

Telefónica Positionspapier zum Vorschlag über die e-Privacy-Verordnung (ePV)

Daten sind ein zentrales Element der digitalen Wirtschaft, die durch Massendaten (Big Data) und datengetriebene Dienste und Unternehmen die Branche und die Gesellschaft als Ganzes grundlegend verändert. Damit die Bürger und Unternehmen in Europa von diesem Wandel in maximaler Weise profitieren, bedarf es sinnvoller und konsistenter rechtlicher Rahmenbedingungen. Diese sollten das Grundrecht auf Vertraulichkeit der Kommunikation und Datenschutz sowie das Erfordernis von Innovation und der Entwicklung wegweisender Dienste in der Europäischen Union in ein angemessenes Gleichgewicht bringen.

Die DSGVO schafft einen adäquaten, technisch neutralen und zukunftssicheren **Datenschutzrahmen, innerhalb dessen alle Industriezweige innovative Dienste entwickeln können, während gleichzeitig ein hohes Maß an Verbraucher- und Datenschutz über die verschiedenen Akteure hinweg gewährleistet ist**, die in der datengetriebenen Wirtschaft tätig sind. **Die DSGVO beinhaltet wichtige Schutzmechanismen** wie transparente Informationen, Widerspruchsrecht und die Möglichkeit zum jederzeitigen Widerruf der Einwilligung, das Erfordernis so genannter Datenschutzfolgenabschätzungen sowie äußerst abschreckende Sanktionen gegenüber Unternehmen, die gegen Vorschriften verstoßen. Dies gilt nicht nur für Telekommunikationsbetreiber, sondern für alle Akteure der digitalen Wirtschaft.

Die vorgeschlagene e-Privacy-Verordnung (ePV) aktualisiert die e-Privacy-Richtlinie und soll das **Recht auf Vertraulichkeit der Kommunikation gewährleisten**. Die **Telekommunikationsbranche hat sich diesem Ziel stets fest verschrieben** und sich mit außergewöhnlich großem Engagement für dessen Erreichung eingesetzt. Telefónica ist der festen Überzeugung, dass die Stärkung und Erweiterung der Pflichten zur Wahrung der Vertraulichkeit auf die gesamte interpersonelle Kommunikation – also über die traditionellen Telekommunikationsdienste hinaus und unter Einbezug von OTT-Diensten – für einen besseren Datenschutz bei der Bereitstellung elektronischer Kommunikationsdienste, wo OTT- und Telekommunikationsanbieter dieselbe Rolle spielen, definitiv ein Schritt in die richtige Richtung sind.

Telefónica ist im Gegenteil der Ansicht, dass der ursprüngliche ePV-Vorschlag der Kommission **für den aktuellen Datenschutzrahmen lediglich Verwirrung bringt**. Dabei stellt Telefónica nicht den Grundsatz der Vertraulichkeit der Kommunikation infrage, sondern die **strikte Behandlung von Verkehrs- und Standortdaten**, bei welcher der ePV-Vorschlag – obwohl es sich per definitionem der DSGVO um „personenbezogene Daten“ handelt – von den in der DSGVO verankerten Rechtsgrundlagen für die Verarbeitung personenbezogener Daten abweicht.

Als Lex specialis soll die ePV die DSGVO ergänzen und nicht für eine unnötige Duplizierung oder, noch schlimmer, für Widersprüche zwischen beiden Instrumenten sorgen. Dennoch berücksichtigt der **ePV-Vorschlag weder den durch die DSGVO gegebenen ausgewogenen Rechtsrahmen noch das Erfordernis von für alle Branchensektoren gleichen Wettbewerbsbedingungen bei der Bereitstellung von Big Data und datengetriebenen Diensten**. Anstatt eine umfassende Abstimmung mit der DSGVO anzustreben, erhält die ePV eine regulatorische Asymmetrie aufrecht, die in datengetriebenen Märkten gleiche Wettbewerbsbedingungen zwischen digitalen Anbietern und Telekommunikationsbetreibern verhindert.

Dieses inkonsistente Datenschutzsystem muss im Kontext der Wettbewerbsfähigkeit der europäischen Industrie neu ausgerichtet werden.

