Stellungnahme der Deutschen Telekom AG zur Bewertung und Überprüfung der Datenschutz-Grundverordnung durch die EU-Kommission gem. Art. 97 DSGVO

Die Datenschutz-Grundverordnung hat im nicht-öffentlichen Bereich eine gute Grundlage für die Datenverarbeitung in der Europäischen Union auf Basis einheitlicher Regelungen geschaffen.

Die bisherigen Erfahrungen zeigen aber, dass die beabsichtigte Harmonisierung und das beabsichtigte „Level Playing Field“ gefährdet sind. Daher sind nach den Erfahrungen der Deutsche Telekom Gruppe Nachbesserungen in der Regulierung (I) und Verbesserungen bei der einheitlichen Anwendung der bestehenden Regelungen (II) notwendig.

I) Regulatorischer Handlungsbedarf

1) Fehlende Nutzung des Kohärenzmechanismus – fehlende einheitliche Rechtsanwendung

Forderung: Der Kohärenzmechanismus muss bei Angelegenheiten von allgemeiner Bedeutung oder mit Auswirkungen in mehr als einem Mitgliedstaat verpflichtend sein. Vom Dringlichkeitsverfahren gem. Art. 66 DSGVO muss stärker Gebrauch gemacht werden.

Sachverhalt: Unbestimmte Rechtsbegriffe werden von nationalen Aufsichtsbehörden unterschiedlich ausgelegt (z.B. Datenportabilität, Umfang Auskunftsersuchen, …). Das widerspricht dem Harmonisierungsziel der Datenschutz-Grundverordnung. Teilweise geben nationale Datenschutzaufsichtsbehörden Handlungsanweisungen heraus, ohne dass erkennbar ist, ob diese von Dauer sind oder ggf. noch das Kohärenzverfahren durchlaufen sollen und anschließend aufgehoben werden.

Problem: Die fehlende Berücksichtigung des Kohärenzmechanismus führt zur Rechtsunsicherheit bei Unternehmen und Bürgern. Zudem führt die unterschiedliche Auslegung zu erheblichen finanziellen Auswirkungen, da Geschäftsmodelle und Prozesse europaweit nicht einheitlich umgesetzt werden können.

Lösung: Art. 64 Abs. 2 DSGVO wird wie folgt gefasst:

*„Jede Aufsichtsbehörde, der Vorsitz des Ausschusses **s** oder die Kommission ~~können~~ beantragen **in angemessener Frist**, dass eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat vom Ausschuss geprüft wird, um eine Stellungnahme zu erhalten, insbesondere wenn eine zuständige Aufsichtsbehörde den Verpflichtungen zur Amtshilfe gemäß Artikel 61 oder zu gemeinsamen Maßnahmen gemäß Artikel 62 nicht nachkommt.“*

Zudem sollte von dem Dringlichkeitsverfahren gem. Art. 66 DSGVO stärker Gebrauch gemacht werden.

2) Unternehmensspezifische unterschiedliche Auslegung je nach Sitz des Unternehmens – einheitliche Durchsetzung

Forderung: Der Kohärenzmechanismus muss bei der Bewertung von vergleichbaren Geschäftsmodellen verschiedener Unternehmen mit Sitz in unterschiedlichen Mitgliedstaaten verpflichtend sein.

Sachverhalt: Bei der Durchsetzung der DSGVO müssen Aufsichtsbehörden nicht zwingend das Kohärenzverfahren nach Art. 63 ff. DSGVO durchlaufen, selbst wenn es sich um eine Angelegenheit von allgemeiner Bedeutung oder mit Auswirkungen in mehr als einem Mitgliedstaat handelt.

Problem: Es ist möglich, dass nationale Aufsichtsbehörden in ihrem jeweiligen Zuständigkeitsbereich Entscheidungen zur Durchsetzung der DSGVO treffen, die von Entscheidungen in anderen Mitgliedstaaten in vergleichbaren Sachverhalten abweichen. Das trifft vor allem unterschiedliche Unternehmen aus derselben Branche in verschiedenen Mitgliedstaaten (z.B. Internet Service Provider X wird in Land A anders behandelt als der Internet Service Provider Y in Land B). Dadurch wird das Harmonisierungsziel der Datenschutz-Grundverordnung gefährdet und erhebliche Rechtsunsicherheit für Unternehmen und Bürger geschaffen. Unterschiedliche Entscheidungen können erheblichen Einfluss auf die Wirtschaftlichkeit von Geschäftsmodellen haben und gefährden damit auch das angestrebte „Level Playing Field“.

