

"Wir alle zahlen für Dienste im Internet mit unseren Daten" – und wie die ePrivacy-Verordnung derartige Praktiken erschweren möchte

Wien, 26. Jänner 2018

1. Status der Umsetzung

Vor ca. einem Jahr, am 10. Januar 2017, hat die EU-Kommission den Entwurf für eine neue ePrivacy-Verordnung¹ (im Folgenden "**eP-VO**") veröffentlicht. Damit soll die sogenannte "e-Datenschutz-Richtlinie"² überprüft und unter Berücksichtigung der seither erfolgten technischen und wirtschaftlichen Entwicklungen aktualisiert werden, wodurch Einklang mit der Datenschutz-Grundverordnung³ (im Folgenden "**DS-GVO**") hergestellt werden soll. Die eP-VO wird, ebenso wie die DS-GVO, als EU-Verordnung unmittelbar anwendbar sein.

Am 19. Oktober 2017 hat der zuständige Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments dem Entwurf zugestimmt. Dort wurde zuvor monatelang über die mehr als 800 Änderungsanträge zum Entwurfsvorschlag beraten; diese große Zahl veranschaulicht die Brisanz des Themas und erinnert an die Verhandlungen um die DS-GVO, als über 3.100 Abänderungsanträge zum Entwurf der EU-Kommission eingebracht wurden.

Nur eine Woche später, am 26. Oktober 2017, hat sich das EU-Parlament mit wenigen Änderungen⁴ für den Entwurf ausgesprochen; große Überzeugung gab es unter den Abgeordneten aber nicht: Bei 20 Stimmenthaltungen stimmten 318 für den Vorschlag, 280 dagegen. Das bedeutet allerdings nicht, dass es bereits einen rechtskräftigen Gesetzestext gibt – und genauso wenig ist derzeit klar, ob der von der Europäischen Kommission vorgesehene Zeitrahmen für das Inkrafttreten der eP-VO, nämlich zusammen mit der DS-GVO am 25. Mai 2018, halten kann. Im Moment sind die Mitgliedstaaten im Rat der Europäischen Union am Zug, die eine gemeinsame Position finden müssen. Anschließend geht der Entwurf in den Trilog (Verhandlungen zwischen Kommission, Parlament und Rat).

2. Anwendungsbereich und rechtliche Grundlagen der eP-VO

Regelungsbedarf entstand nach Auffassung der Kommission aufgrund der Verlagerung von herkömmlichen Kommunikationsdiensten (SMS, Telefonie, E-Mails) hin zu neuen Internetdiensten (zB VoIP-Telefonie, Instant-Messaging). Diese neuen Kommunikationsmittel sollen nun mit der eP-VO geregelt werden, welche die Verarbeitung "*elektronischer Kommunikationsdaten*" in "*Verbindung mit der Bereitstellung und Nutzung elektronischer Kommunikationsdienste*" reguliert. Sie soll diesbezüglich als *lex specialis* zur DS-GVO gelten.

Erklärtes Ziel ist es, die **Vertraulichkeit und Privatsphäre der elektronischen Kommunikation** zu gewährleisten bzw zu steigern. Der Ausdruck "elektronische Kommunikationsdaten" umfasst einerseits die Informationen bezüglich der übermittelten oder ausgetauschten **Inhalte** (u.a. Text, Sprache, Videos, Bilder), andererseits aber auch die Informationen, die zum Zweck der Übermittlung, Verbreitung oder Ermöglichung des Austauschs der Inhalte verarbeitet werden (sogenannte **Metadaten**: zB angerufene Nummern, besuchte Websites, geographische Standorte, Datum, Uhrzeit, Dauer und Art der Kommunikation, unabhängig davon, ob die Signale über Kabel, Funk, Mobilfunknetze oder Stromleitungssysteme übertragen werden). Grund dafür ist, dass sich auch aus Metadaten

Schlussfolgerungen über das Privatleben der Beteiligten ziehen lassen (können), zB in Bezug auf ihre sozialen Beziehungen, Gewohnheiten, Interessen – sprichwörtlich den gesamten Lebensalltag. Laut den Erwägungsgründen der VO soll auch das "Internet der Dinge" (also Geräte und Maschinen, die ohne menschliches Zutun über elektronische Kommunikationsnetze miteinander kommunizieren - zB Drucker, die bei Bedarf selbst Druckertoner nachbestellen) betroffen sein.