Nach dem **ePV-Vorschlag ist die Verarbeitung von Metadaten (Verkehrs- und Standortdaten) ausschließlich nach vorheriger Einwilligung oder vollständiger Anonymisierung gestattet, wobei nur eine sehr begrenzte Zahl von Ausnahmen eingeräumt werden**, die in keiner Weise ausreichend oder zukunftssicher sind. Die ePV sollte auf der neuen DSGVO und nicht auf der alten e-Privacy-Richtlinie aufbauen. Die DSGVO führt neue Konzepte ein (z. B. Rechenschaftspflicht und risikobasierter Ansatz), die in der ePV in keiner Weise berücksichtigt sind. Das ist zusammen mit einer eng gehaltenen Liste von Ausnahmen, nach denen eine Verarbeitung zulässig ist, ein Rückschritt in die Vergangenheit. Damit sind von vornherein zahllose Optionen ausgeschlossen, die sich Telekommunikationsbetreibern ansonsten künftig bieten würden. Tatsächlich ist die Verarbeitung von Metadaten zu vielen eingriffsfreien Zwecken ohne Folgen für die Privatsphäre von Personen möglich, wie bereits im Rahmen der DSGVO anerkannt (z. B. Steigerung der Servicequalität, Netzwerkoptimierung), und würden Nutzer nach vernünftigen Maßstäben erwarten („vernünftige Erwartungen“ gemäß DSGVO), dass ihre Kommunikationsanbieter eine solche Verarbeitung vornehmen. Der ePV-Vorschlag jedoch **bricht mit dem mit der DSGVO erreichten ausgewogenen Ansatz zwischen Innovation und Verbraucherschutz**. Der ePV-Vorschlag gefährdet den Spielraum der Telekommunikationsanbieter, im Zusammenhang mit Big Data- und datengetriebenen Diensten innovative Leistungen zu entwickeln und einzuführen, und überlässt dies in Europa damit ausschließlich anderen Internet-Akteuren, die nicht unter die Bestimmungen der ePV fallen (OTT, wenn sie keine elektronischen Kommunikationsdienste bereitstellen). Das schwache Mandat, welches das Europäische Parlament – ohne Unterstützung der EVP – dem LIBE-Ausschuss erteilt hat, um das Mitentscheidungsverfahren voranzubringen und die Trilog-Verhandlungen mit dem Rat aufzunehmen, sowie die Konsensschwierigkeiten innerhalb des Rates sind klare Signale für die äußerst kontroversen Haltungen zur ePV.

Wenn es der politische Wille der europäischen Mitgesetzgeber ist, ein eigenständiges Rechtsinstrument für e-Privacy aufrechtzuerhalten, dann sollte dies als **Chance für eine bessere Regulierung und zur Vereinfachung sowie zur Erreichung konsistenter Datenschutzrahmenbedingungen** zum Vorteil der europäischen Industrie und der europäischen Verbraucher betrachtet werden. Die Inkonsistenzen zwischen der DSGVO und der künftigen ePV sollten ausgeräumt werden. Blindes Vertrauen auf die Einwilligung ist nicht die richtige Antwort. **Im Hinblick auf die Zukunft der ePV sollten auch andere Rechtsgründe für die Verarbeitung von Metadaten berücksichtigt werden, wie sie bereits in der DSGVO enthalten sind**: Erfüllung eines Vertrags, Einhaltung einer Rechtspflicht, Schutz der grundlegenden Interessen der betroffenen Person, Verarbeitung zum Zwecke der Wahrung

der berechtigten Interessen. Sehr wichtig ist auch die Anerkennung des Grundsatzes der Vereinbarkeit der Weiterverarbeitung.

Eine **umfassende Abstimmung zwischen DSGVO und ePV ist daher unverzichtbar, um die nötige Flexibilität zu schaffen**, damit europäische Telekommunikationsbetreiber im Bereich der datengetriebenen Dienste innovativ sein und gleichzeitig ein hohes Maß an Datenschutz gewährleisten können.