Lösung: Art. 64 Abs. 2 DSGVO wird wie folgt gefasst:

*„Jede Aufsichtsbehörde, der Vorsitz des Ausschuss**es** oder die Kommission ~~können~~ beantragen **in angemessener Frist**, dass eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat vom Ausschuss geprüft wird, um eine Stellungnahme zu erhalten, insbesondere wenn eine zuständige Aufsichtsbehörde den Verpflichtungen zur Amtshilfe gemäß Artikel 61 oder zu gemeinsamen Maßnahmen gemäß Artikel 62 nicht nachkommt.“*

3) Umfang des Auskunftsanspruchs nach Artikel 15 DSGVO – Herausgabe von Unterlagen

Forderung: Klarstellung, dass Art. 15 DSGVO nur Auskunft zu den in Art. 15 DSGVO aufgeführten Informationen umfasst, nicht aber die Herausgabe von Kopien zugrundeliegender Dokumente verlangt werden kann.

Sachverhalt: Teilweise wird nicht nur Auskunft und Kopie der personenbezogenen Daten verlangt, die Gegenstand der Verarbeitung sind, sondern auch die Herausgabe von zugrundeliegenden Kopien der Originaldokumente verlangt.

Problem: Damit stellt sich die Frage der Abgrenzung gegenüber anderen Ansprüchen, wie etwa Art. 20 DSGVO sowie öffentlich-rechtlichen, strafrechtlichen, zivilrechtlichen und insbesondere arbeitsrechtlichen Herausgabeansprüchen von Dokumenten. Art. 15 DSGVO darf sich nicht zum allumfassenden und ersetzenden Auskunftsanspruch entwickeln. Damit würden Rechtsanforderungen und Abwägungsmechanismen, die bei anderen Auskunftsverfahren zur Anwendung kommen müssen, umgangen.

Lösung: in Erwägungsgrund 63 wird hinter Satz 6 folgender Satz eingefügt: *„Dieses Recht umfasst nicht die Herausgabe von Kopien von Originaldokumenten“.*

4) Umfang des Rechts auf Datenübertragbarkeit Art. 20

Forderung: Klarstellung, dass das Recht auf Datenübertragbarkeit keine Daten erfasst, die bei der Nutzung des Dienstes durch die betroffene Person automatisch vom Dienst erzeugt wurden (z.B. Logdateien, Verkehrs- oder Standortdaten).

Sachverhalt: Art. 20 DSGVO gibt der betroffenen Person das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

Problem: Durch aufsichtsbehördliche Vorgaben wird der Begriff „bereitgestellt“ sehr weit ausgelegt. Umfasst sind danach auch Daten, die z.B. bei der Erbringung eines Dienstes in einem IT-System oder z.B. in der Netztechnik eines Telekommunikationsnetzes anfallen. Diese Daten sind für den Betrieb eines Telekommunikationsnetzes erforderlich, sie werden aber nicht durch die betroffene Person zur Verfügung gestellt. Eine Herausgabe würde der betroffenen Person z.B. bei einem Anbieterwechsel keinerlei Nutzen bieten, bei dem Diensteanbieter aber erheblichen Aufwand erzeugen. Außerdem wird mit der weiten Auslegung außer Acht gelassen, dass sich der Gesetzgeber bewusst dafür entschieden hat, auf die von der betroffenen Person „bereitgestellten“ Daten abzustellen. Der Gesetzgeber hat sich im Gesetzgebungsverfahren ausdrücklich dagegen entschieden das Recht auf Datenübertragbarkeit auf alle verarbeiteten personenbezogenen Daten auszudehnen, unabhängig davon, ob sie von der betroffenen Person auch bereitgestellt wurden. Ausgangspunkt war die Ermöglichung des Datentransfers der „Historie“ von einem sozialen Netzwerk zu einem anderen.

Lösung: In Erwägungsgrund 68 wird nach Satz 1 folgender Satz eingefügt: *„Daten, die während der Nutzung eines Dienstes automatisch vom Dienst erzeugt werden und die Nebenprodukte der Nutzung des Dienstes sind (z.B. Logdateien, Verkehrs- oder Standortdaten), sind keine von der betroffenen Person bereitgestellte Daten.“*

5) Meldung von Datenschutzvorfällen

Forderung: Begrenzung meldepflichtiger Datenschutzvorfälle durch Einführung einer klaren Erheblichkeitsschwelle.

Sachverhalt: Aufgrund der veränderten gesetzlichen Definition eines Datenschutzvorfalls, der gesteigerten Mitarbeiter-Sensibilität in den Unternehmen und dem neuen Sanktionsrahmen der DSGVO ist die Anzahl der gemeldeten Vorfälle deutlich gestiegen. Eine Meldepflicht von Datenschutzvorfällen besteht nur dann nicht, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Problem: Die Anwendung des unbestimmten Rechtsbegriffs „Risiko“ führt zu erheblicher Rechtsunsicherheit. Zur Vermeidung von sanktionsbewehrten Fehlern werden im Zweifel alle Vorfälle gemeldet, unabhängig von dem mit einem Datenschutzvorfall potentiell verbundenen

Risiko. Die stark gestiegene Zahl der potentiell meldepflichtigen Vorgänge überlastet Unternehmen und Behörden, ohne den Datenschutz zu steigern.

