, could even have the effect of inhibiting innovation in the long term and favour free riders.

Tighter supervision of abuse, for example by creating rights of access to data, should also not be carried out on a national basis, but a European solution should be found. In any case, national solutions contradict the idea of creating a "Digital Single Market" within the EU. Companies operating across borders need more, not less, harmonisation.

1.3.2.2. State aid law

EU state aid law should focus on promoting investment and innovation in key technologies and thus give European companies better starting opportunities in global competition. Companies must be supported in cost-intensive innovation processes. More space and more legal certainty for horizontal cooperation between companies and the expansion of "Important Projects of Common European Interest" ("IPCEI") are essential elements.

It seems right that the Commission will also look at the relationship between public support for businesses (e.g. for digital transformation). It should be examined whether State aid law can also play a role in the establishment of B2B platforms. To the extent that it can also contribute directly or indirectly to the promotion of voluntary data exchange and data sharing by supporting the cost-intensive transformation processes in the context of digitisation, this is certainly to be welcomed. In our opinion, there is no need for a binding requirement for beneficiaries with regard to data sharing. Such a requirement would also contradict the principle of freedom of contract and economic freedom, which is enshrined in the constitution. Such an approach would result in a data access obligation, which the BDI rejects under competition law (see above under II. 1.).

1.3.2.3. Personal data

Even after almost two years of application, the European Data Protection Regulation (GDPR) is still leading to legal uncertainties in the application practice of companies. Although the GDPR creates a uniform, value-oriented legal framework for all member states, companies are still faced with considerable uncertainty and divergent interpretations in the member states when it comes to the actual application of the law. At the national level, in addition to the GDPR, many other data protection regulations must be taken into account in numerous laws at the federal and state level, which further increase the legal uncertainty for German industrial companies.

In order to prevent the GDPR from becoming a locational disadvantage for European companies, the European Data Protection Committee is called upon to ensure that the GDPR is handled in a uniform and legally secure manner throughout Europe. The high fines of up to four percent of annual turnover which have been threatened in the event of a breach of the GDPR regulations will further increase the uncertainty in the handling of data within companies. SMEs in particular, find this a difficult task to master. In addition, in view of the above findings, the Union legislature is called upon to address the existing problems of companies and to make targeted legal adjustments in the context of the upcoming evaluations of the GDPR. Only through legally secure, practicable and unbureaucratic application, will the GDPR have the potential to establish itself as a global standard in the future.

1.3.2.3.1. Lack of mandatory application of the coherence mechanism in cross-border cases

The coherence mechanism should be mandatory for matters of general importance or with implications in more than one Member State. Undetermined legal concepts are interpreted differently by national supervisory authorities (e.g. data portability, scope of requests for information, etc.). This contradicts the harmonisation objective of the GDPR. In some cases, national data protection supervisory authorities issue instructions for action, without it being clear whether these are permanent or whether they should still go through the coherence procedure and then be repealed. The lack of consideration of the coherence mechanism leads to legal uncertainty for businesses and citizens. In addition, the different interpretations lead to considerable financial consequences, as business models and processes cannot be implemented uniformly throughout Europe. This is also reflected, not least in the different sanctioning practices of data protection supervisory authorities. While some Member States impose fines in the two to three-digit million range, other Member States have so far refrained from imposing sanctions.

1.3.2.3.2. Legally compliant standards for anonymisation

The German industry is aware of its great responsibility in handling personal data. The regulations set out in the GDPR and the freedoms protected by fundamental rights, in particular the right to informational self-determination of the individual, are important cornerstones for the high level of data protection that Europe can boast in international comparison. For this reason, many industrial companies have a great interest in working with anonymised data to a much greater extent, but are currently frequently refraining from this project due to the great legal uncertainty and in the absence of uniform standards.

At present, companies are faced with the challenge in practice that no uniform and legally secure standards exist for the anonymisation of personal data. However, a practicable and legally secure anonymisation is a core requirement for the digital transformation and the functioning of European data spaces. With regard to the legislative requirements, it should be noted that the GDPR does not contain a positive definition of the term "anonymisation". Recital (26) p. 5 and 6 only contains a rough negative definition of personal data, without, however, providing the necessary legal certainty/clarity. In order to maintain or even increase this high level of protection, legal and technical requirements for anonymisation of personal data in conformity with data protection law are indispensable. The BDI considers it to be a central task of the EU Commission to advocate, in the context of the current and future GDPR consultation, that companies are given legally secure handling of the anonymisation of personal data.

