

Stellungnahme

Zum Recht auf Datenübertragbarkeit nach Art. 20 Datenschutz-Grundverordnung

14.03.2017

Seite 1

Bitkom vertritt mehr als 2.400 Unternehmen der digitalen Wirtschaft, davon gut 1.600 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlands-umsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Susanne Dehmel

**Mitglied der Geschäftsleitung
Vertrauen & Sicherheit**

T +49 30 27576-223
s.dehmel@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Thorsten Dirks

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Inhalt

1. Einleitung	3
1.1 Überlegungen zur Auslegung der Vorschrift.....	3
1.2. Überlegungen zur praktischen Umsetzung.....	5
2. Tatbestandsvoraussetzungen	6
2.1. Personenbezogene Daten	6
2.2. „Bereitgestellt“ durch den Betroffenen (=“provided“)	7
2.3 Verarbeitung auf Grundlage eines Vertrags oder Einwilligung.....	8
3. Einschränkungen durch Art. 20 Abs. 3 S.2 DS-GVO	9
4. Bereichsspezifische Vorschriften	10

Anlagen

Anlage 1: Beispiele für die Interpretation des Rechts auf Datenübertragbarkeit

Anlage 2: Beispiele für öffentlich-rechtliche Vorschriften, nach denen ein Arbeitgeber Daten eines Arbeitnehmers verarbeiten muss.

1. Einleitung

Das Recht auf Datenübertragbarkeit, welches neben die auch schon unter der EU-Richtlinie bekannten Betroffenenrechte auf Information, Auskunft, Berichtigung und Löschung tritt, ist ein Novum im Datenschutzrecht.

Neben zahlreichen anderen Datenschutzvorschriften muss auch dieses Recht bis Mai 2018 nicht nur von der Digitalwirtschaft, sondern auch von allen anderen Sektoren umgesetzt werden. Das stellt gerade klein- und mittelständische Unternehmen vor große Herausforderungen.

Bei der Auslegung des Rechts gibt es noch viele offene Fragen, bei deren möglichst einheitlicher Beantwortung die Unternehmen auf die Hilfe der Aufsichtsbehörden angewiesen sind. Ein kooperativer Ansatz und eine Auslegung mit Augenmaß wären aus Sicht des Bitkom wünschenswert, um die Umsetzung der DS-GVO weiter voranzutreiben.

Diese Stellungnahme hat das Ziel, auf Schwierigkeiten bei der Auslegung und Umsetzung des Rechts auf Datenübertragbarkeit hinzuweisen. Dabei wird auch die Entwurfsstellungnahme der Art.29-Datenschutzgruppe (WP29) kommentiert.

1.1 Überlegungen zur Auslegung der Vorschrift

- **Der Wortlaut von Art. 20 DS-GVO sollte die Grundlage für die Auslegung des Rechts auf Datenübertragbarkeit sein.** Darüber hinaus gehende Anforderungen an die Übertragung, die sich nicht aus dem gesetzlichen Wortlaut der DS-GVO ableiten lassen¹, sollten nicht von den EU-Datenschutzaufsichtsbehörden als zwingend erforderlich vorgeschrieben werden, sondern lediglich Empfehlungscharakter haben.
- **Das Recht auf Datenübertragbarkeit darf nicht isoliert von anderen Vorschriften der DS-GVO betrachtet werden, sondern ist systematisch im Zusammenhang mit und in Abgrenzung zu anderen Rechten zu interpretieren.** Datenübertragbarkeit tritt in der DS-GVO neben andere Betroffenenrechte auf Information, Auskunft, Berichtigung und Löschung.
- In diesem Zusammenhang hat der **Gesetzgeber sich ganz bewusst für einen anderen Wortlaut in Art. 20 entschieden** und den Umfang des Rechts auf Datenübertragbarkeit auf Daten begrenzt, die eine betroffene Person einem Verantwortlichen „bereitgestellt hat“. Im Gegensatz dazu sind andere Betroffenenrechte wie beispielsweise das Auskunftsrecht nach Art. 15 weiter formuliert und umfassen alle personenbezogenen Daten, die vom Verantwortlichen über die betroffene Person „verarbeitet werden“. Jede weitergehende Interpretation widerspricht dieser Einschränkung und berührt das ausgewogene Verhältnis der DS-GVO zwischen den Rechten betroffener Personen, Verantwortlicher und Dritter.

¹ Siehe Art.20-Datenschutzgruppe z.B. „all customers must be informed at the time of account closure“, WP 244, S. 11.

- Darüber hinaus sollten auch **Sinn und Zweck der gesetzlichen Vorschrift** bei der Interpretation miteinbezogen werden. Bereits in der Gesetzesbegründung der EU-Kommission heißt es:

*„In Artikel 18 wird das Recht des Betroffenen auf Datenportabilität eingeführt, d. h. das **Recht, seine Daten aus einem automatisierten Datenverarbeitungssystem auf ein anderes System zu übertragen, ohne dass der für die Verarbeitung Verantwortliche ihn daran hindern kann**. Als Voraussetzung für die Ausübung dieses Rechts und um den Zugang natürlicher Personen zu ihren Daten weiter zu verbessern, ist vorgesehen, dass der für die Verarbeitung Verantwortliche diese Daten in einem strukturierten, gängigen elektronischen Format zur Verfügung stellen muss.“²*

Auch in Erw. 68 ist nur aufgeführt, dass die betroffene Person **„eine bessere Kontrolle über die Daten haben soll“**.

