

Erklärung des Europäischen Datenschutzausschusses zur Überarbeitung der ePrivacy-Verordnung und zu den Auswirkungen auf den Schutz der Privatsphäre von Personen im Hinblick auf die Geheimhaltung und die Vertraulichkeit ihrer Kommunikation

Die im Europäischen Datenschutzausschuss vereinten Datenschutzbehörden der Europäischen Union erachten die Überarbeitung der geltenden ePrivacy-Richtlinie (2002/58/EG, zuletzt geändert durch die Richtlinie 2009/136/EG) als wichtigen und notwendigen Schritt, der rasch getan werden muss. Obwohl sich die Nutzung IP-basierter Kommunikationsdienste seit 2009 ausgeweitet hat, fallen sogenannte Over-the-Top-Dienste derzeit nicht unter die geltende Richtlinie. Um sicherzustellen, dass die Vertraulichkeit der Kommunikation von Endnutzern beim Gebrauch dieser neuen Dienste gewährleistet ist, und um gleiche Wettbewerbsbedingungen für die Anbieter elektronischer Kommunikation und funktional gleichwertiger Dienste zu schaffen, rufen wir die Europäische Kommission, das Parlament und den Rat zur Zusammenarbeit auf, um eine rasche Annahme der neuen ePrivacy-Verordnung sicherzustellen. Diese soll nach dem Inkrafttreten der Datenschutz-Grundverordnung im Mai dieses Jahres die derzeit geltende Richtlinie so bald wie möglich ersetzen.

In Anbetracht der Entwicklungen bei den Beratungen über den Vorschlag und als Hilfestellung für die beiden gesetzgebenden Organe hat sich der Europäische Datenschutzausschuss entschieden, weitere Beratung und Klärungen zu einigen spezifischen Fragen anzubieten, welche durch die vorgeschlagenen Änderungen der gesetzgebenden Organe aufgeworfen wurden.

1. Die Vertraulichkeit der elektronischen Kommunikation bedarf eines besonderen Schutzes, der über die Datenschutz-Grundverordnung hinausgeht

Die Vertraulichkeit der Kommunikation (die moderne Version des traditionellen Postgeheimnisses für Korrespondenz) ist ein nach Artikel 7 der Charta der Grundrechte der Europäischen Union geschütztes Grundrecht, das bereits in der geltenden ePrivacy-Richtlinie umgesetzt wird. Dieses Recht auf Vertraulichkeit muss für alle Arten der elektronischen Kommunikation gelten – unabhängig davon, mit welchen technischen Mitteln die Übermittlung vom Sender zum Empfänger erfolgt und ob die Daten zur Übermittlung lediglich durchgeleitet oder gegebenenfalls zwischengespeichert werden. Umfasst von diesem Schutz sind auch die Vertraulichkeit und Integrität des Endgeräts des Nutzers.

Elektronische Kommunikation ist in unseren modernen Gesellschaften der Grundstein für eine Vielzahl an Tätigkeiten, weil sie die Ausübung vieler Grundrechte wie der Gedanken-, Gewissens-, Religions-, Meinungs-, Informations-, Versammlungs- und Vereinigungsfreiheit etc. fördert. Die

Vertraulichkeit und die Neutralität der Dienste zu stärken, die unsere Kommunikation erbringen, ist daher eine Notwendigkeit.

Da die elektronische Kommunikation in unserem digital geprägten Alltag derart wichtig und weit verbreitet ist, wird sie häufig Inhalte enthalten, die als besondere Kategorien personenbezogener Daten einzustufen sind oder den Rückschluss auf besonders sensible Informationen zulassen. Dies kann durch die Verkettung einer großen Menge an elektronischen Inhalts- und Kommunikations- bzw. Metadaten geschehen, wodurch sehr genaue Rückschlüsse auf das Privatleben der Betroffenen möglich werden und somit große Risiken für deren Rechte und Freiheiten bestehen, weshalb eine diesen Risiken entsprechende Verarbeitung elektronischer Kommunikation notwendig ist.

Deshalb unterstützen wir uneingeschränkt den Ansatz der vorgeschlagenen Verordnung mit einem grundsätzlichen Verbot der Verarbeitung, engen Ausnahmen und dem Rückgriff auf Einwilligungen. Dementsprechend sollte es die ePrivacy-Verordnung nicht ermöglichen, eine Verarbeitung von Inhalts- und Metadaten elektronischer Kommunikation auf Grundlage von offenen, nicht eng genug gefassten Rechtsgrundlagen wie z.B. „berechtigte Interessen“ durchführen zu können, die über das, was für die Bereitstellung eines elektronischen Kommunikationsdienstes erforderlich ist, hinausgehen. Zudem sollte es aufgrund der ePrivacy-Verordnung nicht möglich sein, Metadaten elektronischer Kommunikation allgemein zur Durchführung eines Vertrags zu verarbeiten, weil es keine Ausnahmen für die allgemeinen Zwecke der Vertragsdurchführung geben sollte, sondern stattdessen in der Verordnung genau festgelegt werden sollte, zu welchen konkreten Zwecken eine Verarbeitung zulässig ist – wie z.B. die Verarbeitung zu Abrechnungszwecken.