Wie soll nun die Vertraulichkeit gestärkt werden?

- Die eP-VO sieht vor, dass sämtliche **Eingriffe in die Übermittlung** von elektronischen Kommunikationsdaten **ohne Einwilligung aller Beteiligten grundsätzlich untersagt** sein sollen. Ein solcher Eingriff liegt beispielsweise vor, wenn Dritte besuchte Websites und Zeitpunkt der Besuche "tracken", also die Surfgewohnheiten von Nutzern ermitteln, um daraus Benutzerprofile zu erstellen.⁵ Es ist jedoch nicht jeglicher Umgang mit den Daten von vornherein untersagt: So ist beispielsweise die Speicherung zur Gewährleistung der Sicherheit und Kontinuität des Dienstes, zur Prüfung von Sicherheitsbedrohungen oder für die Rechnungsstellung weiterhin ohne gesonderte Einwilligung zulässig. Eine Ausnahme von der Verpflichtung zur Einholung einer Einwilligung greift auch, wenn "*kein oder bloß ein geringfügiger Eingriff in die Privatsphäre*" vorliegt, wobei dies auch bei einem Zugriff erfüllt sein soll, der "*unbedingt notwendig und verhältnismäßig ist für den rechtmäßigen Zweck, die ausdrücklich gewünschte Nutzung zu ermöglichen*". Bei Cookies ist dies zB der Fall, wenn sie für die Dauer einer Sitzung nötig sind, um Eingaben beim Ausfüllen von Online-Formularen über mehrere Seiten mitzuverfolgen. Vereinfacht gesagt: Dem Begriff der "**Datensparsamkeit**" soll insofern Rechnung getragen werden, als elektronische Kommunikationsdaten nur soweit verarbeitet werden, als sie zur Bereitstellung des konkreten jeweiligen Dienstes erforderlich sind; alles, was darüber hinausgeht, bedarf einer Einwilligung des Nutzers.
- Endnutzer wollen (und sollen) damit die **Kontrolle** für die Verwendung der Daten für andere Zwecke als Übertragung der Kommunikation behalten, indem sie vorab in Verarbeitungen "ihrer" Kommunikationsdaten für andere Zwecke einwilligen müssen. Die Praxis der digitalen Wirtschaft zeigt, dass Dienstleistungen, gerade online, heute oft für eine andere Gegenleistung als Geld angeboten werden, beispielsweise dafür, dass den Endnutzern Werbung angezeigt wird. Für solche Modelle gibt es nach der eP-VO Änderungsbedarf. Für eine rechtskonforme **Einwilligung** ist – ähnlich den Anforderungen der DS-GVO – eine eindeutig bestätigende (aktive) Handlung erforderlich, in der freiwillig, für einen bestimmten Fall, in informierter Weise und unmissverständlich die Zustimmung zur konkreten Verarbeitung, zB Speicherung oder Zugriff für einen konkret genannten Zweck, erklärt wird, wobei dies auch nachweisbar sein muss. Eine in den AGB enthaltene Zustimmungserklärung reicht dafür voraussichtlich nicht aus; entsprechende Opt-In-Möglichkeiten müssten hier oft schon für den Besuch einer Website (und damit zeitlich vor einem Zugriff) implementiert werden. Eine Umsetzung nach Vorbild der derzeit häufig genutzten Cookie-Banner ist aber laut eP-VO nicht gewünscht, denn:
- Die Bereitstellung von Informationen und auch die Einholung der Einwilligung sollen so **benutzerfreundlich** wie möglich erfolgen – das bedeutet, dass Nutzer nicht schon beim Besuch einer Website mit Anfragen, Kästchen und Pop-Ups überhäuft werden sollen. Eine mögliche Lösung für das Einholen von Einwilligungen liegt in entsprechenden (Vor-)Einstellungen im Browser oder in der jeweiligen Anwendung, wobei die dort getroffene Auswahl für Dritte verbindlich sein muss. Browser nehmen grundsätzlich eine Sonderstellung ein, weil sie einen Großteil der Vorgänge zwischen Endnutzern und Websites abwickeln. Sie sollen nach der eP-VO Endnutzern dabei helfen, das Speichern und den Zugriff zu Informationen zu regulieren, zB mittels einer Reihe von **Einstellungsmöglichkeiten zu Cookies im Browser** (von "streng: keine Cookies erlauben" bis "niedrig: Cookies immer annehmen"). Auch andere Anbieter von Software, die elektronische Kommunikation ermöglicht, sowie die Hersteller von Betriebssystemen mobiler Endgeräte werden zur Hilfestellung der Nutzer verpflichtet. Nebenbei soll dem Grundsatz "privacy by default", der in der DS-GVO für den gesamten Umgang mit