Gefährdete Dienste

Ohne Abstimmung durch wesentliche Änderungen am ePV-Vorschlag wird Telekommunikationsanbietern die Einführung einer Vielzahl neuer Dienste verwehrt sein, die von großem gesellschaftlichem Nutzen sind. Dazu gehören Folgende:

- **Cybersicherheit, Betrugsbekämpfung im Zusammenhang mit Betreiberdiensten und Dritten** (Banken, Versicherungsunternehmen, Zahlungsdienstleister). Die Betrugsbekämpfung geht über die Rechnungsstellung hinaus (bereits durch den ePV-Vorschlag anerkannt). Die DSGVO räumt explizit ein, dass die Gewährleistung der Netzwerk- und Informationssicherheit ein berechtigtes Interesse ist. Darüber hinaus erkennt sie auch das berechtigte Interesse des Verantwortlichen oder von Dritten an. Macht ein Telekommunikationsbetreiber beispielsweise verdächtige IP-Adressen aus, könnte er diese Informationen nicht nur an die Bank weitergeben, die Gegenstand des Angriffs ist, sondern zur Vermeidung weiterer Attacken auch an andere Parteien.
- **Datenverarbeitung zur Anonymisierung** inklusive der Weitergabe von Daten an Dritte, die Anonymisierungsmaßnahmen durchführen. Die Anonymisierung von Daten stellt an sich bereits eine Verarbeitung von Daten dar, doch besteht auch für die Weitergabe solcher Daten ein berechtigtes Interesse (um jedes Risiko einer Identifikation zu vermeiden).
- **Weitergabe pseudonymer Daten für den Ausbau von Datenmodellen.** Beispiel: Algorithmen zur Erstellung von Bonitätsbewertungen. Will ein Anbieter ein Prognosemodell entwickeln, muss er diese Modelle sondieren/testen, und dazu ist die Verarbeitung pseudonymer Daten erforderlich. Dies entspräche einem berechtigten Interesse im Sinne der DSGVO.
- **Verarbeitung von pseudonymen Daten für Forschungs- und Innovationsprojekte.** Die DSGVO erwähnt wissenschaftliche Forschungszwecke, die ePV jedoch nicht.
- **Business-Intelligence-Analysen, Nutzersegmentierung, Netzwerkdimensionierung.** Dies entspräche einem berechtigten Interesse im Sinne der DSGVO.
- **Verarbeitung von pseudonymen Daten zur Erlangung aggregierter und statistischer Einblicke.** Die DSGVO erwähnt statistische Zwecke, die ePV jedoch nicht.
- **Weitergabe von Daten zwischen Konzernunternehmen.** Die DSGVO erkennt das berechtigte Interesse der Weitergabe personenbezogener Daten innerhalb einer Unternehmensgruppe an. Das betrifft auch personenbezogene Daten von Kunden oder Mitarbeitern.

Der Vorschlag von Telefónica zur Erreichung der erforderlichen Abstimmung mit der DSGVO hat zwei Ansätze:

1. Aufnahme des berechtigten Interesses als Rechtsgrundlage für die Verarbeitung

Die künftige ePV sollte das berechtigte Interesse entsprechend der DSGVO als zusätzliche Rechtsgrundlage für die Verarbeitung anerkennen, wenn eine solche Verarbeitung im Zusammenhang mit den berechtigten Interessen des Anbieters oder eines Dritten erforderlich ist.

Ebenfalls in Übereinstimmung mit der DSGVO, außer in Fällen, in denen solchen Interessen die Interessen oder Grundrechte und -freiheiten der betroffenen Person übergeordnet werden, die den Schutz personenbezogener Daten verlangen.

Die DSGVO erlaubt es dem/verpflichtet den Verantwortlichen, eine gründliche Beurteilung vorzunehmen und dabei seine Interessen gegenüber den Interessen und Grundrechten der betroffenen Person abzuwägen. Das bedeutet, dass der Verantwortliche die Daten nicht verarbeiten kann, wenn die Interessen der betroffenen Person stärker wiegen als seine Interessen.

Die ePV dagegen lässt nicht einmal eine Prüfung der Legitimität der Interessen zu, während es offensichtlich ist, dass die Abwägung von Interessen im Fall von Metadaten zu unterschiedlichen Fazits führen könnte, dies jedoch stets abhängig von einer Prüfung der Umstände im Einzelfall.