Lösung: In Erwägungsgrund 85 wird nach Satz 2 folgender Satz aufgenommen: *„Von einem voraussichtlichen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen sollte ausgegangenen werden, wenn die Verletzung des Schutzes personenbezogener Daten besondere Arten personenbezogener Daten, personenbezogene Daten die einem Berufsgeheimnis unterliegen, personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, personenbezogene Daten zu Bank- oder Kreditkartenkonten oder Authentifizierungsdaten wie Passwörter oder vergleichbare nicht öffentlich zugängliche Kennungen betrifft."*

6) Medienbruch bei Datenschutzhinweisen

Forderung: Klarstellung, dass ein Medienbruch bei Datenschutzinformationen unter bestimmten Umständen erlaubt ist

Sachverhalt: Datenschutzinformationen müssen gem. Art. 13 DSGVO zum Zeitpunkt der Erhebung zur Verfügung gestellt werden. Die Informationen gem. Art. 13 DSGVO sind sehr umfassend.

Problem: Werden Daten z.B. bei einem telefonischen Vertragsabschluss aufgenommen, müssten in diesem Augenblick Datenschutzinformationen z.B. vorgelesen oder eine Bandabsage abgespielt werden. Da Art. 12 Abs. 1 DSGVO verlangt, diese Informationen in leicht zugänglicher Form zur Verfügung zu stellen, ist unklar, ob ein sogenannter Medienbruch, also ein Verweis auf z.B. Datenschutzhinweise im Internet zulässig ist.

Lösung: In Erwägungsgrund 58 wird nach Satz 1 folgender Satz eingefügt: *„Es sollte genügen, wenn diese Informationen nicht unmittelbar aber ohne Aufwand abrufbar sind."*

7) Verzeichnis der Kategorien der Verarbeitung Art. 30 Abs. 2 DSGVO

Forderung: Wird im Auftrag einer großen Zahl von Verantwortlichen (≥ 1000) die gleiche Kategorie von Verarbeitungen erbracht, genügt es, wenn zur Vervollständigung des Verzeichnisses gem. Art. 30 Abs. 2 DSGVO die vollständige Liste der Namen und Kontaktdaten der Verantwortlichen auf Anforderung der Aufsichtsbehörde in angemessener Frist vorgelegt wird.

Sachverhalt: Der Auftragsverarbeiter muss in einem Verzeichnis der Kategorien der Verarbeitung u.a. den Namen und die Kontaktdaten jedes Verantwortlichen aufführen, in dessen Auftrag die Verarbeitung durchgeführt wird.

Problem: Bei Massenmarktprodukten (z.B. Cloud Lösung für Geschäftskunden), muss für jeden einzelnen Kunden ein separater Eintrag in das Verzeichnis vorgenommen werden, während die Kategorie der Verarbeitung immer gleichbleibt. Zudem muss wegen des wechselnden Kundebestands das Verzeichnis fortlaufend angepasst werden. Das erzeugt u.U. mehrere Tausend Einträge für eine Kategorie der Verarbeitung. Das führt zu einer neben den Kundendatensystemen doppelten Datenhaltung die zudem fehleranfällig ist.

Lösung: In Erwägungsgrund 82 wird nach Satz 2 folgender Satz eingefügt: *„Sofern Datenverarbeitungskategorien für mehr als 1000 Verantwortliche zutreffen, ist es ausreichend, wenn der Auftragsverarbeiter die Angaben zu den Verantwortlichen auf Anfrage der zuständigen Aufsichtsbehörde in angemessener Frist zur Verfügung stellt“.*

8) Auftragsverarbeitung, Löschung oder Rückgabe von Daten, Art. 28 Abs. 3 g)

Forderung: In einem Vertrag über die Auftragsverarbeitung muss beim Wahlrecht des Verantwortlichen, ob nach Beendigung der Verarbeitung Daten zu löschen oder zurückzugeben sind, die technische Machbarkeit berücksichtigt werden.

Sachverhalt: In einem Vertrag über die Auftragsverarbeitung ist u.a. vorzusehen, dass der Auftragsverarbeiter nach Abschluss der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt und die vorhandenen Kopien löscht.

Problem: In bestimmten Fällen ist es aufgrund der technischen Realisierung der Verarbeitung nicht möglich, Daten wahlweise zu löschen oder zurückzugeben. Dennoch ist dieses Wahlrecht gem. Art. 28 Abs. 3 g) DSGVO in der Vereinbarung über die Auftragsverarbeitung aufzunehmen.

