67.

WIRTSCHAFTSKAMMER ÖSTERREICH

just-article29wp-sec@ec.europa.eu
presidenceg29@cnil.fr

cc: dsb@dsb.gv.at

Wiedner Hauptstrasse 63 | Postfach 195
1045 Wien
T +43 (0)5 90 900-DW | F +43 (0)5 90 900-243
E rp@wko.at
W http://wko.at/rp

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen, Sachbearbeiter	Durchwahl	Datum
	Rp 1763/17/Ro/MH	3215	24.01.2017

EU-Datenschutz-Grundverordnung; Guidelines der Art 29-Datenschutzgruppe; Stellungnahme der Wirtschaftskammer Österreich

Sehr geehrte Damen und Herren!

Die Wirtschaftskammerorganisation ist die gesetzliche Interessenvertretung für Österreichs Wirtschaft, die mehr als 508.000 Mitglieder aus den Sparten Gewerbe und Handwerk, Handel, Industrie, Bank und Versicherung, Transport und Verkehr, Tourismus und Freizeitwirtschaft, Information und Consulting vertritt.

Zu den im Dezember 2016 angenommenen Guidelines der Art 29-Datenschutzgruppe darf seitens der Wirtschaftskammer Österreich Folgendes mitgeteilt werden:

Allgemein ist zu den Guidelines bzw FAQ der Art 29-Datenschutzgruppe anzumerken, dass Auslegungshilfen und Beispiele zur besseren Verständlichkeit einer Verordnung zwar grundsätzlich sinnvoll sein können, allerdings darf durch diese Gruppe keine Fortentwicklung des Rechts, insbesondere **keine Weiterentwicklung der EU-Datenschutz-Grundverordnung** (DSGVO) selbst erfolgen, was in einigen Passagen jedenfalls geschehen ist. Dies wird klar abgelehnt. Weiters ist es von besonderer Wichtigkeit nochmals hervorzuheben, dass derartige Leitlinien nur **unverbindlich** sein können.

Eine zeitnahme Zurverfügungstellung der Guidelines in deutscher Sprache wäre wünschenswert.

Zu den Guidelines im Konkreten:

1. Guidelines für das Recht auf Datenübertragbarkeit (Artikel 20 DSGVO)

Nach den Leitlinien sollen auch **Metadaten**, wenn möglich in der bestmöglichen Detailgenauigkeit, übermittelt werden. Zum einen fehlt zum jetzigen Zeitpunkt eine rechtlich exakte Definition, was unter „Metadaten" zu verstehen ist (möglicherweise könnte hier der eben erst veröffentliche Entwurf der neuen ePrivacy-Verordnung eine Hilfestellung leisten, diese würde allerdings erst ab deren Inkrafttreten anwendbar sein). Zudem geht diese Einschätzung jedenfalls zu weit. Es stellt sich hierbei auch die Frage der technischen Lösbarkeit, welche die Art 29-Datenschutzgruppe offensichtlich vollkommen außer Acht gelassen hat.

Die Einordnung, welche Daten als *„provided by the data subject"* zu gelten haben, ist höchst problematisch. Lediglich *„inferred data and derived data"* sollen nicht vom Recht auf Datenübertragbarkeit umfasst sein. Die Unterscheidung dieser zwei Begriffe selbst ist schon nicht nachvollziehbar, der Unterscheidung zwischen diesen Daten und jenen, welche der Betroffene aktiv zur Verfügung gestellt hat und *„Observed data are "provided" by the data subject by virtue of the use of the service or the device"* kann kaum mehr gefolgt werden. Die Grenze zu ziehen ist selbst für erfahrene Juristen ausgesprochen schwierig. Unternehmen, insbesondere KMU, können hier kaum Rechtssicherheit erlangen.

Man kann die Formulierung des Art 20 Abs 1 DSGVO ohne weiteres in dem Sinne verstehen, dass es sich um Daten handeln muss, die der Betroffene dem Verantwortlichen aktiv zur Verfügung gestellt hat, wie zB die Kundenstammdaten.

