ISSN 1977-9119

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

EDSB Newsletter

Nr. 42 | Juli 2014

IN DIESER AUSGABE

SCHLAGLICHTER

Die Privatsphäre aus der Kälte retten: Verfahren des Rates zum Einfrieren von Vermögenswerten

Das Einfrieren von Vermögenswerten ist eine der Maßnahmen, die in Ermittlungsverfahren gegen Personen zur Anwendung kommen können, wenn diese bestimmter schwerer Straftaten wie terroristischer Aktivitäten verdächtigt werden oder wenn gegen Personen, die den Regimes in bestimmten Drittländern nahestehen, wegen Menschenrechtsverletzungen ermittelt wird. Auf Empfehlung der Mitgliedstaaten veröffentlicht der Europäische Rat im Amtsblatt der Europäischen Union Listen von Personen, deren Vermögen eingefroren werden soll, sowie die Gründe dafür. Die Finanzinstitute sind dann verpflichtet, auf Grundlage dieser Listen die betreffenden Konten zu sperren.

Der EDSB wurde beauftragt, die Auswirkungen dieses Verfahrens auf den Datenschutz zu bewerten, und unsere Stellungnahme wurde am 7. Mai 2014 veröffentlicht. Im Einklang mit unserem Ansatz in einer früheren *Stellungnahme*, in der es um das von der Europäischen Kommission eingesetzte Verfahren zum Einfrieren von Vermögenswerten ging, haben wir empfohlen, der Rat möge die Menge der Daten begrenzen, die in den Listen veröffentlicht werden. Dies würde bedeuten, dass nur veröffentlicht wird, was für die Identifizierung der betreffenden Personen wirklich erforderlich ist. Insbesondere haben wir unsere Zweifel zum Ausdruck gebracht, ob die Veröffentlichung der Gründe, aus denen jemand in der Liste aufgeführt wird, wirklich notwendig ist.

Gelegentlich stellt sich heraus, dass eine Person irrtümlich gelistet wurde. Dies ist in der Regel die Folge eines Versehens, oder die Gründe für die Listung sind entfallen. Das ist problematisch, denn der Rat streicht die fälschlich in die Liste Aufgenommen zwar wieder, doch der Umstand, dass sie einmal gelistet waren, bleibt im Amtsblatt öffentlich verzeichnet. Um hier Abhilfe zu schaffen, haben wir dem Rat empfohlen, nicht nur die Listen unverzüglich und in regelmäßigen Abständen zu korrigieren, sondern auch zusätzliche Maßnahmen zu ergreifen, um die Namen derer zu löschen, die fälschlich gelistet wurden. Dies könnte beispielsweise dadurch geschehen, dass die Gründe für die Löschung im Änderungsrechtsakt, der im Amtsblatt veröffentlicht wird, oder in einem Schreiben an die betroffene Person aufgeführt werden. Solche Schritte sollten den Betroffenen helfen, ihre Konten zu entsperren und eventuelle negative Folgen für ihren Ruf zu vermindern.

Stellungnahme des EDSB

Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von „Big Data“

Die Erhebung und der Besitz enormer Mengen personenbezogener Daten sind für die größten Akteure im globalen Markt der Internetdienstleistungen eine Quelle von Marktmacht, erklärte der Europäische Datenschutzbeauftragte (EDSB) nach der Veröffentlichung unserer vorläufigen Stellungnahme *Privatsphäre und Wettbewerbsfähigkeit im Zeitalter von „Big Data“: das Zusammenspiel zwischen Datenschutz, Wettbewerbsrecht und Verbraucherschutz in der digitalen Wirtschaft*. Personenbezogene Daten sind zu einer Art von Währung geworden, mit der man für sogenannte „kostenlose“ Online-Dienste bezahlt, und sie bilden für eine wachsende Zahl von in der EU tätigen Unternehmen einen wertvollen immateriellen Vermögenswert. Das macht eine stärkere Interaktion zwischen den verschiedenen Regulierungsstellen erforderlich.

Die Entwicklung von ‚Big Data‘ hat Lücken in der EU-Wettbewerbs-, Verbraucherschutz- und Datenschutzpolitik, die anscheinend nicht mit diesen Entwicklungen schrittgehalten haben, aufgezeigt. Eine intelligentere Zusammenarbeit in diesen sich teilweise überlappenden Politikbereichen wird Wachstum und Innovation unterstützen und mögliche negative Folgen für die Verbraucher minimieren. Der EDSB ist darüber erfreut, dass er Diskussionen zwischen Aufsichtsbehörden und Experten in diesen Bereichen erleichtern kann.“

Peter Hustinx, EDSB

Stellungnahme des EDSB

Geschäftliche E-Mails oder personenbezogene Daten?

Als ein früherer EU-Bediensteter eine Beschwerde beim EDSB einlegte, in der es um den Zugang zu seinem dienstlichen E-Mail-Konto ging, bot sich uns eine Gelegenheit zur Definition, was genau in diesem Zusammenhang als personenbezogene Daten gelten sollte.

