DATENPORTABILITÄT
IN DER PRAXIS

Praktische Umsetzung des Rechts auf Datenübertragbarkeit

Rechtliche, technische und verbraucherbezogene Implikationen

Zusammenfassung und Handlungsempfehlungen

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

Gefördert durch das Bundesministerium des Innern

Das neue Recht auf Datenübertragbarkeit

Zusammenfassung

Mit der europäischen Reform des Datenschutzrechts wird ein Rechtsinstrument eingeführt, das neue Anforderungen an die Praxis beim Umgang mit personenbezogenen Daten stellt. Die EU-Datenschutzgrundverordnung gibt in Artikel 20 jeder natürlichen Person das Recht, die sie betreffenden und von ihr bereitgestellten personenbezogenen Daten in einem strukturierten Format zu erhalten oder transferieren zu lassen.

Die Nutzerinnen und Nutzer können also künftig personenbezogene Daten einer anderen Organisation übermitteln oder übermitteln lassen, ohne dabei von der ursprünglichen Organisation behindert zu werden. Der Gesetzgeber hofft, dass mit der Mitnahmemöglichkeit für „eigene“ Daten die Schwelle zum Wechsel von Anbietern digitaler Dienste sinken wird und die Verbraucher bessere Kontrollmöglichkeiten über ihre personenbezogenen Daten erhalten.

Wie dies in der Praxis funktionieren kann, ist noch unklar: Es gibt kaum praktische Erfahrungen in Wirtschaftsunternehmen und Aufsichtsbehörden und auch keine richterliche Rechtsfortbildung.

Daher untersuchte die Stiftung Datenschutz in einer Studie die rechtlichen, technischen und verbraucherbezogenen Implikationen des Rechts auf Datenportabilität und gibt Empfehlungen, wie das neue Instrument nutzbar gemacht werden kann.

In einem Call for Papers wurden Vertreterinnen und Vertreter der Wissenschaft, der Wirtschaft, von Verbraucherschutzorganisationen und Datenschutzaufsichtsbehörden sowie weitere Interessierte eingeladen, ihre Ansichten, Forderungen und Lösungsansätze einzureichen. Die Beiträge werden in der Studie vorgestellt und um Empfehlungen externer Sachverständiger ergänzt. Schließlich wurden aus den gewonnenen Erkenntnissen Handlungsempfehlungen für Politik und Aufsichtsbehörden abgeleitet.

Erkenntnisse aus dem Projekt

Zielerreichung

Das Recht auf Datenportabilität kann den Nutzern grundsätzlich mehr Kontrolle über ihre personenbezogenen Daten verschaffen. Ob dieses Ziel erreicht werden kann, hängt davon ab, ob es gelingt, das neue Recht praktikabel und funktional umzusetzen. Wenn das Konzept der Datenübertragbarkeit in der Praxis nur uneinheitlich funktioniert, werden die Menschen es kaum nutzen, und der erwünschte Effekt kann sich nicht einstellen. Daher wird es darauf ankommen, die Praktikabilität in den Vordergrund zu stellen.

Bei der Interpretation des Art. 20 DSGVO sollten diejenigen Daten erfasst werden, deren Übertragbarkeit der informationellen Selbstbestimmung und dem Verbrauchernutzen konkret dient. Der Aufwand für die Normumsetzung sollte in angemessenem Verhältnis zum tatsächlichen Nutzen für die Datensubjekte stehen. Im Sinne der Datensparsamkeit ist kritisch zu bedenken, dass mit der Datenübertragung eine Vervielfältigung des Datensatzes einhergeht. Dies gilt jedenfalls dann, wenn die Nutzerinnen und Nutzer von der übertragenden Stelle nicht zugleich auch Löschung der portierten Daten verlangen.