Der Europäische Datenschutzausschuss betont, dass Metadaten der elektronischen Kommunikation weiterhin ohne Einwilligung weiterverarbeitet werden dürfen, nachdem sie vollständig anonymisiert wurden¹. Der Ausschuss möchte die Anbieter elektronischer Kommunikation ermutigen, von dieser Möglichkeit Gebrauch zu machen, um unter Wahrung der Privatsphäre innovative Dienste zu entwickeln.

2. Die ePrivacy-Richtlinie ist bereits in Kraft

Der Schutz der Vertraulichkeit von Kommunikation ist ein Recht, das schon heute besteht. Durch die im Jahr 2009 geänderte ePrivacy-Richtlinie von 2002 wurde bereits ein allgemeines Verbot für die Verarbeitung von Inhalts- und Metadaten der elektronischen Kommunikation eingeführt. Zulässig sind demnach einzig Verarbeitungen

- nach vorheriger Einwilligung des Nutzers oder
- bei denen die Voraussetzungen für eine der in der ePrivacy-Richtlinie genannten Ausnahmen (Übermittlung elektronischer Kommunikation, Abrechnung) erfüllt sind.

Übermittlungsdienste, die zur Erbringung von Maschine-zu-Maschine-Diensten genutzt werden, fallen ebenfalls in den Anwendungsbereich der geltenden Richtlinie. Diese Bestimmungen werden im Verordnungsvorschlag beibehalten.

Auch gibt es bereits ein Recht auf den Schutz von Endgeräten. Hinsichtlich der Nutzung der Speicherfunktionen des Endgeräts eines Nutzers greift dieses Recht technologieunabhängig. Nicht nur Cookies, sondern auch sämtliche andere Verfolgungs-Technologien bedürfen der Einwilligung des Nutzers oder unterliegen einer der in der ePrivacy-Richtlinie genannten Ausnahmeregelungen.

¹ Wie in der Stellungnahme [WP216](#) definiert; pseudonymisierte Daten jedoch bleiben personenbezogene Daten.

Zudem sieht der Verordnungsvorschlag in der vom Mitgesetzgeber geänderten Fassung verschiedene neue Ausnahmen vor, die von der Artikel-29-Datenschutzgruppe vorgeschlagen wurden², etwa Sicherheits-Updates und Reichweitenmessungen. Diese Ausnahmen stehen in Zusammenhang mit bestimmten Arten der Verarbeitung, die nur sehr geringe Risiken für die Nutzer bergen.

3. Der Verordnungsvorschlag zielt auf eine einheitliche Anwendung in allen Mitgliedstaaten und durch jede Art von Verantwortlichem ab

Die derzeitige ePrivacy-Richtlinie gilt nicht für elektronische Kommunikationsdienste, die via Internet verbreitet werden – ungeachtet der Tatsache, dass sie einen funktional gleichwertigen Dienst anbieten.

Diese Anbieter werden jedoch in den Anwendungsbereich der vorgeschlagenen Verordnung fallen. Der Europäische Datenschutzausschuss betont, dass ein auf funktional gleichwertige Dienste einschließlich sogenannter Over-the-Top-Dienste erweiterter Anwendungsbereich der Verordnung ein wesentlicher Bestandteil der Reform ist. Jede im Verordnungsvorschlag vorgesehene Änderung, die diesem Ziel zuwiderlaufen könnte (beispielsweise Vorschläge zur Einschränkung des Schutzes von Kommunikationsdaten bei der Übermittlung), sollte vermieden werden, um gleiche Ausgangsbedingungen für alle Anbieter zu garantieren.

Die vorgeschlagene Verordnung gilt auch ab dem Moment, in dem Daten in Zusammenhang mit dem Nutzerverhalten erfasst werden, ganz gleich, ob die Nutzer ein Konto für einen Dienst eingerichtet haben oder nicht. Dieser Ansatz gewährleistet für die Nutzer dieser Dienste nicht nur den Schutz, den sie verdienen, sondern sorgt auch für einen fairen Wettbewerb der Verantwortlichen. Es sei darauf hingewiesen, dass die Einwilligung, die nach der ePrivacy-Verordnung eingeholt werden muss, dieselbe Bedeutung hat wie jene nach der Datenschutz-Grundverordnung. Insbesondere die Notwendigkeit, eine freiwillige Einwilligung einzuholen, wird Diensteanbieter davon abhalten, sogenannte Cookie-Walls³ für Nutzer einzusetzen, und die Verpflichtung zu einer spezifischen Einwilligung wird gleiche Voraussetzungen für Anbieter schaffen, unabhängig von einem Log-in des Nutzers.

Durch die Schaffung bestimmter Sanktionen bei Verstößen gegen die ePrivacy-Verordnung in Kombination mit einem erweiterten territorialen Geltungsbereich – beides im Gleichlauf mit den Vorgaben der Datenschutz-Grundverordnung – werden die Datenschutzbehörden zudem in die Lage versetzt, die Anwendung der Verordnung in Bezug auf alle von EU-Nutzern verwendeten elektronischen Kommunikationsmittel durchzusetzen.