Unsere Bewertung dieses Aspekts folgte dem Ansatz des *Papiers der Artikel 29-Arbeits-gruppe* zum Begriff „personenbezogene Daten". Auf dieser Grundlage gelten die E-Mail-Adresse, der Name des Bediensteten, wenn er in E-Mails und deren Anhängen erwähnt wird, sowie die zugehörigen Verbindungsdaten zum Zeitpunkt, zu dem ein Bediensteter die E-Mail gesendet oder empfangen hat, als personenbezogene Daten der betreffenden Person. Der Inhalt der E-Mails und der zugehörigen Anhänge in einem E-Mail-Konto gelten aber nur als personenbezogene Daten eines Bediensteten, wenn sie auf ihn als betroffene Person Bezug nehmen. Hierzu könnten E-Mails zur Beurteilung und zu Aspekten des Arbeitsvertrages des Bediensteten, zu ihn betreffenden internen Untersuchungen oder Verfahren sowie die persönliche Einschätzung bestimmter Situationen des Bediensteten oder seines Verhaltens zählen.

Nur weil jemand das Recht auf Zugang zu personenbezogenen Daten hat, folgt daraus aber nicht, dass er automatisch berechtigt ist, Kopien aller Dokumente oder E-Mails zu erhalten. Welche Maßnahme zu ergreifen ist, hängt von den Umständen ab: Manchmal wird es erforderlich sein, eine Kopie der Dokumente bereitzustellen, in anderen Situationen jedoch könnte es beispielsweise angemessener sein, in den Räumen der EU-Einrichtung oder des Organs direkten Zugang zu den Dokumenten zu gewähren – was nach der *EU-Datenschutzverordnung* als *„Mitteilung in verständlicher Form"* einzustufen ist.

Festlegung einer Definition von personenbezogenen Daten

Zum selben Thema haben wird eine Entscheidung über eine Beschwerde gegen das Europäische Amt für Betrugsbekämpfung (OLAF) angenommen. Der Beschwerdeführer brachte u. a. vor, OLAF habe sein Zugriffsrecht nicht in vollem Umfang geachtet.

Im Umgang mit dem Beschwerdeführer hatte das OLAF eine eingeschränkte Auslegung von Artikel 2 der *Verordnung (EG) Nr. 45/2001* vertreten. Der EDSB ist jedoch der Auffassung, dass Artikel 2 der Verordnung den Begriff der personenbezogenen Daten viel weiter fasst. Nach Artikel 2 Buchstabe a der Verordnung sind personenbezogene Daten nämlich „alle Informationen über eine bestimmte oder bestimmbare natürliche Person".

Diese Definition schließt offensichtlich mehr als nur den Namen einer Person ein. Auch hier haben wir zur Begründung unserer Entscheidung wieder auf den Ansatz der *Artikel 29-Arbeitsgruppe* zurückgegriffen. Die Artikel 29-Arbeitsgruppe stellt klar, dass zu den Informationen „über" eine Person im Sinne von Artikel 2 Buchstabe a auch Informationen gehören, die die Identität, die Merkmale oder das Verhalten einer Person betreffen, oder die verwendet werden, um die Art festzulegen oder zu beeinflussen, in der die Person behandelt oder beurteilt wird, oder deren Verwendung sich auf die Rechte und Interessen dieser Person auswirken könnte. Im Lichte dieser Definition von personenbezogenen Daten forderte der EDSB das OLAF daher auf, die Antwort zu überdenken, die es dem Beschwerdeführer auf dessen Zugriffsersuchen ursprünglich erteilt hatte.

Datenschutzgrundsätze gegen Vorratsdatenspeicherung

Im Rahmen einer internen Untersuchung bei einer anderen europäischen Einrichtung forderten die Untersuchungsbeauftragten des Europäischen Amtes für Betrugsbekämpfung (OLAF) die Unterlagen zu dienstlichen Telefongesprächen an, die über das dienstliche Mobiltelefon der Person geführt worden waren, gegen die ermittelt wurde. Wie sich herausstellte, war ein Datenumfang von mehreren Jahren verfügbar. Nach der *EU-Datenschutzverordnung* ist die Speicherung solcher Daten länger als sechs Monate aber unzulässig, wenn diese nicht für ein Gerichtsverfahren benötigt werden, das am Ende dieses Zeitraums bereits anhängig ist.

In der Konsultation wurden wir um Prüfung gebeten, ob diese Unterlagen dem OLAF noch zur Verfügung gestellt werden könnten. Angesichts des Umstands, dass schon die Speicherung dieser Unterlagen unrechtmäßig war, empfahlen wir, diese Unterlagen nicht den Ermittlern zu übergeben, sondern zusammen mit allen anderen Kommunikationsbelegen, die die Einrichtung länger als sechs Monate gespeichert hatte, zu vernichten. Außerdem empfahlen wir der betreffenden Einrichtung die Einführung eines Systems um sicherzustellen, dass Aufbewahrungsfristen in Zukunft nicht überschritten werden. Die Einrichtung hat entsprechend reagiert und beide Empfehlungen umgesetzt.

Die EU soll einen Raum der Freiheit, der Sicherheit und des Rechts schaffen, in dessen Mittelpunkt die Rechte des Einzelnen stehen

Der EDSB hat den Europäischen Rat dazu aufgefordert, die Rechte von Personen in den Mittelpunkt der Rechts- und Sicherheitspolitik der kommenden Jahre zu stellen. Die Absicht des Europäischen Rates, unter den aktuellen Verträgen strategische Leitlinien für die weitere gesetzgeberische und operative Planung im Raum der Freiheit, der Sicherheit und des Rechts zu definieren, ist eine Möglichkeit, den Ansatz der EU in diesen Themen¬bereichen neu zu beleben und den Vertrauensverlust nach den Enthüllungen zur Massen¬überwachung zu reparieren. In seiner heute veröffentlichten Stellungnahme zur weiteren Entwicklung des Raums der Freiheit, der Sicherheit und des Rechts betont der EDSB, dass es einer umfassenderen Integration des Schutzes der Privatsphäre und des Datenschutzes in die Tätigkeiten aller EU-Einrichtungen bedarf.