Mit der Anerkennung berechtigter Interessen als Rechtsgrundlage für die Verarbeitung werden Telekommunikationsbetreiber in der Lage sein, die vorstehend aufgezählten Dienste anzubieten, die jetzt in Gefahr sind.

Entsprechend beantragen einige Mitgliedsstaaten in Gesprächen mit der AG des Rates die Anerkennung des berechtigten Interesses, um bei gleichzeitiger Wahrung des Datenschutzes für Endnutzer mehr Flexibilität zu erhalten (Spanien, Finnland, Dänemark, Irland, Belgien, Polen).

2. Aufnahme des Grundsatzes der Vereinbarkeit der Weiterverarbeitung

Nach Artikel 6 Absatz 4 der DSGVO gilt ferner der Grundsatz, dass eine sekundäre Verarbeitung dadurch legitimiert wird, dass die ursprüngliche Verarbeitung bereits ihre eigene Rechtsgrundlage hatte. Tatsächlich sollten Netzwerk- und Dienstanbieter in Fällen, in denen die Verarbeitung zu einem anderen Zweck als dem, zu dem die Metadaten ursprünglich erfasst wurden, nicht auf einer Einwilligung beruht (z. B. Übertragung der Kommunikation, Sicherheit, Rechnungsstellung), die Metadaten elektronischer Kommunikation verarbeiten dürfen, wenn diese Weiter-/Sekundärverarbeitung vereinbar mit dem Zweck ist, zu dem die Daten ursprünglich erfasst wurden, und wenn zweckmäßige Sicherheitsmaßnahmen wie eine Pseudonymisierung durchgeführt wurden.

Bei der Feststellung, ob die Verarbeitung für einen anderen Zweck vereinbar ist mit dem ursprünglichen Zweck, würde der Anbieter der elektronischen Kommunikation die strengen Kriterien aus Artikel 6 Absatz 4 der DSGVO anwenden. Dazu gehört u. a. Folgendes:

- jeder Zusammenhang zwischen den Zwecken, zu denen die personenbezogenen Daten erfasst wurden, und den Zwecken der vorgesehenen Weiterverarbeitung;
- der Kontext, in dem die personenbezogenen Daten erfasst wurden, insbesondere im Hinblick auf die Beziehung zwischen den betroffenen Personen und dem Verantwortlichen;
- die Art der personenbezogenen Daten;
- die möglichen Konsequenzen der vorgesehenen Weiterverarbeitung für betroffene Personen;
- die **Existenz zweckmäßiger Schutzmaßnahmen wie der Pseudonymisierung.**

Pseudonymisierung ist ein grundlegendes Hilfsmittel für die Entwicklung von Big Data-Diensten und würde es **Telekommunikationsanbietern ermöglichen, wettbewerbstechnisch auf Augenhöhe mit anderen digitalen Anbietern zu agieren.** Sie ist für die Bereitstellung und Entwicklung zahlreicher innovativer digitaler Dienste unverzichtbar. Bei der politischen Einigung über die DSGVO zwischen dem Rat und dem Europäischen Parlament im Dezember 2015 stellte die Europäische Kommission Folgendes fest: „...Pseudonymisierung [wird] gefördert, um die Vorteile von massendatenbezogenen Innovationen bei gleichzeitigem Schutz der Privatsphäre nutzen zu können“ (http://europa.eu/rapid/press-release_IP-15-6321_de.htm).

Kriterien für eine vereinbare Weiterverarbeitung sollten in der künftigen ePV eine ebenso zentrale Rolle spielen wie in der DSGVO.

Mit Blick auf alle vorstehenden Erwägungen **bittet Telefónica die europäischen Mitgesetzgeber, das Erfordernis einer zweckmäßigen Abstimmung zwischen der DSGVO und der ePV sorgfältig abzuwägen, um Telekommunikationsunternehmen nicht die Möglichkeiten zu nehmen, wettbewerbsfähige und innovative Big Data- und datengetriebene Dienste in Europa zum Vorteil der europäischen Nutzer und der Gesellschaft als Ganzes zu entwickeln.**