Die Betroffenen sollten transparent darauf hingewiesen werden, dass mit der Datenübertragung an eine andere Stelle weder eine automatische Löschung beim alten Anbieter noch eine Kündigung bestehender Verträge einhergeht. Eine sehr weitgehende Auslegung der Norm könnte in Verbindung mit der zu erwartenden Duplizierung von Datensätzen schlimmstenfalls neue Datenschutzrisiken schaffen und zugleich unverhältnismäßig großen Aufwand beim Kategorisieren und Herausziehen von Datensätzen bei den datenverarbeitenden Stellen bereiten.

Beim Recht auf Datenübertragbarkeit werden die Nutzer ein Wahlrecht zwischen einer Übermittlung ihres Datensatzes an sie selbst oder direkt an einen anderen Dienstanbieter haben. Falls die Nutzer vor allem die Variante der Direktübermittlung nutzen werden, ist das Entstehen neuer Geschäftsmodelle denkbar, bei denen die betroffenen Personen von Datensammlern animiert werden (z.B. durch geldliche Anreize), ihre Nutzungsdaten mithilfe von Art. 20 DSGVO an sie übertragen zu lassen.

Geeignete Umsetzungsstrategien

Typischerweise werden die Nutzer ihre Daten von einem Anbieter zu einem anderen des gleichen Bereiches mitnehmen wollen – von einem sozialen Netzwerk zum anderen; von einer Versicherung zur anderen. Angesichts dieser hauptsächlich zu erwartenden praktischen Anwendungsfälle sollten branchenspezifische Lösungsansätze verfolgt werden. Deren Vorteil bestünde darin, dass Datenarten, Formate und besondere Datenschutzaspekte den speziellen Anforderungen des jeweiligen Sektors angepasst werden könnten. Außerdem kann die Ausarbeitung und Einigung auf spezifische Tools innerhalb einzelner Branchensektoren schneller zustande kommen als bei komplexeren branchenübergreifenden Einigungsprozessen.

Hinsichtlich der gesetzlichen Vorgabe, dass Nutzer auch eine direkte Übertragung zwischen Organisationen verlangen können, „soweit [dies] technisch machbar“ ist, sollte keine generalisierende Sichtweise, sondern eine Einzelfallbetrachtung vorgenommen werden.

Technische Gestaltung

Die Datenschutzgrundverordnung sieht vor, dass organisatorische und technische Verfahren zu schaffen sind, um ihre Ziele wie die Datenportabilität effektiv umzusetzen. Dabei bleibt das Gesetz technologieneutral und gibt keine bestimmten Formate oder Standards vor. Die Projektstudie untersuchte daher auch, wie die gesetzliche Vorgabe eines „strukturierten, gängigen und interoperablen“ Formats konkret ausgefüllt werden kann. Es zeigte sich, dass sowohl für einfache als auch für komplexere Anforderungen auf bereits vorhandene Formate zurückgegriffen werden kann, die zugleich die Anforderungen zur Maschinenlesbarkeit und Interoperabilität erfüllen.

In jedem Fall sollte bei der Datenübertragung der Datensicherheit große Bedeutung zugemessen werden, beispielsweise per Verschlüsselung.

Zudem ist stets mit geeigneten Identifizierungsmaßnahmen sicherzustellen, dass die zu portierenden Daten nur an den tatsächlich Anspruchsberechtigten oder den von ihm benannten Empfänger übermittelt werden. Eine eindeutige Authentifizierung der anfragenden Person und die Gewährleistung eines gleichwertigen Datenschutz- und Datensicherheitsniveaus sind nötig, um missbräuchliche Datenübertragungsbitten zu verhindern.

Handlungsempfehlungen

1. Zielrichtung der Norm

Die Umsetzung der Norm sollte im Sinne ihrer ursprünglichen Intention erfolgen – der Stärkung der informationellen Selbstbestimmung der Verbraucher. Dies meint primär **Kontrollmöglichkeiten über die Weitergabe personenbezogener Daten.**

Vom Recht auf Datenübertragbarkeit **müssen zumindest diejenigen Daten erfasst sein, deren Übertragbarkeit tatsächlich die informationelle Selbstbestimmung fördert** und die vom Nutzer entsprechend verwendet werden können. Der Aufwand für die Normumsetzung muss verhältnismäßig sein, auch im Hinblick auf die tatsächliche Wirksamkeit für die Datensouveränität der Verbraucher.