Die Tatsache, dass der Gerichtshof der Europäischen Union kürzlich die Richtlinie zur Vorratsdatenspeicherung als übermäßigen Eingriff in das Recht auf Datenschutz für nichtig erklärt hat, sollte einen Weckruf für die EU darstellen. Die Politikgestalter müssen angemessene Begrenzungen und Schutzmaßnahmen in einer besser informierten und systematischeren Weise einbringen, wenn sie Vorschläge, die signifikante Auswirkungen auf Grundrechte haben, vorlegen.

Peter Hustinx, EDSB

Stellungnahme des EDSB:

Arbeitsuche leicht (und datenschutzfreundlich) gemacht

Das EURES-Portal zur beruflichen Mobilität bietet Arbeitsuchenden aus der gesamten EU Informationen, Beratung und Arbeitsvermittlungsdienste. Arbeitsuchende können ihren Lebenslauf in die EURES-Datenbank hochladen und nach Stellen suchen und sich darauf bewerben, während Arbeitgeber nach Lebensläufen suchen können, die ihren offenen Stellen entsprechen. EURES wird derzeit umgestellt; dadurch wächst die Fähigkeit des Portals, Stellenanzeigen und Stellengesuche automatisch abzugleichen. Dies ist für Arbeitsuchende zwar von Vorteil, erhöht aber das Risiko für die Privatsphäre. Aus diesem Grund hat die Europäische Kommission eine neue Verordnung vorgeschlagen, die den Rechtsrahmen des Portals auf den neuesten Stand bringen und die Daten der Arbeitsuchenden besser schützen soll.

In unserer Stellungnahme vom 3. April 2014 haben wir begrüßt, dass der Vorschlag der Kommission die ausdrückliche Einwilligung der betroffenen Arbeitskräfte verlangt und ihren Rechten auf Auskunft über ihre Daten und auf deren Berichtigung angemessen Rechnung trägt. Wir haben außerdem empfohlen, dass der Vorschlag klarer regeln sollte, wer Zugang zu der Datenbank haben kann, welche Vorkehrungen vorgesehen sind, um einem Missbrauch des Systems vorzubeugen, und wie der automatische Abgleich funktioniert. Wir haben ferner empfohlen, dass die Verordnung eine Regelung vorsehen sollte, nach der Personen, die das EURES-Portal abfragen, keinen direkten Zugriff auf Namen, Lebensläufe oder andere direkt identifizierbare personenbezogene Daten von Bewerbern erhalten, sofern eine Arbeitskraft nicht entschieden hat, ihren gesamten Lebenslauf bei EURES einzustellen. Wir haben schließlich empfohlen, den Zweck der Verarbeitung und die annehmbare Bandbreite der Weiterverwendung der bei EURES gespeicherten Daten genau festzulegen.

Stellungnahme des EDSB

Eine Strategie für den Schutz von Geschäftsgeheimnissen

In ihrem Bestreben, in der EU wirtschaftliches Wachstum zu fördern, einen wettbewerbsfähigen Arbeitsmarkt zu schaffen und Produkte und Dienstleistungen von hoher Qualität bereitzustellen, hat die Europäische Kommission 2011 ihre Strategie *Ein Binnenmarkt für Rechte des geistigen Eigentums* vorgestellt. In deren Rahmen nahm die Kommission Ende 2013 einen Vorschlag für eine Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung an, zu der der EDSB konsultiert wurde.

In diesem Vorschlag wird das Konzept des Geschäftsgeheimnisses bzw. der „Geschäftsinformationen" als etwas beschrieben, das „über das technologische Wissen hinausgeht und auch Geschäftsdaten wie Informationen über Kunden und Lieferanten" einschließt – hierzu zählen auch personenbezogene Daten.

Der Vorschlag der Kommission konzentriert sich auf die Rechte der Person, die im Besitz des Geschäftsgeheimnisses ist. Er zielt darauf ab, ein ausreichendes und vergleichbares Rechts-schutzniveau innerhalb des Binnenmarkts in Fällen einer rechtswidrigen Aneignung von Geschäftsgeheimnissen sicherzustellen und gleichzeitig ausreichende Schutzmaßnahmen zur Verhinderung eines missbräuchlichen Verhaltens zu treffen. Auf diese Weise sollen durch den Vorschlag Investoren angezogen und gebunden und das Vertrauen in die Wettbewerbs-fähigkeit europäischer Unternehmen erhöht werden. Um der Richtlinie nachzukommen, müssten die Mitgliedstaaten Maßnahmen ergreifen, um geheime Informationen zu schützen, die rechtmäßig im Besitz natürlicher oder juristischer Personen sind.

In unserer Stellungnahme vom 12. März 2014 haben wir uns auf die Verpflichtungen der Träger von Geschäftsgeheimnissen konzentriert, die für die Verarbeitung personenbezogener Daten den Personen gegenüber verantwortlich sind, für deren Daten sie verantwortlich sind (für die Verarbeitung Verantwortliche gegenüber betroffenen Personen). Unsere Empfehlungen bezogen sich u. a. auf folgende Punkte:

- Der Zusammenhang zwischen personenbezogenen Daten und dem Begriff des Geschäftsgeheimnisses muss geklärt werden,
- zwischen „Geschäftsgeheimnis" und „Betriebs- oder Geschäftsgeheimnis" muss genau unterschieden werden,
- die Anwendung anderer EU-Rechtsvorschriften ist weiter zu klären, und
- die vorgeschlagene Richtlinie darf die Rechte der EU-Bürger und insbesondere ihr Recht auf Zugang zu den verarbeiteten Daten nicht beeinträchtigen.