Lösung: Art. 28 Abs. 3g) wird wie folgt gefasst: *„nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen* ***unter Berücksichtigung der Art der Datenverarbeitung und der technischen Machbarkeit*** *entweder löscht oder zurückgibt und die vorhandenen Kopien löscht, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.“*

II) Einheitliche / angemessene Auslegung und Anwendung

1) Missbrauch des Auskunftsanspruchs nach Artikel 15 DSGVO

Forderung: Der missbräuchliche Anreiz zur Geltendmachung von Auskunftsrechten wird untersagt.

Sachverhalt: Auskunftsansprüche nach Artikel 15 DSGVO haben stark zugenommen. Seit dem 25. Mai haben sich die Anfragen bei der Deutschen Telekom verdoppelt, in der Einführungsphase sogar mehr als verdreifacht.

Problem: Ein erheblicher Teil der Auskunftsanfragen wird durch professioneller Anbieter erzeugt, die zur Geltendmachung von Auskunftsansprüchen motivieren. Diese Anbieter verfolgen häufig durch die Generierung einer möglichst hohen Anzahl von Auskunftsanfragen ein eigenes kommerzielles Interesse gegenüber dem Verantwortlichen.

Lösung: Stellungnahme des Europäischen Datenschutzausschusses, dass der durch Anbieter mit eigenen kommerziellen Interessen gesetzte Anreiz zur Geltendmachung von Auskunftsansprüchen ein Verstoß gegen das Prinzip der Datenvermeidung bzw. Datenminimierung darstellt, der zu untersagen ist.

2) Entwickelte Verfahrensweisen in Frage gestellt – Anonymisierung

Forderung: Die etablierte und bisher rechtlich zulässige Anonymisierung personenbezogener Daten zum Zweck ihrer weiteren Verarbeitung ist weiterhin möglich.

Sachverhalt: Bislang ist die Anonymisierung personenbezogener Daten zum Zweck der weiteren Verarbeitung dieser anonymen Daten etabliert und mit Datenschutzaufsichtsbehörden abgestimmt. Darauf basierende Geschäftsmodelle sind kommerziell erfolgreich.

Problem: Die Anonymisierung personenbezogener Daten zum Zweck der weiteren Verarbeitung dieser anonymen Daten wird wegen des angeblich neuen Verarbeitungsbegriffs der DSGVO in Zweifel gezogen. Dabei unterscheidet sich dieser Begriff nicht von der Definition in der Richtlinie 95/46 EG.

Lösung: Der Verarbeitungsbergriff des Art. 4 Nr. 2 DSGVO entspricht dem Verarbeitungsbegriff des Art. 2 b) der Richtlinie 95/46 EG. Der Europäische Datenschutzausschuss sollte klarstellen, dass eine unter der Richtlinie 95/46 EG zulässige Anonymisierung auch unter der DSGVO zulässig ist. Bislang etablierte Verfahrensweisen sollten mit Augenmaß überprüft und bei dieser Bewertung insbesondere eine Fortführung von Regelungen aus der Richtlinie 95/46 EG in der DSGVO berücksichtigt werden.

3) Klärung der Reichweite der Rechtsgrundlagen für die Verarbeitung

Forderung: Klärung der Reichweite der drei Rechtsgrundlagen, Erfüllung eines Vertrags, Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen und der Einwilligung sowie deren Verhältnis zueinander.

Sachverhalt: Derzeit werden personenbezogene Daten in vergleichbaren Situationen auf ganz unterschiedlichen Rechtsgrundlagen verarbeitet, abhängig von der Rechtsauffassung des jeweiligen Verantwortlichen. Eine Hilfestellung der Aufsichtsbehörden fehlt.

Problem: Die Verarbeitung personenbezogener Daten in vergleichbaren Situationen auf Basis unterschiedlicher Rechtsgrundlagen behindert die Harmonisierung im Rahmen der DSGVO und führt zu Rechtsunsicherheit für die Verantwortlichen. Je nach Rechtsgrund müssen die Verantwortlichen sehr unterschiedliche Anforderungen an die Verarbeitung berücksichtigen. Es ist unklar, wo der Zweck der Verarbeitung endet, der durch die Rechtsgrundlage „Erfüllung eines Vertrags“ abgedeckt ist und die Notwendigkeit einer neuen Rechtsgrundlage wie der Einwilligung oder der Wahrung berechtigter Interessen des Verantwortlichen beginnt.

Lösung: Leitlinien des Europäischen Datenschutzausschusses, die den Verantwortlichen Hilfestellungen zur Reichweite der in der DSGVO vorgesehenen Rechtsgrundlagen für die Verarbeitung geben, insbesondere für die Erfüllung eines Vertrags, die Verarbeitung zum Zweck der Wahrung der berechtigten Interessen sowie der Einwilligung.