Die **Wirksamkeit der Norm muss einem Praxistest unterzogen werden.** Das beinhaltet u.a. verhaltensökonomische Untersuchungen zur tatsächlichen Nutzerbereitschaft, die Datenportabilitätsmöglichkeiten in Anspruch zu nehmen. Die Ergebnisse sollten in die Evaluation der EU-Datenschutzgrundverordnung einfließen.

Die Einführung des Rechts auf Datenübertragbarkeit sollte von Informationskampagnen über seine Reichweite und Möglichkeiten begleitet werden (z.B. durch nationale Datenschutzbehörden oder Informationsplattformen).

2. Bestimmung des Anwendungsbereichs

Bei der Bestimmung des Anwendungsbereichs sollte der **Verbrauchernutzen im Vordergrund** stehen, um Akzeptanz und Erfolg des neuen Rechts zu erhöhen.

Die **Definition der „bereitgestellten Daten" sollte sich an Sinn und Zweck der Norm ausrichten.**

Die Aufsichtsbehörden sollten über die Stellungnahme der Artikel-29-Datenschutzgruppe hinaus **präzisieren, was „bereitgestellte Daten" sind und Beispiele für umfasste Datenkategorien geben.**

Bei der **Frage, ob sowohl Bestandsdaten als auch Nutzungsdaten vom Anwendungsbereich erfasst sind, sollte im Einzelfall und dienstbezogen entschieden** werden können. Es ist zu prüfen, in welchen Fällen die Übertragung aller „bereitgestellten" Nutzungsdaten zu einem anderen Anbieter tatsächlich die Kontrollrechte der betroffenen Person stärkt.

Hinsichtlich des Datenformats und der geforderten Interoperabilität ist das **Wettbewerbsrecht zu berücksichtigen.** Es ist zu prüfen, inwieweit Kriterien entwickelt werden müssen, um eine europaweit

einheitliche Sichtweise sowie ein differenziertes Ergebnis im Hinblick auf Wettbewerbsrecht und Datenschutzrecht zu schaffen. **Kartellrechtliche Probleme bei Einigungen zu Verfahren der Datenübertragung sind zu vermeiden.** Der Schutzzweck der Norm, nämlich die Erleichterung des Anbieterwechsels, muss zum Tragen kommen.

Im Hinblick auf Schutzrechte Dritter ist ebenfalls bei Datenverarbeitung durch eine natürliche Person zu ausschließlich persönlichen oder familiären Zwecken zu berücksichtigen, ob personenbezogene Daten zu einem kommerziellen Anbieter übertragen werden oder auf einem eigenen privaten Gerät verarbeitet werden. Hier müssen Verhaltensregeln dahingehend ausgearbeitet werden, inwieweit zukünftig eine weitere Verarbeitung aufgrund berechtigter Interessen oder Zweckänderung durch kommerzielle Anbieter tatsächlich ausgeschlossen ist.

Es empfiehlt sich die Prüfung, ob ein einheitliches technisches und juristisches Verständnis des Begriffs „Metadaten“ besteht. Dies gilt insbesondere auch, um entscheiden zu können, welche Metadaten aus technischer Sicht für eine erfolgreiche Umsetzung der Datenportabilität sowie der Entwicklung eines Formats erforderlich und aus rechtlicher Sicht zulässig sind.

Bei der Ausübung des Rechts auf Datenübertragbarkeit sollten die beteiligten Stellen stets Transparenz herstellen. Die jeweils betroffene Person darf nicht den Überblick über die Datenverantwortlichen und die ihr zustehenden Löschungsansprüche verlieren. Ihr müssen alle Informationen, die sich auf die Verarbeitung durch den alten und neuen Verantwortlichen beziehen, bekannt sein.