4. Durch die neue Verordnung müssen das Einwilligungserfordernis für Cookies und ähnliche Technologien durchgesetzt und Diensteanbietern technische Tools für das Einholen der Einwilligung angeboten werden

Wie von der Europäischen Kommission vorgeschlagen, soll gemäß Artikel 10 des Verordnungsvorschlags den Nutzern die Kontrolle über die Nutzung der Speicherfunktionen ihrer Endgeräte gegeben werden. Artikel 10 wurde vom Parlament dahingehend erweitert, dass Voreinstellungen zum Schutz der Privatsphäre bei Software-Einstellungen vorgeschrieben und für Websites eine technische Lösung für das Einholen einer wirksamen Einwilligung zur Verfügung gestellt werden.

Der Europäische Datenschutzausschuss unterstützt uneingeschränkt eine Stärkung dieses Artikels und ist der Auffassung, dass er explizit für die Betriebssysteme von Smartphones, Tablets oder

² Siehe [WP194](#) und [WP240](#).

³ Eine Cookie-Wall hindert Nutzer, die nicht einwilligen, am Besuch einer Website oder der Nutzung eines Dienstes.

andere End-Systemteile gelten sollte, um sicherzustellen, dass bei Kommunikationsanwendungen die Entscheidungen der Nutzer berücksichtigt werden, ungeachtet der eingesetzten technischen Mittel.

Darüber hinaus sollten es Privatsphäre-Einstellungen erleichtern, Einwilligung und Widerruf auf einfache, rechtsverbindliche und gegenüber allen Parteien durchsetzbare Weise zu äußern. Den Nutzern sollte bereits bei der Installation eine eindeutige Auswahlmöglichkeit gegeben werden, ihre Einwilligung zu geben, wenn sie dies wünschen. Zudem sollten Website- und mobile Anwendungen über die Privatsphäre-Einstellungen eine mit der Datenschutz-Grundverordnung konforme Einwilligung einholen können.

5. Schlussfolgerungen

Der Europäische Datenschutzausschuss vertritt die Auffassung, dass

- die ePrivacy-Verordnung das Schutzniveau der derzeit geltenden ePrivacy-Richtlinie nicht herabsenken sollte;
- die ePrivacy-Verordnung bei allen Arten elektronischer Kommunikation auf technologieneutrale Weise Schutz bieten sollte, also auch bei jenen Formen, die über Over-the-Top-Dienste erfolgen;
- die Einwilligung der Nutzer systematisch in einer technisch realisierbaren und durchsetzbaren Weise eingeholt werden sollte, bevor elektronische Kommunikationsdaten verarbeitet oder bevor die Speicher- oder Verarbeitungsfunktionen der Endgeräte eines Nutzers verwendet werden. Es sollte keine Ausnahmen für die Verarbeitung dieser Daten auf Grundlage eines „berechtigten Interesses“ des Verantwortlichen oder zu allgemeinen Zwecken der Vertragsdurchführung geben;
- in Artikel 10 ein wirksamer Weg zum Einholen der Einwilligung für Websites und mobile Anwendungen vorgesehen werden sollte. Generell sollten Voreinstellungen die Privatsphäre der Nutzer schützen, und die Nutzer sollten angeleitet werden, nach Erhalt transparenter einschlägiger Informationen Einstellungen auszuwählen. In dieser Hinsicht sollte die Verordnung technologieneutral bleiben, um zu gewährleisten, dass sie ungeachtet der Anwendungsfälle konsequent angewandt wird;
- bei etwaigen Ad-hoc-Ausnahmen, die die Gesetzgeber zusätzlich zu den bereits in den Entwürfen der Kommission und des Parlaments enthaltenen in Betracht ziehen könnten, mit größter Gründlichkeit vorgegangen werden sollte. Dies gilt insbesondere für allgemein formulierte Ausnahmen in Fällen, in denen „eine Behörde“ die Datenverarbeitung anfordert; zudem sollte der Vorschlag weder die wahllose Überwachung des Standorts der Nutzer noch die Verarbeitung ihrer Metadaten erlauben;
- die Einwilligung freiwillig im Sinne der Datenschutz-Grundverordnung erfolgen sollte und der Zugang zu Diensten und Funktionalitäten, nicht von der Einwilligung eines Nutzers zur Verarbeitung personenbezogener Daten oder von der Verarbeitung von Informationen, die in Zusammenhang mit dem Endgerät von Endnutzern stehen oder durch diese verarbeitet werden, abhängig gemacht werden sollte. Dies bedeutet, dass Cookie-Walls ausdrücklich verboten werden sollten;
- die Nutzung vollständig anonymisierter elektronischer Kommunikationsdaten gefördert werden sollte;
- die vorgenannten Entwicklungen die Privatsphäre von Endnutzern in allen relevanten Zusammenhängen schützen und Wettbewerbsverzerrungen verhindern werden.