Stellungnahme des EDSB

Privatsphäre und internationale Sicherheit ins Gleichgewicht bringen

Das Abkommen zwischen der EU und den USA über das Programm zum Aufspüren der Finanzierung des Terrorismus (*Terrorist Finance Tracking Program*, TFTP) wird zur Informationssammlung und zur Verhütung terroristischer Angriffe durch den Austausch von Informationen über finanzielle Transaktionen zwischen der EU und den USA genutzt. *Artikel 11 des EU-USA-TFTP* verpflichtet die Europäische Kommission zur Durchführung einer Studie über die mögliche Einführung eines mit dem TFTP vergleichbaren EU-Systems, dem System zum Aufspüren der Terrorismusfinanzierung (*Terrorist Finance Tracking System*, TFTS), das eine gezieltere Datenübermittlung aus der EU in die USA erlaubt. Mit diesem System hätte die EU eine stärkere Kontrolle über die Daten ihrer Bürger, als dies beim derzeitigen Abkommen der Fall ist, von dem viele glauben, es gefährde die Daten von EU Bürgern.

Die von der Kommission zur Einführung des TFTS durchgeführte Folgenabschätzung – ein rechtlicher und technischer Rahmen für die Extraktion der Daten auf dem Gebiet der EU – enthält eine Analyse, die sich auf die Grundsätze von Notwendigkeit, Angemessenheit, Kostenwirksamkeit und Schutz der Grundrechte stützt. In Anbetracht dieser Grundsätze kommt die Kommission zu dem Schluss, dass „derzeit keine klare Notwendigkeit besteht, einen Vorschlag zur Schaffung einer EU-eigenen TFTS vorzulegen".

In unseren förmlichen Kommentaren vom 17. April 2014 haben wir diese Schlussfolgerung sowie die ihr zugrunde liegende Argumentation begrüßt. Allerdings haben wir darauf hinge-wiesen, dass die Kommission dieselbe Analyse hätte durchführen sollen, um zu prüfen, ob das TFTP-Abkommen zwischen der EU und den USA fortgesetzt, geändert oder gekündigt werden sollte, und betont, dass eine umfassende Analyse durchgeführt werden muss. Nach den Überwachungsenthüllungen des letzten Jahres, die viele dazu veranlasst haben, die Zuverlässigkeit und Sicherheit des TFTP-Abkommens erneut in Frage zu stellen, und vor dem Hintergrund des jüngsten Urteils des Gerichtshofs der Europäischen Union zur Vorratsdatenspeicherung (verbundene Rechtssachen C-293/12 und C-594/12 *Digital Rights Ireland*), mit dem die Richtlinie 2006/24/EG für ungültig erklärt wurde, ist dies besonders wichtig.

Im Hinblick auf die Folgenabschätzung fanden wir enttäuschend, dass die Analyse keine gründlichere Untersuchung anderer Optionen einschloss, die für die EU an Stelle eines TFTS verfügbar sind. Auch wurden weder die Schlussfolgerungen des Berichtes der *Gemeinsamen Kontrollinstanz (GKI)* von Europol über ihre Kontrolle der Durchführung des Abkommens noch die Analyse der *Artikel 29-Arbeitsgruppe* berücksichtigt, die sich mit der massiven Natur des Transfers von Finanzdaten aus der EU in die USA und den Grenzen eines wirksamen juristischen und administrativen Rechtsschutzes befasst. Die Klärung dieser Fragen ist von entscheidender Bedeutung, wenn die EU ein besseres Konzept entwickeln soll.

Kommentare des EDSB

EDSB fordert ICANN auf, die Erhebung und Speicherung personenbezogener Daten zu beschränken

Die Internet Corporation for Assigned Names and Numbers (*ICANN*) hat in Zusammenhang mit ihrem Registrar-Vertrag 2013 eine öffentliche Konsultation zur Erhebung und Speicherung von Daten durchgeführt. Als unterzeichnetes Abkommen zwischen ICANN und den Registraren, die Eigner der Domainnamen sind, soll der Vertrag die Rechenschaftspflicht und Transparenz in der Domainnamen-Branche fördern.

In unserem Schreiben vom 17. April 2014 forderte der EDSB ICANN auf, an führender Position dafür zu sorgen, dass bei der Konzeption neuer Tools und Instrumente oder neuer Internetstrategien der Schutz der Privatsphäre und der Datenschutz standardmäßig berücksichtigt werden (eingebauter Datenschutz), und zwar zum Nutzen aller Internetnutzer, nicht nur der europäischen. Wir empfahlen ICANN, die Anforderungen an die Erhebung personenbezogener Daten im Registrar-Vertrag „standardmäßig" auf das zu reduzieren, was für die Erfüllung des Vertrags zwischen dem Registrar und dem Registranten (z. B. Abrechnung) oder für andere kompatible Zwecke wie die Bekämpfung von Betrug bei der Registrierung von Domainnamen unbedingt erforderlich ist. Außerdem sollten die Daten nicht länger gespeichert werden, als es für diese Zwecke erforderlich ist, und auch nicht für andere Zwecke wie die Strafverfolgung oder die Durchsetzung von Urheberrechten.

