STIFTUNG DATENSCHUTZ

DATA PORTABILITY

POLICY PAPER

TABLE OF CONTENT

Author: Prof. Dr. Anne Riechert, Stiftung Datenschutz/Frankfurt University of Applied Sciences

INTRODUCTION

The Stiftung Datenschutz discussed the topic of data portability in three workshops with participation of experts from politics, supervisory authorities, industry, science and society. Impulse for initiating the talks was given by facebook, since the company had published a White Paper on portability in which several issues were pointed out which also the Stiftung had an eye on. On this occasion, the Foundation revisited the content of its 2017 project work. The aim was to take stock of the questions: (How) has the right to data portability arrived in practice? Which chances and risks of this – still young – data subject right from the DSGVO may arise?

The workshops were summarized and evaluated by Stiftung Datenschutz in aggregated form and the respective conclusions were linked in an overall summary (see the following chapters). Based on this, recommendations for action were drawn up.

In practice, there is still little experience in managing the right to data portability. Overall, however, there is a great need for a comprehensive analysis of how the existing portability law affects both the market and society and which technical challenges need to be tackled. Various initiatives are currently dealing with this topic, such as the "Data Transfer Project", the "Data Portability Cooperation" of various telecommunications providers or the idea of "New Governance" with a focus on cross-sector data transfer.[1] From the point of view of data protection law, all activities must focus on strengthening the right of data subjects to exercise control in accordance with recital 68, so that new business models may not be allowed to undermine this right of control in any way – for example by referring to a service-oriented interpretation. This paper therefore also identifies challenges to which neither the GDPR nor the previous guidelines on the right to data portability can provide a clear answer. Although the Data Ethics Commission, appointed by the Federal Government, has set a corresponding objective by recommending that data portability should not be extended (at least for the time being),[2] the focus should be on a possible European-wide interpretation and corresponding implementation. In this context, the expectation was expressed in the workshops that Article 20 GDPR would not be amended in the coming years. Therefore, a clear guideline for the interpretation of the text of the Regulation is all the more urgently needed in practice.

It should be emphasized that the 2017 study "Practical Implications of the Right to Data Portability in practice" by the Stiftung Datenschutz and the resulting practical recommendations are still up-to-date.[3] In this context, the Data Ethics Commission, in its report published on 23.10.2019, also referred to the importance of industry-specific rules of conduct and standards.[4] In addition, other important issues were worked out in the discussions which the Stiftung Datenschutz has analyzed with regard to legal, technical and social implications. Own findings were also included into the evaluation and the recommendations for action.

1 In the summary and evaluation of the first and second workshops, these projects are explained in more detail.
2 See the report of the Data Ethics Commission, published on 23.10.2019, https://sds-links.de/Datenethikkommission. Under the topic "Improving controlled access to personal data", p.21, the Data Ethics Commission recommends (for the time being) refraining from extending the portability right, for example to data other than those provided or to real-time transfer, and that a corresponding evaluation should first be carried out.
3 Study by the Stiftung Datenschutz "Practical Implementation of the Right to Data Portability", p. 250, https://sds-links.de/Studie2017.
4 Report of the Data Ethics Commission, p. 136.

COURSE OF ACTION

The workshop series focused on the following key issues:

- What are the objectives of data portability?
- What are the requirements and basic principles?
- How does portability meet people's needs?
- When is there a case of data portability?
- Which data should be transferable?
- Whose data should be transferable?
- What should be done with data relating to more than one person?
- How should individuals and controllers choose third parties? Should third parties follow any rules, and if so, how can this be ensured? Would such rules be compatible with the objectives of portability under the GDPR? What, if any, should people be told about the purposes to which they could port data?
- How can secure and fair data transfers be ensured?
- How can industry implement the right to data portability while ensuring data protection? And how can this be realized for other forms of portability?
- Which legal and technical questions arise from the mobility of data?
- What checks and balances are the right ones and who is responsible in the event of incidents or breaches?

WE WOULD LIKE TO THANK THE FOLLOWING PARTICIPANTS FOR THEIR VALUABLE CONTRIBUTIONS TO THE DISCUSSION:

Bock, Kirsten (Privacy Expert)

Brandt, Liz (Ctrl-Shift)

Chavez, Jessie (Google)

de Bièvre, Matthias (visionspol.eu)

Dion, Olivier (OneCube)

Dittmar, Thorsten (polypoly.eu)

Frank, Sabine (Google)

Jakobi, Timo (Berlin University of the Arts)

Mache, Lutz (Google)

Madhani, Bijan (Facebook)

Molavi, Ramak (iRIGHTS law)

Quiel, Philipp (reuschlaw Legal Consultants)

Rens, Semjon (Facebook)

Schätzle, Daniel (Härting Rechtsanwälte)

Teubner, Timm (Technical University Berlin / Einstein Center for Digital Future)

van den Boom, Jasper (Tilburg University)

van der Valk, Thomas (Facebook)

Willard, Brian (Google)

... and others.

RECOMMENDATIONS FOR ACTION

OBJECTIVES

The right to data portability is focused on **strengthening the control rights** of data subjects. An interpretation of the law in the sense of a more **service-oriented perspective** requires a examination in advance, weighing up whether such an interpretation could be contrary to the control rights of the data subjects. Ethical aspects should be taken into account.

As a control right, the right to data portability enables **GDPR-compliant processing and has to be requested by the data subject**. Data portability cannot legitimize the transfer of data that would otherwise require a legal basis or informed consent from the data subject. This should be taken into account both in terms of concepts such as "data mobility" and new business models in practice.

The right to data portability allows data subjects to transfer a whole data set or only a part of it to any other service provider without giving reasons; it does not include automatic deletion of data and must be distinguished from the right of access. Due to the **high complexity** of the right to data portability, **data literacy** of data subjects and consumers should therefore be fostered and their knowledge of possibilities and limitations of the new right should be increasedby **information campaigns**.

The **law is ahead of technology and practice** and therefore it should be examined to what extent the right to data portability can at present be implemented in practice, particularly regarding the sanctions imposed by the GDPR.

SCOPE OF APPLICATION

It could be useful to examine which **raw- and metadata** needs to be transferred in order to realize the right to data portability both from the technical and practical point of view and in the interest of the data subject. In addition, user surveys could be carried out to determine which kind of data is of **interest for transfer**.

The interpretation of the term **"observed data"** should be based on the strengthening of the data subject's rights of control. It should be clarified to what extent a comprehensive transfer of usage data and a broad definition of "data provided" can infringe the **personal right of data subjects**, in particular due to the economic (own) interests of service providers in the exploitation of this data.

With regard to new business models, clear conditions could be developed regarding the requirements for a "request" by the data subject. The **technology should not prescribe and define the law**, but rather the technology should be based on legal requirements.

The **European Data Protection Board** could use the example of the transfer of a contact directory to a webmail service, which is described in its guidelines, in order to clarify in what specific cases the **third parties rights** can be infringed in a data transfer and to what extent processing for **legitimate interests or scientific purposes** is possible. In addition, codes of conduct could be helpful.

It could be useful to clarify to what extent the data subject or the provider should or could be subject to own (verification) obligations prior to a data transfer. In this context, it should be taken into account that the provider is committed to the principle of **"privacy by design"** and that the data subject regularly processes data exclusively for personal and household activities.

IMPLEMENTATION STRATEGIES

Companies have to find a good level of user information when implementing data portability. They should create appropriate transparency without overloading users with information. High attention has to be payed to proper authentication of requesting persons in order to avoid data breaches and unnecessary risks to privacy. Although GDPR interdicts controllers to hinder portability requests, precautions should be made to mitigate risks of personal user data being ported to third parties that are not trustworthy.

Standards can help to strengthen users' trust in the existing infrastructure. Standards should be created on the basis of specific use cases and should always be updated in order to clearly point out the opportunities and risks. In order to stimulate data portability in practice, the choice of use cases could – as a first step – be made by the companies.

The development and the commitment to a standard both builds trust in a company and can serve as a **marketing instrument**. Corresponding **open source projects** can help small businesses realize the right to data transfer in practice.

The right to data portability is associated with **data sovereignty**. A clear definition of data sovereignty could therefore be established, reflecting the data subject's rights of control equally. In this spirit, the **right to informational self-determination could be further developed** at European level. **"Sovereign"** should be understood literally as **competence, knowledge and awareness of a data subject** to make **autonomous and superior decisions** in a digital world.

Helpful for operationalizing data portability might be solutions from the PIMS sector. Those Personal Information Management Systems could act as hubs between the entities which the requested datasets should be ported between.