First of all, a clear directional decision is needed here, in the sense that an effective anonymisation under the GDPR does not have to be "absolute", but rather, a "relative" approach is sufficient. This "relative" approach ensures that legally secure anonymisation is only feasible in practice. In the opinion of the BDI, the process of anonymisation by the GDPR is privileged overall, so that this is not processing in the sense of data protection law.

1.3.2.3.3. E-Privacy

Within the framework of the revision of the current e-privacy directive through the draft regulation, which has been under discussion for more than three years now, a clear separation of the areas of application of the GDPR and e-Privacy Regulation, in particular with regard to the sometimes contradictory and overlapping rules on the protection of the processing of personal data, which must be treated separately from the principle of confidentiality of communications. The implementation of the GDPR remains a major challenge for many companies. It is therefore all the more important to achieve alignment and thus avoid overlapping areas of application with regard to the processing of communications data) of the E-

Privacy Regulation and GDPR in order to create the necessary legal certainty for companies.

1.3.2.3.4. Personal data rooms

The BDI supports the Commission's approach that individuals should be strengthened by the enforcement of their individual rights. One possible solution could be a model with a trustee for personal or personally identifiable data in selected fields of application, who could make it available to companies - after the consent of the individuals. This could counteract a structural imbalance in negotiating power. Nevertheless, there is still too much uncertainty for a final assessment as to what role and function a data trustee should play as an intermediary between companies and individuals and what (legal) competences are to be transferred to him. In particular, it should be clarified in advance in which sectors trustee models are suitable, whether the corresponding platform should be operated by the state or the private sector, and whether the trustee model itself should administer the data or rather, allow access to further databases.

1.3.2.4. Intellectual property rights

The policy paper mentions that an "evaluation of the IPR framework will be carried out with a view to further improving data access and use (with a possible revision of the Database Directive and a possible clarification of the applicability of the Directive on Trade Secrets as a legal framework)".

However, this wording does not reflect the Commission's objectives. Against this background, it should be pointed out at this point that a substantial change to the existing regulations would be rather critical at this stage. A separate "data IP law" has been intensively discussed in recent years. However, such an amendment would raise more problems than it would bring advantages. If, for example, a new IP law were to be created, there would again be the danger of shielding valuable data by pooling, similar to patent pools, in the context of which, similar discussions would have to be held in advance, if necessary, as is currently the case with essential standard patents. Liability questions would also arise immediately: Who is liable for the fact that the corresponding reference database is statistically correct and representative? It would also have to be rejected that the existing important and correct regulations on databases and the protection of trade secrets would now be softened in order to ensure better access for third parties.

Nor is it appropriate to restrict or amend the provisions of Section 87a et seq. of the German Copyright Act (UrhG) or the regulations on the protection of business secrets. Both the provisions on database protection in the Copyright Act and those on the protection of business secrets do not protect data per se,

but rather the rights of the owners. A restriction of these rights would hence go beyond access to data. There would therefore be a danger that the rights of the owners would be unduly restricted.

In general, the warning must be given that it will be very difficult to find formulations in the definition of access rights to data that can be interpreted and applied in a legally secure manner. This has already been referred to in the discussion on the introduction of an IP right to data.

Overall, therefore, it must be noted that data protection is currently regulated in a number of special legal standards, although scattered. However, these regulations fulfil their purpose and offer a balance between the protection of the rights holders and the interests of the data users. Any current deficits in data use are therefore not due to a lack of protection by industrial property rights or copyrights. The content of the existing regulatory framework should therefore not be changed.

1.3.2.5. Contract and liability law

The current liability regime in its current version basically allows for an appropriate solution of liability issues. If, however, a possible need for adaptation is deemed necessary due to the increasingly digital nature of products, then an open and purposeful discussion must be held, which allows the clear and adequate delimitation of content-related concepts.

1.4. Analysis of the importance of data in the digital economy in the context of the Digital Services Act

In principle, the BDI welcomes the fact that the EU Commission, through the Observatory for the Online Platform Economy, is investigating the role of large amounts of data on negotiating power and imbalances. Since the Commission will deal with this separately in the future legal act on digital services, we will also take a separate position on this subject area.

2. Prerequisites: investment in data and in strengthening European capacities and infrastructures for hosting, processing and using data and interoperability

The second pillar focuses on investment in data and strengthening infrastructures. The Commission wants Europe to provide an environment that supports data-driven innovation and stimulates demand for products and services.