Kommentare des EDSB

Verkehrsinformationsdienste schlagen neue Richtung ein

Zwischen Dezember 2013 und März 2014 hat die Europäische Kommission eine öffentliche Konsultation zu EU-weiten Echtzeit-Verkehrsinformationsdiensten durchgeführt. Diese Dienste versorgen Verkehrsteilnehmer mit hilfreichen und zeitnahen Informationen zu Themen wie Verkehrsvorschriften, Fahrtrouten, geschätzten Fahrzeiten und möglichen Verzögerungen bei der Reise. Mit der öffentlichen Konsultation sollten die Meinungen interessierter Kreise gesammelt werden, um herauszufinden, welche Probleme es mit den derzeitigen Diensten gibt, um Verbesserungsmöglichkeiten zu ermitteln sowie Spezifikationen und Standards für die künftige Bereitstellung dieser Dienste zu erarbeiten.

In unseren förmlichen Kommentaren vom 12. März 2014 betonten wir, dass die Erhebung und Verwendung von Echtzeit-Verkehrsinformationen die Verarbeitung personenbezogener Daten zur Folge haben kann. Dies ist besonders für den Umgang mit Ausrüstungen wie der ECall-Plattform oder GPS von Bedeutung, über die Nutzerdaten erhoben werden. Wir haben daher empfohlen, dass die Kommission bei der Umsetzung künftiger Spezifikationen oder Rechtsvorschriften in diesem Bereich das EU-Datenschutzrecht und insbesondere die Richtlinien 95/46/EG und 2002/58/EG in vollem Umfang berücksichtigen sollte. Dazu muss die Kommission sicherstellen, dass das Konzept der Privatsphäre schon während der Entwurfsphase in der IT-Infrastruktur und in der Software berücksichtigt wird (eingebauter Datenschutz). Außerdem muss es angemessene Garantien für die Erhebung und Weiterverwendung von Ortungsdaten geben, und wir haben die Kommission erinnert, dass der EDSB vor der Annahme von neuen Spezifikationen in diesem Bereich zu konsultieren ist.

Kommentare des EDSB

Ein modernes Internet-Governance Modell sollte universell sein und Grundrechte wahren

Die Bemühungen der EU zur Schaffung eines Modells, das Internet-Governance und Datenschutz integriert, sollte durch eine effektive Reform des EU-eigenen Rechtsrahmens und die zügige Annahme der Datenschutz-Grundverordnung ergänzt werden, sagte der EDSB nach der Veröffentlichung seiner Stellungnahme zur Mitteilung der Kommission zur Internet-Politik und Internet-Governance – Europas Rolle bei der Mitgestaltung der Zukunft der Internet-Governance.

Stellungnahme des EDSB
EDSB Pressemitteilung

Zehn Jahre EDSB: Unsere Rolle und die Organe und Einrichtungen der EU

Der EDSB hat ein neues Strategiepapier veröffentlicht, in dem er erläutert, wie wir die EU-Einrichtungen in den Bereichen Politik und Rechtsvorschriften beraten. Darin werden insbesondere die bedeutenden Veränderungen im rechtlichen, wirtschaftlichen und technologischen Umfeld berücksichtigt, zu denen es seit 2004, dem Gründungsjahr unserer Einrichtung, gekommen ist, darunter vor allem das Inkrafttreten des Vertrags von Lissabon sowie eine Reihe von richtungsweisenden Entscheidungen des Europäischen Gerichtshofs, in denen die Bedeutung der Privatsphäre und des Datenschutzes als integrale Bestandteile der Entscheidungsfindung in der EU unterstrichen wurde.

Nach Artikel 28 Absatz 2 der Datenschutzverordnung ist die Kommission zur Konsultation des EDSB verpflichtet, wenn sie einen Vorschlag für Rechtsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten annimmt. Die Reichweite dieser Verpflichtung ist groß, und so ist es bewährte Praxis, dass der EDSB auch *informell* konsultiert wird, bevor solche Vorschläge von der Kommission angenommen werden.

Um die Wirkung und den Nutzen unserer Arbeit zu maximieren, entwickeln wir einen „Politikbaukasten", der eine allgemeine Anleitung für den Gesetzgeber enthält, beispielsweise in Form von themenbezogenen oder branchenspezifischen Leitlinien. Er soll den Einrichtungen helfen, fundierte Entscheidungen zu den Auswirkungen neuer Vorschläge auf den Datenschutz zu treffen.

Strategiepapier


The EDPS as an advisor to EU institutions on policy and legislation: building on ten years of experience