Hinsichtlich der Forderung „soweit technisch machbar“ muss entschieden werden, ob objektive Kriterien entwickelt werden können oder ob die individuelle Leistungsfähigkeit des jeweiligen Datenverantwortlichen (subjektiver Maßstab) zugrunde gelegt wird.

Auch bei der Auslegung von Art. 20 DSGVO sowie im Rahmen der Ausarbeitung der Verhaltensregeln gemäß Art. 40 DSGVO ist auf eine europäische Harmonisierung und konsistente Interpretation hinzuwirken.

3. Umsetzungsstrategien

Es sollten **Ansätze einer „regulierten Selbstregulierung“** entwickelt werden, bei denen unter staatlicher Aufsicht ein Rahmen etabliert wird, in dem die Aufsichtsbehörden, NGOs sowie Unternehmen Umsetzungsstrategien und Standards für die Datenportabilität entwickeln.

Für eine effektive Ausgestaltung der Datenübertragbarkeit und Herstellung von Rechtskonformität sollten besonders betroffene Unternehmen und Branchen in formelle **Konsultationsprozesse der Aufsichtsbehörden** eingebunden werden.

- Ein **branchenspezifisches Vorgehen empfiehlt sich bei Übertragung sektorspezifischer Datensätze** innerhalb einer Kategorie von verantwortlichen Stellen und in Fällen, in denen bereits etablierte brancheninterne Portabilitätsverfahren bestehen.

- **Lösungsansätze auf Grundlage von Personal Information Management Systems (PIMS) erscheinen bei sektorübergreifenden Sachverhalten vielversprechend.**

In Fällen, in denen voraussichtlich mit einer geringen Nachfrage nach Datenübertragung zu rechnen ist, könnte auf einzelfallbezogene direkte Übertragung von Datensätzen zurückgegriffen werden.

Zur Schaffung von Orientierung sollte auf die Entwicklung von **Verhaltensregeln zur Portabilitätspraxis** hingewirkt werden (Art. 40 DSGVO).

4. Technische Gestaltung

Mindestvoraussetzung für Datenportabilität und Interoperabilität sollte die Nutzung des CSV-Formats sein. Es ist eine einfache Beschreibung hinzuzufügen, wie die Daten in der Datei angeordnet sind.

Für umfangreichere Lösungen sollten die Formate XML oder JSON genutzt werden. Diese Formate ermöglichen feinere Granularitätsstufen, enthalten sowohl Inhaltsdaten als auch beschreibende Metadaten und haben aufgrund ihrer Struktur ausreichende Tiefe, um auch komplexe Datengerüste abbilden zu können. Die enthaltenen Informationen sind nicht nur maschinenlesbar, sondern können über Standardsoftware von dem Betroffenen selbst gelesen werden, was zugleich die Wahrnehmung der Informationsrechte der Nutzer unterstützt.

- Die Datenschutzbehörden sollten **definieren, welche konkreten Anforderungen an die Authentifizierung gestellt werden,** damit Rechtsunsicherheiten für die Verantwortlichen und Risiken für die Betroffenen vermieden werden.

- Sowohl bei Einzelfalllösungen als auch bei branchenspezifischen oder branchenübergreifenden und universellen Ansätzen muss sichergestellt werden, dass die technischen **Lösungsansätze durch offene Schnittstellen grundsätzlich untereinander interoperabel** sind.

- Im Hinblick auf die effektive Weiterverwendung der portierten Daten sollte das PDF-Format im Bereich der Datenübertragbarkeit regelmäßig nicht zum Einsatz kommen, auch wenn es im Rahmen des Auskunftsrechts mit Blick auf die transparente Information als elektronisches Format ausreichend ist.

Um welche Daten geht es?

