Stellungnahme

Vorschlag für eine E-Privacy-Verordnung – Verhandlungen im Rat der Europäischen Union

Bundesverband der Deutschen Industrie e.V.

Stand: 30.05.2018

Kernforderungen

- Der Vorschlag für eine E-Privacy-Verordnung (E-Privacy-VO) muss kohärent mit der EU-Datenschutz-Grundverordnung (DS-GVO) sein. Überschneidungen mit der DS-GVO müssen aufgehoben werden.

- Die deutsche Industrie warnt eindringlich vor einer zusätzlichen Verschärfung des Datenrechts. Es ist dringend mehr Flexibilität im Sinne eines risikobasierten Ansatzes nach dem Vorbild der DS-GVO geboten. Auf bürokratische Hürden, die die Entwicklung von Industrie 4.0 und Anwendungen im Bereich der Künstlichen Intelligenz oder des automatisierten und vernetzten Fahrens behindern, ist zu verzichten.

- An der Schnittstelle von DS-GVO und E-Privacy-VO bedarf es einer präzisen Definition des materiellen Anwendungsbereichs. Es muss klar sein, welche Regeln für Kommunikationsdaten auf dem Übertragungsweg einerseits, und welche Regeln für Daten, die im Auftrag des Nutzers von einem Anbieter auf dessen Servern gespeichert werden andererseits, gelten sollen.

- Bei „machine-to-machine communication“ (M2M-Kommunikation) muss die Weiterverarbeitung von Metadaten aufgrund eines berechtigten Interesses und für kompatible Zwecke nach dem Vorbild der DS-GVO möglich sein. Geeignete Schutzmaßnahmen wie Pseudonymisierung und Verschlüsselung müssen zur Anwendung kommen.

- In Anlehnung an den risikobasierten Ansatz der DS-GVO sollte generell die Weiterverarbeitung von Metadaten für kompatible Zwecke unter Verwendung geeigneter Sicherheitsmaßnahmen (Pseudonymisierung) erlaubt sein.

- Eine E-Privacy-VO muss technologieneutral sein.

- Eine juristische Person muss als "Endnutzer" die Einwilligung für seine Mitarbeiter erteilen können.

- Die einmalige Einwilligung muss den Grundsatz, nicht die Ausnahme bilden.

- Die E-Privacy-VO darf keine zusätzlichen Hürden für Software-Updates, die keine Änderung der Datenschutz-Einstellungen betreffen, aufstellen.

Einleitung

Die deutsche Industrie bekennt sich zu hohen Datenschutz- und Vertraulichkeitsstandards in der digitalen Wirtschaft. Gleichzeitig dürfen Innovationspotenziale nicht über das Maß hinaus behindert werden. Mit großer Sorge verfolgt der BDI daher die Entwicklung für den Verordnungsvorschlag der Europäischen Kommission über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation (E-Privacy-VO). Der jüngste Vorschlag eines Verordnungstextes der EU-Ratspräsidentschaft wirft trotz einiger positiver Entwicklungen derart viele Fragen auf, dass Rechtsanwender aus der gesamten Wirtschaft, also nicht nur im Kommunikationssektor, mit einer erheblichen Rechtsunsicherheit konfrontiert werden. Eine E-Privacy-VO ist aus Sicht der deutschen Industrie momentan nicht beschlussfähig, insbesondere vor dem Hintergrund der sich abzeichnenden praktischen Anwendungsprobleme der DS-GVO.

1. Abgrenzung zwischen DS-GVO und E-Privacy-VO

Mit der DS-GVO wird am 25. Mai 2018 ein einheitlicher europäischer Datenschutz eingeführt. Für die Wirtschaft, insbesondere für kleine und mittelständische Unternehmen, sind die neuen Regeln bereits eine massive Herausforderung. Verschärfend kommt nun hinzu, dass der Vorschlag der E-Privacy-VO mit den Vorgaben der DS-GVO an vielen Stellen nicht kohärent ist und die mühsam gefundenen Kompromisse wieder in Frage stellt. Die eigentlich sektorspezifische E-Privacy-VO würde durch die vielen Rechtsunklarheiten und seinem breiten Anwendungsbereich zum lex generalis. Die Abgrenzung zwischen DS-GVO und E-Privacy-VO in seiner aktuellen Form ist für einen Großteil der Unternehmen nicht verständlich und deshalb nicht anwendbar.