SUMMARY

CHALLENGES AND OPPORTUNITIES

The original intention of the right to data portability, to facilitate the switch to data protection-friendly networks, is increasingly fading into the background. When data portability is currently being discussed, the focus is often on the free flow of data, which has been paved the way by the guidelines of the Article 29 Data Protection Working Party (confirmed by the European Data Board) due to the nearly unlimited transfer possibilities of data across industries.[1] However, implementation in practice faces a number of challenges. Comprehensive data portability can only succeed if companies cooperate and create the appropriate conditions. But often there are concerns about cooperation with large providers. Nevertheless, portability cannot be successful if everyone develops its own system. To achieve comprehensive, cross-sector data portability, concerns has therefore to be reduced and common standards developed so that new benefits and new services can emerge. On the other hand, this issue requires particular awareness, especially with regard to very sensitive data, such as insurance data, health data, etc. Open source projects and cooperations – such as those mentioned in the introductory chapter – can support this and enable companies with smaller market shares and start-ups to implement data portability.

From a technical point of view, companies are currently still facing the challenge of developing common and interoperable data formats. This may involve the compilation of playlists of different services, but also the transfer of health data. In addition, with each new service a new format must be found, so that the challenge also is to keep pace with the respective system.

The law is ahead of technology and practice and – despite and because of the statements made in the workshops that no amendment of law is to be expected – an evaluation could clarify to what extent the right to data portability can be implemented in practice considering the sanctions of the GDPR. Besides, open source projects may help small businesses to realize the right to data portability.

1 See the guidelines of the Article 29 Working Party adopted on 13 December 2016 last revised and adopted on 5 April 2017, are available in different languages on: https://sds-links.de/Leitlinien. The European Data Protection Board confirmed the Article 29 Working Party guidelines at its first plenary meeting on 25 May 2018, see https://sds-links.de/EDPB.

SCOPE OF APPLICATION

In the discussion about the issue data portability other terms such as “data access rights/access to data”, “data sharing” or “data mobility” were regularly referred to. These terms must be distinguished from the right to data portability, especially since this often includes regulatory and/or political issues. In the context of “access to data”, reference was made to possible specific legal regulations that could apply as a matter of priority (e.g. the PSD2 Directive was mentioned). On the other hand, the terms “access to data” and “data sharing” are also used in the public debate in connection with anonymized data, so that in this case the GDPR would not apply. It could, however, be examined to what extent a concept such as “data mobility” is important from a political or social point of view. This was discussed under the aspect of the extent to which other technical standards or differing requirements for guidelines, policies, etc. might be necessary. However, the legal assessment shows that the term “data mobility” has no particular legal impact. At most, with a view to new business models and their implementation in practice, it has to be clear and unambiguous that data portability is subject to the requirements of Article 20 GDPR which is a control right of the data subject but not a company right. If a further data flow is to be carried out, the transfer of personal data is a data processing which requires a legal basis, for example in the form of consent under the requirements of Article 4 No. 11 and Article 7 GDPR.

It was also discussed whether the concept of “data mobility” could be considered for data which are not covered by Article 20 GDPR, such as data collected by the data controller on the basis of legitimate interests or data which do not relate to individuals. In these cases the formal requirements of the article 20 GDPR would not be fulfilled, so that a legal impact is given only then, if a corresponding extension is fixed by guidelines of the European Data Protection Board or by an amendment of law. It could be however necessary to face the challenge that facts are created in practice by new business models.

It should also be emphasized as an essential requirement that data portability as the data subject’s right of control always requires a clear request by the data subject. The boundaries between “initiation”, “nudge” and “request” can be blurred. In this context, the question could be raised of to what extent the underlying technology has an impact on this. The technology should not, however, predefine the law, but the question should be asked in which cases there is a “request” from the data subject and what specific requirements exist. This question can arise, for example, with one-click solutions or when generated data is continuously transferred via an API interface. Guidelines should be developed for this case.

Data portability is a control right of the data subject and ensures the realization of GDPR-compliant processing. Overall, it must therefore be ensured that there is no transfer of data that requires a legal basis. With regard to possible business models, clear conditions could be developed regarding the requirements for a “request” by the data subject. In this context, the technology should not predefine the law.

CONTROL RIGHTS AND TRANSPARENCY

In practice, reference is often made to the need to interpret the right to data portability in a "service-oriented" way, according to the interests of users. It is important to keep recital 68 in focus at all times: Data portability should strengthen the control rights of the data subject! It is therefore necessary to examine which data are of interest to the user. It was also pointed out that in today's fast-moving world the tweet from last week might already be uninteresting. On the other hand, the argument was raised that even an objective photograph (e.g. sunset) can be compared with a personal commentary, and that this transfer is covered by the original idea of data portability. The analysis of user interest could be accompanied by a corresponding survey: In which data do users have a transfer interest? In this context, it also matters whether the term "observed data", as defined in the Article 29 Working Party guidelines, needs to be restricted. Under the present interpretation, data based on cookies could in principle also be included (prior to their evaluation and classification as "inferred data"), provided that the user has given his consent to the setting of cookies, or other usage data, e.g. clicks generated by the user. In this context, there is still the unsolved problem of how to ensure the so-called "law literacy" or "data literacy" of the data subjectwhich could also affect the assessment of the value of data. It is therefore a question overall of ensuring the necessary transparency. When data is transferred directly to another service provider, it is also important that the data subject can grasp the "how" of further data processing in order to avoid frustration. The data subject should also be aware, on the one hand, that the transfer of the data does not involve automatic deletion by the original service provider and, on the other hand, of the extent to which the new service provider may process data on the basis of its own legitimate interests.

The interpretation of the term "observed data" should be based on the strengthening of the data subject's rights of control. In this respect, it should be clarified to what extent a comprehensive transfer of usage data and a broad definition of "data provided" can infringe the personal right of data subjects, in particular due to the economic (own) interests of service providers in the exploitation of this data.

Besides, as a basis for a fair and transparent process, further clear guidelines and codes of conduct could be developed with regard to "legitimate interests", "scientific purposes" and "further processing", taking into account new business models of data portability and specific applications in practice. Beyond this, clear and common standards could help to ensure a fair process.

In addition and regarding the complexity of the right to data portability, further educational work, possibly in the form of information campaigns, is necessary to strengthen the user with regard to the essential "law literacy". This could be done by neutral institutions or the supervisory authorities.

THIRD-PARTY RIGHTS

With regard to the rights of third parties, the question arises to what extent the provider transferring the data should be responsible, even if the guidelines of the Article 29 Working Party assign responsibility to the new provider. On the one hand, the principle of "Privacy by Design" could allocate such a responsibility, in particular since the data subject is often not in a position to actually check the "rights of third parties" and, moreover, in the case of social networks, the processing of the data is usually carried out for exclusively personal and household activities. For example, the provider could implement consent mechanisms. Nevertheless, it is argued that the data subject should be responsible for the third party rights.[2] On the other hand, the provider should also not be allowed to control the data transfer, for example, by warnings. In this respect, the Article 29 Group guidelines need clarification concerning the transfer of a contact directory to a webmail service as an example of portability.[3] Although the processing for own purposes, such as marketing purposes, was excluded, further guidance could be helpful regarding "legitimate interests" or "scientific research purposes" already described in the previous explanations. This could be worked out on the basis of specific use cases and could also be done by a negative or positive list. Otherwise, it would have to be clearly stated that any processing of the data of third parties by the new provider is prohibited, so that the transfer of the data would merely represent a change of storage medium.[4] In this case, however, the new provider might not be able to process the data in a way that could be permitted to the original provider.

It could be clarified under which conditions the right to data portability does not infringe the rights of third parties and to what extent the data subject or the provider may be subject to own (verification) obligations prior to a data transfer. It should be noted in this context that the data subject regularly uses services for purely personal or household activities, and is insofar not subject to the obligations of the DSGVO, and the Provider has to take into account the principle of "Privacy by Design".

2 Herbst in: Kühling/Buchner, DSGVO/BDSG, Artikel 20 DSGVO (GDPR), recital 17.
3 Guidelines of the Article 29 Working Party, p. 13. See also the evaluation of the second workshop.
4 See the evaluation of the second workshop.

GOVERNANCE

The participants in the discussion also focused on the fundamental question of how a future data policy and related governance structure could be designed. In this context, different models were discussed – over and above the formal requirements for the right to data portability – which could comprehensively guarantee a transparent and fair data processing in practice.

The implementation of standards, certificates, personal information management systems (PIMS) and the establishment of a neutral organization were discussed as instruments for a transparent and fair process which could also serve to strengthen the control rights of users equally and which are explained in more detail below. It was emphasized that ensuring neutrality is essential – without economic interests in connection with the management of the system. In particular, the social importance of neutral social networks, neutral e-mail and chat solutions was pointed out.

Overall, the implementation of so-called "New Governance" was proposed as an option. The focus of such a new structure is always on decentralized data storage by the user (which is advantageous from a data protection point of view). An independent supervisory body should coordinate different actors, such as companies, organizations and institutions, and ensure the necessary balance of interests. The aim is to develop technological standards for portability and the protection of personal data as well as good practices by using specific use cases. In this respect, it would be a matter of self-regulation that works on the basis of a democratic structure and a body that monitors the balance of the various interests. These standards are intended to be part of a digital infrastructure. Besides, these standards could be established in practice in parallel with certificates, guidelines or codes of conduct. Guidelines and codes of conduct could, for example, be the (abstract) basis, while the standards describe individual specific application examples.