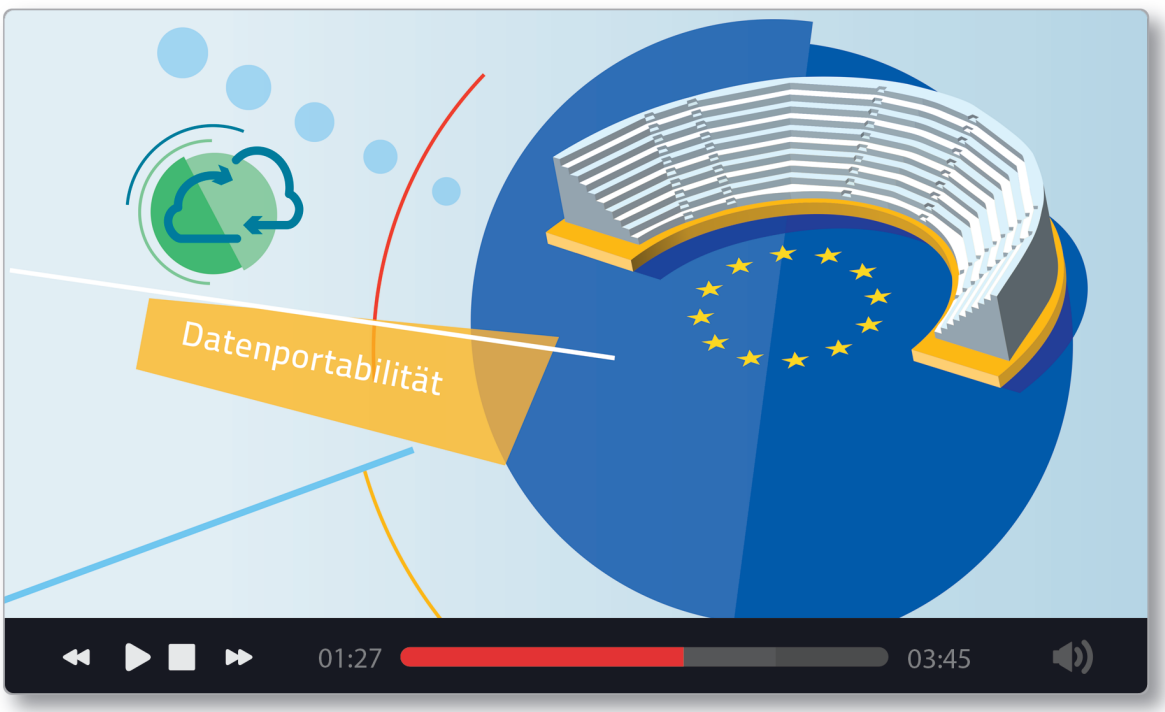
Trotz der Leitlinien der Gruppe der europäischen Datenschutzbehörden herrscht weiter Uneinigkeit darüber, welche Daten vom Anwendungsbereich des neuen Rechts erfasst sein sollen. Der Begriff der „bereitgestellten Daten“ ist in der EU-Datenschutzgrundverordnung nicht definiert. Die Datenschutzaufsicht sieht vom Anwendungsbereich mehr umfasst als nur die nutzerseitig direkt bereitgestellten Daten (z.B. im Formular eines webshops). Auch solche personenbezogenen Daten sollen portierbar sein, die bei der Inanspruchnahme eines Dienstes erzeugt und erfasst werden. Diese Sicht stößt bei anderen Akteuren auf deutliche Kritik. Sie fordern, dass nur das zur Mitnahme bereitzustellen sei, was das Datensubjekt aktiv und bewusst zur Verfügung gestellt hat. Es solle sich auf solche Daten konzentriert werden, die für den Anbieterwechsel erforderlich seien – denn dies sei die gesetzgeberische Motivation des Rechts auf Datenübertragung. Neben dem Regelungsziel spreche für eine enge Auslegung auch die Historie des Gesetzgebungsverfahrens. Einig sind sich alle Seiten darin, dass Daten, die der Verantwortliche erst auf Basis der bereitgestellten oder bei der Nutzung beobachteten Daten selbst erzeugt hat („inferred data“, etwa Score-Werte), nicht portierbar sein müssen.