2.1. High-impact project for European data spaces

The BDI shares the Commission's assessment that supporting measures are needed to fully exploit the potential of cross-sectoral data use and to promote the emergence of a European ecosystem for data. These measures include the availability of trustworthy data infrastructures, which are an important prerequisite for promoting responsible data use, exploiting innovation potential and safeguarding the sovereignty of the state, citizens and companies. With the "High-impact project for European data spaces" announced in the European data strategy, the Commission is addressing the corresponding framework conditions. The following points should be taken into account when implementing the key measures envisaged:

1. **Basic principles**

With a view to the "High-impact project for European data spaces", fundamental principles in the area of cloud competences, a trustworthy digital infrastructure and cyber security must be observed, which will be discussed below.

2.1.1. Strengthening European Cloud Capabilities

The BDI welcomes measures that aim to strengthen digital sovereignty in the cloud computing field. Reliable, high-performance, data protection-compliant and, at the same time, secure cloud solutions are indispensable in the course of ongoing digitisation. Since, against the background of the international competitive situation, the development of national solutions within the EU is not promising in the long term, a pan-European approach must be consistently pursued. Within the EU, therefore, the creation of an interoperable platform for cloud solutions that can be connected to future technologies must be promoted, which brings together existing cloud offers with the needs of users in line with market requirements and is based on open interfaces. The "GAIA-X" project, which is being driven forward by the German government and representatives from companies, associations and science, represents an important contribution towards achieving this goal. A European project that meets the needs of all Member States must now be built on this project without delay.

Exploiting the demand potential of the public sector is another critical success factor: both the EU institutions and the public authorities in the individual member states should bring their demand power to bear so that the services provided via a European solution can scale up more quickly. In this context, a stronger EU-wide coordination of public sector digitisation activities should also be sought.

In addition to the availability of trustworthy cloud proposals, the further expansion of edge computing technologies is also of major importance in the industrial environment, as these enable device-oriented data processing with numerous advantages, e.g. in terms of security, robustness and energy efficiency. While today, about 80 percent of all data is still processed in the cloud and only 20 percent close to the device (i.e. in the edge), this ratio will reverse in a few years. German suppliers of electronic components and systems can make a substantial contribution to this.

2.1.2. Building trusted digital infrastructures

In addition to the availability of trustworthy cloud infrastructures, the cross-border existence of a powerful, trustworthy and secure digital (Gigabit) infrastructure in Europe is a basic prerequisite for the implementation of data-driven business models and the use of new, digital technologies (including telemedicine) On the way to the European gigabit society, 5G technology in particular, plays a key role for the European economy. The potential is huge: Infrastructures are indispensable for the vision of fully networked driving, efficiency increases in logistics, and networking in the smart factory. In this context, the EU Commission should support a 5G rollout in the member states as quickly as possible. The allocation of the necessary frequencies for mobile broadband is a basic prerequisite for the success of 5G. Given the large differences in frequency allocation between the Member States, a more harmonised and innovation-friendly EU spectrum policy is needed. The EU Commission should therefore develop appropriate recommendations for uniform, appropriate and fair frequency auctions in Europe. It should also drive forward the 5G standardisation processes together with industry and its industrial requirements. Finally, the EU Commission should publish a 6G action plan at an early stage to identify challenges and opportunities at an early stage.

The security of the networks has the highest priority. In order to strengthen the Digital Single Market and prevent unauthorised access, uniform security standards are therefore needed throughout Europe to protect the integrity and confidentiality of data and the availability of networks and services. The EU Toolbox is an important and appropriate first step in this direction. The EU Commission should now offer the Member States assistance in transposition issues, ensure that the deadlines for transposition are met and impose sanctions in the event of infringement. In addition, the European Cyber

Security Agency ENISA must develop technical requirements based on the EU Cybersecurity Act before the end of this year as a basis for the certification of 5G network components. Any requirements must be manufacturer-independent and take a risk-based approach.

In addition to the expansion of the fixed and mobile networks, the EU Commission should strengthen the competitiveness of European data centres. By building high-performance computing capacities on EU territory, it must be ensured that European companies and research institutions have an infrastructure at their disposal on which they can build research, innovation and the establishment of new business models. A corresponding infrastructure must be ready for future technologies from the outset.

2.1.3. Cybersecurity

A high degree of cyber-resilience is a basic prerequisite for the trouble-free functioning of highly digitized and thus data-based processes, networkable products, services and infrastructures. This is because the damage caused by cyber security incidents is enormous in both the private and industrial sectors. Current estimates suggest that by 2021, the annual costs caused worldwide by cybercrime and state-motivated cyber attacks will amount to six trillion US dollars. This would be twice the amount of damage estimated for 2015[7]. These figures illustrate that an increasing degree of interconnectedness correlates strongly with the expected amount of damage caused by cyber security incidents.