Wenn man das Portabilitätsrecht wie es die EU-Kommission beschrieben hat als Recht des Betroffenen versteht, seine Daten aus einem automatisierten Datenverarbeitungssystem auf ein anderes System zu übertragen, ohne dass der für die Verarbeitung Verantwortliche ihn daran hindern kann, reicht es aus, dass der Betroffene nur **diejenigen Daten transportiert bekommt, die er benötigt, um einen neuen Dienst sinnvoll weitzunutzen zu können**. Der Schwerpunkt sollte also auf Daten liegen, die eng mit der Dienstleistung (vom Verantwortlichen A) verknüpft sind und notwendig sind, um den Service (von Verantwortlichen B) nützlich zu machen. Alle anderen Daten werden bereits durch andere Betroffenenrechte adressiert. Genannt sind von der WP29 z.B. die Playlist beim Streaming Service und die Leistungsaufzeichnung beim Fitnessarmband – beides gehört wohl unzweifelhaft zum Service. Da Art. 20 verschiedene Branchen und Geschäftsmodelle betrifft, wird dies von Fall zu Fall unterschiedlich sein und die Abgrenzung mal leichter und mal schwerer fallen. Eine solche enge Auslegung würde jedoch verhindern, dass geistiges Eigentum und Geschäftsgeheimnisse sowie die Rechte und Freiheiten Dritter tangiert werden. Dies entspricht dem Rechtsgedanken des Art. 20 Abs. 4 DS-GVO, der vorschreibt, dass bei einer direkten Übertragung zwischen den Verantwortlichen die Rechte und Freiheiten anderer Personen nicht beeinträchtigt werden dürfen.

Sachfremde Erwägungen wie „die Stärkung des Wettbewerbs“ oder die „Förderung der Entwicklung neuer Dienstleistungen“ aus dem Arbeitspapier der WP29 finden sich dagegen weder in den Erwägungsgründen wieder noch lassen sie sich datenschutzrechtlich begründen. Zwar stützt sich die DS-GVO im Grundsatz neben dem Schutz natürlicher Personen (Erw.9) auch auf den „freien Verkehr von personenbezogenen Daten“. Allerdings soll dieser gemäß Erw.13 durch die EU-weite Harmonisierung der Datenschutzvorschriften erfolgen, die wiederum zu mehr Rechtssicherheit und Transparenz für Wirtschaftsteilnehmer führen soll. Dies soll zur Stärkung des digitalen Binnenmarktes führen.

Ein weiteres Argument zur Beschränkung des Anwendungsbereichs auf Service relevante Daten ist sicherlich die potenzielle Missbrauchsgefahr des Rechts auf Portabilität. Denkbar wäre ein Szenario, bei dem (insbes.

² S.10, Vorschlag der Kommission vom 25.01.2012.

außereuropäische) Unternehmen (bzw. Briefkastenfirmen) der betroffenen Person finanzielle Anreize für die Ausübung des Portabilitätsrechts setzen, um ihre Daten anschließend außerhalb der EU/EWR für beliebige Zwecke weiterzuverwenden und/oder zu verkaufen. Zwar gilt die DS-GVO nach dem Marktortprinzip auch außerhalb Europas, allerdings ist dort die Durchsetzung schwierig, sodass Missbrauch nicht verhindert werden kann. Die Beschränkung des Anwendungsbereichs dient somit auch dem Schutz der betroffenen Person, ohne ihn in der Nutzung und dem Wechsel von Diensten merklich einzuschränken.

- **Das Recht auf Datenübertragbarkeit ist nicht schrankenlos.** „Eine wesentliche Einschränkung resultiert bereits daraus, dass personenbezogene Daten Dritter schon tatbestandlich nicht erfasst sind, denn es handelt sich um den Anspruchsinhaber betreffende Daten“.³ Auch sollen nach Art. 20 Abs. 4 „**die Rechte und Freiheiten anderer Personen**“ nicht beeinträchtigt werden oder das Recht soll nach Art. 20 Abs.3 S.2 ausgeschlossen sein, soweit die **Verarbeitung im öffentlichen Interesse liegt oder in der Ausübung öffentlicher Gewalt**. Zudem müssen **auch andere Gesetze nach EU und nationalem Recht** (z.B. aus dem Telekommunikationssektor als *lex specialis*) berücksichtigt werden. Schließlich muss auch der **Verhältnismäßigkeitsgrundsatz** bei der Auslegung von Art. 20 DS-GVO berücksichtigt werden.