(personenbezogenen) Daten verankert ist, entsprochen werden, indem im Gerät oder Browser standardmäßig die datenschutzfreundlichste Auswahl getroffen ist. In Österreich gibt es derartige Verpflichtungen (in abgeschwächter Form) für bestimmte Anbieter bereits in § 96 Abs 3 Telekommunikations-Gesetz (TKG).

- Der Entwurf enthält außerdem Bestimmungen zu "**unerbetener Kommunikation**" (zB Spam, Direktwerbung; durch Möglichkeiten der Rufnummernunterdrückung, Nummernsperrern), wobei diese Bestimmungen bereits im TKG umgesetzt sind und keine inhaltliche Anpassung der nationalen Rechtslage erfordern.
- Es erfolgt eine Angleichung der **Sanktionen** an die Bestimmungen der DS-GVO, wodurch ein Strafraum bis zu € 20 Mio. bzw 4 % des weltweiten Jahresumsatzes eingeführt wird.

3. Praktische Auswirkungen für Nutzer und Anbieter

Schon aus dem Anwendungsbereich der eP-VO ergibt sich, dass hauptsächlich die Anbieter elektronischer Kommunikation vom Entwurf betroffen sind, ebenso aber u.a. die gesamte Medienindustrie, Werbewirtschaft und Softwareprovider. Von den genannten Branchen kam auch bereits heftige Kritik am Entwurf: Laut einer deutschen Studie⁶ könnte die Verordnung dazu führen, dass die gesamten digitalen Werbebudgets in Deutschland um ein Drittel zurückgehen. *"Die zu erwartenden Einnahmeverluste können für alle Online-Angebote existenzbedrohend sein, die sich maßgeblich über Displaywerbung refinanzieren"*, heißt es darin. Werbewirtschaft ist im Netz derzeit zumeist so organisiert, dass auf Websites eine große Anzahl von Distributoren für Bannerwerbung eingebunden ist. Für deren Anbieter ist es dadurch möglich, den Browser des Benutzers auszulesen oder Cookies zu setzen, darunter auch Tracking-Cookies, die nicht für die Funktionalität einer Website benötigt werden, sondern dem digitalen Marketing dienen. All diese Mechanismen sind jedoch, wie oben beschrieben, nach der eP-VO an Einwilligungserfordernisse gebunden – dabei ist aber fraglich, ob Nutzer solche Einwilligungen, so sie die Möglichkeit zur Verweigerung haben, erteilen würden. Berücksichtigen die Anbieter nämlich zusätzlich das **datenschutzrechtliche Kopplungsverbot**, so dürfen sie ihr Service-Angebot nicht von einer Einwilligung des Nutzers abhängig machen, die über die *"zur Erbringung einer Dienstleistung notwendige Datenverarbeitung"* hinausgeht. Das bedeutet, dass der Nutzer beispielsweise Online-Dienste nutzen können muss, auch wenn er einer (für die Werbewirtschaft gewünschten) Datensammlung durch Cookies gerade nicht zustimmt. Eine Finanzierung von derzeit (allerdings bloß scheinbar) "unentgeltlichen" Angeboten wie zahlreichen Websites, zB auch Nachrichtendiensten, wäre über Werbung nicht mehr oder jedenfalls nur unter erschwerten Bedingungen möglich. Diese Thematik ist auch in wettbewerbsrechtlicher Hinsicht auf EU-Ebene aktuell in den Fokus gerückt, wobei die zuständige EU-Kommissarin fordert, dass die Menschen sorgsamer werden sollten, was ihr Verhalten im Netz betrifft: *"Es ist Zeit, mit der Fiktion aufzuräumen, dass Bürger im Internet für Dienste nichts zahlen. Natürlich tun sie das. Sie zahlen mit ihren Daten, und das nützt jemand aus und macht damit Geld. (...) Als Staatsbürger wird es unsere Aufgabe für die Zukunft sein herauszufinden, was der angemessene Preis für unsere Daten online ist."*⁷, so die dänische EU-Wettbewerbskommissarin in einem Interview am 12. Januar 2018.