Die Art 29-Datenschutzgruppe versteht die Regelung aber weit und verlangt, dass *"the data controller must also include the personal data that are generated by and collected from the activities of users in response to a data portability request .....the terms "provided by" includes personal data that relate to the data subject activity or result from the observation of an individual's behaviour but not subsequent analysis of that behaviour. By contrast, any personal data which have been generated by the data controller as part of the data processing, e.g. by a personalisation or recommendation process, by user categorisation or profiling are data which are derived or inferred from the personal data provided by the data subject, and are not covered by the right to data portability."* In der Folge wird von der Datenschutzgruppe auch mehrfach beispielhaft auf die Übertragung von Daten zu Transaktionen auf Bankkonten Bezug genommen, wobei auch noch verlangt wird, dass die Verantwortlichen *"implement tools to enable data subjects to select the relevant data and exclude (where relevant) other data subjects' data."*

Die zu übertragenden Daten müssen vom Verantwortlichen (hier der kontoführenden Bank) nach Art 20 DSGVO in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden. Die Art 29 Datenschutzgruppe stellt in ihren Guidelines Überlegungen dazu an und *"encourages cooperation between industry stakeholders and trade associations to work together on a common set of interoperable standards and formats to deliver the requirements of the right to data portability."*

Der technische Aufwand zur Bewerkstelligung der (für den Kunden kostenfreien) Datenübertragbarkeit ist per se schon erheblich. Wenn davon auch Daten zu Kontobewegungen erfasst sein sollen, steigt der Aufwand nochmals erheblich an.

Aus Bankensicht stellt eine Übermittlung von Bewegungs- und Transaktionsdaten im gesetzlich vorgeschriebenen Format zu beispielsweise einem bestehenden Konto (die Art 29-Datenschutzgruppe führt als explizites Beispiel das Recht zur Übermittlung von Details zu Banktransaktionen an) einen enormen finanziellen, personellen und technischen Aufwand dar und ist problematisch, wie derart umfangreiche Anfragen in der Praxis in der dafür nur sehr kurz bemessenen Zeitspanne entsprechend beantwortet werden sollen. Der in den Guidelines definierte Umfang der Daten, die vom Recht auf Datenportabilität umfasst sein sollen, stellt eine erhebliche Hürde dar und es ist daher eine angemessene Einschränkung des angedachten Umfangs anzustreben.

Dies auch im Hinblick auf die weiteren Verpflichtungen, die der Verantwortliche gemäß der DSGVO sowie den zusätzlichen Ausführungen der Art 29-Datenschutzgruppe einzuhalten hat bzw.

auf die Voraussetzungen, die bei der Übermittlung der Daten gemäß Art 20 zu beachten sind, darunter insbesondere:

Frist: Die Zurverfügungstellung der Daten hat unverzüglich und jedenfalls innerhalb eines Monats ab Zugang der Anfrage zu erfolgen. Eine Fristverlängerung auf 3 Monate wird ausschließlich bei komplexen Anfragen gewährt. Art 12 DSGVO verbietet es dem Verantwortlichen grundsätzlich, Entgelte für die Übermittlung der Daten nach Art 20 DSGVO - selbst bei neuerlichen Anfragen, die dem Betroffenen unter bestimmten Voraussetzungen zustehen - zu verrechnen. Obwohl sich die Bestimmung des Art 12 DSGVO nicht ausschließlich auf das Recht auf Datenübertragbarkeit bezieht, kommt diesem Grundsatz vor allem auch in diesem Zusammenhang weitreichende Bedeutung zu.

Eine derartige Herangehensweise kann nicht mit den bereits angesprochenen und damit verbundenen finanziellen und wirtschaftlichen Belastungen in Einklang gebracht werden, insbesondere aufgrund der zu erwartenden Anforderungen an eine umfassende Umsetzung des Rechts auf Datenübertragbarkeit. Es wäre vielmehr von Bedeutung, eine analoge Lösung zur bisherigen Handhabe bei Auskünften nach § 26 Abs. 6 DSG 2000 anzustreben, wonach die Ausübung des Rechts auf Datenübertragbarkeit und die Datenübertragbarkeit als solche nur dann unentgeltlich zu erteilen ist, sofern „im laufenden Jahr noch kein" derartiges Ersuchen an den Datenverantwortlichen herangetragen worden ist. Es ist durchaus problematisch, dass eine vergleichbare zeitliche Komponente nunmehr gänzlich fehlt und ist dies mit dem bereits angesprochenen Aufwand nicht vereinbar. Eine dahingehende Klarstellung wäre wünschenswert und eine Abkehr von der - beinahe faktisch absolut geltenden - Unentgeltlichkeit unumgänglich.

Die eingangs angesprochene Fortentwicklung der DSGVO ist nicht Aufgabe der Artikel 29 Datenschutzgruppe; daher sollte sich die Auslegung des Art 20 DSGVO weiterhin auf Daten, welche vom Betroffenen aktiv bereitgestellt wurden, beschränken. Das entspräche auch der Zielsetzung dieser Bestimmung.