1.2 Überlegungen zur praktischen Umsetzung

- Das Recht auf Datenübertragbarkeit bringt nicht nur eine Reihe von Fragen bezüglich der Auslegung mit sich, sondern stellt die datenverarbeitende Wirtschaft auch vor praktischen Herausforderungen. **So müssen gemeinsame Standards und interoperable Systeme erst noch geschaffen werden**, die eine leichte Ausübung des Rechts für den Betroffenen ermöglichen. Dabei wird man durch die unterschiedlichen Branchen, die betroffen sind, nicht auf eine Einheitslösung wie APIs abstellen können. Die Entwicklung technischer Standards ist ein komplexer Prozess, der von vielen Beteiligten, einschließlich Aufsichtsbehörden und öffentlichen Stellen, viel Zeit und Arbeit erfordert. Zum Zeitpunkt des Inkrafttretens der Verordnung werden diese Standards noch nicht vorliegen.
- **Im Allgemeinen werden Standards innerhalb bestimmter Bereiche wie Banken, Telekommunikation, Gesundheitswesen, Transport oder Einzelhandel entwickelt werden müssen.** Der Vorteil des Datenportabilitätsrechts liegt nicht nur in der einfachen Datenübertragung, sondern darin, die Daten, die übertragen werden, tatsächlich in einem neuen Dienst nutzen zu können. Sinn und Zweck der Vorschrift sollten hier daher Beachtung finden. Die gezwungene Entwicklung sektorübergreifender Standards würde dem Grundsatz der Verhältnismäßigkeit widersprechen, da sie sowohl eine übermäßige Belastung für Unternehmen darstellt als auch in den meisten Fällen technisch nicht realisierbar ist. Es ist auch nicht notwendig, um der betroffenen Person einen Anbieterwechsel zu ermöglichen. Die WP29 sollte daher Branchen dazu ermutigen, Standards und Formate zu entwickeln, die es dem Betroffenen ermöglichen seine einmal bereitgestellten Daten mittels des Rechts auf Datenübertragbarkeit zu einem anderen

³ Jülicher/Röttgen/v. Schönefeld: Das Recht auf Datenübertragbarkeit – Ein datenschutzrechtliches Novum.

Anbieter „mitzunehmen“ und „wiederverwenden“, um den Anbieterwechsel innerhalb eines Sektors zu erleichtern.

- **Authentifizierungsverfahren bei Betroffenenrechten einschließlich Recht auf Datenportabilität**

Art.29-Datenschutzgruppe: *"In any case, data controllers must implement an authentication procedure in order to strongly ascertain the identity of the data subject requesting his or her personal data or more generally exercising the rights granted by the GDPR."*

Die Verantwortlichen müssen ein Authentifizierungsverfahren einführen, um die Identität der Person, die das Recht auf Datenportabilität geltend machen will, klar festzustellen. Dabei ergeben sich Unsicherheiten für Verantwortliche, wie diese Verfahren ausgestaltet werden müssen auch in Hinblick auf nationale Vorschriften wie §309 Nr. 13 BGB (Form von Anzeigen und Erklärungen). **Um Widersprüche zu vermeiden, sollten die Aufsichtsbehörden einen Leitfaden veröffentlichen und EU-weit klären, welche Ansprüche an Authentifizierungsverfahren gestellt werden.** So sollten beispielsweise auch Ausführungen und Beispiele gemacht werden, wann nach Ansicht der WP29 ein berechtigter Zweifel vorliegt und welche weiteren Informationen geeignet sind, um eine zweifelsfreie Identifikation sicherzustellen.

2. Tatbestandsvoraussetzungen

1. Personenbezogene Daten i.S.d Art. 4 Nr. 1 DS-GVO
2. Daten müssen vom Betroffenen bereitgestellt worden sein
3. Verarbeitung muss auf einer Einwilligung oder einem Vertrag beruhen
4. Verarbeitung muss mit Hilfe automatisierter Verarbeitung erfolgen⁴

2.1 Personenbezogene Daten

Es erscheint klar, dass die Vorschrift nur auf personenbezogene Daten i.S. d. Art. 4 Nr. 1 DS-GVO und auf natürliche Personen beschränkt ist. Die Anforderung „den Betroffenen betreffenden personenbezogenen Daten“ ist nach Ansicht der Art. 29 Working Party nicht zu eng auszulegen.

Als Beispiel (S.7) nennt sie, dass bei Telefonübersichten in der „account history“ des Betroffenen auch Details von Dritten umfasst sein können, wenn sie angerufen haben oder vom Betroffenen angerufen wurden. Auch wenn hier Daten Dritter enthalten sind, soll es dem Betroffenen ermöglicht werden, diese Aufzeichnungen zu erhalten. Wo jedoch solche Aufzeichnungen zu einem anderen Verantwortlichen übermittelt werden sollte dieser die Daten nicht für Zwecke verarbeiten, die in die Rechte und Freiheiten der Dritten eingreifen würden.

Dieses Beispiel stellt aus Sicht des Bitkoms einen Sonderfall dar und ist schwierig zu verallgemeinern, da hier *lex specialis* Vorschriften aus dem TK-Bereich gelten. So kann ein Verantwortlicher nicht einfach Daten veröffentlichen, die die Vertraulichkeit Dritter verletzen würden. Auch der Betroffene sollte nicht in die schwierige Lage gebracht

⁴ Wird in diesem Papier nicht thematisiert.

werden für die Verletzung von Rechten und Freiheiten Dritter, z.B. unter zivilrechtlichen Ansprüchen, haftbar gemacht zu werden.

