Rechtliche Stellungnahme

zur ePrivacy-Richtlinie

Prof. Dr. Anne Richert

I. Zusatz zur rechtlichen Stellungnahme vom Dezember 2016

Prof. Dr. Anne Riechert, Stiftung Datenschutz / Frankfurt University of Applied Sciences
Stand: Januar 2017, begründet auf:

Proposal „Regulation on Privacy and Electronic Communications", (10.01.2017) – 2017/0003 (COD)

Allgemein

Der Vorschlag der EU-Kommission („Regulation on Privacy and Electronic Communications" – im Folgenden: „Vorschlag") beinhaltet Regelungen zum Schutz der Privatsphäre und der personenbezogenen Daten in der elektronischen Kommunikation und soll die Richtlinie 2002/58/EG ersetzen. Klarstellend wird darauf verwiesen, dass diese Richtlinie „lex specialis" zur Datenschutz-Grundverordnung darstellt (siehe 1.2). Dies entspricht insoweit der aktuellen Rechtslage im Hinblick auf das Verhältnis der Richtlinie 2002/58/EG zur Datenschutz-Richtlinie (95/46/EG). Unberührt bleiben gemäß dem Vorschlag die Regelungen der Richtlinie 2000/31/EG (siehe Artikel 2 Nr. 4). Darüber hinaus steht es den Mitgliedstaaten ebenfalls frei, Regelungen zur Vorratsdatenspeicherung zu erlassen (siehe 1.3 des Vorschlags)

In dem Vorschlag sind unter anderem die Ergebnisse einer öffentlichen Befragung (durch Beteiligung von Verbraucherorganisationen, Industrie und Behörden) umgesetzt. Außerdem wurden Workshops sowie eine Meinungsumfrage unter EU-Bürgern durchgeführt (siehe 3.2 des Vorschlags). Aufgrund letzterer wurde beispielsweise festgestellt, dass 78% der Befragten es sehr wichtig finden, dass ein Zugang zu den auf einem Computer, Smartphone oder Tablet gespeicherten persönlichen Informationen nur aufgrund ihrer Erlaubnis möglich ist, und dass 89% mit der vorgeschlagenen Möglichkeit einverstanden sind, aufgrund von Voreinstellungen im Browser das Teilen ihrer persönlichen Informationen zu verhindern.

Des Weiteren basiert der Vorschlag auf einer Folgenabschätzung unter Berücksichtigung von Effektivität und Wirtschaftlichkeit, wobei nach der Untersuchung von unterschiedlichen möglichen Maßnahmen die Option befürwortet wurde, die eine maßvolle bzw. gemäßigte Stärkung von Privatsphäre und Vereinfachung beinhaltet. Damit ist gemäß den Ausführungen in dem Vorschlag vor allem gemeint, die Vertraulichkeit der elektronischen Kommunikation durch geeignete technische Einstellungen zu verbessern sowie das Regelungsumfeld zu vereinfachen, indem der Handlungsspielraum für die Mitgliedstaaten verringert wird (siehe 3.4 des Vorschlags).

Cookies

In Bezug auf Cookies verweist der Vorschlag gemäß Erwägungsgrund 21 darauf, dass für erforderliche Cookies keine Einwilligung eingeholt werden muss (z. B. das Ausfüllen von Online-Formularen über mehrere Seiten, das Messen des Traffic der Webseite). In Erwägungsgrund 22 wird detailliert aufgeführt, dass technische Voreinstellungen in Bezug auf Tracking-Cookies für den Nutzer übersichtlicher sind als Anfragen hinsichtlich seiner Zustimmung, wobei in Erwägungsgrund 23 im Besonderen auf die damit verbundene Anforderung des Artikel 25 Datenschutz-Grundverordnung hingewiesen wird („Privacy by Design").

Die Umsetzung dieses Anspruch sollte danach durch unterschiedliche und für den Nutzer leicht erkennbare Privatsphäreeinstellungen erfolgen, die beispielsweise Funktionen wie „Cookies niemals akzeptieren" bis „Cookies immer akzeptieren" bieten, aber ebenso die Option „nur Erstanbieter Cookies akzeptieren" umfassen.

