



## SCHUTZ PERSONENBEZOGENER DATEN

Der Schutz personenbezogener Daten und die Achtung der Privatsphäre sind wichtige Grundrechte. Das Europäische Parlament betont seit jeher, dass ein ausgewogenes Verhältnis zwischen der Stärkung der Sicherheit und der Wahrung der Menschenrechte hergestellt werden muss, was auch den Datenschutz und den Schutz der Privatsphäre umfasst. Im Mai 2018 traten neue Datenschutzregelungen der EU in Kraft, durch die die Rechte der Bürger gestärkt und die Vorschriften für Unternehmen im digitalen Zeitalter vereinfacht wurden.

### RECHTSGRUNDLAGE

Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV);  
Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union.

### ZIELE

Die Union muss für die konsequente Anwendung des in der Charta der Grundrechte der EU verankerten Grundrechts auf Datenschutz sorgen. Die Position der EU zum Schutz personenbezogener Daten muss bei allen EU-Maßnahmen, einschließlich jener in den Bereichen Strafverfolgung und Verbrechensvorbeugung, sowie in den internationalen Beziehungen gestärkt werden, insbesondere in einer globalen Gesellschaft, die von raschem technologischem Wandel geprägt ist.

### ERGEBNISSE

#### A. Institutioneller Rahmen

##### 1. Vertrag von Lissabon

Vor dem Inkrafttreten des Vertrags von Lissabon waren die Rechtsvorschriften zum Datenschutz im Raum der Freiheit, der Sicherheit und des Rechts (RFSR) zwischen der ersten Säule (Datenschutz für private und gewerbliche Zwecke, unter Anwendung der Gemeinschaftsmethode) und der dritten Säule (Datenschutz für Strafverfolgungszwecke, auf zwischenstaatlicher Ebene) aufgeteilt. Daraus ergab sich, dass sich der Beschlussfassungsprozess in den beiden Bereichen an zwei verschiedenen Regelwerken ausrichtete. Der Vertrag von Lissabon löste die Säulenstruktur auf und bietet so eine bessere Grundlage für die Entwicklung eines eindeutigeren und effektiveren Datenschutzsystems. Gleichzeitig sah er neue Befugnisse des Europäischen Parlaments vor und machte es zum Mitgesetzgeber. Gemäß Artikel 16 AEUV erlassen das Europäische Parlament und der Rat Vorschriften



über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen.

## **2. Strategische Leitlinien für den Raum der Freiheit, der Sicherheit und des Rechts**

Nach dem Programm von Tampere (Oktober 1999) und dem Haager Programm (November 2004) billigte der Europäische Rat im Dezember 2009 das mehrjährige Programm zum Raum der Freiheit, der Sicherheit und des Rechts für den Zeitraum 2010-2014, das sogenannte Stockholmer Programm. In seinen Schlussfolgerungen vom Juni 2014 legte der Europäische Rat gemäß Artikel 68 AEUV die strategischen Leitlinien für die legislative und operative Planung im RFSR in den nächsten Jahren fest. Eines der vorrangigen Ziele ist ein besserer Schutz personenbezogener Daten in der EU. Eine Halbzeitüberprüfung dieser Leitlinien wurde 2017 eingeleitet.

### **B. Wichtigste Rechtsakte zum Datenschutz**

#### **1. Charta der Grundrechte der Europäischen Union**

In Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union werden die Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten als eng verbundene, aber dennoch eigenständige Grundrechte angesehen. Die Charta wurde in den Vertrag von Lissabon einbezogen und ist für die Organe und Einrichtungen der EU sowie für ihre Mitgliedstaaten bei der Umsetzung des EU-Rechts rechtlich bindend.

#### **2. Europarat**

##### **a. Übereinkommen Nr. 108 von 1981**

Das Übereinkommen Nr. 108 des Europarates vom 28. Januar 1981 über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten ist das erste international verbindliche Rechtsinstrument im Bereich Datenschutz. Zweck des Übereinkommens ist es, „für jedermann [...] sicherzustellen, dass seine Rechte und Grundfreiheiten, insbesondere sein Recht auf einen Persönlichkeitsbereich, bei der automatischen Verarbeitung personenbezogener Daten geschützt werden“.

##### **b. Europäische Menschenrechtskonvention (EMRK)**

In Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950 ist das Recht auf Achtung des Privat- und Familienlebens verankert: „Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz“.