Policy paper

Brussels, 4 June 2014

ANGELEGENHEITEN VOR DEM GERICHTSHOF

Google zur Achtung des „Rechts auf Vergessen" verurteilt

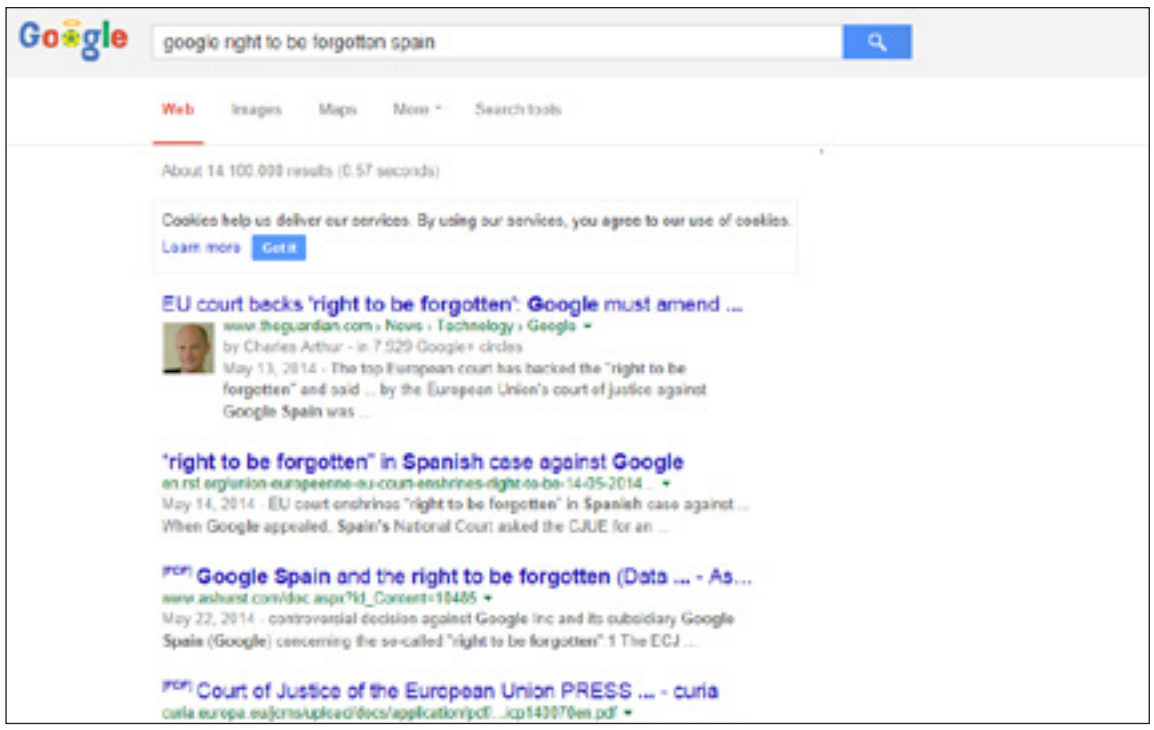
Am 13. Mai 2014 hat der Gerichtshof der Europäischen Union erneut ein außerordentlich wichtiges Urteil gefällt. Bei dieser Sache mussten einige Schlüsselbestimmungen der Datenschutzrichtlinie 95/46/EG im Kontext einer Einzelperson ausgelegt werden: Herr Costeja Gonzalez hatte beantragt, seine personenbezogenen Daten aus der Ergebnisliste zu streichen, die von der Google-Suchmaschine veröffentlicht wird.

Der Gerichtshof stellte erstens klar, dass die Aktivität einer Internet-Suchmaschine tatsächlich als „Verarbeitung personenbezogener Daten" einzustufen ist, und dass der Betreiber der Suchmaschine der für diese Verarbeitung *Verantwortliche* ist. Zweitens hat der Gerichtshof entschieden, dass die Datenschutzrichtlinie auf Unternehmen mit Sitz in einem Drittland (wie den USA) anzuwenden ist, die in der EU über eine Zweigniederlassung oder Tochterfirma tätig sind. In dieser Sache wurde die Richtlinie für anwendbar gehalten, weil die Tätigkeiten von Google Inc. (die Suchmaschine) und von Google Spanien (das für die Förderung des Verkaufs der Werbeflächen verantwortlich ist) „untrennbar miteinander verbunden" sind. Zum sogenannten „Recht auf Vergessen" entschied der Gerichtshof schließlich, dass Personen berechtigt sind, die Löschung ihrer Daten zu fordern – Grundlage hierfür sind das Recht auf Löschung und das Widerspruchsrecht, die beide in der Richtlinie verankert sind , und zwar nicht nur, wenn die personenbezogenen Daten ungenau sind, sondern immer dann, wenn die Verarbeitung den Bestimmungen der Richtlinie nicht entspricht. Entsprechende Anträge können direkt bei der Suchmaschine gestellt werden.

Die an der Artikel 29-Arbeitsgruppe beteiligten europäischen Datenschutzbehörden werden die Entscheidung jetzt prüfen und Leitlinien bereitstellen, um einen gemeinsamen Ansatz für die EU-weite Umsetzung der Entscheidung zu entwickeln.

Urteil

Pressemitteilung der Artikel 29-Arbeitsgruppe



Gerichtshof erklärt EU-Richtlinie zur Vorratsdatenspeicherung für ungültig

Am 8. April hat der Gerichtshof der Europäischen Union sein Urteil in den verbundenen Rechtssachen C-293/12 und C-594/12 *Digital Rights Ireland und Seitlinger u. a.* gesprochen. In einer richtungsweisenden Entscheidung (zu der der EDSB vom Gerichtshof eingeladen worden war, sich in einer Anhörung zu äußern) erklärte der Gerichtshof die Richtlinie über die Vorratsspeicherung von Daten 2006/24/EG für ungültig.

