LANDTAG
NORDRHEIN-WESTFALEN
17. WAHLPERIODE
NEUDRUCK
STELLUNGNAHME
17/290
Alle Abg

Stellungnahme der Deutschen Telekom anlässlich der Anhörung des Ausschusses für Digitalisierung und Innovation - "Hohe Datenschutzstandards sicherstellen – Wirtschaft bei Umsetzung der Europäischen Datenschutzreform unterstützen!"

Erreichte Harmonisierung bewahren

Die Datenschutz-Grundverordnung hat im nicht-öffentlichen Bereich eine gute Grundlage für die Datenverarbeitung in der Europäischen Union auf Basis einheitlicher Regelungen geschaffen. Der EU-Gesetzgeber hat sich sehr bewusst und nach ausführlichen Abwägungen für die Einführung einer unmittelbar in den Mitgliedstaaten der Europäischen Union geltenden Verordnung entschieden. Der mit der Datenschutz-Grundverordnung erreichte Grad der Harmonisierung sollte bewahrt und nationale Regelungen nur dort getroffen werden, wo diese zwingend erforderlich sind. Das auf europäischer Ebene für international tätige Unternehmen wichtige „Level Playing Field" darf nicht durch nationale oder gar regionale Alleingänge gefährdet werden. Vor diesem Hintergrund muss die Datenschutz-Grundverordnung zunächst anhand und mit diesen Regelungszielen umgesetzt und evaluiert werden, bevor ergänzende nationale Gesetze beschlossen werden. Dies muss auch im übergreifenden Dialog zwischen Aufsichtsbehörden, Wirtschaftsunternehmen und Verbrauchervertretern erfolgen.

Für eine rechtssichere Anwendung der Datenschutz-Grundverordnung sollte darüber hinaus ein gemeinsames Verständnis über zentrale Rechtsbegriffe und typische Datenverarbeitungen geschaffen werden. Hierzu zählt insbesondere die Erarbeitung einheitlicher und sicherer Grundlagen für die Pseudonymisierung personenbezogener Daten. Eine gute Diskussionsgrundlage hat die „Fokusgruppe Datenschutz" des IT-Gipfels mit dem Whitepaper zur Pseudonymisierung vorgelegt (https://www.gdd.de/downloads/whitepaper-zur-pseudonymisierung).

Sektorspezifische Regulierung vermeiden

Die Deutsche Telekom spricht sich gegen sektorspezifische Sonderregelungen für elektronische Kommunikationsdienste aus. Mit der Datenschutz-Grundverordnung wurde ein Instrument für ein europaweit einheitliches hohes Datenschutzniveau geschaffen. Die Datenschutz-Grundverordnung ist technologieneutral und bietet mit ihrem risikobasierten Ansatz eine gute datenschutzrechtliche Grundlage, die für sämtliche Marktteilnehmer in der Europäischen Union einheitliche Regeln schafft. Ein über den Schutz der Vertraulichkeit der elektronischen Kommunikation hinausgehender Regelungsbedarf besteht daher nicht.

Der von der Europäischen Kommission vorgelegte Verordnungsentwurf über Privatsphäre und elektronische Kommunikation (ePrivacy Verordnung) würde in seiner jetzigen Ausgestaltung die in der Datenschutz-Grundverordnung sorgfältig ausgewogene Balance zwischen dem Schutz personenbezogener Daten und der Ermöglichung innovativer Geschäftsmodelle stark gefährden, indem unter der Datenschutz-Grundverordnung zulässige Verarbeitungsmodelle entweder unter strengere Auflagen gestellt oder gänzlich verboten werden. Die in der Datenschutz-Grundverordnung gefundenen Ansätze für eine flexible Datenverarbeitung unter gleichzeitiger Wahrung eines hohen Datenschutzniveaus würden damit konterkariert. Dies würde den Aufbau einer europäischen digitalen Datenwirtschaft maßgeblich erschweren und damit der Strategie eines digitalen Binnenmarkts zuwiderlaufen.