Die deutsche Industrie warnt eindringlich vor einer zusätzlichen Verschärfung des Datenrechts. Die in der DSGVO gefundenen Ansätze für eine flexible Datenverarbeitung unter gleichzeitiger Wahrung eines hohen Datenschutzniveaus würden konterkariert. Der Aufbau einer europäischen digitalen Datenwirtschaft würde maßgeblich erschwert. Bei den anstehenden Verhandlungen im Rat der Europäischen Union sollte daher dringend darauf hingewirkt werden, dass die E-Privacy-VO mehr Flexibilität im Sinne eines risikobasierten Ansatzes bietet. Überschneidungen mit bzw. ungerechtfertigte Abweichungen von der DS-GVO sollten ausgeschlossen werden.

An der Schnittstelle von DS-GVO und E-Privacy-VO bedarf es einer präzisen Definition des materiellen Anwendungsbereichs dahingehend, welche Regeln für Kommunikationsdaten auf dem Übertragungsweg und welche Regeln für Daten, die im Auftrag des Nutzers von einem Anbieter auf dessen Servern gespeichert werden gelten sollen.

Ferner fehlt nach Ansicht der deutschen Industrie auch in Bezug auf Standortdaten die Kohärenz mit der DS-GVO. Während Standortdaten aus elektronischer Kommunikation der E-Privacy-VO im Hinblick auf deren Verarbeitung unterfielen, unterlägen sonstige Standortdaten basierend auf GPS, die wesentlich genauer ausfallen als Standortdaten aus der elektronischen Kommunikation, der DS-GVO. Diese ungleiche Behandlung der gleichen Art von Daten verhindert das in Europa für den digitalen Binnenmarkt angestrebte „Level Playing-Field" unterschiedlicher technischer Anbieteransätze gleicher Datenarten.

Schließlich regt die deutsche Industrie an, einen Erlaubnistatbestand für die Erhebung von Hardware- und Softwaredaten unabhängig von der Einwilligung des Endnutzers zu schaffen, sofern die Erhebung ausschließlich zur Betrugsabwehr und Missbrauchsverhinderung dient.

2. M2M-Kommunikation und maschinelles Lernen

Es bestehen erhebliche Unklarheiten welche Auswirkungen der aktuelle Verordnungsvorschlag auf M2M-Kommunikation haben wird. M2M-Kommunikation ist die Basis für das Internet der Dinge (IoT) und stellt eines der bedeutendsten Zukunftsfelder für die industrielle Wertschöpfung in Deutschland und der EU insgesamt dar. Der Austausch von Daten und Signalen zwischen Maschinen würde zumindest hinsichtlich der Übermittlung als elektronischer Kommunikationsdienst im Sinne von Artikel 6 E-Privacy-VO gelten und damit dessen strengen Vorgaben sowie engen Ausnahmen unterliegen. Dies ist weder sinnvoll, noch vom eigentlichen Sinn und Zweck der Verordnung gedeckt. Daher sollte auch eine klare Ausnahme für den eng definierten Bereich der M2M-Kommunikation erfolgen, die weder die Privatsphäre noch die Vertraulichkeit berührt.

Dem Grundsatz nach ist es zwar begrüßenswert, die Vertraulichkeit des Kommunikationsprozesses an sich zu wahren. In diesem Sinne wird richtigerweise zwischen „Anwendung" („application-layer") und „Übermittlung" („transmission-layer") differenziert (s. Erwägungsgrund 12, Ratsdokument 8537/18 vom 4. Mai 2018). Dabei muss aber klar herausgestellt werden, dass die E-Privacy-VO nur dann gilt, wenn die Übermittlung der M2M-Kommunikation selbst durch einen Dritten, also nicht durch die betroffenen Parteien, durchgeführt wird.