Auch schreibt die WP29 vor (S. 7), dass "pseudonymous data that can be clearly linked to a data subject (e.g. by him or her providing the respective identifier, cf. Article 11 (2)) is well within the scope." (S.6).

Es sollten Beispiele und detaillierte Ausführungen ergänzt werden, unter welchen Umständen die Voraussetzung „data can be clearly linked to a data subject“ als erfüllt angesehen werden muss. Es sollte hervorgehen, wie die Stellungnahme des Generalanwalts zum Personenbezug von IP-Adressen in dieser Richtlinie Berücksichtigung findet.

2.2 „Bereitgestellt“ durch den Betroffenen (=“provided“)

Noch schwieriger ist die Abgrenzung von bereitgestellten Daten zu sonstigen Daten, da sich in der Verordnung keine Legaldefinition des Bereitstellens findet.

*Die WP29 unterscheidet hier zunächst zwischen **wissentlich und aktiv bereitgestellten Daten** wie z.B. Bestandsdaten (Account Data wie E-Mail Adresse, Nutzername, Alter), die durch Online-Formulare eingegeben werden und zwischen Daten, die durch den Nutzer z.B. durch Nutzung eines Dienstes oder Produkts erzeugt und vom Verantwortlichen gesammelt werden wie z.B. die Rohdaten, die ein Smart Meter erfasst. Beides fällt laut WP29 unter den Begriff „bereit gestellt“. Nicht bereit gestellt sind laut WP29 jedoch solche Daten, die vom Verantwortlichen selbst erzeugt werden wie z.B. ein Nutzerprofil, das durch die Analyse der von einem Smart Meter gesammelten Rohdaten gewonnen wurde.*

*Die WP29 nennt als weiteres Beispiel für „bereit gestellte“ Daten die Suchhistorie einer Person, Verkehrs- und Standortdaten (**„observed data“**).*

*Nicht bereitgestellt, sondern **„abgeleitete“ („inferred“ or „derived“)** Daten sind solche, die vom Verantwortlichen aus bereitgestellten Daten abgeleitet wurden z.B. ein Credit Score oder das Ergebnis einer Gesundheitsprüfung. Solche Daten sollen nicht unter das neue Datenportabilitätsrecht fallen.*

Bei den Daten, die durch die Nutzung eines Dienstes oder Produkts entstehen, stellt sich die Frage, ob hiermit nur die Daten gemeint sind, die auch für die Funktionalität des Dienstes relevant sind und daher eben auch für einen möglichen Anbieterwechsel eine Rolle spielen oder ob ebenfalls z.B. als Nebenprodukt entstehende Daten (wie z.B. Log Files und Verkehrsdaten) umfasst sein sollen.

Da der Begriff des Bereitstellens in der DS-GVO nicht legal definiert ist, lässt sich der Begriff nur interpretieren. Dabei sollten die in 1.1. gemachten Überlegungen berücksichtigt werden. Wenn man miteinbezieht, dass der Gesetzgeber sich ganz bewusst für den Wortlaut „bereitgestellt“ entschieden hat in Abgrenzung zum Wortlaut „verarbeitet“, sollte es ausreichend sein nur die Daten zu berücksichtigen, die der Betroffene kontrolliert und über die er selbst verfügt (z.B. Bilder, E-mails während der Laufzeit des Vertrages). Dies schließt Nutzungsdaten aus. Insbesondere

Stellungnahme Datenportabilität

Seite 8|16

sollten keine Daten unter das Recht fallen, die bei Nutzung des Dienstes automatisch generiert werden (z.B. Logfiles, Verkehrsdaten). **Beispiel zu Verkehrs- und Standortdaten siehe Anlage 1.**

Aus technischer Sicht: Die meisten Diensteanbieter verfügen nicht über separate Datenbanken, die nur Rohdaten enthalten, sodass diese nicht leicht von den Algorithmen, um Profile für Kundenanalysen zu erstellen, getrennt werden können. Die Übermittlung dieser Daten an einen anderen Verantwortlichen würde in fast allen Fällen detaillierte Hintergrundinformationen über die technische Einrichtung des ursprünglichen Verantwortlichen und die verwendeten Algorithmen geben. Dies würde zur Aufdeckung von Kerntechniken und Geschäftsinformationen führen, die in den meisten Fällen durch geistige Eigentumsrechte und als Geschäftsgeheimnisse geschützt sind, aufdecken. Da die „Rechte und Freiheiten“ Dritter nicht berührt werden dürfen, sollte eine enge Auslegung gewählt werden.

2.3 Verarbeitung auf Grundlage eines Vertrags oder Einwilligung

Drittens muss die Verarbeitung auf einer Einwilligung oder einem Vertrag gem. Art. 6 Abs. 1 lit. b DS-GVO beruhen.