Vor diesem Hintergrund bedarf es einer grundlegenden Überarbeitung des vorliegenden Kommissionsvorschlags. Insbesondere muss im Einklang mit der Datenschutz-Grundverordnung die Weiterverarbeitung von Metadaten auch ohne vorherige Einwilligung möglich sein, wenn der neue Verarbeitungszweck kompatibel und damit mit dem ursprünglichen Erhebungszweck vereinbar ist. Bei der Ermittlung der Kompatibilität der Weiterverarbeitung nach der Datenschutz-Grundverordnung spielt die Anwendung geeigneter Schutzmaßnahmen wie Pseudonymisierung und Verschlüsselung eine hervorgehobene Rolle. Wie verschiedene Anwendungsbeispiele zeigen, könnten damit für den Verbraucher nützliche Dienstleistungsmodelle geschaffen werden, die mit anonymen Informationen nicht möglich sind (Anlage „Anwendungsbeispiele für pseudonymisierte Datenverarbeitung im Telekommunikationsumfeld“).

Ferner unterfallen Standortdaten aus elektronischer Kommunikation der ePrivacy Verordnung, während sonstige Standortdaten basierend auf GPS, die wesentlich genauer ausfallen als Standortdaten aus der elektronischen Kommunikation, der Datenschutz-Grundverordnung unterliegen. Diese ungleiche Behandlung der gleichen Art von Daten (Standortdaten) verhindert das in Europa angestrebte „Level Playing Field“. Sektorspezifische strengere Regelungen für den Telekommunikations-Sektor sollten daher aufgehoben werden. An dieser Stelle ergibt sich ein unmittelbarer politischer Handlungsdruck ggü. der geschäftsführenden Bundesregierung, aber auch ggü. den Institutionen der Europäischen Union, welcher auch aus landespolitischer Sicht stimuliert werden kann.

„Datenstandort NRW“

Darüber hinausgehend können und sollten für konkrete neue Geschäftsmodelle, welche sich vor allem durch eine entsprechende, im Sinne der nachhaltigen Entwicklung des Digitalstandorts Nordrhein-Westfalen förderliche, Innovationsdynamik auszeichnen, Testräume geschaffen werden. In diesen können Wirtschaft, Politik und Aufsichtsbehörden gemeinsam den datenschutzrechtlichen Schutzbedarf ermitteln sowie mögliche Maßnahmen, um selbige einzuhalten, entwickeln – dies soll und kann wie oben bereits dargelegt auch mittels technischer Schutzmechanismen wie einer guten Pseudonymisierung erfolgen. Hier kann und sollte Nordrhein-Westfalen gerade angesichts seiner bundespolitischen Stellung als Vorreiter agieren. Gewonnene Erkenntnisse müssen anschließend wieder auf eine europäische Ebene gehoben werden, um eine einheitliche Anwendung der Datenschutz-Grundverordnung durch den Europäischen-Datenschutzausschuss, die Unternehmen aber auch etwaige Zertifizierungsstellen und sonstige Rechtsanwender zu gewährleisten.

Anwendungsbeispiele für pseudonymisierte Datenverarbeitung im Telekommunikationsumfeld

Zusammengefasst:

Bei verschiedenen Dienstleistungsmodellen, die dem Verbraucher nützlich sein können, kann wegen fehlender Zuordenbarkeit nicht mit anonymen Informationen gearbeitet werden. Andererseits brauchen diese Dienstleistungen für möglichst verlässliche Aussagen einen möglichst großen Datenpool, mit dem sie arbeiten können. Hierfür ist eine pseudonymisierte Datenverarbeitung erforderlich.

Beispiele

Bessere Versorgung mit eTankstellen:

Wenn ein Anbieter von Elektrotankstellen sein Netz mit Ladestationen effizient ausbauen will, benötigt er Informationen darüber, wie viele Elektrofahrzeuge auf bestimmten Strecken fahren. Erforderlich sind insbesondere Informationen darüber, in welchen Bewegungsrichtungen Elektrofahrzeuge fahren und ob die Menge der Fahrzeuge zunimmt. Diese Informationen können mit anonymen Daten nicht gewonnen werden.

Soweit die Elektrofahrzeuge mit Mobilfunk SIM-Karten ausgestattet sind, können Standortinformationen aus Mobilfunkzellen die Bewegungsverläufe von Elektrofahrzeugen auf diesen Strecken mit einem pseudonymen Identifier nachvollziehen. Können auf Autobahnen gegebenenfalls noch in standardisierten Abständen eTankstellen angelegt werden, so können solche Annahmen in ländlichen Regionen nicht zugrunde gelegt werden. Dort ist nicht prognostizierbar, wie genau die Bewegungsabläufe der Fahrzeuge sein werden. Gerade in den ländlichen Regionen ist der Handlungsbedarf für eTankstellen aber gegeben. Außerdem ermöglicht der pseudonyme Identifier die Unterscheidung, ob dasselbe Fahrzeug die gleiche Strecke fährt, oder ob es unterschiedliche sind. Ob die Strecke mehrfach oder nur einmal genutzt wird.