Ferner bleibt weiterhin unklar, wann genau die Übermittlung beginnt und wann sie abgeschlossen ist. Wenn beispielsweise Daten in eine Cloud transferiert und heruntergeladen werden, ist nicht eindeutig, wann die Übermittlung beendet ist. Dies wird umso schwieriger, als dass Daten in der digitalen Wirtschaft ununterbrochen abgerufen und hochgeladen werden, teilweise in Echtzeit. Im M2M-Kontext ist zudem weiterhin fraglich, welcher Endnutzer eigentlich die Einwilligung geben müsste. Auch ist ungewiss, wer der Betreiber des Kommunikationsnetzwerkes ist. Gerade auch mit Blick auf die Entwicklung der Künstlichen Intelligenz dürfen die Möglichkeiten des

maschinellen Lernens (sog. „machine learning“ und „deep learning“) nicht verbaut werden.

Beispiele

- Durch die Nutzung von Metadaten und anderer Informationen können Logistiksysteme erheblich verbessert werden. So können Sensoren, die auf Containern angebracht werden prognostizieren, wann ein bestimmter Container am Bestimmungsort ankommen wird. Durch die Auswertung der verschiedensten Daten wie Witterungsbedingungen am Standort, Verfügbarkeit von Kränen oder Streiks, kann die Ankunft des Containers ganz genau berechnet werden. Je mehr Metadaten diesem intelligenten System zur Verfügung stehen, desto besser kann es lernen und prognostizieren.
- Nach derzeitigem Stand der Verhandlungen könnte auch das vernetzte Fahren unter die e-Privacy-VO fallen, wenn das Fahrzeug als Endeinrichtung („*terminal equipment*“) im Sinne des Artikels 8 E-Privacy-VO eingeordnet wird. Auch kooperative intelligente Transportsysteme („C-ITS"), welche die Kommunikation zwischen Fahrzeugen und der Infrastruktur wie Ampeln ermöglichen, könnten als elektronisches Kommunikationsnetzwerk im Sinne des Artikels 6 E-Privacy-VO gelten. Beim vernetzten Fahren ist die Verarbeitung von Metadaten wichtig. Nur durch die Auswertung von Metadaten kann der Automobilhersteller eine Problembehandlung überhaupt durchführen und beispielsweise überprüfen, warum eine Signalübertragung nicht funktioniert hat und ob das Problem beim Fahrzeug oder Mobilfunknetz liegt.
- In Deutschland ist der Einsatz von intelligenten Messsystemen und modernen Messeinrichtungen („Smart Meter“) bei Strom und Gas verpflichtend. Hierbei werden Zählernummer und Verbrauchsdaten von Endkunden elektronisch übertragen. Die Sicherstellung der System- und Versorgungssicherheit setzt bei der Integration einer Vielzahl dezentraler Anlagen die intelligente Vernetzung und automatisierte Steuerung von Erzeugungs- und Verbrauchsanlagen voraus. Auch eine effiziente Abrechnung sowie die Folgeprozesse setzen voraus, dass Daten elektronisch ausgetauscht und verarbeitet werden. Das Erfordernis einer Einwilligung würde dazu führen, dass etwa Letztverbraucher durch die Verweigerung der Einwilligung in die erforderliche elektronische Kommunikation oder einen späteren Widerruf, das oben genannte Anforderung an „Smart Meter“ konterkarieren könnten. Sollte diese Art der elektronischen Kommunikation der Energieversorgungsunternehmen als „elektronische Kommunikationsdienst, der nicht öffentlich zugänglich ist“ gar nicht in den Anwendungsbereich der Verordnung fallen, erfordert das eine entsprechende Klarstellung in den Erwägungsgründen.

Diese Beispiele zeigen exemplarisch, dass bei der Regelung von M2M-Kommunikation deutlich mehr Flexibilität erforderlich ist. Eine Datenverarbeitung auf Basis eines zur Vernetzung eines Fahrzeugs abgeschlossenen Vertrages oder eine nach den Grundsätzen der DS-GVO abgegebene Einwilligung in die Datenverarbeitung muss ausreichen. Eine weitere Einwilligung nach den Erfordernissen der E-Privacy-VO ist an dieser Stelle überflüssig. Daher sollte bei der M2M-Kommunikation die Weiterverarbeitung von Metadaten aufgrund eines solchen Vertrages oder eines berechtigten Interesses und für kompatible Zwecke nach dem Vorbild der DS-GVO möglich sein.