Hier ist zu klären, ob tatsächlich alle „**Betroffenen**“ vom Anwendungsbereich umfasst sein sollen. In allen Diskussionen und bei den Beispielen wurde auf eine Anbieter-Kundenbeziehung abgestellt. Nach dem Wortlaut „Betroffener“ käme jedoch auch der Arbeitnehmer in seinem Verhältnis zum Arbeitgeber als Berechtigter in Frage.

Bitkom:

Wenn man Art. 20 allerdings wie oben erläutert nicht als elektronische Variante des Art. 15 interpretiert, sondern dessen Ziel darin sieht, dass es einer natürlichen Person erleichtert werden soll, durch einen elektronischen Datentransfer Anbieter zu wechseln, reduziert sich der Anwendungsbereich für Arbeitnehmer erheblich.

Die Voraussetzung, dass der Arbeitnehmer die Daten im Rahmen einer erteilten Einwilligung oder für die Erfüllung/Abwicklung des Vertragsverhältnisses bereitgestellt hat, wird zudem nur für einen Teil der Datenverarbeitung im Arbeitsverhältnis gelten. Auf Basis der Einwilligung werden nur die Daten verarbeitet, die nicht für die Durchführung des Arbeitsverhältnisses erforderlich sind (z.B. freiwilliges Bonusprogramm? Private Handynutzung?). Da der Anwendungsbereich für Einwilligungen im Arbeitsverhältnis sehr eng ist, wird der Großteil der im Arbeitsverhältnis verarbeiteten Daten entweder auf Basis des Art. 6 Abs.1 lit. b) oder c) erfolgen. **Beispiel zu Arbeitnehmern siehe Anlage 1.**

Schließlich ist nach unserem Dafürhalten der Verweis auf Art. 20 Abs. 3 Satz 2 DS-GVO auch geeignet, die Anwendbarkeit bei Arbeitnehmern um die Daten zu reduzieren, die der Arbeitgeber zwar in der Regel direkt vom Arbeitnehmer erhält, aber die er in Umsetzung öffentlich-rechtlicher Vorschriften, die im öffentlichen Interesse liegen, verarbeitet. Zur Veranschaulichung ist der Stellungnahme in Anlage 2 eine nicht abschließende Aufzählung einiger Vorschriften beigefügt, die der Arbeitgeber zu beachten hat. **Beispiel zu öffentlich-rechtlichen Vorschriften siehe Anlage 2.**

Eine diesbezügliche Klarstellung der Aufsichtsbehörden könnte helfen, hier Missverständnisse und Fehlinterpretationen frühzeitig zu vermeiden.

3 Einschränkungen durch Art. 20 Abs. 3 S.2 DS-GVO

- Verarbeitung erfolgt im öffentlichen Interesse oder liegt in der Ausübung öffentlicher Gewalt (Art. 20 Abs. 3 S.2)
- Die Übertragung der Daten darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen (Art. 20 Abs. 4)

Art. 29-Datenschutzgruppe: *"With respect to data covered by intellectual property and trade secrets: The rights and freedoms of others mentioned in Article 20(4) can also refer to "the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software" mentioned in recital 63, in order to protect the business model of data controllers (Article 15). Even though these rights should be considered before answering a data portability request, "the result of those considerations should not be a refusal to provide all information to the data subject".*

...

A potential business risk cannot, however, in and of itself serve as the basis for a refusal to answer the portability request and data controllers can transfer the personal data provided by data subjects in a form that does not release information covered by trade secrets or intellectual property rights."

- Gemäß der **deutschen Fassung der DS-GVO**, darf das Recht gem. **Abs.2** nicht die Rechte und Freiheiten anderer Personen beeinträchtigen. Die englische Fassung wiederum verweist auf **Abs.1**. Hier handelt es sich offensichtlich um ein Redaktionsversehen. **Eine Klarstellung seitens der Aufsichtsbehörden wäre hier wünschenswert.**
- **Darüber hinaus sollte deutlich gemacht werden, dass die Ausübung des Rechts auf Datenübertragbarkeit nicht zu einer Verletzung geschützter Rechte Dritter führen darf. Hier gibt es ein großes Missbrauchspotenzial.** Das Recht auf Datenübertragbarkeit ist nicht absolut und muss mit entgegenstehenden Rechten Dritter auf informationelle Selbstbestimmung, Schutz der Vertraulichkeit, Schutz von Geschäftsgeheimnissen sowie anderen wettbewerbsrechtliche Aspekte, Urheberrechte etc. in Einklang gebracht werden. **Griffige Beispiele und Empfehlungen wären hier wünschenswert.**

4 Bereichsspezifische Vorschriften

- **Darüber hinaus sollte geklärt werden wie sich das Recht auf Datenübertragbarkeit zu spezialgesetzlichen Vorschriften verhält** wie beispielsweise §630g BGB, der eine Regelung zur Herausgabe von Patientenakten enthält.