At the same time, however, it is also true that 100% cyber security cannot be achieved, let alone guaranteed, because attack vectors are constantly changing, new vulnerabilities are identified and human error can never be completely avoided. This makes it all the more important for companies to ensure that their efforts to strengthen cyber-resilience are not thwarted by inconsistent regulations, national go-it-alone initiatives, unilateral requirements and excessive bureaucratic reporting obligations. Since more than one regulation is regularly applicable to products, consistent and coherent requirements are essential for European companies competing with companies from markets that are partly unregulated or regulated differently. Only consistent regulatory requirements can ensure that economic operators can apply and comply with the applicable requirements to their products, processes, services and systems. In particular, requirements on production processes should be congruent with those on products and services.

In concrete terms, the EU Commission, together with the EU member states, is called upon to observe the following five principles when strengthening the European data economy with a view to maintaining the cyber-resilience of products, processes, services, infrastructures and systems:

[7] Cf. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021.

- *Ensure coherent regulatory requirements to strengthen Europe's cyber-resilience while avoiding competitive disadvantages for European companies.*
- *European requirements are preferable to national solo efforts in order not to jeopardise the success of the European internal market.*
- *Take a risk-based approach to ensure adequate and effective protection.*
- *Actively integrate European standardisation work according to the principles of the New Legislative Framework (NLF).*
- *Actively and holistically involve all parties involved - from hardware and software manufacturers to commercial operators and private users - in strengthening cyber-resilience.*

2.2. Agreement with Member States on the Cloud Merger

Promising initiatives to increase the trustworthiness and interoperability of cloud infrastructures already exist in the member states of the European Union. However, a pan-European approach is generally preferable to national solutions in order to ensure the highest possible scalability of European cloud offerings. The BDI therefore welcomes the EU Commission's plan to press ahead with the networking of existing initiatives within the EU and, as a first step, to conclude agreements with the Member States on cloud integration.

The agreements should aim to exploit synergies between existing projects from the outset and define concrete steps for a rapid transformation of national initiatives into a pan-European cloud initiative. They should take into account as much as possible, the preparatory work done at national level (e.g. reference architectures already developed) in order to provide a market-ready pan-European offering, as soon as possible.

2.3. Creation of an EU Cloud Regulatory Framework

The offerings and services provided via a European marketplace for cloud services must be based on standards that fully comply with the European legal and value system, thereby ensuring the highest degree of digital sovereignty. In addition to a high level of trustworthiness, the standards should also ensure a high degree of interoperability. The standards must be uniform and transparent so that market participants can benefit from harmonised rules throughout Europe and increased transparency with regard to the regulatory frameworks underlying the cloud services offered.

In developing the 'cloud' regulatory framework envisaged in the EU data strategy, existing and market-established regulatory frameworks should be used as far as possible. The development of the rules should also be closely coordinated with existing self-regulatory initiatives, in order to avoid the development of parallel structures.

2.4. Creating a European marketplace for cloud services

To achieve high market penetration and acceptance, European cloud services must be provided in a user-friendly manner. Via a marketplace solution, such as that offered by EU Commission at this point, corresponding low-threshold access to European cloud offers can be realized in principle.

Against this background, the BDI welcomes the plan by the EU Commission to create a European marketplace that covers the full range of Cloud services. What is needed is an interoperable platform that can be connected to future technologies, which brings together existing cloud offers with the needs of users in line with market requirements and is based on open interfaces. In addition, a special focus must be placed on ensuring that the offerings provided via the marketplace are also easily accessible to SMEs.

3. Competences: Strengthening the capacity of individuals to act, investing in competences and in SMEs

It is true that there is still a considerable amount of catching up to do in terms of basic digital skills in the population in order to meet the demands of the future and ensure innovation and competitiveness. The EU can provide support here within the given framework, e.g. through the education programmes or the ESF, and set corresponding priorities, e.g. to strengthen STEM education or ICT skills. Insofar as existing transparency instruments can be further developed in a meaningful and practicable way so that digitally acquired skills can also be made more visible, these possibilities should be used. It must be ensured that they can be linked to existing national solutions.

4. Common European Data Spaces in strategic sectors and areas of public interest

The BDI welcomes the EU Commission's approach of thinking in terms of the creation of data rooms, not only horizontally, but also in a differentiated way for specific sectors. In order to make the data usable here, the data rooms would have to be defined according to easily understandable principles in order to better highlight the sectors for which they are relevant. At the same time, it is important not to see the individual sectors as completely separate and detached from each other. Instead, there is often a smooth transition between sectors, as is the case with the common European industrial data space, for example, and other data spaces, such as the common European mobility data space. Only in this way is it practicable for companies to make use of the strategic data spaces on a voluntary basis.