Auch Mobilitätsunternehmen, die sich derzeit intensiv mit Forschung im Bereich des "Internets der Dinge" beschäftigen, warnen vor den Auswirkungen der eP-VO. Sie sehen die Regeln als überzogen an und meinen, die eP-VO schütze personenbezogene Daten im Umfeld der Maschine-zu-Maschine-Kommunikation in unangemessener Weise.⁸ Facebook und andere "Datenriesen" hingegen könnten am wenigsten betroffen sein von der geplanten VO. Zum einen gibt der Konzern die erhobenen Metadaten (größtenteils) nicht an Dritte weiter, sondern vermarktet sie konzernintern; zum anderen gibt es wenig Schwierigkeiten mit der Zustimmung der Benutzer, auch wenn die Services auf

Websites Dritter eingebunden sind, da die User fast alle bereits irgendwann davor der umfassenden Datenverarbeitung durch Facebook (via Facebooks "Nutzungsbedingungen" und "Datenrichtlinie") zugestimmt haben. Wer sich daran noch erinnern kann – und in welchem Umfang er darüber tatsächlich und nicht bloß laut Häkchen informiert war – steht allerdings auf einem anderen Blatt.

Das in der eP-VO angehobene Strafrisiko und der absehbare erhebliche Implementierungsaufwand, der über jenen zur DS-GVO noch hinausgeht, lassen vor allem bei Anbietern den Wunsch nach Rechtssicherheit wachsen. Wie oben beschrieben ist der bis zum Inkrafttreten noch zu bewältigende Weg ein langer. Eine Beschäftigung mit der Thematik ist v.a. für Unternehmen aus den Bereichen Medien, Werbewirtschaft und Softwareentwicklung so früh wie möglich zu empfehlen.

¹ Verordnung des europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG.

² Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

³ VO (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

⁴ <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2017-0324&language=EN>

⁵ ErwGr 15.

⁶ Studie für das BM für Wirtschaft und Energie des Wissenschaftlichen Instituts für Infrastruktur und Kommunikationsdienste: "Wirtschaftliche Auswirkungen der Regelungen der ePrivacy-Verordnung auf die Online-Werbung und werbefinanzierte digitale Geschäftsmodelle", November 2017, abrufbar unter: http://www.wik.org/fileadmin/Studien/2017/2017_ePrivacy-BMW.pdf

⁷ <https://mobil.derstandard.at/2000071987922/EU-Wettbewerbskommissarin-Buerger-zahlen-im-Internet-mit-ihren-Daten>

⁸ <https://www.welt.de/wirtschaft/article171191916/Ueberzieht-Bruessel-beim-Datenschutz.html>