Anlage 1

Beispiel 1) Verkehrs- und Standortdaten:

Sinn und Zweck der Norm

- Nicht erforderlich, um den Dienst auch für die Zukunft bei einem Dritten zu beziehen
- Wenn überhaupt, kann nur die Nummer des B-Teilnehmers als vom A-Teilnehmer „bereitgestellt“ angesehen werden, der er diese „gewählt“ hat;

Bereitgestellt durch den Betroffenen

- Verkehrs- und Standortdaten werden nicht von Nutzer bereitgestellt; dieser initiiert allein den Kommunikationsvorgang
- Verkehrs- und Standortdaten fallen erst im Rahmen der Signalisierung innerhalb des TK-Netzes an; insbesondere Standortdaten beziehen sich auch nur auf Standorte von TK-Anlagen/-Linien (Mobilfunk-Antennen)
- Verkehrs- und Standortdaten fallen als Folge standardisierter Protokolle an und hängen nicht am Willen der Beteiligten

Verarbeitung auf der Grundlage einer Einwilligung/des Vertrages

- Erhebung von Verkehrs- und Standortdaten erfolgt – auch unter hypothetischer Geltung der e-Privacy-Verordnung – allein auf der Grundlage spezifischer Erlaubnistatbestände und nicht auf der Grundlage eines Vertrages oder gar einer Einwilligung; das mag dort anders sein, wo erhobene Daten auf Grundlage einer Einwilligung für weitere Zwecke verarbeitet werden dürfen. Aber auch in diesen Fällen beruht die Erhebung der Daten auf gesetzlichen Erlaubnistatbeständen und fällt daher nicht in den Anwendungsbereich der Norm.

Betriebs- und Geschäftsgeheimnisse sowie Rechte Dritter

- Wenn überhaupt, dann wird nur die Nummer des B-Teilnehmers vom A-Teilnehmer „bereitgestellt“; und gerade im Hinblick auf diese gelten kollidierende Interessen des B-Teilnehmers; somit wären diese Informationen zumindest vom Anspruch nach Art. 20 Abs.2 DS-GVO ausgeschlossen.

Entgegenstehende Rechtsnormen

- Kollision mit den (abschließenden) Erlaubnisnormen des TKG/ePR-V

- Konterkariert z.B. die engen Voraussetzungen, unter denen ein EVN erstellt werden muss und darf

Der Bitkom vertritt daher die Auffassung, dass Verkehrs- und Standortdaten aus dem Anwendungsbereich des Art. 20 DS-GVO fallen.

Beispiel 2) Daten von Arbeitnehmern:

Sinn und Zweck der Norm

- In vielen Fällen nicht erforderlich, um den Dienst auch für die Zukunft bei einem Dritten zu beziehen

Verarbeitung auf der Grundlage einer Einwilligung/des Vertrages

- Auf Basis der Einwilligung werden nur die Daten verarbeitet, die nicht für die Durchführung des Arbeitsverhältnisses erforderlich sind (z.B. freiwilliges Bonusprogramm? Private Handynutzung?). Da der Anwendungsbereich für Einwilligungen im Arbeitsverhältnis sehr eng ist, wird der Großteil der im Arbeitsverhältnis verarbeiteten Daten entweder auf Basis des Art. 6 Abs.1 lit. b) oder c) erfolgen.

Ausnahme öffentlich-rechtlicher Vorschriften nach Art. 20 Abs. 3 S.2

- Art. 20 Abs. 3 Satz 2 DSGVO geeignet, die Anwendbarkeit bei Arbeitnehmern um die Daten zu reduzieren, die der Arbeitgeber zwar idR direkt vom Arbeitnehmer erhält, aber die er in Umsetzung öffentlich-rechtlicher Vorschriften, die im öffentlichen Interesse liegen, verarbeitet.

Der Bitkom vertritt daher die Auffassung, dass Daten von Arbeitnehmern daher aus dem Anwendungsbereich des Art. 20 DS-GVO fallen.

Anlage 2

Beispiele für öffentlich-rechtliche Vorschriften, nach denen ein Arbeitgeber Daten eines Arbeitnehmers verarbeiten muss

§ 28a SGB IV (Aufstellung der wichtigsten Meldungen)

DEÜV-Meldung allgemein

(1) Der Arbeitgeber oder ein anderer Meldepflichtiger hat der Einzugsstelle für jeden in der Kranken-, Pflege-, Rentenversicherung oder nach dem Recht der Arbeitsförderung kraft Gesetzes Versicherten