In Erwägungsgrund 24 und Artikel 9 Absatz 1 des Vorschlags wird sodann auf die Geltung der Einwilligungsvoraussetzungen gemäß Artikel 4 Nr. 11 sowie Artikel 7 Datenschutz-Grundverordnung verwiesen. Davon unberührt ist gemäß Artikel 9 Absatz 2 Datenschutz-Grundverordnung jedoch die Verpflichtung, dort wo es „technisch möglich und machbar ist", für die Zwecke von Artikel 8 Absatz 1b des Vorschlags (für Informationen, die im Endgerät des Nutzers gespeichert sind), die Einwilligung des Nutzers durch geeignete technische Einstellungen mittels einer Softwareapplikation einzuholen. Erwägungsgrund 24 regelt hierzu näher, dass im Falle von „Third-Party-Cookies" die Nutzer aktiv auswählen sollen, dass sie mit „Third-Party-Cookies" einverstanden sind und diese Einwilligung bestätigen sollen. Dies gilt unter der Maßgabe, dass sie die notwendigen Informationen erhalten haben, diese Auswahl treffen zu können.

Im Sinne der oben bereits genannten Option (=maßvolle bzw. gemäßigte Stärkung von Privatsphäre und Vereinfachung) bezieht sich der Vorschlag darauf, eine Dialogbox zwischen Nutzer und besuchten Webseiten einzurichten, die dem Nutzer die Ablehnung von „Third-Party-Cookies" ermöglicht (siehe 3.4 des Vorschlags). Gemäß den Ausführungen in dem Vorschlag könnten damit Cookie-Banner und Benachrichtigungen umgangen werden, was zur Vereinfachung, aber auch Kosteneinsparung führen würde. Klarstellend wird darauf verwiesen, dass Webseitenbetreiber jedoch nach wie vor das Recht haben, eine Einwilligung aufgrund einer individuellen Anfrage beim Endnutzer einzuholen (siehe 3.4 des Vorschlags).

Aus wirtschaftlicher Sicht wird auf eine geschätzte, aber nicht näher begründete Kosteneinsparung von 948.8 Million Euro verwiesen (siehe 3.4 des Vorschlags).

Als Verantwortliche für diese technische Umsetzung könnten Internet Browser, Drittanbieter (die das Tracking durchführen) und die Webseiten in Betracht kommen (siehe 3.4 des Vorschlags). Gemäß Artikel 10 in Verbindung mit Artikel 23 des Vorschlags müssen Anbieter von elektronischer Kommunikationssoftware die Möglichkeit bieten, „Third-Party-Cookies" zu verhindern und die Einwilligung der Nutzer einzuholen. Anderenfalls können Bußgelder bis zu 10.000.000 EURO, alternativ 2% des weltweiten Jahresumsatzes drohen.

Relevanz im Hinblick auf die rechtliche Stellungnahme zum Einwilligungsassistenten und Handlungsempfehlung

Insgesamt besteht die Intention des Vorschlags darin, eine Einwilligung durch Unterstützung von Software, im Besonderen durch Internet Browser, einzuholen. Internet Browser stellen aber nur eine Möglichkeit dar. In den Handlungsempfehlungen der rechtlichen Stellungnahme vom Dezember 2016 (siehe Studie) wurden die Entwickler bereits zur Prüfung aufgefordert, ob ihr Konzept ebenso auf Cookies erweitert werden könnte.

In Bezug auf Cookies stellen die Erwägungsgründe klar, dass eine Einwilligung durch eine bestätigende Handlung erteilt werden soll, beispielsweise dadurch, dass von den Nutzern verlangt wird, eine Einstellung „accept third party cookies“ aktiv auszuwählen (Erwägungsgrund 26). Daraus lässt sich die Absicht entnehmen, dass ausdrücklich (nicht konkludent) durch Auswahl und aktiver Bestätigung unterschiedlicher Optionen ein Dialog stattfinden soll. Aufgrund dessen, dass dies aber (nur) ein Ausführungsbeispiel darstellt und gemäß Artikel 9 Absatz 2 zudem der Vorbehalt der „technischen Möglichkeit und Machbarkeit“ enthalten ist sowie außerdem unter 3.4 darauf verwiesen wird, dass Webseitenbetreiber das Recht haben, eine Einwilligung aufgrund einer individuellen Anfrage beim Endnutzer einzuholen, kann sich eine weitere Klarstellung empfehlen. So könnten im Hinblick auf die „technische Machbarkeit“ klare Regelfälle definiert werden. Außerdem wäre eine Betonung dahingehend möglich, dass ausschließlich (und nicht nur beispielsweise) durch die aktive Auswahl des Nutzers (Checkbox) von unterschiedlichen Optionen eine Einwilligung zustande kommt, damit eine transparente Information unter Weiternutzung des Dienstes deutlich ausgeschlossen ist (siehe etwa Rechtspraxis auf der Webseite der unabhängigen Datenschutzaufsichtsbehörde (ICO) von Großbritannien – aufgeführt in der rechtlichen Stellungnahme zum Einwilligungsassistenten).