3. Pseudonymisierung

Im Einklang mit der DS-GVO (Artikel 6 (4) DS-GVO) muss die Weiterverarbeitung von Metadaten möglich sein, wenn der neue Verarbeitungszweck mit dem ursprünglichen Erhebungszweck vereinbar ist und geeignete Schutzmaßnahmen wie Pseudonymisierung und Verschlüsselung zur Anwendung kommen. 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 zwingend erforderlich.

Beispiele

- Verkehrs- und Parkplatzleitsystem können erhebliche Verbesserungen für den Stadtverkehr der Zukunft bedeuten. 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. Auch Staus könnten deutlich reduziert werden. Bei nur anonym vorliegenden Informationen wäre die Einzelzuordnung nicht möglich und damit auch keine Verkehrsbewegung darstellbar.
- Für eine sinnvolle Unfallvorsorge sind pseudonymisierte Daten zwingend notwendig, beispielsweise im Straßenverkehr bei einer Schlaglochwarnung oder einer drohenden Kollision mit einem anderen Fahrzeug.

4. Einwilligung juristischer Personen

Die deutsche Industrie begrüßt, dass die geplante E-Privacy-VO nicht nur natürliche Personen, sondern auch juristische Personen schützt. Daher muss aus der Verordnung aber klar hervorgehen, dass auch eine juristische Person (d. h. das „Unternehmen“) ein "Endnutzer" sein kann, wenn sie der Vertragspartner für einen Kommunikationsdienst ist (siehe Art. 6 und 8 E-Privacy-VO). Wenn das Unternehmen einen elektronischen Kommunikationsdienst abonniert hat, oder ein Endgerät im geschäftlichen Kontext verwendet wird, sollte auch ausschließlich die juristische Person über die Einwilligung in solche Dienste entscheiden, soweit diese für geschäftliche Zwecke betreffen (z. B. Aktualisierung von Unternehmenssoftware). Eine zusätzliche Einwilligung der jeweiligen Angestellten darf nicht notwendig sein, zumal hier auch der Schutzzweck der Verordnung ins Leere laufen würde. In solchen Konstellationen muss differenziert werden. Einwilligungen für Apps, die für die innerbetriebliche Funktionalität unerlässlich sind, müssen vom Unternehmen abgegeben werden können. Es ist ein wesentlicher Unterschied, ob es um eine nichtbetriebliche App auf dem Betriebshandy eines Mitarbeiters, eine technische Einrichtung, die von mehreren Mitarbeitern genutzt wird, oder um ein Update von Diensten, die für den Fortbetrieb der industriellen Lieferkette wichtig sind, geht. Auch ist zu differenzieren, inwieweit das Gerät mit unternehmensinterner Soft- und Hardware verbunden ist. Insbesondere bei den komplexen Wertschöpfungsketten in der Industrie 4.0 dürfen die Sicherheit und die Kontinuität des Betriebsablaufs nicht vom Willen eines einzelnen Mitarbeiters abhängen. Schließlich muss im Sinne der Effektivität der Grundsatz einer einmaligen Einwilligung gelten.

5. Einwilligung für Softwareupdates

Es ist nicht sinnvoll, dass Software-Updates, soweit diese keine Änderung der Datenschutzeinstellungen betreffen, dem datenschutzrechtlichen Regulierungsregime der E-Privacy-VO unterworfen werden sollen. Für Softwareupdates, die keinen unmittelbaren datenschutzrechtlichen Bezug haben, ist das Erfordernis einer Einwilligung sowohl unverhältnismäßig als auch vom Regelungsziel des Datenschutzrechts nicht gedeckt. Ändert ein Softwareupdate die Datenschutzeinstellungen, ergeben sich die entsprechenden datenschutzrechtlichen Anforderungen bereits aus der DS-GVO. Es bleibt völlig unklar, weshalb mit der E-Privacy-Verordnung hier eine zusätzliche Regulierung eingeführt werden soll.