Another possibility discussed was the establishment of a neutral platform to exercise the rights of the user. Such a representative body could – in principle – play a decisive role in ensuring the necessary neutrality. This could also be of interest in connection with the monetization of data, for example as a trust model. In this context it is repeatedly pointed out in literature and practice that data subjects are no longer in a position to make a self-determined decision due to the complex data processing. With regard to the monetization of data, this context is therefore about fair participation possibilities in the value creation process of data, as is already known from copyright law.[5] However, this requires a comprehensive and in-depth examination of the personal rights. It is an extremely sensitive issue, as it is not yet clear whether it is at all possible to respect the personal right of the data subject, in particular the right to informational self-determination within such an organization. A particular challenge is who is responsible for this platform and who monitors it structurally.[6]

In addition, personal information management systems (PIMS), which were already the subject of the study "New ways of providing consent in data protection" by the Stiftung Datenschutz in 2016, can be used to monitor and ensure a transparent process.[7] However, depending on the design of the system, one challenge is the "purpose limitation" as well as the simple and user-friendly handling and usability of the system.

5 Further details can be found, above all, in the evaluation of the third workshop.
6 In principle, the Data Ethics Commission has also recommended further research into trust models.
7 Study by the Stiftung Datenschutz "New ways of providing consent in data protection" which examined different kinds of personal information management systems (PIMS) (https://sds-links.de/PIMS).

Overall, in the discussion about a possible governance structure, the question of where the data should be stored – whether it should be stored centrally or decentrally – was also taken into account.

From an economic point of view in particular, however, the objection was raised that the main objective was access to the relevant data and that the storage location was not important.

Different possibilities are currently being discussed as to how a governance structure could be designed in the future. Overall, a neutral structure provides the necessary trust and transparency and ensures independence from large, market-dominating companies.

DATA SOVEREIGNTY

The right to data portability is associated with the term “data sovereignty”. Thus a user can transfer a complete data set or parts of it to any new provider without giving reasons. However, the question remains whether “data sovereignty” means more than the right to informational self-determination. The focus should always be on whether the data sovereignty associated with Article 20 GDPR is advantageous for the data subject and strengthens the rights of control. The question is therefore whether data portability allows more privacy or whether it leads to the opposite.

On the whole, the term data sovereignty can be helpful to achieve a common understanding of modern data protection law at European level and to develop a European-wide definition, since the right to informational self-determination was coined by the Federal Constitutional Court. However, there is a need to examine what is meant by data sovereignty and in what way this can be implemented in favour of the data subject. A transparent procedure should be ensured – corresponding to the actual meaning of the word “sovereign” and thus understood in this context as enabling the exercise of the right to data portability. Therefore, if the right to data portability is an instrument for exercising data sovereignty, in practice it is necessary to provide the necessary tools for this purpose in terms of simple, usable and practicable applications. Only then will the law be implemented in such a way that a data subject can act independently, superiorly and without restriction. This also includes so-called “law literacy” and an awareness of the possible value and use of personal data for others or (concretely) for companies with own business interests.

Above all, data sovereignty may not be associated with the risk that other persons, institutions, etc. make decisions that are detrimental to the user. This should also be considered in the context of the personal information management systems (PIMS) and trust models described above. It is always necessary to critically question who offers these systems and to what extent conflicts of interest can exist “within the system”. In literature and practice, reference is made to an “information asymmetry” that could arise as a result of submission to management or assistance systems.[8]

The greatest challenge in the future will therefore be that data subjects make self-determined decisions based on their own free will, without being led there by “recommendations” from a system that does not act neutrally. With regard to data sovereignty, “sovereign” should therefore be understood in its literal sense: The data subject should act in a deliberate and superior manner, not the system. Privacy therefore also includes the elimination of asymmetries in knowledge. This should be a necessary part of a definition of “data sovereignty” in the digital age. Digital ethics will be more than necessary in the future.

8 Ramge/Mayer-Schönberger, Das Digital: Das neue Kapital – Markt, Wertschöpfung und Gerechtigkeit im Datenkapitalismus.

STIFTUNG DATENSCHUTZ

WORKSHOP

#01 – September 11, 2019

SUMMARY, EVALUATION AND ANALYSIS

A VISION FOR DATA PORTABILITY

INTRODUCTION

Overall, the implementation of the right to data portability in the GDPR by the European legislator is visionary. Nevertheless, services such as Facebook or Google have already provided users with the right to data portability in the past, without any corresponding legal obligation (e.g. Google Take out). In other industrial sectors (on the other hand) data portability is still completely lacking and some companies do not seem dissatisfied that data portability is not yet the focus of user attention. One challenge is therefore to convince companies and users alike of the benefits of data portability – especially across sectors. The restraint of companies has so far also been due to concerns about giants such as Facebook and Google. During the workshop it was pointed out that companies such as banks and insurance companies would prefer to develop their own systems for data portability instead of working with these service providers. To achieve comprehensive, cross-sector data portability, concerns should therefore be reduced and common standards developed so that new benefits and new services can evolve. On the other hand, this issue requires special awareness, in particular with regard to data on policyholders, health data, etc. Accordingly, this law should be developed with the maximum diligence and in line with the cross-border transfer of data. It is therefore a matter of trust, shared values and, ultimately, ethical standards – for both personal and even non-personal data.

WHAT ARE THE GOALS OF DATA PORTABILITY?

It is agreed that the right to data portability is a personal right. Furthermore, the parallel right of access has to be distinguished: Although the right of access enables the user to request a copy of data for the purpose of transparency and information, it may also enable him to exercise further rights or take legal action. But overall and regarding the right of access, there are fewer options available to the data subject. The right to data portability includes the possibility to transfer a complete data set or parts of it to any other provider for any reason. The transfer must be carried out in a machine-readable format, so that the data can be used without problems and processed automatically (further) by another service provider. Data portability is therefore about more sovereignty. The so called "law literacy" or "data literacy" of the data subjects is of enormous importance here. From the point of view of a data subject, there are two parallel rights that may not always be easy to separate. In addition, data portability only refers to s data provided by the data subject, and this does not imply automatic deletion rights – which may not be expected by all data subjects – but which would in any case have no effect if the original provider still had a contract term. In order to avoid frustration with the user, it is therefore important to understand the possibilities offered by the law.

HOW DOES PORTABILITY MEET PEOPLE'S NEEDS?

Which solutions are needed to make data portability interesting for users and companies as a whole? From a user perspective, sharing data on all the platforms they use, such as music lists, may be part of modern life in the future. However, the import or export of data is not common. It should also be taken into account that some users have no interest at all in transferring all data, but only part of it. But it seems that users still have the idea that data portability is the transfer of all data from one social network to another. So to what extent can the interest in data portability be enhanced as a tool to support "data sovereignty"? Does the tool just have to be convenient or should financial aspects be included? The privacy paradox has to be considered in this context. Simple and practicable instruments facilitate the transfer, but a carelessly implemented download button can also contain a risk of misuse. On the other hand, companies have to consider ways to integrate privacy and data protection policies into existing mechanisms.

In this context, data storage is another challenge and the related question of whether it is appropriate to store data in a central location. In this context, it is often pointed out that – like in other countries – a large data pot could be established. On the other hand, from the point of view of data protection law, the more preferable option of decentralised storage (for the respective user) can also be considered. Particularly from an economic point of view, however, there is the argument that the question of the storage location is not relevant and that many companies are not interested in storing data, but that the main objective would be to provide access to the relevant data.

The message is: Now is the time to make the basic decisions for practical implementation – How the future of data governance should be structured.

WHEN IS A TRANSFER DATA PORTABILITY?

During the workshop, apps that access and transfer user data and data of third parties were also discussed. A parallel to data portability is drawn from a technical point of view, since both cases may involve unlawful data transfer and it is therefore questionable to what extent a provider is obliged to carry out a prior check, since – on the other hand – he shall transfer the data "unhindered" in order to fulfil the right to data portability. Both in the case of a request by the data subject and in the case of an app, access to the data might take place without the involvement of the third party (or the data subject). However, it has also been argued that apps that have access to user data and transfer this data are not cases of data portability.

In addition, the following should be pointed out in this context: If it is a request from the user, it is questionable to what extent the provider may or should refuse this request. The transfer of data from third parties requires a legal basis which can also be based on Article 6 (1f) GDPR. The question, however, is whether the provider should weigh up the interests or the user. According to the GDPR, the user has no obligations in the course of a purely personal or household activity (Article 2 (2) GDPR). In the context of data portability, however, it is argued that the provider is not obliged to check, but the data subject shall decide which data should be transferred.[1] But also from the point of view of "privacy by design" it might be fair if the provider hosting the technology in its whole is (also) responsible. Binding standards should be developed for these cases. All in all, this is a question of the allocation of roles and a question of regulations.

WHAT ARE THE REQUIREMENTS AND KEY PRINCIPLES?