4.1. A common European industrial data space

A voluntary exchange of industrial data within the EU, based on private autonomous agreements, is an essential prerequisite for exploiting the value-added potential of data-based business models in industry. To ensure the smoothest possible cross-border data flows, companies depend on harmonised standards and rules throughout Europe. Against this background, the BDI basically welcomes the objective of establishing a common European industrial data area. With regard to the access to data to be regulated, there should be no general obligation to grant access to data in relation to B2B data exchange. Contractual agreements and self-regulation approaches should be the preferred option, unless there is a specific legal obligation. The concrete design of a European Data Space should also have a special focus on the technical conditions for a smooth exchange of industrial data within the EU, while at the same time pursuing the approach of creating international standards.

A trustworthy digital infrastructure is particularly important for data exchange in industry, regardless of the individual sectors[8]. Furthermore, the relevance of mobility data for industrial value creation should be emphasised. The competitiveness of European industry is increasingly dependent on the extent to which global and regional transport and logistics processes can be integrated into industrial value creation, right through to manufacturing (the "Industry 4.0" and "Smart factory" models). Such deep networking of the two sectors leads to increased productivity, efficiency and transparency in the supply and dispatch chain. Typical applications are tracking and tracing, for example via "closed loops" and "open loops", as well as telematic solutions

[8] Cf. also the explanations in Chapter B.

that provide the transport progress of individual loads in real time. An example of a powerful technical operationalization is the International Data Space (IDS) model. The exploitation of all these innovations and efficiency potentials requires the increased availability, exchange and processing of freight transport and logistics data. To this extent, there are strong interdependencies between the creation and regulation of the "Common European Industrial Data Space" and the "Common European Mobility Data Space"[9].

4.2. A Common European Data Space for the European Green Deal

The EU Commission has set itself an ambitious goal with the project of creating a European Environmental Data Space to combat climate change and promote recycling management for greater sustainability, as part of the European Green Deal. However, in all efforts to achieve this important goal, care should be taken not to lapse into excessive actionism. All measures, especially if they are mandatory, should be subjected to careful cost-benefit analysis. A negative example of this is the SCIP database. Suppliers and importers of articles within the meaning of REACH are to provide information on substances of very high concern (SVHCs) in an article to this database from 5 January 2021 (Article 33(1) REACH). The purpose of the database is to use information on SVHCs in waste to optimise recycling and improve the quality of secondary raw materials. However, the purpose, which is undisputedly sensible from the point of view of industry, is missed here. Because, since the directive contains no restrictions, this requirement applies to every product that is placed on the market. The article-based approach of the requirement means that exorbitantly large quantities of data are entered into the database without the data actually being used and needed by waste management companies. The disproportionately high effort required to determine and provide the data and, in particular, the as yet unclear benefits for the waste disposal companies, calls the whole project into question.

It is therefore important that a data room for the European Green Deal is created voluntarily and in close cooperation with industry, if possible, in a narrowly defined area. Common data rooms are only useful if they offer real added value for all actors involved. Particularly in the case of particularly sensitive data, protection must also be provided against possible data misuse. That is why, when creating the data room, especially when it concerns industrial plants, the protection of company secrets and protection against sabotage and terrorist attacks must also be taken into account. After all, even if individual pieces of data are not classified as secret in themselves, improper networking and use of different information can damage the business

[9] Cf. Chapter D III.

interests of companies. In addition, the procurement of information for sabotage purposes can be considerably simplified.

4.3. A Common European Mobility Data Space

The BDI welcomes the EU Commission's approach of giving mobility and logistics a high priority in the data strategy. At the same time, it is right to take greater account of the potential offered by digitisation and standardised data rooms for more sustainable, climate- and resource-saving and safe mobility, particularly in the context of the announced "strategy for intelligent and sustainable transport".

It remains important to take into account all modes of transport and their improved networking as well as logistics processes. As far as the automotive industry is concerned, the BDI recommends waiting until existing industry solutions have been fully implemented and used, before considering further regulatory steps. In the freight transport and logistics field, it is necessary to expand suitable platforms for the provision of public sector data, to facilitate the rapid introduction of electronic freight documents for all modes of transport and to introduce uniform standards for the European toll system and digital control systems in road freight transport. Air freight transport could also benefit from the creation of a platform involving all actors in the supply chain.