Erklärfilm Datenportabilität

Große Teile der Bevölkerung sind noch nicht ausreichend über ihr künftiges Recht auf Datenportabilität informiert. Um einen Einstieg in eine nötige Aufklärungskampagne der Bürger zu geben, hat die Stiftung Datenschutz im Rahmen ihres Projekts einen informativen Erklärfilm zur Datenportabilität erstellt.

In kurzen Sequenzen geht der Film auf die wichtigsten rechtlichen Aspekte und die derzeit noch strittigen Fragen bei der Umsetzung des Artikels 20 der europäischen Datenschutzgrundverordnung ein. Damit bietet er in praxisnaher, kurzweiliger Form sowohl Bürgern als auch Unternehmensvertretern einen ersten Einstieg in die komplexe Materie.

Der Film steht zur freien Verfügung und kann unter www.stiftungdatenschutz.org angesehen und heruntergeladen werden.



DATENPORTABILITÄT
IN DER PRAXIS

Practical Implementation of the Right to Data Portability

Legal, Technical and Consumer-Related Implications

Summary and Recommendations for Action

Foundation for Data Protection
Foundation with legal capacity under the civil code

Karl-Rothe-Straße 10–14
04105 Leipzig
Germany

Phone +49 341 / 5861 555-0
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org

Founded in 2013 by the German federal government

The New Right to Data Portability

Summary

With the reform European data protection law, a legal instrument will be introduced which creates new practical requirements for the processing of personal data. In Article 20, the European General Data Protection Regulation grants every individual the right to receive or transfer the personal data concerning them, which they have provided to a controller, in a structured format.

This means that in the future, users can transfer personal data to another organisation or have it transferred without being prevented to do so by the first organisation. The legislative authorities hope that this possibility of transfer for their "own" data will lower the barriers for consumers to change from one provider of digital services to another and give them better means of control over their personal data. However, it is still unclear how this should be implemented practically: There is little to no practical experience in business enterprises and regulatory authorities and no further development of the law by judges, either.

Based on this, Stiftung Datenschutz has examined the legal, technical and consumer-related implications of the right to data portability in a study and gives recommendations, how this new instrument can be applied in a useful way.

In a Call for Papers, representatives from research, industry, consumer protection organisations and data protection authorities as well as other interested parties were invited to submit their opinions, requests and proposals for solutions. These submissions will be presented in the study and complemented by recommendations from external experts. Finally, we will derive recommendations for action for politics and regulatory authorities from the findings gained.

Findings from the Project

Achievement of objectives

Basically, the right to data portability can give the users more control over their personal data. Whether this objective can be achieved depends on whether this new right can be implemented in a workable and functional manner or not. If the concept of data portability does not function in a consistent way in practice, people are not very likely to use it and the desired effect will not be achieved. Therefore, it will be important to focus on practicability.

The interpretation of Art. 20 GDPR should include the data where portability directly serves the protection of data privacy ("informational self-determination") and consumer benefits. The efforts required for the implementation of the regulation should be proportionate to the actual benefits for data subjects. With respect to data minimisation ("Datensparsamkeit") we have to critically bear in mind that any transfer of data also results in a duplication of the data sets. At least, this is the case when users do not also request the deletion of their transferred data by the transferring organisation. It should be pointed out to the concerned persons in a transparent way that a data transfer to another organisation does not mean that the data is automatically deleted by their old provider or that existing contracts are

terminated. In a worst-case scenario, a very broad interpretation of the regulation in combination with the expected duplication of data sets could lead to new data privacy risks and at the same time result in a disproportionately high amount of work regarding the categorisation and extraction of data sets for the data controllers.

Under the right to data portability, users will have the right to chose between having their data set transferred to themselves or directly to their new service provider. In case users should prefer the second version of a direct transfer, new business models could emerge in which data collectors encourage the concerned persons (e.g. with monetary incentives) to transfer their user data to them with the help of Art. 20 GDPR.