Die Entscheidung betont den Wert, der dem Schutz der Grundrechte als zentralem Element der EU-Politik beigemessen wird. Tatsächlich ist dies das erste Mal, dass eine Richtlinie ausschließlich aufgrund ihrer Unvereinbarkeit mit der EU-Grundrechtecharta insgesamt für ungültig erklärt wird. Außerdem werden klare Grenzen für jede flächendeckende staatliche Überwachung von Verbindungsdaten (oder „Metadaten") gesetzt. Der Gerichtshof unterstrich insbesondere, dass die Vorratsdatenspeicherung einen gravierenden und ungerechtfertigten Eingriff in das Grundrecht auf Privatheit darstellt, das in Artikel 7 der EU-Grundrechtecharta verankert ist. Wenn ein EU-Rechtsakt Pflichten auferlegt, die in dieses Recht eingreifen, muss der europäische Gesetzgeber für die notwendigen Garantien sorgen; er darf diese Verantwortung nicht vollumfänglich den Mitgliedstaaten überlassen.

Das Urteil bedeutet auch, dass die EU in Diskussionen mit Drittländern, darunter insbesondere die USA, in Bezug auf den Zugang zu Verbindungsdaten von EU-Ansässigen und ihre Verwendung eine feste Haltung einnehmen sollte.

Urteil

Angriff auf den Kern der Privatsphäre im Internet

Im April dieses Jahres wurde in OpenSSL, einem beliebten Verschlüsselungstool, das bei der Internetkommunikation für den Schutz der Privatsphäre und für Sicherheit sorgen sollte, eine gravierende Schwachstelle entdeckt: der Heartbleed-Bug (CVE-2014-0160). Bei anfälligen Versionen von OpenSSL ermöglicht der Heartbleed-Bug das Lesen von Daten, die geschützt werden sollten, und den Zugriff darauf. Damit bleiben Internetanwendungen wie E-Mails, Sofortnachrichten, Websurfen und und virtuelle private Netze (VPN) gegen die Ausbeutung und den möglichen Diebstahl personenbezogener Daten ungeschützt.

Die Schwachstelle ist Teil der OpenSSL-Versionen seit 2012. Die anfälligen Funktionen werden auch in vielen verbreiteten Softwarepaketen genutzt, darunter einige kommerzielle Spiele- und Bürosoftware.

Angesichts der umfassenden und gravierenden Auswirkungen hat die Sicherheits-gemeinschaft insgesamt rasch auf den Fehler reagiert. Internetdienste wie Wikipedia, Yahoo und Amazon schienen alle angreifbar zu sein und haben anscheinend alle erforderlichen Maßnahmen ergriffen, um den Fehler in ihren Systemen schnell zu beheben. Auch die europäischen Einrichtungen haben Maßnahmen eingeleitet, um zu sichern, dass ihre Dienste nicht angegriffen werden können. Nutzern von betroffenen Diensten wurde empfohlen, ihre Passwörter zu ändern, und die für die Verschlüsselung des Internetverkehrs zwischen betroffenen Websites verwendeten Zertifikate wurden ausgetauscht. Als Reaktion auf diesen Vorfall hat die *Linux Foundation* eine neue Initiative gestartet, die darauf abzielt, die Qualität der Sicherheitsprüfungen für weit verbreitete quelloffene Software zu verbessern. Trotz aller dieser Maßnahmen kann es aber immer noch nicht aktualisierte Server geben, die daher immer noch die anfällige Software verwenden.

Heartbleed bedroht den Schutz personenbezogener Daten in gravierender Weise und zeigt gleichzeitig, dass es von entscheidender Bedeutung ist sicherzustellen, dass Computer und Internetsysteme, die zur Verarbeitung personenbezogener Daten verwendet werden, wirksam geschützt sind.

Technischer Schutz der Privatsphäre: Die IPEN-Initiative

Edward Snowdens Enthüllungen über die massive Internetüberwachung lösten eine Debatte zwischen Internettechnikern aus, die es als ihre Aufgabe ansehen, für den *Schutz der personenbezogenen Daten und der Privatsphäre* von Internetnutzern zu sorgen. Daraufhin wurden verschiedene bemerkenswerte Projekte in Angriff genommen, die Internetnutzer und ihre Privatsphäre besser schützen sollen. Das *Internet Privacy Engineering Network* (IPEN), das vom EDSB in Zusammenarbeit mit nationalen Datenschutzbehörden, akademischen Forschern und Ingenieuren ins Leben gerufen wurde, ist eines dieser Projekte. Es soll als Plattform für die Zusammenarbeit und den Gedankenaustausch zwischen Datenschutz-behörden (DSB) und Internettechnikern dienen.

Das IPEN will die Lücke zwischen technischen Hilfsmitteln (unter der Ägide von Ingenieuren und IT-Experten) und Datenschutzerfordernissen (für die das Gesetz maßgeblich ist) dadurch schließen, dass es die Entwicklung datenschutzfreundlicher Lösungen für verbreitete technische Probleme fördert und Entwickler zur Erkenntnis befähigt, wann ihre technischen Wahlmöglichkeiten Auswirkungen auf die Grundsätze der Privatsphäre haben.

Das IPEN soll ein Netz bilden, an dem sich Experten aus den Bereichen Technik, Entwicklung und Politik beteiligen. Die Zusammenarbeit in diesem Netz ist auf drei Hauptaufgaben ausgerichtet:

- Informationsaustausch über laufende Initiativen und Projekte, deren Gegenstand Entwicklungserfordernisse mit Bezug auf den Schutz der Privatsphäre sind,
- Identifizierung von *„use cases"* (Anwendungsfällen) – hierbei entwickeln Ingenieure eine Folge von Schritten, mit denen sie ein bestimmtes Problem lösen können –, bei denen der Schutz der Privatsphäre auf Entwurfsebene umgesetzt werden kann, und
- Einleitung von Entwicklungsprojekten für Instrumente und Baublöcke, die den Schutz der Privatsphäre ermöglichen und verbessern.