4.3.1. Vehicle industry

For security reasons, data from the means of transport should only be transferred to third parties via a backend, implemented and certified by the manufacturer of the means of transport. The regulatory framework for implementing this requirement must be defined. The use of data generated in the vehicle can improve road safety and traffic flow and generate innovative business models. Since 2014, the corresponding ISO working group "Extended vehicle/Remote diagnostics" has been working on standards as part of a large-scale "Extended vehicle" standardisation project, which are already being used by vehicle manufacturers. The European AFCAR group is also currently developing the "Open Telematics Platform (OTP)". In this way, the automotive industry is already creating the technical prerequisites for external service providers to offer mobility services to drivers in the future. The service providers can call up and receive data via the vehicle manufacturers' backend servers. The vehicle manufacturers or service providers are responsible for designing the web platforms. To this end, the necessary standards and norms will be developed in an international context, defining, for example, structures, processes and, above all, security mechanisms.

Third parties can - with appropriate authorisation - receive the same data generated in the vehicle, at the same time as the vehicle manufacturers. The data can be obtained and used via a standardised interface from the vehicle manufacturers' own servers or from neutral servers. Uniform conditions are thus available for all players, so that fair competition for the development of digital innovations and new business models can take place.

The vehicle owner has full control over his personal data transferred from the vehicle at all times. He can decide for himself which data he wishes to make available to whom for what purpose, and from which providers he obtains services.

The German automotive industry has already developed a concept that enables the secure transfer of data generated in the vehicle and makes it available to both public authorities and private actors. This "NEVADA-Share & Secure" concept[10] offers sustainable protection of the vehicle security sphere and the business interests of all economic players who want access to vehicle data. The data transfer and data use provided for in the "NEVADA-Share & Secure" concept is based on the guidelines of the European Union and the guidelines of the German "Ethics Committee on Automated Driving". This concept has already been introduced by manufacturers and will be finally rolled out by the industry by the end of 2020. Full implementation and use should be awaited before considering further regulatory steps. The planned review of EU legislation for the type approval of motor vehicles in the first quarter of 2021 provides the right framework for this.

4.3.2. Freight transport and logistics

The availability, exchange and processing of mobility data of freight transport and logistics play an important role for the stronger integration of transport and logistics services in industrial value-added processes, for intelligent and more efficient supply chains, the stronger interlocking of transport modes and the independent networking of load-to-load and load-to-manufacture locations. Data-driven solutions in freight transport and logistics have an enormous innovation potential and are developing into an increasingly decisive location and competitive factor for industrial companies. As a result, logistics and supply chains will increasingly be organized across company and country borders via platforms.

The collection and analysis of large amounts of data from various sources can provide information that offers great potential for the optimization of logistics processes. An essential prerequisite for this is the provision of public sector data. Suitable platforms must be expanded for this purpose, especially

[10] NEVADA = Neutral Extended Vehicle for Advanced Data Access.

at, and with the support of, the EU level. The provision of the data generated by the truck toll collection system in Europe alone could make a major contribution to increasing the efficiency of logistics processes.

In the road transport sector, the obligation to have the transport accompanying documents available in all languages of the EU Member States through which the goods pass is an anachronism. The rapid introduction of electronic transport documents should be made possible for all modes of transport. In addition, road freight transport requires the introduction of uniform standards for a European toll system and digital control systems ("digital tachograph") to ensure compliance with minimum wage requirements and driving and rest periods. The development of cross-border data platforms to enable Intelligent Truck Parking (ITP) should be promoted.

4.3.3. Air freight logistics

In the field of air freight transport, the next step towards a more data-driven approach is to create a platform in which all actors, such as shippers, consignees and customs authorities, can participate. In this cloud, all relevant data will be integrated and can thus be passed on to all participants in the supply chain. This would include pricing, availability, relevant shipping and tracking information. However, this requires that all necessary data is available in digital form and can be exchanged securely. This step requires adapted framework conditions for data protection and data security, for example with regard to the transfer of information on air freight to logistics partners.

A further measure for cross-modal logistics of shared data use is the digitalisation of freight documents in air freight - in the electronic Air Waybill (eAWB). The introduction and implementation of the eAWB requires efforts in standardisation and the joint implementation of "digital routes". This requires in particular that all participants in the supply chain switch to integrated data flows and consistent electronic documentation. A worldwide renunciation of paper documents in the air cargo logistics chain can only succeed with the support of the entire industry, be it in the areas of customs, taxes or security. It is particularly important for international airfreight that existing international data standards and processes are taken into account. In order to speed up (airfreight) logistics as a whole, it is ultimately necessary to think and act digitally, even with the government interface partners.