Suitable Implementation Strategies

Typically, users will want to transfer their data from one provider to another within the same sector – from one social network to another; from one insurance to another. Based on these practical application cases, which are mainly to be expected, industry-specific approaches to solutions should be taken. This would have the advantage that data types, formats and special data protection aspects could be adjusted to the specific requirements of the respective sector. In addition, specific tools could be developed and agreed on within a shorter time in individual industry sectors than it would be the case for more complex cross-industry unification processes.

With respect to the statutory provision that users can also demand a direct transfer between organisations “where technically feasible”, each case should rather be examined individually instead of a generalised approach.

Technical Realisation

The General Data Protection Regulation determines that organisational and technical processes have to be set up in order to efficiently achieve its objectives such as data portability. At the same time, the act is neutral with respect to technology and does not indicate specific formats or standards. Therefore, this project study also examined how the legal requirement of a “structured, commonly used and interoperable format” can be fulfilled in practice. We came to the result that already existing formats can be used for both simple as well as more complex requirements, if they fulfil the requirements for machine-readability and interoperability at the same time.

In any case, data privacy should be given a high priority during the data transfer, for example by means of encryption.

Additionally, suitable measures of identification should be implemented in order to make sure that the transferred data are actually only sent to the entitled person or a recipient indicated by them. In order to avoid fraudulent data transfer requests, it is necessary to clearly authenticate the person making the request and to guarantee an equivalent level of data protection and data privacy.

Recommendations for Action

1. Objectives of the Regulation

The regulation should be implemented in line with its original intention – the improvement of data privacy ("informational self-determination") for the consumers. This refers primarily to **possibilities of control over the transmission of personal data.**

The right to data portability **has to include at least such data whose portability actually supports informational self-determination** and which can correspondingly be utilised by the users. The efforts and expenses required for the implementation of the regulation have to be proportionate, also with regard to the consumers' data sovereignty.

The **effectiveness of the regulation has to be tested in practice.** This includes for example behavioural economic surveys examining the actual willingness of the users to make use of data portability options. The results should be taken into account in the evaluation of the EU General Data Protection Regulation.

The introduction of the right to data portability should be accompanied by information campaigns regarding its scope and possibilities (e.g. by national data protection authorities or through information platforms).

2. Determination of the Scope of Application

The determination of the scope of application should focus on the **consumer benefits** in order to increase acceptance and success of the new right.

The **definition of "data provided" should be based on the spirit and purpose of the regulation.**

Apart from the statement of the Article 29 Working Party, the regulatory authorities should **specify what "data provided" means exactly and give examples for the data categories included under this term.**

The **question whether the scope of application could include inventory data as well as usage data should be answered based on each individual case and on the respective service.** It has to be examined, in which cases the transfer of "provided" usage data to another service provider would actually support the control rights of the person concerned.

With respect to the data format and the requested interoperability, **issues of competition law have to be taken into account.** It has to be examined, to what extent criteria have to be developed in order to achieve a consistent perspective across Europe as well as a differentiated result with respect to competition law and data protection law. **Antitrust issues with respect to agreements on methods for data transfer have to be avoided.** The protective purpose of the regulation, i.e. to facilitate a switch from one provider to another, has to be realised in an effective way.

In case of data processing by an individual person exclusively for personal or family purposes, it has to be taken into account with regard to third-party protection rights whether personal data are transmitted to a commercial provider or if they are processed on their own private devices. In this regard, rules of conduct have to be elaborated indicating to what extent further processing by commercial providers due to legitimate interests or a change of purpose would be actually ruled out in the future.

It is advisable to check whether there is a consistent technical and legal understanding of the term "metadata". This is particularly relevant in order to decide which metadata are required for the successful implementation of data portability as well as for the development of a format from a technical point of view and which are permissible from a legal point of view.