Um zu verlässlichen Werten zu kommen, sind für diese Zwecke alle Elektrofahrzeuge zu erfassen. Das ist mit pseudonymen Daten möglich. Durch technisch/organisatorische Maßnahmen kann eine hohe Sicherheit der Daten gewährleistet werden.

Parkleitsysteme, verbesserte Parkplatzsuche

Reisenden kann in Innenstadtbereichen ein Verkehrs- und Parkplatzleitsystem angeboten werden, das Empfehlungen an mobile Endgeräte oder Fahrzeuge mit SIM-Karte versenden kann. Dazu werden die Standortdaten der Fahrer aus den Mobilfunkzellen im Innenstadtbereich mit Informationen über freie Parkplätze zusammengeführt. Bei den Standortinformationen der Fahrer werden lediglich die Pseudonyme der Geräte verwendet, die sich im betreffenden Innenstadtbereich bewegen. Die Fahrer können dann individuell in Echtzeit zu einem freien Parkplatz geleitet werden.

Darüber hinaus könnte diese Technik auch eine sehr viel genauere Verkehrsleitung ermöglichen und dadurch Feinstaub und CO2-Ausstoß reduzieren helfen. Das käme nicht nur der Natur und der Gesundheit des Menschen zugute; auch Staus könnten deutlich reduziert werden. Bei nur anonym vorliegenden Informationen wäre die Einzelzuordnung nicht möglich und damit auch keine Verkehrsbewegung darstellbar. Eine Einwilligung unter Verwendung von Klardaten ist für den Dienst nicht erforderlich; es wäre aber auch nicht ausreichend, nur mit den

einwilligungsbasierten Informationen zu arbeiten. Nur mit Einwilligungen erreicht man keine ausreichende Menge an Daten für einen solchen Service. Für ein verlässliches Leitsystem muss möglichst der tatsächliche Verkehrsfluss im Innenstadtbereich zugrunde gelegt werden.

Bessere Verbindungen mit der Bahn

Derzeit weiß die Deutsche Bahn nicht, wie viele Fahrgäste sich in jedem Regionalzug befinden. Im Falle einer Verspätung kann es vorkommen, dass ein Zug voller Fahrgäste eine Verbindung zum anderen Zug/Bus verpasst, der pünktlich abfährt. Durch die Verwendung von Standortinformationen der Reisenden aus den Mobilfunkzellen entlang der Bahnstrecke erhält die Bahn ein präzises Bild über die Auslastung einzelner Züge. Dafür genügen Pseudonyme, Klardaten sind nicht erforderlich.

Mit pseudonymen Echtzeitdaten könnte die Bahn z.B. den Anschlusszug / Bus zurückhalten, um den meisten Fahrgästen auch im Falle einer Verspätung die beste Verbindung zu bieten. Auch könnte die Bahn auf Grundlage genauer Auslastungs-Informationen eine viel genauere Streckenplanung vornehmen. Anonyme Informationen sind in diesem Zusammenhang zu ungenau, da sie nur auf aggregierte Datensätze von mindestens 30 bzw. 50 Personen im Cluster zugreifen können. Wären also bei einer für eine anonyme Verarbeitung erforderlichen Mindestzahl von 50 Personen nur 49 Personen in einem Zug, könnte dies nicht erkannt und damit der Anschlussverbindung nicht zurückgehalten werden.

Verbesserte Reiseangebote

Um bessere Angebote z.B. durch Öffentliche Verkehrsmittel anbieten zu können, ist eine Analyse von Bewegungsrichtungen zwischen Städten / Regionen einschließlich der Anzahl der Personen erforderlich. Diese Bewegungsrichtungen und Mengen werden aus den Standortinformationen aus den Mobilfunkzellen gewonnen.

Anonyme Informationen sind in diesem Zusammenhang zu ungenau, da sie nur auf aggregierte Datensätze von mindesten 30 bzw. 50 Personen im Cluster zugreifen können. Anbieter öffentlicher Verkehrsmittel können auf der Basis pseudonymer Daten kosteneffiziente Angebote für den Schienenverkehr und Regionalbusse anbieten, die mit dem Luftverkehr und Privatfahrzeugen konkurrieren. Die gegenwärtige langfristige Planung der Verkehrsinfrastruktur basiert auf Bedarfsschätzungen. Diese geschätzten Daten sind nicht präzise genug.