With regard to the electronic bill of lading, interoperability or uniformity/equivalence between EU standards and international procedures is essential, as air freight transport is already organised worldwide in a highly

standardised way with regard to customs procedures and data exchange. Further steps should be in line with the approaches of IATA (in particular the "ONE Record" initiative to further develop the technical and procedural framework for data transmission).

Data use will fundamentally change the air transport industry. New products and services and optimised processes will reduce flight, waiting and taxiing times as well as delays, fuel consumption and pollutant emissions. Air traffic management will play a central role in this process. In order to optimise this, improved networking of all those involved, more efficient and flexible communication systems and system-wide information management are needed, and these must be promoted and uniformly implemented in the EU.

4.4. A common European health data area

Health data is the key to the medical care of the future. The BDI therefore expressly welcomes the establishment of a common European Health Data Spaces (EHDS), as envisaged in the data strategy of the EU Commission. The industrial health industry will be providing important impulses and innovations to this health data space or will be producing innovations from it and should therefore be seen as a partner in its design and be involved in it on an ongoing basis.

A common European health data area will first and foremost benefit citizens: a European approach to the exchange of health data will enable citizens to be treated efficiently when travelling on business or on holiday. It will also make it much easier to find medical experts abroad. Medical professionals and researchers should be able to pool their resources (data, expertise, computing and storage capacity) across the EU to enable better healthcare and faster and more personalised diagnosis and treatment. The EHDS can also set standards for the secure exchange of health data. Ultimately, a common European infrastructure for health data in all Member States can improve the quality of care, reduce healthcare costs and generally achieve an even stronger focus of healthcare systems on the needs of patients.

For medical research, the establishment of an EHDS can give an enormous boost to innovation, especially in the field of individualised medicine. The exchange of high-quality, interoperable health data - especially Real-World Data - is of increasing importance for the research and development of innovative drugs and medical technologies. The EHDS must therefore promote both primary and secondary use of health data and make health data available for research purposes across all sectors of the health care system. The industrial health economy is one of the main pillars of medical research. Therefore, this boost to innovation can only be achieved by linking industry

to the EHDS. A single data space for health data with the involvement of industry will also help to ensure that Europe remains an attractive location for medical research and a centre of medical excellence.

From the perspective of the industrial health industry, however, some points must be set in the right direction early on in the development of the EHDS if the common European area for health data is to be a success for all the players involved.

4.4.1. Governance model and infrastructure

A leading European body for health data should moderate the implementation of the EHDS and lead it to success. This body should bring together decentralised data rooms and enable the cross-border and cross-sectoral exchange of data. It should also serve as a centre of excellence for data science and policy, provide technical support to Member States, take responsibility for the development of standards and help to resolve ethical issues. It can also promote international outreach through cooperation with other initiatives and promote the sharing of data (including data from public sources) for research, development and innovation purposes. The precise role of the Health Data Unit should be defined in dialogue with all stakeholders.

In terms of interoperability, the European Commission's work on the EHR exchange format is a first step in the right direction, but both its scope and level of implementation remain limited and should be extended to increase the relevance of EHR data for the purposes of research, development, innovation and improved clinical decision-making. A framework is needed that establishes interoperability and quality standards for data while remaining flexible enough to allow for the specific implementation required for each sector (or type of data or use case). Premature enforcement of a single, rigid interoperability standard could inhibit innovation. Standards for quality and interoperability should be developed in cooperation with relevant industry groups.

Particular attention should be paid to connecting already existing national health data infrastructures (e.g. telematics infrastructure in Germany) to the EHDS. Furthermore, it is of central importance to ensure interoperability with existing pilot projects (e.g. EHDEN or MIDAS) and research networks (e.g. EIBIR).

The quality of the data should be transparent, with the identification of the source and validation/certification of the data sets being an important step. Powerful semantic search engines should be implemented to improve the findability and analysis of the data and facilitate the initiation of Europe-wide research projects.

4.4.2. Data structures and purposes

The EHDS can trigger a further innovation boost in the research and development of new therapies and medical technologies. However, this will only succeed if health data can also be used for secondary purposes. As one of the most research-intensive industries, the pharmaceutical and medical technology industries should, in principle, be given equal access to health data - always under the premise that every citizen retains sovereignty over his or her data and that the processing of health data is in line with the DPA. Concrete, consistent rules for access to data must be established to ensure that the data is secure and that the individual's right to privacy is protected. At the same time, these rules must apply equally and consistently to all actors in the private and public sectors, as well as to SMEs and large companies.