The key principle of data portability is a comprehensive view that includes all possible perspectives (consumer, technology, law) in the risk and also opportunity evaluation. Different mechanisms can be created for this purpose. One question is whether there is a need to use the broader concept of "data mobility" and how to distinguish it from the concept of "data portability" – whether these are two different areas. This is particularly supported from a technical point of view and from the point of view that different strategies/policies are needed.

There are already two concepts in this area that focus on data portability and data mobility. One idea was developed by Ctrl-Shift in the UK.[2] The focus is on data mobility in various areas of life, such as health management, private household management, private financial management, etc. A further project is insofar more abstractly defined, since an overall concept for a so-called "New Governance" is to be developed in a new way.[3]

CTRL-SHIFT

Within the framework of this project, it is planned to develop an infrastructure that supports individuals in managing their private areas of life. Interoperability has also to be ensured. This could be a so-called "sandbox" in which users of different services import their data and export it to another service. The key principle for the success of this project is – above all – to ensure usability and not only technological implementation. The challenge is to implement this for different stakeholders and different users. The question of storing data should also be considered: One consideration is to link the data without storing it in a central location.

NEW GOVERNANCE

This project focuses on the development of data circulation and protection standards to tackle the challenges of the digital world.[4]

For the implementation of this project, standards and tools are required above all. The basis for this is a democratic structure that defines the processes and supports standards, but also helps people to find the best solution. For this purpose, an independent control committee shall be formed to coordinate the various actors. Technological standards for portability and the protection of personal data as well as good practices in accordance with the principles of the GDPR shall be developed. As a result of the intended tests in real use cases by experts, these can be able to be applied directly by the market players.

1 Herbst in: Kühling/Buchner, DSGVO/BDSG, Artikel 20 DSGVO (GDPR), recital 17.
2 https://www.ctrl-shift.co.uk/.
3 https://www.privacytech.fr/livre-blanc/.
4 In April 2019, Olivier Dion coordinated a white paper – a new governance for data in the XXI century – for the French Parliament with 50 organisations (including MyData) from 14 countries to demonstrate the benefits of portability and the need for new governance for data protection standards. A new design phase for the new governance began in June 2019: https://mydata2019.org/presenter/olivier-dion/.

CONCLUSION

The original intention of data portability to facilitate the switch to data protection-friendly networks is increasingly becoming secondary. The discussion on data portability often focuses on the free flow of data, which has been paved the way by the Article 29 Working Party guidelines due to the almost unlimited transfer possibilities of data across industry boundaries. A new term that has been created is “data mobility”. In this context, it remains to be clarified to what extent this requires other technical standards or policy requirements. The possibility of transferring data offers a new value and benefit to the data subjects. But this new value needs regulations.

From a data protection perspective, it is essential to implement standards that still focus on the personal rights of users. Ethical aspects also play an important role. In the future, it will become more and more important for companies to focus on ethical aspects, to transparently align their corporate culture accordingly. Furthermore, users need the necessary education and the knowledge to decide on the processing and the related value of “their” data. “Law literacy” or “data literacy” are the corresponding keywords in this context, as well as the vision of a “New Governance” that can take on a pioneering role for fair and transparent data processing on the basis of democratic, independent structures. Digital ethics – we still have a long way to go.

STIFTUNG DATENSCHUTZ

WORKSHOP

#02 – October 01, 2019

SUMMARY, EVALUATION AND ANALYSIS

DATA PORTABILITY IN PRACTICE

INTRODUCTION

In both workshops participants pointed out that neither legal amendments to Article 20 GDPR nor amendments to the guidelines of the Article 29 Working Party on the right to data portability will be expected in the coming years.[1] Nevertheless, there is still a need for discussion in practice, especially with regard to new business models.

Overall, this second workshop explained the challenges that may arise in developing a common format for different services. Besides, with regard to the so-called "observed data", the question was also raised as to how broadly this term should be interpreted and whether a broad interpretation might conflict with the protection of the personal right of a data subject. Furthermore, it seems not be clear whether other data which are not based on the legal basis of contractual necessity or consent can also be considered for a transfer. Particularly from the point of view of companies, reference is made to the need for users to interpret the right to data portability in a service-oriented manner. Even though the Data Ethics Commission has recommended in its final report that the right to data portability should not be extended,[2] the digital reality cannot be ignored: There are different scenarios and use cases for which guidelines and assessments could be helpful and which could weigh up the advantages and disadvantages of an enlargement. In addition, the Data Ethics Commission merely points out that it does not recommend a broadening of the Act for the time being, so that a different interpretation cannot be ruled out in the future. Overall, in order to answer these questions, the focus must always be on recital 68: The control rights of a data subject shall be strengthened!

1 This point of view was stressed as well in the first discussion round on 11.09.2019 as the second workshops on 01.10.2019. Furthermore, see the guidelines of the Article 29 Working Party adopted on 13 December 2016 last revised and adopted on 5 April 2017, are available in different languages at: https://sds-links.de/Leitlinien. The European Data Protection Board confirmed the Article 29 Working Party guidelines at its first plenary meeting on 25 May 2018, see https://sds-links.de/EDPB.

2 See the report of the Data Ethics Commission, published on 23.10.2019, https://sds-links.de/Datenethikkommission.

LEGAL SITUATION

PROVIDED DATA

The right to data portability pursuant to Article 20 GDPR is a personal right despite the original intention of the lawmaker to facilitate the change of provider or the switch to a data protection-friendly network. It is a right of the data subject. The guidelines of the Article 29 Working Party define a broad scope of application. Accordingly, the right to data portability applies across borders and sectors. It applies both to data that a user actively provides for a service ("inventory data") and to so-called "observed data" ("usage data"). Due to this broad interpretation, industry has already demanded in the past that the term "data provided" be limited to data actively provided by the user.[3]

DATA SOVEREIGNTY

The right to data portability is also associated with the term "data sovereignty". Thus a user can transfer a complete data set or parts of it to any new provider without giving reasons. However, the question remains whether "data sovereignty" means more than the right to informational self-determination. It seems, for example, that the right to data portability can enable a user to trade with his or her data. This is particularly relevant when new business models are developed which support this. However, it is problematic that the value of the data remains unclear. It is also referred to here as the "deliberately blind spot" of data protection law.[4] It is also unclear whether the user has the competence for such a "data business", as he or she will find it difficult to assess which "observed data" ("usage data") he or she has generated can also be regarded as valuable from an economic point of view. In this context, it does not seem to be clear whether it is helpful in all cases for the protection of the personal right to receive the personal data in a machine-readable format, e.g. also data based on cookies for which he has given his consent or a link- or click-list, as this can also lead to a "sell-out" of data. In addition, according to the Article 29 Data Protection Working Party, the data controllers should "provide personal data together with useful metadata at the highest possible level of granularity".[5] Some critics refer to this as an "alarming" practice of transferring an entire data set and then checking whether all the data is actually needed. Therefore, it seems that many data may be affected for which the term "data sovereignty" needs to be defined.

THIRD-PARTY RIGHTS

With regard to the rights of third parties, the Article 29 Working Party has presented in its guidelines an example in which a user transfers a directory of contacts, friends and family to another provider (webmail service). However, the requirement of the consent of the third party is not mentioned as a condition for this example. The Article 29 Working Party merely clarifies that the new provider may not use the directory for marketing purposes.[6]

This example is followed by the question of whether a controller could nevertheless refer to legitimate interests under Article 6(1)(f) GDPR or scientific purposes under Article 89 GDPR or whether any processing is prohibited. If any processing were prohibited, it would only be a matter of changing the storage medium – although it is more than questionable whether this is realistic in practice. On the other hand, it has to be taken into account that according to Article 6 (1f) GDPR and Article 89 GDPR a balancing of interests has to take place and thus it would be possible in principle that there are no objections to the processing.[7] To this end, it would be necessary to develop appropriate criteria in advance. For example, the Data Protection Conference drew up a list of processing activities for which a data protection impact assessment must be carried out. Even if such a list is not a requirement of the GDPR with regard to "legitimate interests", this would not be a barrier to create one. An exemplary list (negative or positive list) could also be drawn up within the framework of codes of conduct. However, this would be obsolete if any transfer of third party data to a provider were prohibited from the outset without the consent of the third party. However,

3 See, for example, Bitkom's opinion of 14.03.2017, available as follows: https://sds-links.de/Bitkom. On p. 7/8 it is stated that it should be sufficient to consider only the data which the data subject controls and possesses (e.g. pictures, e-mails during the term of the contract). This excludes usage data. In particular, Bitkom is of the opinion that no data that is automatically generated when using the service (e.g. log files, traffic data) should fall under the law.

4 V. Lewinski, Wert von personenbezogenen Daten, in: Stiftung Datenschutz – DatenDebatten III, p. 215.

5 Guidelines oft he Article 29 Working Party, p. 21.

6 Guidelines of the Article 29 Working Party, p. 13.

7 According to Article 89 GDPR appropriate safeguards for the rights and freedoms of the data subject are demanded.

the example of the Article 29 Working Party would not be consistent with this result.