1. bei Beginn der versicherungspflichtigen Beschäftigung,
2. bei Ende der versicherungspflichtigen Beschäftigung,
3. bei Eintritt eines Insolvenzereignisses,
4. (weggefallen)
5. bei Änderungen in der Beitragspflicht,
6. bei Wechsel der Einzugsstelle,
7. bei Anträgen auf Altersrenten oder Auskunftersuchen des Familiengerichts in Versorgungsausgleichsverfahren,
8. bei Unterbrechung der Entgeltzahlung,
9. bei Auflösung des Arbeitsverhältnisses,
10. auf Anforderung der Einzugsstelle nach § 26 Absatz 4 Satz 2,
11. bei Antrag des geringfügig Beschäftigten nach § 6 Absatz 1b des Sechsten Buches auf Befreiung von der Versicherungspflicht,
12. bei einmalig gezahltem Arbeitsentgelt,
13. bei Beginn der Berufsausbildung,
14. bei Ende der Berufsausbildung,
15. bei Wechsel von einem Beschäftigungsbetrieb im Beitrittsgebiet zu einem Beschäftigungsbetrieb im übrigen Bundesgebiet oder umgekehrt,
16. bei Beginn der Altersteilzeitarbeit,
17. bei Ende der Altersteilzeitarbeit,
18. bei Änderung des Arbeitsentgelts, wenn die in § 8 Absatz 1 Nummer 1 genannte Grenze über- oder unterschritten wird,
19. bei nach § 23b Absatz 2 bis 3 gezahltem Arbeitsentgelt oder
20. bei Wechsel von einem Wertguthaben, das im Beitrittsgebiet und einem Wertguthaben, das im übrigen Bundesgebiet erzielt wurde, eine Meldung zu erstatten.

Jahresmeldung

- 2) Der Arbeitgeber hat jeden am 31. Dezember des Vorjahres Beschäftigten nach Absatz 1 zu melden (Jahresmeldung).

Stellungnahme Datenportabilität

Seite 13|16

Jahresmeldung Unfallversicherung

(2a) Der Arbeitgeber hat für jeden in einem Kalenderjahr Beschäftigten, der in der Unfallversicherung versichert ist, zum 16. Februar des Folgejahres eine besondere Jahresmeldung zur Unfallversicherung zu erstatten. Diese Meldung enthält über die Angaben nach Absatz 3 Satz 1 Nummer 1 bis 3, 6 und 9 hinaus folgende Angaben:

1. die Mitgliedsnummer des Unternehmers;
2. die Betriebsnummer des zuständigen Unfallversicherungsträgers;
3. das in der Unfallversicherung beitragspflichtige Arbeitsentgelt in Euro und seine Zuordnung zur jeweilig anzuwendenden Gehaltstarifstelle.

Meldung für landwirtschaftliche Berufsgenossenschaft

Die Meldungen enthalten für jeden Versicherten insbesondere

1. seine Versicherungsnummer, soweit bekannt,
2. seinen Familien- und Vornamen,
3. sein Geburtsdatum,
4. seine Staatsangehörigkeit,
5. Angaben über seine Tätigkeit nach dem Schlüsselverzeichnis der Bundesagentur für Arbeit,
6. die Betriebsnummer seines Beschäftigungsbetriebes,
7. die Beitragsgruppen,
8. die zuständige Einzugsstelle und
9. den Arbeitgeber.

Zusätzlich sind anzugeben

1. bei der Anmeldung
 - a) die Anschrift,
 - b) der Beginn der Beschäftigung,
 - c) sonstige für die Vergabe der Versicherungsnummer erforderliche Angaben,
 - d) die Angabe, ob zum Arbeitgeber eine Beziehung als Ehegatte, Lebenspartner oder Abkömmling besteht,
 - e) die Angabe, ob es sich um eine Tätigkeit als geschäftsführender Gesellschafter einer Gesellschaft mit beschränkter Haftung handelt,
 - f) die Angabe der Staatsangehörigkeit,
2. bei allen Entgeltmeldungen
 - a) eine Namens-, Anschriften- oder Staatsangehörigkeitsänderung, soweit diese Änderung nicht schon anderweitig gemeldet ist,
 - b) das in der Rentenversicherung oder nach dem Recht der Arbeitsförderung beitragspflichtige Arbeitsentgelt in Euro,
 - c) (weggefallen)
 - d) der Zeitraum, in dem das angegebene Arbeitsentgelt erzielt wurde,
 - e) Wertguthaben, die auf die Zeit nach Eintritt der Erwerbsminderung entfallen,
 - f) (weggefallen)

Stellungnahme Datenportabilität

Seite 14|16

g) (weggefallen)

h) (weggefallen)

3. (weggefallen)

4. bei der Meldung nach Absatz 1 Satz 1 Nummer 19

a) das Arbeitsentgelt in Euro, für das Beiträge gezahlt worden sind,

b) im Falle des § 23b Absatz 2 der Kalendermonat und das Jahr der nicht zweckentsprechenden Verwendung des Arbeitsentgelts, im Falle der Zahlungsunfähigkeit des Arbeitgebers jedoch der Kalendermonat und das Jahr der Beitragszahlung.

Zahlstellenmeldung

(3a) Der Arbeitgeber oder eine Zahlstelle nach § 202 Absatz 2 des Fünften Buches kann in den Fällen, in denen für eine Meldung keine Versicherungsnummer des Beschäftigten oder Versorgungsempfängers vorliegt, im Verfahren nach Absatz 1 eine Meldung zur Abfrage der Versicherungsnummer an die Datenstelle der Rentenversicherung übermitteln; die weiteren Meldepflichten bleiben davon unberührt. Die Datenstelle der Rentenversicherung übermittelt dem Arbeitgeber oder der Zahlstelle unverzüglich durch Datenübertragung die Versicherungsnummer oder den Hinweis, dass die Vergabe der Versicherungsnummer mit der Anmeldung erfolgt.