Zur Klarstellung: Hierbei geht es nicht um die Frage, ob ein Nutzer prinzipiell in der Lage sein soll, die Installation eines Software-Updates im Einzelfall zu verhindern, sondern um die Frage, ob es künftig für jedes denkbare Update einer spezifisch datenschutzrechtlichen Zustimmung des Nutzers bedürfte,

die dann auch den weitreichenden Anforderungen des Art. 7 DSGVO unterläge.

Erwägungsgrund 21a des Ratsdokuments 8537/18 vom 4. Mai 2018 legt eine solche Auslegung der E-Privacy-Verordnung nahe, da die hier entsprechende Ausnahme von einem allgemeinen Einwilligungserfordernis (nur) für Sicherheitsupdates angeordnet wird. Im Umkehrschluss hätte die E-Privacy-VO demnach für sämtliche anderen Updates, insbesondere Funktionsupdates ein datenschutzrechtliches Einwilligungserfordernis zur Folge. Dies beträfe nicht nur klassische Kommunikationsdienste, sondern aufgrund des insofern deutlich weiteren Anwendungsbereichs des Art. 8 jedes Software-Update auf Endgeräten im Sinne von Art. 1 Abs. 1 der RL 2008/63/EG. Erfasst wären damit sämtliche mit dem Internet verbundenen Geräte, also künftig insbesondere auch IoT-Endgeräte, Maschinen oder Fahrzeuge.

Unabhängig davon, ob das Update einen datenschutzrechtlichen Bezug hat, müssten alle formellen Anforderungen des Art. 7 DS-GVO – wie Dokumentationspflichten und Zweckbestimmung – eingehalten werden. Diese zusätzliche administrative Mehrbelastung ist für Unternehmen nicht hinzunehmen, unverhältnismäßig und mit dem Schutzzweck des Datenschutzrechts nicht vereinbar. Die Unternehmen nun zusätzlich mit einer neuen Vorgabe zu belasten, die vor allem auch außerhalb des Regelungskreises des Datenschutzrechts liegt, erscheint in Anbetracht des hohen Umsetzungsaufwands der DS-GVO und auch der E-Privacy-VO nicht vertretbar.

Gerade im B2B-Bereich müssen Updates vorab angekündigt und geplant werden, um Ausfallzeiten zu steuern. Ferner ist die Differenzierung zwischen Sicherheitsupdates und anderen Softwareupdates nicht praxistauglich, weil sich Sicherheitsupdates und Feature-Updates nicht strikt separieren lassen. Verhindert etwa eine Nutzer über längere Zeit ein Update der Software, ist es technisch nicht möglich später ein reines Sicherheitsupdate auf eine – insoweit veraltete – Fassung einer Software anzuwenden, weil sich mit jedem Update letztlich auch die Architektur verändert, an der Sicherheitspatches ansetzen.

Über den BDI

Der BDI transportiert die Interessen der deutschen Industrie an die politisch Verantwortlichen. Damit unterstützt er die Unternehmen im globalen Wettbewerb. Er verfügt über ein weit verzweigtes Netzwerk in Deutschland und Europa, auf allen wichtigen Märkten und in internationalen Organisationen. Der BDI sorgt für die politische Flankierung internationaler Markterschließung. Und er bietet Informationen und wirtschaftspolitische Beratung für alle industrierelevanten Themen. Der BDI ist die Spitzenorganisation der deutschen Industrie und der industrienahen Dienstleister. Er spricht für 36 Branchenverbände und mehr als 100.000 Unternehmen mit rund 8 Mio. Beschäftigten. Die Mitgliedschaft ist freiwillig. 15 Landesvertretungen vertreten die Interessen der Wirtschaft auf regionaler Ebene.

Impressum

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

Ansprechpartner

Stefanie Ellen Stündel
Referentin
Telefon: +3227921015
s.stuendel@bdi.eu

Marek Jansen
Referent
Telefon: +493020281459
m.jansen@bdi.eu

BDI Dokumentennummer: D 0940