Therefore, the overall question to be answered is whether any processing by the new service provider without the consent of the third party is excluded (and how this can be ensured in practice) or whether processing could in principle be considered, for instance on the basis of legitimate interests.[8] In addition, it would be necessary to clarify whether there are other personal data which could also be transferred. In this case, the guidelines would have to be revised, and it might also be necessary to develop codes of conduct under Article 40 GDPR, which would also cover "legitimate interests", "further processing" and "scientific purposes".

In this context, it should be noted in particular that this question cannot be answered in any other way than the (permitted) data storage at the former provider. The user regularly stores data, such as photos, etc., for personal or household activities. If such storage is possible without the consent of the third party concerned, this evaluation should also apply to the new provider. Differences can only arise if it is clear that the new provider does not comply with the specified level of the GDPR.

PROJECTS IN PRACTICE[9]

DATA TRANSFER PROJECT

The "Data Transfer Project" was launched in 2018 to improve data portability for users and service providers.[10] In this project different companies (e.g. Facebook and Google) work together. The aim of the project is to create an open source platform for data portability: Every user should be able to exchange data between online service providers on the Internet at any time. This will be technically implemented with the help of service-specific adapters. This means that the existing APIs can be used to access data, but data can still be transferred to a common format and then back into the API of the new service. The practical result for the users is that data can be transferred directly from and to any provider participating in this project. Using a hypothetical example, the Data Transfer Project white paper shows how a user can transfer their photos from Google to Microsoft OneDrive.[11] This requires the integration of Google's file transfer interface, where the user selects the destination and approves the transfer. The selected files are automatically copied and forwarded to the destination.[12]

TELECOMMUNICATIONS SECTOR

In the telecommunications industry, an initiative for data portability was also launched by various providers in 2017: Data Portability Cooperation.[13] It is a working group moderated by the GSMA and managed by European telecommunications companies such as Deutsche Telekom, Orange and Telefónica.[14] It is planned to develop a common Code of Conduct. The focus is on transparency and control for users. Tools and services are to be developed to give users an overview of the use of their data and thus ensure the privacy of users. This also includes common data formats.

8 Study by the Stiftung Datenschutz "Practical Implementation of the Right to Data Portability", p. 250, https://sds-links.de/Studie2017.
9 The projects "New Governance" or "CTRL-Shift" have already been presented in the first workshops of 11.09.2019. See there for further evidence.
10 "Data Transfer Project" is available as follows: https://datatransferproject.dev/.
11 https://datatransferproject.dev/dtp-overview.pdf.
12 https://datatransferproject.dev/dtp-overview.pdf.
13 https://sds-links.de/Telekom.
14 The GSMA represents the interests of mobile operators worldwide. It includes manufacturers of mobile phones and devices, software companies, device providers and Internet companies (https://sds-links.de/Telekom).

CHALLENGES IN TECHNICAL IMPLEMENTATION

FORMATS

Within the framework of the "Data Transfer Project", a first use case for photos is currently being carried out. It turned out that due to the different orientation of the services the export can be associated with difficulties in individual cases. Due to the open source initiative and the use of an appropriate adapter, the formats of different service providers can be compared with each other and data can be transferred. For example, the new provider can recognize the location, which telephone and which camera were used and which data were recorded. However, there may be problems if the services contain different services, e.g. if a provider carries out a so-called "social tagging" on the photographs.[15] Problems with data transfer can also occur with data other than photos, such as music lists or videos. The "Data Transfer Project" is currently working on these challenges and is confronted, among other things, with the question of how the playlists of different services can be compiled, e.g. the favourite song or which song has been shared with the family, since there is no format for this so far. The development of new services can also be problematic, as in this case an appropriate format would have to be found. The challenge is to keep up with the particular system. In the workshop it was also pointed out that there is no common format for health data and that the transfer has to be done partly via pdf or CSP, so that the use of existing APIs could simplify the procedure.

Consequently, it is remaining to be seen for which services a common data format can be developed.

With regard to companies with smaller market shares and small start-ups, open source projects could be helpful in order to enable and facilitate data portability for these companies and to create the basis for new product developments, e.g. the transfer of location data for (travel) recommendations or fitness data for insurance companies.

INFRASTRUCTURE

The infrastructure is of great importance, especially with regard to the users. Thus, technical solutions are developed in which the user has to agree to the use by the exporting party and the use of the API by the importing party, so that there are different levels of agreement and authorization.

Other projects, such as Ctrl-Shift,[16] focus on management systems that act for the user or agree to the use of the data instead of the user. The management system may also include an examination of the underlying general terms and conditions. These proposals must, of course, always respect the principle of purpose limitation and answer the question of the extent to which these systems are comprehensible and transparent for the user. This issue has already been addressed in the context of the study by the Stiftung Datenschutz.[17] It should therefore always be critically examined to what extent such a system can actually meet the requirements of the GDPR. In this context, however, it should be noted that the Data Ethics Commission has drawn attention not only to the conceivable possibility of trust models, but also to the practical use of privacy management systems (personal information management systems), which should be examined in the future.[18]

CHALLENGES IN LEGAL IMPLEMENTATION

WHICH DATA SHOULD BE TRANSFERRED?

The question is whether other data not formally covered by Article 20 GDPR should also be covered by the right to data portability. This could include both anonymous data and data based on legal bases other than those mentioned in Article 20 GDPR, e.g. collected by the service provider on the basis of legitimate interests. However, this would only be voluntary service offered by companies to their users, as neither the Article 29 Working Party guidelines nor the law currently support such an

15 At this point it should be emphasized that this is exclusively a technical statement – independent of the question of the legitimacy under data protection law.

16 See the summary of the first workshop. Furthermore: Study by the Stiftung Datenschutz "New ways of providing consent in data protection" which examined different kinds of personal information management systems (PIMS) (https://sds-links.de/PIMS).

17 https://sds-links.de/PIMS.

18 See the report of the Data Ethics Commission, p. 136, https://sds-links.de/Datenethikkommission.

interpretation. In this sense, the Data Ethics Commission also recommends in its final report that a rash decision for an extension of data portability, for example to data other than those provided, should be avoided – at least for the time being. [19] Nevertheless, a different interpretation is conceivable in the future. In this case, data portability can be used to bring the service concept to the fore (with a view to the user). However, data protection may not fall by the wayside in order to avoid the already mentioned "sell-out of data". The focus should always be on whether "data sovereignty" associated with Article 20 GDPR is to the advantage of the data subject and serves to strengthen his or her control rights.

In this context, it should also be pointed out that data portability is not associated with (automatic) data deletion. For some users it may be unsatisfactory to copy the data because they only want to use a new service. It is therefore necessary to examine what users' expectations are, and technical development can be designed accordingly.

IN WHICH CASES IS DATA PORTABILITY INVOLVED?

If simple "one-click options" of data to a service provider are offered, it is questionable to what extent the necessary transparency can be ensured, e.g. a transfer of data to another provider (in the moment of its generation) like location data for recommendations.[20] In its final report, the Data Ethics Commission pointed out that a real-time transfer of data should be avoided (at least for the time being).[21] In this context, it should be stressed that data portability is not a legal basis, but a right of the data subject to be exercised by him. According to Article 12 GDPR, the English version states "request" and the German version is translated as "Antrag", but means nothing other than that the service provider must comply with this (control) right within a certain period of time at the user's own query.

It is important to ensure that no transfer of data takes place without a deliberate and informed decision by the data subject, which would otherwise require a legal basis. When transferring data to another service provider, the question may therefore also arise to what extent consent pursuant to Article 7 GDPR is the necessary legal basis. The controller shall be able to demonstrate that the data subject has consented to processing of the personal data and the requirements for consent are subject to stricter formal requirements. Furthermore the control rights of data subjects pursuant to Article 12 et seq. GDPR are linked to (lawful) data collection that has already taken place and a provider cannot refer to Article 20 GDPR; he always needs the request of the data subject. Authentication also plays an important role here. An identification process should be started, both with regard to the user and with regard to the new provider. The question should also be to what extent action is taken in accordance with Article 6 GDPR. With regard to apps that forward data to other service providers, reference is made to the evaluation of the first workshop.[22] In addition, it was explained in the course of this second round of discussions that transparent mechanisms should be developed so that users can ensure and decide with whom they share their data. However, in this context, reference was made to existing API mechanisms.

In addition, it could be examined whether the use of API mechanisms can influence or exclude the legal classification of a transfer as data portability within the meaning of Article 20 GDPR. It should be noted, however, that the technology should not determine the law and only the external circumstances can provide indications for the legal classification. The question as to whether the individual case concerns the exercise of the right to data portability should therefore be focused on whether it is a (voluntary and deliberate) request by the user or the way in which such a request is to be defined. The underlying technology should be irrelevant.