Außerdem wird das IPEN eine Datenbank relevanter Ressourcen aufbauen, deren Ergebnisse und Wissensgrundlagen für alle Teilnehmer, Entwickler und Privatsphärenexperten zugänglich sind.

Bislang ist das IPEN auf einer Reihe von Veranstaltungen vorgestellt worden und hat bei „Hackern", Entwicklern von quelloffener Software, Internet- und Webingenieuren, akademischen Forschern und Entwicklern sowie bei Experten der nationalen DSB Unterstützung gefunden.

Um weitere Informationen zu erhalten oder sich der IPEN-Initiative anzuschließen, setzen Sie sich bitte mit *ipen@edps.europa.eu* in Verbindung.

VERANSTALTUNGEN

Privatsphäre, Verbraucher, Wettbewerb und „Big Data“

Am 2. Juni 2014 war der EDSB Gastgeber eines Workshops, auf dem die Zusammenhänge zwischen den EU-Konzepten für Wettbewerb, Verbraucherschutz und Datenschutz vor dem sich rasch entwickelnden Hintergrund der digitalen Wirtschaft diskutiert werden sollten.

Zu den Experten aus Hochschulen, Denkfabriken und Rechtspraxis auf beiden Seiten des Atlantiks gesellten sich nationale und europäische Politikgestalter und Vertreter von Aufsichtsbehörden, um sich mit den verschiedenen Themen zu befassen, die der EDSB in seiner am 26. März 2014 veröffentlichten *vorläufigen Stellungnahme* erkundet hatte, darunter die Einschätzung von Marktmacht und Marktbeherrschung, das Interesse an der Verbraucherwohlfahrt und das Potenzial für Missbrauch und Ausnutzung in Branchen, in denen personenbezogene Daten im Austausch für „kostenlose“ Dienste als Währung gehandelt werden – häufig ohne dass sich der Verbraucher dessen in vollem Umfang bewusst wäre. Programmatische Vorträge eines früheren und eines derzeitigen Kommissars der *Federal Trade Commission* (FTC) machten die US-amerikanische Sicht auf Probleme deutlich, die als Folge der globalen und grenzenlosen Natur des „Big-Data-Ökosystems“ zunehmend auch andernorts auftreten.

Die Diskussionen bestätigen, dass in den verschiedenen Politikbereichen zwar unter-schiedliche Begriffe verwendet werden, sie aber mehr gemeinsam haben, als man zunächst annehmen würde. Der EDSB nahm mit Genugtuung zur Kenntnis, dass er einen Beitrag zur Förderung des Gesprächs zwischen Meinungsbildnern aus verschiedenen Fachgebieten leisten konnte. Es bestand ein klarer Konsens, dass mit der Ermittlung von Lücken und Synergien fortzufahren sei, und dass mit der Klärung begonnen werden müsse, welche Maßnahmen erforderlich sind und wer sie durchführen sollte.

Es handelte sich um eine geschlossene Veranstaltung nach der „Chatham-House-Regel“, um freie und ehrliche Diskussionen zu ermöglichen.

BEHÖRDLICHE DATENSCHUTZBEAUFTRAGTE

Die nächste Ausgabe des EDSB-Newsletters erscheint im Herbst.
Wir wünschen Ihnen einen schönen Sommer!

VORTRÄGE UND VERÖFFENTLICHUNGEN

- Redenotizen (*PDF*) zum Vortrag von Giovanni Buttarelli auf der Inet 2014, „*Internet: Privacy and Digital Content in a Global Context*“ (Internet: Privatsphäre und digitaler Inhalt in einem globalen Kontext), Istanbul (21. Mai 2014)
- „Wiederherstellung des Vertrauens in die transatlantischen Beziehungen“, Artikel (*PDF*) von Peter Hustinx, veröffentlicht in „*TELOS, Revista de Pensamiento sobre Comunicación, Tecnologia y Sociedad*“ (2. Mai 2014)

Über diesen Newsletter

Dieser Newsletter wird vom Europäischen Datenschutzbeauftragten herausgegeben – einer unabhängigen Behörde der EU, die im Jahr 2004 errichtet wurde und folgende Aufgaben hat:

- Überwachung der Verarbeitung personenbezogener Daten durch die EU-Verwaltung;
- Beratung zu Rechtsvorschriften im Bereich des Datenschutzes;
- Zusammenarbeit mit vergleichbaren Behörden, um einen kohärenten Datenschutz sicherzustellen.

Sie können diesen Newsletter über unsere Website abonnieren / abbestellen.

KONTAKT

www.edps.europa.eu
Tel: +32 (0)2 2831900
Fax: +32 (0)2 2831950
NewsletterEDPS@edps.europa.eu

POSTANSCHRIFT

EDSB
Rue Wiertz 60 – MTS Gebäude
B-1047 Brüssel
BELGIEN

DIENSTSTELLE

Rue Montoyer 30
B-1000 Brüssel
BELGIEN

Folgen Sie uns auf Twitter: @EU_EDPS

EDSB – Der europäische Hüter des Datenschutzes

QT-AC-14-002-DE-C doi:10.2804/61938 ISBN 978-92-95076-39-6