Sofortmeldung

(4) Arbeitgeber haben den Tag des Beginns eines Beschäftigungsverhältnisses spätestens bei dessen Aufnahme an die Datenstelle der Rentenversicherung nach Satz 2 zu melden, sofern sie Personen in folgenden Wirtschaftsbereichen oder Wirtschaftszweigen beschäftigen:

1. im Baugewerbe,
2. im Gaststätten- und Beherbergungsgewerbe,
3. im Personenbeförderungsgewerbe,
4. im Speditions-, Transport- und damit verbundenen Logistikgewerbe,
5. im Schaustellergewerbe,
6. bei Unternehmen der Forstwirtschaft,
7. im Gebäudereinigungsgewerbe,
8. bei Unternehmen, die sich am Auf- und Abbau von Messen und Ausstellungen beteiligen,
9. in der Fleischwirtschaft.

Die Meldung enthält folgende Angaben über den Beschäftigten:

1. den Familien- und die Vornamen,
2. die Versicherungsnummer, soweit bekannt, ansonsten die zur Vergabe einer Versicherungsnummer notwendigen Angaben (Tag und Ort der Geburt, Anschrift),
3. die Betriebsnummer des Arbeitgebers und
4. den Tag der Beschäftigungsaufnahme.

Die Meldung wird in der Stammsatzdatei nach § 150 Absatz 1 und 2 des Sechsten Buches gespeichert. Die Meldung gilt nicht als Meldung nach Absatz 1 Satz 1 Nummer 1.

(4a) Der Meldepflichtige erstattet die Meldungen nach Absatz 1 Satz 1 Nummer 10 an die zuständige Einzugsstelle. In der Meldung sind insbesondere anzugeben: 1.

die Versicherungsnummer des Beschäftigten,

2. die Betriebsnummer des Beschäftigungsbetriebes,

3. das monatliche laufende und einmalig gezahlte Arbeitsentgelt, von dem Beiträge zur Renten-, Arbeitslosen-, Kranken- und Pflegeversicherung für das der Ermittlung nach § 26 Absatz 4 zugrunde liegende Kalenderjahr berechnet wurden.

Berufsständische Versorgungseinrichtung

11) Der Arbeitgeber hat für Beschäftigte, die nach § 6 Absatz 1 Satz 1 Nummer 1 des Sechsten Buches von der Versicherungspflicht befreit und Mitglied in einer berufsständischen Versorgungseinrichtung sind, der Annahmestelle der berufsständischen Versorgungseinrichtungen monatliche Meldungen zur Beitragserhebung zu erstatten. Absatz 10 Satz 2 gilt entsprechend. Diese Meldungen enthalten für den Beschäftigten

1. die Mitgliedsnummer bei der Versorgungseinrichtung oder, wenn die Mitgliedsnummer nicht bekannt ist, die Personalnummer beim Arbeitgeber, den Familien- und Vornamen, das Geschlecht und das Geburtsdatum,

2. den Zeitraum, für den das Arbeitsentgelt gezahlt wird,

3. das beitragspflichtige ungekürzte laufende Arbeitsentgelt für den Zahlungszeitraum,

4. das beitragspflichtige ungekürzte einmalig gezahlte Arbeitsentgelt im Monat der Abrechnung,

5. die Anzahl der Sozialversicherungstage im Zahlungszeitraum,

6. den Beitrag, der bei Firmenzahlern für das Arbeitsentgelt nach Nummer 3 und 4 anfällt,

7. die Betriebsnummer der Versorgungseinrichtung,

8. die Betriebsnummer des Beschäftigungsbetriebes,

9. den Arbeitgeber,

10. den Ort des Beschäftigungsbetriebes,

11. den Monat der Abrechnung.

Soweit nicht aus der Entgeltbescheinigung des Beschäftigten zu entnehmen ist, dass die Meldung erfolgt ist und welchen Inhalt sie hatte, gilt Absatz 5.

B § 39 Lohnsteuerabzugsmerkmale EStG⁵ (ELStAM)

4) Lohnsteuerabzugsmerkmale sind

1. Steuerklasse (§ 38b Absatz 1) und Faktor (§ 39f),
2. Zahl der Kinderfreibeträge bei den Steuerklassen I bis IV (§ 38b Absatz 2),
3. Freibetrag und Hinzurechnungsbetrag (§ 39a),
4. Höhe der Beiträge für eine private Krankenversicherung und für eine private Pflege-Pflichtversicherung (§ 39b Absatz 2 Satz 5 Nummer 3 Buchstabe d) für die Dauer von zwölf Monaten, wenn der Arbeitnehmer dies beantragt,
5. Mitteilung, dass der von einem Arbeitgeber gezahlte Arbeitslohn nach einem Abkommen zur Vermeidung der Doppelbesteuerung von der Lohnsteuer freizustellen ist, wenn der Arbeitnehmer oder der Arbeitgeber dies beantragt.

⁵ § 39 of the German Income Tax Law (EStG).