19 See the report of the Data Ethics Commission, published on 23.10.2019, https://sds-links.de/Datenethikkommission. Under the topic "Improving controlled access to personal data", p.21, the Data Ethics Commission recommends (for the time being) refraining from extending the portability right, for example to data other than those provided or to real-time transfer.

20 The Data Ethics Commission refers to the concepts of "real-time streaming of data flows" and dynamic real-time portability, see p. 137.

21 Report of the Data Ethics Commission, p. 21.

22 See the evaluation and analysis of the first workshop of 11.09.2019.

RISKS ASSOCIATED WITH THE EXTENSION OF DATA PORTABILITY LAW

In principle, data subject rights (pursuant to Articles 12–23 GDPR) include requirements for GDPR-compliant data processing, but do not constitute the legal basis for the processing of data. They also contain requirements which a service provider shall implement in order to comply with the obligations under Article 24 GDPR. With regard to the right to data portability, the intention of Article 20 GDPR to strengthen the control rights of the data subject may therefore not be reversed and a basis created for companies to transfer and use data in an easy way by means of a service-oriented view or an extension of the term "data provided". It should be stressed once again that a provider cannot refer to Article 20 GDPR; he always needs the (deliberate) request of the data subject.

The original intention of data portability was to transfer data from a social network to a possibly more data protection-friendly network. At present, however, it is not ruled out that "one-click solutions" are offered in both directions across industries: On the one hand, it is possible that the original service provider would implement a "data transfer" button (possibly even to initiate a transfer to partner companies). On the other hand, the new service provider could offer a "Bring my Data in" button. The question is not only whether processing takes place that otherwise requires a legal basis, but also whether the obligations according to Article 30 GDPR or Article 35 GDPR could be circumvented. Thus, within the framework of Article 30 GDPR, a description must be prepared for each individual processing activity in accordance with Art. 30 GDPR, whereby processing activity is generally understood to be a business process at an appropriate level of abstraction. A strict standard should be applied, so that each new purpose of the processing represents its own processing activity.[23] This requirement would have to be met, for example, in the legal basis for consent which also requires comprehensive information and the right to withdraw. If a data transfer takes place, e.g. to a service provider who makes recommendations on the basis of the transferred database, the original service is changed for a different purpose. If, however, the service provider refers to the position that he "merely" fulfils the rights of the data subject, the question arises to what extent this actually corresponds to the strengthening of the rights of the data subject. The "original" service provider would in principle be exempted from proving that the data subject has given his consent to the processing of his personal data for one or more specific purposes or to the transfer of data to another service provider for a specific purpose. Nor would he have to provide information on the right of withdrawal. It is true that the new service provider is responsible for, and should be able to demonstrate compliance with the principles relating to the (subsequent) processing of personal data. However, this does not necessarily have to be based on a contract or consent, but could in principle also be based on legitimate interests.

It should therefore be decided in which scenarios data processing is carried out for which a legal basis (e.g. consent) is required, and in which cases data portability is concerned, so that the focus is on strengthening the control rights of the data subject.

23 For more information on the records of processing activities, read the explanations on: https://sds-links.de/Verzeichnis.

USE CASES

TRANSFER OF A MUSIC LIST

This can be considered as a typical case of data portability, which is also exemplarily listed in the guidelines of the Article 29 Working Party.[24]

TRANSFER OF PHOTOS

When transferring photos, the rights ("ownership") regarding the photo must first be clarified. In this second workshop it was pointed out that even in the case of an object-related photograph (e.g. sunset) the original idea of data portability is involved, namely to be able to take one's history to another provider as a user. A user should be allowed to transfer such a photograph as well as a personal comment. However, there was no uniform discussion as to whether this is a personal information, which is a condition of Article 20 GDPR. This could be indicated by the fact that the data subject photographed it. Otherwise such a transfer could be an additional service. In this context, reference was again made to the term "data mobility", but "data sharing" was also mentioned as a possible option. The legal basis for this would be consent (according to the GDPR if it is personal data).

With regard to photographs, it should also be taken into account that other persons may be depicted on them. If the infringement of third parties´ rights shall be ruled out, the transfer would have to involve a change of storage medium only. However, practice shows that own analyses of the database are regularly carried out. The question therefore arises as to whether a prohibition of the analysis can be guaranteed in practice at all. Guidelines that clearly define what should be defined as "legitimate interests" or "scientific purposes" or "further processing" could support this. It is – in principle – a similar situation as if the data were stored by the original provider. The provider may not violate the rights of the data subject or the third party. Otherwise, penalties may be imposed.

The pivotal point is that the compliance with the GDPR should always be the focus of attention and the corresponding data protection level must be kept.

TRANSFER OF FINANCIAL INFORMATION

In practice, services are offered that enable users to integrate all payment information or transaction history from their banking transactions into a single interface (savings account, stock account, etc.). An existing API is used (PSD2).

In order to assess whether data portability is involved, the PSD2 guideline should be taken into account. The requirements of this Directive must be met. From a data protection point of view, PSD2 implies the necessity for third-party providers to require consent. The existence of consent is symbolized by the access data that the user receives from the third-party provider. This allows third-party providers to trigger payment transactions directly. From a consumer perspective, there is only contact between the third-party provider and the customer and there is no connection between the customer and the bank. It is another approach that differs from data portability.

In these second workshops it was argued that, due to the specific requirements of the PSD2 Directive, it should be data access from a legal point of view, even if it is implemented accordingly from a technical point of view of data portability.

24 See the guidelines of the Article 29 Working Party, p. 5, 9.

CONCLUSION

In practice, it must be ensured that the right to data portability is regarded as a right of the data subject and not as a company right. Data portability serves to ensure GDPR-compliant processing and is not a separate legal basis for new services. In practice, however, there is still the idea that the right to data portability should increasingly be regarded as a service for users. Therefore, it is all the more important that the personal right remains in focus. The possibility of transferring data not covered by the term "data provided" (as defined in Article 20 GDPR and the guidelines of the Article 29 Working Party) is often intended. This also raises the question of the extent to which object-related photography (e.g. sunset) is covered by the legal right to data portability and whether it can even be considered as personal data. In this context, it should be taken into account that, in practice, there is still no experience of which data contribute to strengthening control rights. In this sense, the Data Ethics Commission also recommended that the term "data provided" should not be extended – at least for the time being. However, a future extension is not excluded; even an extension by creating facts in practice does not seem to be excluded. For this reason, guidelines and socio-economic studies containing ethical assessment standards are needed to ensure the core of the right to data portability: Strengthening the control rights of a data subject. In this context, it should be borne in mind that the term "provided data", respectively the term "observed data" still needs to be defined in terms of its scope. Especially with regard to possible future business models, it cannot be ruled out that a competing company might be more interested in receiving usage data, location data, etc. in a machine-readable format "with one click" than the user. This also includes a definition of the term "request by the user". The data subject should exercise or actively claim this right. In practice, however, the boundary between "initiation", "nudge" and "request" by a company (possibly with its own business interests) can become blurred. Therefore, an interpretation and a guideline are also required as to which minimum requirements should be met. With regard to medical data, there is also a demand to refrain from "one-click solutions" in principle.

The question is whether data portability allows more privacy or whether it leads to the opposite. Overall, the term data sovereignty can be helpful in this context to achieve a uniform understanding of modern data protection law at the European level and to develop a Europe-wide definition, since the right to informational self-determination was defined by the Federal Constitutional Court. However, there is a need to examine what is to be comprised by the concept of "data sovereignty" and in what way "this" can be implemented in favor of the data subject. A transparent method should be ensured – corresponding to the actual meaning of the word "sovereign" as a qualification to exercise one's right to data portability. Therefore, if the right to data portability is an instrument for exercising data sovereignty, in practice it is necessary to provide the necessary tools – in the meaning of simple, comprehensible and practicable applications. Only in that case will the law be implemented in such a way that the data subject is able to act independently, competently and without restriction. This also includes "law literacy" and an awareness of the potential value and possibilities of using personal data for others, i.e. for companies with their own business interests.

Data sovereignty should avoid risks for the personal right. Also in the context of privacy management systems and trust models, it has to be impossible for other persons, institutions, etc. to make decisions that have negative consequences for the user. The "call" for data portability must always originate from the data subject as an own "request". All in all, data protection is a human right.

STIFTUNG DATENSCHUTZ

WORKSHOP

#03 – November 01, 2019

SUMMARY, EVALUATION AND ANALYSIS

PRACTICAL CHALLENGES & SOLUTIONS IN IMPLEMENTING DATA PORTABILITY

INTRODUCTION

The third workshop focused on the necessary requirements for users to exercise more control over their data. This also includes adequate safeguards to ensure the rights of third parties when data is transferred directly to another provider. In addition, the participants also discussed fundamental requirements for a future structure and governance that could ensure fair and transparent data processing in a comprehensive manner.