4.4.3. Consumer and data protection

Public confidence in a secure exchange of health data is a crucial component for the success of the EHDS. Surveys show that a large proportion of European citizens are willing to make their data available for medical research. The infrastructure of the EHDS must provide secure protection against cyber attacks in order to build long-term trust. In addition, it is important to raise awareness among citizens about the risks and value of sharing data. Understanding individuals when it makes sense to share their data (e.g. for insights generated by AI/machine learning) and when and how the right to privacy can be exercised, is the key to a trustworthy EHDS.

The protection of patient data has a particularly high priority. The GDPR provides an appropriate legal framework for the exchange of personal health data. At the same time, the opening clauses that the GDPR offers for research and development are applied very differently in the European states. The inconsistent application of data protection regulations in different countries and at different levels is an obstacle to Europe-wide research projects. For this reason, national governments should be motivated in the European dialogue to apply the opening clauses of the GDPR and interpret them in a research-friendly manner. In this context, reference must unfortunately be made to Germany as "bad practice", where 17 data protection commissioners (federal government + 16 federal states) contribute to the fragmentation of data protection and make research projects more difficult. While the GDPR undoubtedly is a valuable framework and underlines the European approach of a digital strategy with simultaneously high data protection standards, the data protection regulations should be further developed or specified to the extent that they do not make research-relevant data use impossible per se. One starting point would be to abandon the opening clause in the DPA

regarding health data, in order to guarantee and promote cross-border European research.

Given the risks associated with the sharing and analysis of health data, a framework that creates confidence in the area of data sharing (digital literacy) is appropriate. These can be formulated and reinforced as ethical principles, e.g. in the EU guidelines on ethics in artificial intelligence. The creation of a common vocabulary specifically for data that enables a common understanding in the data space should be considered. This will help partners to navigate more effectively within complex data ecosystems and help individuals to build data literacy, which in turn will help to build confidence in data ecosystems as a whole. Educating individuals about the risks and value of data sharing is also important. Enabling individuals to understand when it is appropriate to share their data (e.g. for AI/machine learning insights) and when and how to exercise the right to privacy is key to a strong, trusted data ecosystem.

The Code of Conduct for the processing of personal data in the health sector (under Article 40 of the DPA), which the Commission is considering in the context of the European health data area, should provide guidelines to overcome obstacles in a legally secure manner and in the interests of citizens. As already explained elsewhere[11], the legal definition of anonymisation is particularly unclear. It must be recognised that health data can be made anonymous; strong pseudonymisation and the lack of adequate means of identifying data constitute anonymisation in this context. A Europe-wide solution should also be found for what happens to further processed personal data (e.g. in AI models) when citizens withdraw their consent. In this respect, it would be helpful to further develop the GDPR in accordance with the provisions of Section 24 (2) and Section 27 BDSG, which also permit the processing of special categories of personal data by non-public bodies for research purposes. The Code of Conduct could provide a mechanism to minimise this divergent interpretation and encourage stakeholders to make use of the right to transferability of data.

4.5. European Cloud for Open Science

The openness of innovation systems is an important lever for strengthening competitiveness, as it increases the available stock of knowledge and encourages participants in the science and innovation system to perform better. A European Open Science Cloud (EOSC) can play an important role here in providing interdisciplinary access to the methods and results of

[11] Cf. Chapter A III. c) bb).

current research work and making them available for the benefit of a wide range of issues. The goal of ensuring a trustworthy and open, decentralized data environment and associated services must be accompanied by interfaces to make this data space as accessible as possible, especially for European players in science and industry, for the benefit of innovations. However, the protection of intellectual property (IP) and confidential business information (CBI) - especially in public-private partnerships and research projects involving industry - must be guaranteed.

About the BDI

The BDI transports the interests of German industry to the political leaders. In this way it supports companies in global competition. It has an extensive network in Germany and Europe, in all important markets and in international organisations. The BDI provides political support for international Market development. And it offers information and economic policy advice on all industry-related topics. The BDI is the umbrella organisation of German industry and industry-related service providers. It speaks for 40 industry associations and more than 100,000 companies with around 8 million employees. Membership is voluntary. 15 state representatives represent the interests of industry at regional level.

Imprint

Federation of German Industries (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

Contact person

Dr. Michael Dose
Senior Manager
Department "Digitalisation and Innovation“

T: +49 30 2028 1560
M.Dose@bdi.eu

Stefanie Ellen Stündel
Senior Manager
Department "Digitalisation and Innovation"

T: +32 27921015
S.stuendel@bdi.eu

BDI document number: D 1204

Transparency register number: 1771817758-48