Bedarfsgerechte TV Programmgestaltung

Moderne TV Plattformen bieten die Möglichkeit, über pseudonyme Daten die Programmauswahl der TV Zuschauer zu analysieren. Auf dieser Basis können TV Programme bedarfsgerecht gestaltet und produziert oder weniger erfolgreiche Formate aus dem Programm genommen werden. Ohne diese Information wird die Programmgestaltung durch die Sendeanstalten ohne Berücksichtigung des Gesamtbildes der Verbraucherinteressen, z.B. auf Grundlage einer Befragung von kleinen Personengruppen, vorgenommen. Die Verwendung von Klardaten ist dazu nicht erforderlich.

Die Verwendung von Pseudonymen Daten verhindert, dass die individuelle Programmauswahl und damit die TV-Gewohnheiten einzelnen Personen konkret zugeordnet werden können. Es bedarf aber einer Gesamtbetrachtung (kritische Masse), um verlässliche Ergebnisse zu erhalten. Die Auswertung der Daten von einigen Einwilligungen ist dafür nicht geeignet.

Möglich sind auch Filmvorschläge aufgrund des bisherigen TV Verhaltens unter Verwendung von Pseudonym. Auch in diesem Fall sind die Vorschläge dem Nutzer nicht namentlich zuordenbar.

Sichere Angebote im Gesundheitsbereich, Telemonitoring

Im Gesundheitsbereich gibt es zunehmend Dienste, bei denen Patienten ihre Gesundheitswerte in Echtzeit durch mobile Verbindungen überwachen lassen (müssen). Bei diesen Diensten ist eine hohe Verfügbarkeit der Mobilfunkverbindungen unerlässlich. Die Verfügbarkeit der Mobilfunkverbindungen kann durch eine regelmäßige Überprüfung mit pseudonymen Daten überwacht und sichergestellt werden. Klardaten sind dazu nicht erforderlich. Anonyme Daten sind naturgemäß nicht ausreichend, weil eine Zuordnung des Mobilfunkanschlusses nicht erfolgen kann. In diesen Fällen kann auch nicht das Auftreten eines Fehlers „abgewartet werden", wie dies der Entwurf der ePrivacy Verordnung heute vorsieht.

Bessere Preisgestaltung gegenüber Kunden

Das Netz ist regional und zu bestimmten Uhrzeiten unterschiedlich ausgelastet. Damit könnten dynamische Tarifierungen und damit Preissenkungen in Abhängigkeit von der Netzauslastung in bestimmten Regionen angeboten werden. So wie der Strompreis regional und zeitabhängig schwankt, so kann auch die Netzauslastung in einzelnen Regionen als Parameter der Tarifierung genutzt und Preisvorteile für den Kunden angeboten werden.

Die Kunden in dem jeweiligen Netzbereich erhalten dann unter Pseudonym ein günstiges Angebot bei schwacher Netzauslastung. Bei der Verwendung anonymer Netzauslastungsinformationen können die einzelnen Kunden nicht für die Angebote in dem jeweiligen Netzbereich adressiert werden, da nicht bekannt ist, in welchem Netzbereich sie sich befinden.

Weitere Anwendungsfälle

Die gesetzlichen Weiterverarbeitungstatbestände der ePrivacy Verordnung sind auf Fälle der Sicherheit und Betriebsstörungen etc. im Zusammenhang mit den Kommunikationsdienstleistungen bezogen. Nicht abgedeckt sind dabei u.E. auch folgende Fallgruppen:

Unfallvermeidung

Zusammenführung von Standortdaten aus Fahrzeugen, so dass Gefahrensituation prognostiziert werden können, die aus der Kombination Autofahrer / Fußgänger / Fahrradfahrer entstehen könnten.

Von Autosensoren erfasste Straßenschäden i.v.m. Mobilfunk Standortdaten können zur Unfallvermeidung genutzt werden. Klardaten sind in diesen Fällen nicht erforderlich, aber Pseudonyme.

Information über Ereignisse in der näheren Umgebung

Benachrichtigung von Endkunden, wenn in räumlicher Nähe ihres Aufenthaltsbereichs eine Umweltbelastung, ein Terrorakt oder eine Naturkatastrophe stattfindet.