All of the involved parties should always ensure transparency when the right to data portability is exercised. The respective concerned persons should not lose track of the data controllers and the rights of erasure they are entitled to. They have to know all of the information relating to the processing by the old and the new controller.

With regard to the request "where technically feasible", it has to be decided whether objective criteria can be developed or if the individual capacities of the respective data controller (subjective standard) are taken as a basis.

It is also important to strive for a harmonisation and consistent interpretation across all of Europe in construing Art. 20 GDPR as well as in the elaboration of rules of conduct according to Art. 40 GDPR.

3. Implementation Strategies

EIt is advisable to develop **approaches of "regulated self-regulation"** establishing a framework under state supervision within which regulatory authorities, NGOs as well as companies develop implementation strategies and standards for data portability.

For an effective definition and arrangement of data portability and realisation of legal compliance, companies and industries which will be particularly affected should be involved in formal **consultation processes of the regulatory authorities.**

- **In case of the transfer of sector-specific data sets** within one category of controllers and in cases where there are already existing internal portability solutions within the industry, an industry-specific procedure is recommended.

- **Solution approaches based on Personal Information Management Systems (PIMS) seem very promising for cross-sectoral application cases.**

In cases in which a low demand for data transfers is to be expected, individual solutions for the direct transfer of data sets could be applied.

In order to allow for better orientation, the responsible bodies should work towards **rules of conduct for the practical implementation of portability** (Art. 40 GDPR).

4. Technical Realisation

The minimum requirement for data portability and interoperability should be the use of the CSV format. To this, a simple description of how the data is arranged in the file has to be added.

For more complex solutions, the formats XML or JSON should be used. These formats allow for finer granularity levels, contain content data as well as describing metadata and have sufficient depth due to their structure so that they are able to represent even complex data structures. The information contained in these files is not only machine-readable but it can also be read by the persons concerned themselves using standard software, which at the same time supports the users‘ exercise of their information rights.

- The data protection authorities should **define which specific requirements are imposed with regard to authentication** in order to avoid legal uncertainties for the controllers as well as risks for the persons concerned.

- It has to be made sure for individual solutions as well as for industry-specific or cross-sectoral and universal approaches that the technical **solutions are as a matter of principle made interoperable with each other by means of open interfaces.**

- With regard to the efficient reuse of the transferred data, the PDF format should not be used as a standard in the field of data portability, even if it is sufficient as an electronic format within the scope of the right of access with respect to transparent information.

Which Types of Data Are Concerned?

Despite the guidelines of the Working Party of the European data protection authorities, there is still some disagreement as to which data should be included in the scope of application of the new regulation. The term “data provided” is not defined in the EU General Data Protection Regulation. The data protection authorities believe that the scope of application includes more than just the data directly provided by the users (e.g. in the entry mask of a web shop). According to their opinion, it should also be possible to transfer personal data which is created and collected during the use of a service. This opinion is met with strong criticism by other stakeholders. They demand that only such data should be made available for transfer which was actively and intentionally provided by the data subject. The arrangements should focus on the data which is required for changing the provider, because this was the legislator‘s motivation for the right to data portability. They argue that apart from the objectives of the regulation, a narrow interpretation was also supported by the history if the legislative procedure. However, all of the parties agree that data which was created by the processor itself based on the data provided or observed during usage (“inferred data”, e.g. score values) does not have to be made available for transfer.

Explanatory Film on Data Portability

Large parts of the population are still not sufficiently informed about their future right to data portability. In order to provide a starting point for a necessary public awareness campaign, Stiftung Datenschutz has created an informative explanatory film on data portability within the scope of their project.

In short sequences, the film deals with the most important legal aspects as well as some issues concerning the implementation of Article 20 of the European General Data Protection Regulation, which are currently still disputed. It provides a first insight into the subject matter for citizens and corporate representatives alike in a hands-on and entertaining form.

The film is freely available and can be accessed and downloaded under www.stiftungdatenschutz.org.