Weiters möchten wir in diesem Zusammenhang auf eine **Kollision der von der Art 29-Datenschutzgruppe vorgenommenen Auslegungsvariante mit dem (österreichischen) Telekommunikationsgesetz** (vgl § 100 TKG) hinweisen. Von einer Datenübertragbarkeit ausgenommen müssen in jedem wie auch immer gearteten Interpretationsfall **Verkehrsdaten** werden. Diese werden uE auch nicht vom Betroffenen bereitgestellt. Unproblematisch sind lediglich Fälle wie die Übertragung von Forumseinträgen oder Voicemail-Sprachnachrichten. Alles darüber Hinausgehende ist abzulehnen, auch vor dem Hintergrund der Problematik bzgl Vorratsdatenspeicherung, welche in manchen Mitgliedstaaten weiterhin in Kraft ist und in manchen nicht. Ein etwaiger Auslegungs- respektive Wettbewerbsvorteil dieser Mitgliedstaaten bzgl Rechtsicherheit ist nicht nachvollziehbar. UE ist auch die Beeinträchtigung von Interessen Dritter wesentlich gefährdet; die Leitlinien gehen auf dieses Thema nur sehr eingeschränkt ein und verweisen hauptsächlich darauf, dass dies nach Übertragung durch den Betroffenen selbst oder durch den Verantwortlichen, an den die Daten übertragen wurden, zu gewährleisten sei.

Seitens der Bundessparte Bank und Versicherung wird zumindest eine beispielhafte Aufzählung von Alternativen des **Formates**, in welchem die Daten dem Betroffenen zur Verfügung gestellt werden sollen, gewünscht und weiters speziell Folgendes ausgeführt:

„**Interessen Dritter:** Bei der Übermittlung der Daten an den Betroffenen sind insbesondere auch die Interessen bzw. Rechte Dritter zu berücksichtigen. Sollen nun - wie bereits oben ausgeführt - Bewegungs- und Transaktionsdaten zu einem bestehenden Konto zur Verfügung gestellt werden, kann stets davon ausgegangen werden, dass in diesen Datensätzen auch personenbezogene Daten Dritter beinhaltet sind. Der neue Datenverantwortliche, an den der Datensatz gemäß

entsprechendem Kundenwunsch übertragen werden soll, darf diese Daten jedoch nur im Einklang mit den Vorschriften der DSGVO erhalten. Eine Verarbeitung solcher Bewegungs- und Transaktionsdaten ist für den neuen Datenverantwortlichen jedoch aufgrund der umfassenden Grundsätze der DSGVO (insbesondere Zweckbindung, Minimalisierung), die bei einer Verarbeitung zu berücksichtigen sind, faktisch nicht oder nur sehr eingeschränkt möglich. Dies wiederum verdeutlicht, dass der Umfang der Daten bei der Ausübung des Rechts auf Datenportabilität den praktischen Bedarf, Nutzen sowie die Verwertbarkeit deutlich übersteigen.

Aus Bankensicht ist die weite Interpretation der Art 29-Datenschutzgruppe insbesondere aus wirtschaftlicher Sicht nicht vertretbar und es muss bezogen auf das Geschäftsfeld der Kreditwirtschaft eine engere Interpretation herangezogen werden, wonach dem Betroffenen - im Einklang mit dem Wortlaut der DSGVO - „nur" eine Übersicht jener personenbezogenen Daten übermittelt wird, die dem Verantwortlichen bereitgestellt werden, insbesondere:

- Daten, die zum Zeitpunkt der Anfrage beim Datenverantwortlichen gespeichert sind;
- im Rahmen des Vertragsabschlusses
- bei Abschluss weiterer Produkte
- bei Änderung der personenbezogenen Daten bezogen auf die Geschäftsverbindung
- als auch Daten über die Geschäfte, die der Kunde aktiv hat (z.B. Konto sowie Details zu Kontonummer und Kontostand, etc), ausgenommen jedoch Bewegungs- und Transaktionsdaten.

Darüber hinaus kann dem Recht auf Datenportabilität - wie auch den weiteren Betroffenenrechten der DSGVO - ausschließlich unter der Voraussetzung entsprochen werden, dass der Betroffene seine Identität in geeigneter Form nachweist (vgl § 26 Abs 1 DSG 2000).

Durch die Änderung im vorliegenden Vorschlagspapier entsteht dem Datenverarbeiter ein enormer technischer und prozessualer Aufwand (Downloadmöglichkeiten schaffen, Application Programming Interface (API)).