Hinsichtlich der Einwilligungsvoraussetzungen insgesamt verweist Artikel 9 Absatz 1 auf die Voraussetzungen der Datenschutz-Grundverordnung (Artikel 4 Nr. 11 und Artikel 7 Datenschutz-Grundverordnung), so dass auch hier auf die Ausführungen in der rechtlichen Stellungnahme verwiesen wird (siehe etwa die Problematik im Hinblick auf die konkludente Einwilligung oder der Auslegung der Begriffe „explicit“ und „specified“).

Die rechtliche Verantwortung wird aufgrund der Regelungen in Artikel 10 und 23 des Vorschlags ebenso auf den Softwareentwickler verlagert, was in der Datenschutz-Grundverordnung in einer solch namentlich benannten Formulierung nicht vorgesehen ist. In der Datenschutz-Grundverordnung ist zwar der Grundsatz „Datenschutz durch Technik“ gemäß Artikel 25 enthalten, aber im Vorschlag „Regulation on Privacy and Electronic Communications” wird ausdrücklich benannt, dass auch der Anbieter von Software zur Umsetzung verpflichtet ist und ihm Geldbußen auferlegt werden können. Im Hinblick auf die Datenschutz-Grundverordnung könnte daher der Begriff des Verantwortlichen gemäß Artikel 4 Nr. 7 präzisiert werden, inwieweit ein Softwareanbieter als „Verantwortlicher“ im Sinne der Verordnung eingeordnet werden kann, da er Mittel der Verarbeitung bereit stellt und daher mit entscheiden könnte. Insgesamt muss vermieden werden, dass ein Dienstanbieter sich auf die mangelnde Umsetzung oder Entwicklung der erforderlichen softwareseitig sicherzustellenden Einwilligungsvoraussetzungen eines Softwareanbieters beruft (siehe Artikel 9 Absatz 2 „technically possible and feasible“), da Browserlösungen unter Umständen Entwicklungszeit benötigen.

Klarstellend könnte daher geregelt werden, dass jeder Anbieter verpflichtet ist, eine ausdrückliche Einwilligung durch Bereitstellung von interaktiven Auswahlmöglichkeiten einzuholen. Damit wäre eine aktive Entscheidung der Nutzer sichergestellt, die nicht in der Weiternutzung des Dienstes (auch nicht durch transparente Information) bestehen kann. In diesem Zusammenhang sei ebenso darauf verwiesen, dass Konzepte wie P3P in der Vergangenheit vom Windows-Browser seit der Version Windows 10 nicht mehr unterstützt wurden. Externe Softwareentwickler und Browseranbieter müssen daher in Bezug auf „technische Machbarkeit“ eng zusammenarbeiten.

Darüber hinaus wäre als vertrauensbildende Maßnahme für die Nutzer an dieser Stelle zertifizierte Software hilfreich.
Empfehlenswert wäre bei einer Verlagerung des Datenschutzes auf die technische Seite außerdem, eine Bildungsoffensive zu starten. Es ist ganz entscheidend, dass Nutzer keine Vorbehalte oder Ressentiments gegenüber einem technischen Datenschutz haben, sich die Bedienung von vorneherein zutrauen und nachvollziehen können, aus welchem Grunde technische Maßnahmen wichtig sind. Hier geht es im Besonderen um die Nachvollziehbarkeit des Selbstdatenschutzes, da dadurch gleichermaßen ein verantwortungsvoller Umgang der Daten seitens des Nutzers erwartet wird. Im Hinblick auf „Big Data“ muss einem Nutzer bekannt sein, wo die Gefahren von Third-Party-Cookies liegen. Um überhaupt eine Entscheidung treffen zu können, darf ihm die Entscheidung, welche Arten von Cookies er akzeptiert, nicht aus Unwissenheit „egal sein“.

Daher ist sowohl die Schul- als auch Erwachsenenbildung über (technischen) Datenschutz sehr bedeutsam.

STIFTUNG DATENSCHUTZ

Stiftung Datenschutz
rechtsfähige Stiftung bürgerlichen Rechts
Karl-Rothe-Straße 10–14
04105 Leipzig
Deutschland

Telefon 0341 / 5861 555-0
mail@stiftungdatenschutz.org
www.stiftungdatenschutz.org