Overall, new business models that combine data transfer with financial incentives can be a problem. The Stiftung Datenschutz already pointed out this risk in her study in "New ways of providing consent in data protection".[1] For example, a service is currently offered which exercises the right to data portability on behalf of its customers (subscribers). The service provider focuses primarily on the transfer of data from loyalty programs and promises its customers corresponding benefits.[2] All in all, it is not just a matter of control, but also of ensuring the necessary knowledge and decision-making skills for the user, especially with regard to the value of the data. For example, "price tags" for data were highlighted as helpful in this current workshop. Reference was also made to the possibility that the exercise of user rights could also be carried out by a neutral organization.

1 Study by the Stiftung Datenschutz "New ways of providing consent in data protection" which examined different kinds of personal information management systems (PIMS) (https://sds-links.de/PIMS).

2 https://sds-links.de/IAPP: "In a nutshell, in order to promote the services of the platform, including the exercise of the right to portability on behalf of the data subjects, Weople promises its subscribers benefits proportional to the amount and quality of personal data conferred to the platform and collected through different sources (basically the loyalty programs where the data subjects have a subscription), which the platform exploits to create commercial value."

CONTROL

The discussion highlighted that a lot has already been done in the past to draw users' attention to data protection issues. Nevertheless, the availability of alternatives is particularly important: Data subjects should have a choice between different services. Transparency, e.g. by means of icons, or the supply of data protection-friendly technology alone cannot therefore be a solution. Real autonomy or sovereignty requires a choice between different service providers, but also the ability to make decisions. The amount of information can be a particular challenge. There is a risk that the more information provided, the lower the user's attention. Again, the so-called "Law literacy" or "Data literacy" already discussed in the first two workshops plays an important role. In this context, reference was made to public campaigns as a possible model that could inform users of their rights.

The so-called "New Governance", already discussed in the first workshop, was mentioned as an option of an overarching model for creating transparency and control. In order to implement this model, it was emphasized that companies should first be motivated to create use cases that are advantageous for them. In practice, this could best be ensured by companies that are not in direct competition with each other. The needs of the users should also be taken into account in order to address the mass of users.

THIRD PARTY RIGHTS

With regard to the rights of third parties, the possibility of consent was discussed. For example, a message could be sent to the third parties and they could be asked for permission. On the one hand, it was expected that in a large number of cases this process would take place very quickly – even if several persons were involved (e.g. in a photo showing several people). On the other hand, the argument was raised that it could be overloaded and inconvenient for users, especially in the context of social networks, to have to agree to the transfer of data several times a day. The example of the Article 29 Working Party on the transfer of contact details to another webmail provider should also be taken into account in this case.[3] The Article 29 Working Party does not mention the third party's consent as a condition of transfer, only a prohibition of use for its own purposes, such as marketing purposes. However, this raises the further question of how this can be ensured in practice and whether, on the other hand, there could be permitted use, for example on the basis of "legitimate interests" or "scientific research purposes".[4] As part of its legal evaluation of the second workshop, the Stiftung Datenschutz referred to the possibility of guidelines or Code of Conducts, possibly also in the form of a positive or negative list. Even if the procedure of concerted Code of conduct under Article 40(7) to (10) GDPR can last a long time, it seems to be a good option. In this way, the different data protection levels of the services can be faced and entrepreneurs and users can be provided with a decision-making guide. Users will regularly not be able to decide without further explanation or assistance whether they agree to the processing of their data for a new service. The keywords "tagging" and "tracking" (e.g. when the faces of friends are "tracked" using a corresponding algorithm) are particularly important when looking at photographs. Consent could be given for this, but it is also possible to stop these practices. Code of Conducts can support the establishment of a standard for specific use cases. In this way, users can become aware of the practices of companies that do not adhere to standards. Compliance with and commitment to agreed standards could equally serve as marketing instruments, for example through highlighting this on the company websites.

All in all, it is important to keep an eye on the technical possibilities and, as part of an ongoing process, to check the compliance of the various use cases with the personal rights of the data subjects (in the interests of users and third parties) and to update the standards. This also has a direct influence on a transparent procedure if the ethically justifiable and legally allowed possibilities for services – both in the context of the original data

3 Guidelines of the Article 29 Working Party adopted on 13 December 2016 last revised and adopted on 5 April 2017, are available in different languages on:https://sds-links.de/Leitlinien. The European Data Protection Board confirmed the Article 29 Working Party guidelines at its first plenary meeting on 25 May 2018,https://sds-links.de/EDPB.

4 On this question, refer to the legal evaluation of the second workshop.

transfer and in the context of the processing after a data transfer – are clearly presented.[5] The same question arises for the first provider – whether a photo may be stored without the consent of the third party and with regard to the personal rights of the third party – even if the photo is stored for the user exclusively for private or household activities. In this context, reference is made to the legal analysis of the second workshop.

RESPONSIBILITY

In the literature, the opinion is that the user is responsible for the transfer of the data and must ensure that no third-party rights are infringed.[6] On the one hand, this might not be sufficient regarding "Privacy by Design". On the other hand, it should be noted that users often process data for personal and household activities. For this reason, the user or the data subject will regularly have no responsibility within the scope of the GDPR. During the workshop it was also argued that it might be the responsibility of the first provider to obtain consent. Nevertheless, the responsibility of the original provider was also viewed critically to the extent that he may not use this "power" as a controlling instrument in the event of a potential change to another network. He should therefore not be allowed to influence the "whether" of a change or issue a warning ("red flags"). The opinion was that a control should even be prohibited and he should be allowed to transmit the data without further ado. In this context, the possibility of an authority carrying out the audit or issuing warnings was also proposed.

At present, there is no equivalent obligation for the Provider to check the transfer, either under the law or under the guidelines of the Article 29 Working Party. Rather, the guidelines of the Article 29 Working Party provide that the receiving service provider is legally responsible for the further processing of the data. In this sense, it is pointed out that equally legitimate interests pursuant to Article 6 (1f) GDPR may be considered as a legal basis for the transfer and the "new" processing of the data.[7] But overall (as already described above) this also requires a fundamental decision, clear guidelines and, if necessary, standards in order to ensure a transparent procedure.

INTEGRITY OF AN ECOSYSTEM

The participants in the discussion also focused (as already described in the introduction) on the fundamental question of how a future data policy and an associated governance structure could be designed. In this context – beyond the formal requirements for data portability – different models were discussed that could ensure transparent and fair data processing in practice. In this respect, reference was also made to possible monetization interests, which will be dealt with separately in the following section.

As instruments for a transparent and fair procedure, the implementation of standards and a neutral organization were discussed during this third workshop (as already described above). Such a neutral organization could also be established between the user and the respective provider – for example in the meaning of a platform to which reference was already made during the second workshop. This would be a third person – in the sense of a person of trust – who represents the users and exercises their rights.[8]

The aforementioned standards are intended to be part of a digital infrastructure. It was emphasized that ensuring neutrality is also essential in this context – without economic interests in connection with the operation of the system. In particular, the social relevance of neutral social networks, neutral e-mail and chat solutions was pointed out: Although there are currently standardized data formats, many other necessary standards are still missing, such as technical, legal standards, business model standards, design standards and industry norms. The vision is to unify these guide-

5 For more information, see the results of the second workshop.
6 Herbst in: Kühling/Buchner, DSGVO/BDSG, Artikel 20 DSGVO (GDPR), recital 17.
7 Herbst in: Kühling/Buchner, DSGVO/BDSG, Artikel 20 DSGVO (GDPR), recital 18.
8 Please refer to the trust models already mentioned, which are also discussed under the heading "Monetisation interests" below. This was already discussed in the second workshop, and the Data Ethics Commission also proposed to examine these models in more detail.

lines under one infrastructure. This would require a common interest, as no single company or institution could do this on its own. A governance body, for example organized in the form of a public institution or a non-profit organization, has been proposed to democratically include all interests and set rules and standards so that no single interest prevails, but rather all interests are represented: Private companies, scientists, institutions entering into a public-private partnership. This would make it possible to coordinate different use cases with the involvement of all interests and to make use of already existing know-how.[9]

With regard to the standardization of Messenger-services, reference was made to the open e-mail protocol, which had not only proven itself in practice to be functional, but also enabled new business models and new functionalities. Messengerservices, on the other hand, are silos. On the contrary, it was argued that it is not technically difficult to establish a secure communication mechanism for Messengers, but that companies often have no interest in it but prefer to stay in their silos. The potential competitive disadvantage of smaller companies cooperating with a larger Messenger service was also highlighted.

With reference to the "integrity of services", the opportunities of PIMS systems, which were already the subject of the Stiftung Datenschutz study in 2016, were also discussed.[10] However, depending on the objective and design of these systems, the implementation of "purpose limitation" can be a big challenge. In addition, these systems also require corresponding standards in order to implement transparency and fair data processing and thus generate acceptance and trust among users. Above all, the user should be able to easily manage and control the system. In principle, the implementation of many PIMS systems is based on a procedure that was already covered by the well-known P3P protocol:[11] P3P is a free protocol and enables the machine-readable description of data protection declarations. The data subjects make presettings regarding their preferred data use and answer a standardized list of multiple-choice questions in advance regarding the preferred handling of their personal data.