Unter III/1. Aufzählungspunkt wird angeführt, welche „processing operations" umfasst sind. Festgehalten wird, dass Papierakten nicht umfasst sind. Im Bankgeschäft ist es mittlerweile üblich, dass Akte zu Archivzwecken gescannt werden. Papierakte werden nicht aufbewahrt. Von der Datenportabilität sollten auch (gescannte) Archivdaten ausgenommen werden.

Beim Zahlungsverkehr sollten nur solche Daten erfasst sein, die in der IT für bestehende und künftige Geschäfte gespeichert sind (z.B. Daten zu Daueraufträgen). Nicht erfasst sein sollten historische Daten zu Kontobewegungen und die dazu gescannten Belege.

Weiters sollte die Kundenkorrespondenz mittels elektronischer Post ausgenommen sein. Wille des Gesetzgebers war es sicher nicht, jede elektronische Post, die (im Einzelfall) an Kunden geschickt wird, unter die Portabilität fallen zu lassen.

Personenbezogene Daten sollen weiterhin einen besonderen Schutz genießen und nicht kurzfristig auf ungesicherten, eventuell privaten, Datenträgern gespeichert werden. Personenbezogene Daten sind in ihrer Anzahl überschaubar und werden bei jeder Geschäftseröffnung im Rahmen des Beratungsgesprächs ohnehin vom Kunden erfragt und gespeichert. Ein Vorab- oder im Nachhinein-Einspielen der Daten bringt daher keinen zeitlichen Vorteil. Es sollten keine Schnittstellen eröffnet werden müssen, die potenzielle Cybercrimegefahren verursachen.

Abschließend ist festzuhalten, dass aus den Guidelines nicht hervorgeht, wer die Haftung von beschädigten, missbräuchlich verwendeten, manipulierten oder verlorenen Daten - auf dem Weg der Datenübertragung - übernimmt.

Aus oben genannten Gründen sollte von einer verpflichtenden Datenübertragbarkeit in der vorgeschlagenen Form Abstand genommen werden.

Zusammenfassend ist das Recht auf Datenportabilität im vorgeschlagenen Ausmaß im Hinblick auf den Datenumfang für konventionelle Datenverarbeitungen in unternehmensinternen Datenbanken nicht sachgerecht, geht mit enormen Implementierungsaufwänden und -kosten einher und greift unverhältnismäßig in die Interessen von Unternehmen ein. Es muss sichergestellt werden, dass sich das Bereitstellungs- bzw. Übertragungsrecht ausschließlich auf solche Daten beschränkt, die der Kunde selbst eingemeldet bzw. bekannt gegeben hat. Zudem muss verhindert werden, dass ganze Bankkundenakten zu einem fungiblen Gut und kostenlos Wettbewerbern (insbesondere im außereuropäischen Ausland) zur Verfügung gestellt werden."

Hinsichtlich der **Beispiele**, welche für einen wahrscheinlichen Übertragungsanspruch ausgewiesen sind, ist weiters auszuführen, dass gegen die Übertragung einer **Playlist eines Musikstreamingdienstes** auch urheberrechtliche Bedenken sprechen können. Zum einen sind solche Daten (was es klar zu stellen gilt) keine personenbezogenen Daten, wenn diese Playlist von Dritten, wie dem Streamingdienst selbst bereitgestellt wurden, zum anderen können an der Ausgestaltung dieser Playlist urheberrechtliche Ansprüche dieses Dritten gekoppelt sein.

Angeregt wird auch, die Rollen (Verantwortlicher/Auftragsverarbeiter) in den gewählten Beispielen zu schärfen bzw. in den Beispielen auf diese Rollen Bezug zu nehmen.

Auch die Sinnhaftigkeit der **Übertragung von Informationen über Einkäufe** erscheint praxisfremd. Einerseits stellt sich die Frage, ob derartige Daten überhaupt generell generiert wurden, andererseits ist die Begründung, nämlich die Erstellung einer C02 Bilanz, höchst fragwürdig. Für Onlineshops würde dies massive technische Umrüstung bedeuten (was im Falle von KMU nicht zu rechtfertigenden finanziellen Aufwand mit sich bringen würde). Hinsichtlich der **Rohdaten aus Smartmetern**, welche aus der Verhaltensweisen des Betroffenen generiert und gesammelt wurden und Daten aus Beobachtungen wie Sucherverlauf, Verkehrsdaten, Standortdaten, etc aus Smartwatches benötigt es eine Klarstellung, an welche Zielgruppe sich diese Formulierung richtet und keine Daten des Mobilfunknetzes gemeint sind.

Die Interpretation der Informationspflichten geht zu weit. Auf das Bestehen des Rechtes ist laut DSGVO hinzuweisen, aber es gibt kein Recht auf vorgängige Information darauf, welche Daten konkret davon umfasst sein sollen und welche nicht und auch kein Recht auf Information beim Schließen eines Accounts.

Am Ende der Leitlinien wird auch die Empfehlung ausgesprochen, der Verantwortliche solle sich um die Sicherheit der Datenspeicherung insofern kümmern, als dieser den Betroffenen Empfehlungen über angemessene Formate oder Maßnahmen zur Verschlüsselung geben solle. Das ist in der Praxis kaum durchführbar. Wir möchten nochmals eindringlich ersuchen, die Sinnhaftigkeit gewisser Leitlinien und Beispiele zu hinterfragen, v.a. auch im Hinblick auf die entsprechenden Implementierungskosten für Unternehmen, insbesondere für KMU.

2. Datenschutzbeauftragter (Artikel 37ff DSGVO)

Hinsichtlich der Verpflichtung zur Benennung eines Datenschutzbeauftragten (DSB) sollten keine weiteren Verpflichtungen außerhalb der in der DSGVO ausgewiesenen Fälle implementiert werden.

Auf Seite 15 der Leitlinien wird ausgeführt, dass der **DSB nicht über die Datenanwendung selbst bzw die Daten bestimmen darf** (*„conflict of interest"*). Das mag in einem großen Unternehmen mit breit angelegter Mitarbeiterstruktur durchaus möglich sein, man sollte hier allerdings auch auf die breite Masse der Unternehmer, KMU und EPU, ebenfalls Rücksicht nehmen, welche eine solche Vorgabe kaum erfüllen können. Eine derart weitgehende Interpretation des Interessenkonflikts macht es für KMU kaum leistbar, einen DSB zu bestellen. Fraglich ist auch, wie EPU hier vorzugehen haben - sind diese in jedem Fall verpflichtet, einen externen DSB oder einen Mitarbeiter zu engagieren? Und wenn ja, in welchem Ausmaß? Die Kosten, welche hierbei auf Unternehmen zukommen, sind massiv.

Rechtlich ist fragwürdig, ob der DSB tatsächlich das **Verfahrensverzeichnis** führen sollte bzw für Dokumentationspflichten verantwortlich sein sollte. Die Verzeichnisführung ist eine weitere Aufgabe des Verantwortlichen. Es wäre ja gerade mit einem Interessenkonflikt verbunden, wäre der DSB für dieses Verzeichnis verantwortlich, müsste aber andererseits den Verantwortlichen hierüber beraten (und bekommt beispielsweise anderslautende Anordnungen). Weder wäre er hier sodann weisungsfrei noch frei von Interessenkonflikten.

Es wird weiters ausgeführt, dass auch der DSB, welcher aufgrund eines **externen Dienstleistervertrages** agiert, nicht aufgrund seiner Tätigkeit benachteiligt werden darf (*„no unfair termination of service contract for activities as DPO"*). Das kann im Einzelfall naturgemäß Schwierigkeiten der Auslegung mit sich bringen, v.a. wann eine Kündigung als *„unfair"* einzuordnen ist. Weiters stellt dies einen massiven Eingriff in die Privatautonomie dar. Die Schutzbestimmung sollte wohl in erster Linie für Angestellte gelten, welche nun die Position des DSB zu bekleiden haben und nicht für externe Serviceleister. Auch hier möchten wir darauf verweisen, dass eine Weiterentwicklung der DSGVO durch die Artikel 29-Datenschutzgruppe nicht zulässig ist.

3. Identifizierung einer federführenden Aufsichtsbehörde (Artikel 51ff, insbesondere 56 DSGVO)

Zur Zuständigkeit der federführenden Aufsichtsbehörde bei grenzüberschreitenden Sachverhalten sei ganz allgemein darauf hingewiesen, dass die Leitlinien uE keine Hilfestellung bieten. Weder die Erläuterungen noch die „Checkliste" scheinen geeignet um in dieses sehr komplexe Verfahren Einblick zu gewähren. Ob KMU hier die Aufsichtsbehörde identifizieren können, erscheint äußerst fragwürdig. Die Artikel 29-Datenschutzgruppe ist eher dazu angehalten, den Prozess zur Erstellung von Binding Corporate Rules transparenter zu gestalten, hier Templates, welche auch tatsächlich von allen europäischen Aufsichtsbehörden zu akzeptieren sind, zu erstellen und in einer Sprache (zB zusätzlich zur Amtssprache auch Englisch) zu kommunizieren.

Mit der Bitte um Berücksichtigung der Anmerkungen und freundlichen Grüßen

[redacted]

Abteilungsleiterin