Furthermore, "certifications" can contribute to ensuring integrity. During the discussion it was emphasized that the user should be able to rely on them. In addition, an examination should be carried out by an independent, neutral organization. This corresponds to the requirements of Article 42 of the GDPR. According to short paper No. 9 of the Data Protection Conference (Datenschutzkonferenz) "Certification according to Article 42 GDPR", the supervisory authorities are working on the development of coordinated, cross-national principles to avoid a " uncontrolled growth " of numerous different certification procedures especially with a view to a uniform European level of data protection in the interest of all participants.[12] In this context, the user should also be able to figure out whether an entire system has been certified or only a part of it. In the latter case, it must be transparent to what extent this affects the security of the data and the personal rights of the data subject.

Overall, it is an essential requirement that data subjects and third parties have clear, transparent and binding rights in practice. Standards and certifications can support this. This could also solve the so-called "fatigue problem".

MONETIZING INTERESTS

The case of a company exercising the right to portability on behalf of its subscribers, as already described in the introduction, raises the problem of the merchantability of personal data. There is also a risk that the company may copy and use this data for its own purposes, which is contrary to the interests of users. In this context, it would also be helpful to ask which data is actually of interest to

9 This includes the idea of "New Governance", so that reference is made to the evaluation of the first workshop.

10 Study by the Stiftung Datenschutz "New ways of providing consent in data protection" which examined different kinds of personal information management systems (PIMS) (https://sds-links.de/PIMS).

11 The following description of P3P can be found in the studies and evaluations already carried out by the Stiftung Datenschutz, namely p. 10 of the study "New ways of providing consent in data protection", https://sds-links.de/Studie2016 and p. 6 "Legal aspects (Riechert)" https://sds-links.de/Riechert."It is necessary that both users and website operators implement this protocol so that an automated check can be made as to whether the privacy policy of a website corresponds to the user's default settings for data protection. In case of differences, a warning appears (e.g. when accepting cookies). However, P3P has not been supported by the Windows browser since version Windows 10, and Microsoft has recommended avoiding P3P privacy policies on webpages." See also, where it is described that Microsoft no longer supports P3P.

12 Paper of the Data Protection Conference (Kurzpapier Nr. 9 der Datenschutzkonferenz), https://sds-links.de/Zertifizierung.

the user. It was pointed out in the discussion that there is often no interest in the transfer of an outdated database – this could include, for example, the tweet from last week in fast-moving times. In addition, it is equally important to investigate which raw data is interesting for a transfer from the user's and company's point of view – weighing up the opportunities and risks and, if necessary, redefining the term "observed data" to strengthen the control rights of the data subject.[13]

With regard to the monetization of data, the question remains whether a user is at all in a position to make a sovereign decision due to the complexity of the processing process. Therefore, both literature and practice discuss the establishment of a neutral, independent organization that could exercise these rights for users. In addition, the Data Ethics Commission has recommended further research on privacy management systems and trust models.[14] In the current workshop it was pointed out that it may not be the same organization that monetizes the data and exercises the rights.

In this context, the following additional points would like to be pointed out by the Stiftung Datenschutz:: In the digital reality, data is traded. This reality is underpinned from a legal point of view, since the Directive on certain aspects concerning contracts for the supply of digital content and digital services [15] applies (Article 3) where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader. The aim is also to bring consumers who do not pay money as a counter-performance into a position comparable to that of paying customers in relation to providers of this content.[16] It is also often pointed out that consumers have an interest in being involved in the value creation process of their data.[17] However, economic exploitation has not yet been intended. Thus one refers also to the "deliberate blind spot" of European data protection law.[18]

In digital reality, therefore, data is considered to have economic value – even if the Data Ethics Commission argues in favour of refraining from using the term "data as a counter-performance".[19] However, the opinion of the Data Ethics Commission also states that the GDPR already permits the commercial exploitation of personal data in many ways and that, in addition to consent (Art. 6 1 lit.a GDPR), there are five other cases of justification, some of which are explicitly tailored to economic interests and needs.[20] The question of necessary participation is therefore becoming all the more important. In literature and practice, for example, it is being discussed whether individuals should participate in the value of the data they generate. Participation is (in principle) part of a democratic and liberal system.[21] This basic idea of value creation is, moreover, taken up by the Data Ethics Commission to the extent that it recommends explicitly mentioning in § 311 BGB the special relationship between a party which in fact contributed to the generation of data in a value creation process and the party which in fact controls the data.[22] Other opinions point out that it is no longer possible for individuals to exercise their right to self-determination "due to a lack of experience and complexity in data processing" and that trust models can therefore be considered – according to the practice in copyright law.[23] More abstractly, reference is made to the possibility of a representative body exercising civil rights.[24] When implementing such proposals, however, it is always important to take into

13 Please refer to the evaluation of the second workshop.

14 See the report of the Data Ethics Commission, published on 23.10.2019, https://sds-links.de/Datenethikkommission, p. 133, 140.

15 DIRECTIVE (EU) 2019/770 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, https://sds-links.de/DigitaleInhalte .

16 Bokor, DIE RICHTLINIENVORSCHLÄGE DER KOMMISSION ZU VERTRÄGEN ÜBER DIGITALEN INHALT UND ONLINE-WARENHANDEL, p. 1, https://sds-links.de/Bokor.

17 Specht, Stiftung Datenschutz – DatenDebatten III, p. 313. With regard to consumers, for example, Specht points out that they have an interest in being involved in the value creation process of data in accordance with their contribution, i.e. there is an interest in monetization in addition to an interest under data protection law.

18 V. Lewinski, Wert von personenbezogenen Daten, in: Stiftung Datenschutz – DatenDebatten III, p. 215. V. Lewinski refers to the "deliberately blind spot" of European data protection law and the deliberate ignorance of the merchantability of personal data, which led to the lack of a market regime ensuring contractual justice.

19 See the report of the Data Ethics Commission, p. 105. In this context, the demand of the Data Ethics Commission to offer consumers reasonable alternatives to the release of data for commercial use (e.g. correspondingly designed payment models) is an extremely important instrument of consumer protection law.

20 Report of the Data Ethics Commission, p. 141.

21 Fezer, Digitales Dateneigentum – ein grundrechtsdemokratisches Bürgerrecht in der Zivilgesellschaft, in: Stiftung Datenschutz – DatenDebatten III, who discusses participation within the framework of data ownership.

22 Report of the Data Ethics Commission, p. 22, 147, 156.

23 Buchner, Eigentumsrechte an persönlichen Daten?, DGRI Jahrbuch 2011, Köln 2012, p. 51, 58.

24 Fezer, Digitales Dateneigentum – ein grundrechtsdemokratisches Bürgerrecht in der Zivilgesellschaft, in: Stiftung Datenschutz – DatenDebatten III, p. 152: "The representative realization of citizen's rights represents a very inherent principle of the organization of democratic social systems."

account the concerns expressed – for example – in the literature: “Who monitors the guards?[25]

Overall and in the context of the monetization of data, the question of the organization of a representative body in order to exercise the rights of data subjects has also to be answered – with a view to all the possible risks this might involve for the personal rights of the data subjects.

CONCLUSION

All in all, standards can help to strengthen users’ confidence in the existing infrastructure. A company’s business model is otherwise too complex. The user should be able to trust that the process is legally compliant and does not contradict his interests. A parallel process could be initiated in this context: Rules of conduct could be drawn up, which could be converted into a specific form in practice by means of certain use cases and updated at all times. In this way, binding standards can be created. A commitment to a standard by a company also creates confidence in this company and can serve as a marketing instrument.

Specific use cases can in particular highlight the opportunities and risks of data portability, which ultimately leads to the creation of standards. This also influences the transparency of a service, whereby public campaigns could support this. In this way, a learning process can be started in the practical implementation of what information should be provided and, above all, what information should be clearly given to the user in order to make an autonomous and sovereign decision – whether or not exercising the right to data portability. In this way, more and more standards can be developed over time. This could be a long process, but it could be beneficial, because the technical development is not predictable and problems can be tackled by applying “real” use cases. Representative bodies can play a decisive role in ensuring the necessary neutrality. With regard to the monetization of data, this context is also about fair participation opportunities in the value creation process of data.

Taken as a whole, a separation of tasks and powers is needed in order to create a neutral infrastructure and to include interests by means of a democratic structure. This could be organized in the form of a public or non-profit organization. An important requirement for success is cooperation between different companies, organizations and institutions. In this way, common, open standards can be developed to implement data transfer for all in practice.

25 Schneider asks this question in: Regulierungsansätze in der Datenökonomie, p. 9, https://sds-links.de/Schneider.

STIFTUNG
DATENSCHUTZ

Stiftung Datenschutz
rechtsfähige Stiftung bürgerlichen Rechts
Karl-Rothe-Straße 10–14
04105 Leipzig
Deutschland

Telefon 0341 / 5861 555-0
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

gestiftet von der Bundesrepublik Deutschland
vertreten durch den Vorstand Frederick Richter