#### **3. Derzeitige EU-Rechtsakte zum Datenschutz**

Aufgrund der früheren Säulenstruktur wurde der Datenschutz auf EU-Ebene bis vor Kurzem durch verschiedene Rechtsakte geregelt. Dazu gehören die im Rahmen der früheren ersten Säule verabschiedeten Rechtsakte, wie beispielsweise die Richtlinie 95/46/EG zum Datenschutz (im Mai 2018 durch die Datenschutz-Grundverordnung ersetzt), die Richtlinie 2002/58/EG über Datenschutz in der elektronischen Kommunikation (2009 geändert; neuer Vorschlag wird derzeit geprüft) und die (wegen ihres schwerwiegenden Eingriffs in das Privatleben und den



Datenschutz am 8. April 2014 vom Gerichtshof der Europäischen Union für ungültig erklärte) Richtlinie 2006/24/EG über die Vorratsdatenspeicherung, sowie die Verordnung (EG) Nr. 45/2001 über die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft (neuer Vorschlag wird derzeit geprüft) und Rechtsakte im Rahmen der früheren dritten Säule wie der Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (im Mai 2018 ersetzt durch die Richtlinie zum Datenschutz bei der Strafverfolgung).

**a. Datenschutz-Grundverordnung (DS-GVO)**

Die Verordnung (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 (Datenschutz-Grundverordnung) trat im Mai 2018 in Kraft. Die Vorschriften dienen dazu, alle EU-Bürger in einer zunehmend datengestützten Welt vor Verletzungen der Privatsphäre und Datenschutzverletzungen zu schützen und gleichzeitig einen klareren und kohärenteren Rahmen für Unternehmen zu schaffen. Zu den neuen Rechten der Bürger gehören eine eindeutige und bestätigende Zustimmung zur Verarbeitung ihrer Daten und das Recht, klare und verständliche Informationen darüber zu erhalten, das Recht auf Vergessenwerden – Bürger können darum ersuchen, dass ihre Daten gelöscht werden –, das Recht auf Übertragung von Daten an einen anderen Dienstleistungsanbieter (z. B. bei einem Wechsel von einem sozialen Netz zu einem anderen) und das Recht, informiert zu werden, wenn sich jemand unberechtigten Zugang zu ihren Daten verschafft hat. Die neuen Vorschriften gelten für alle Unternehmen, die in der EU tätig sind, auch wenn sie ihren Sitz außerhalb der EU haben. Außerdem wird es möglich sein, Abhilfemaßnahmen wie Warnungen, Anordnungen oder Geldbußen gegen Unternehmen zu verhängen, die gegen die Vorschriften verstoßen.

**b. Richtlinie zum Datenschutz bei der Strafverfolgung**

Die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates trat im Mai 2018 in Kraft. Durch die Richtlinie wird das Grundrecht der Bürger auf Datenschutz bei der Verwendung personenbezogener Daten durch die Strafverfolgungsbehörden gewahrt. Dadurch wird sichergestellt, dass personenbezogene Daten von Opfern, Zeugen und Verdächtigen ordnungsgemäß geschützt werden, und die grenzüberschreitende Zusammenarbeit bei der Verbrechens- und Terrorismusbekämpfung wird erleichtert.

**4. Europäischer Datenschutzbeauftragter (EDSB) und Europäischer Datenschutzausschuss**

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Aufsichtsbehörde, die die Einhaltung der Datenschutzverpflichtungen durch die



Organe und Einrichtungen der EU sicherstellt. Die wichtigsten Aufgaben des EDSB sind Überwachung, Beratung und Zusammenarbeit. Der Europäische Datenschutzausschuss, die ehemalige Artikel-29-Datenschutzgruppe, hat den Status einer Einrichtung der EU mit Rechtspersönlichkeit und verfügt über ein unabhängiges Sekretariat. Der Europäische Datenschutzausschuss bringt die nationalen Datenschutzbehörden der EU, den EDSB und die Kommission zusammen. Der Europäische Datenschutzausschuss verfügt über weitreichende Befugnisse, um bei Streitigkeiten zwischen den nationalen Aufsichtsbehörden zu entscheiden und zu zentralen Konzepten der Datenschutz-Grundverordnung und der Richtlinie zum Datenschutz bei der Strafverfolgung zu beraten und zu unterstützen.

## **ROLLE DES EUROPÄISCHEN PARLAMENTS**

Das Parlament betont seit jeher, dass ein ausgewogenes Verhältnis zwischen der Stärkung der Sicherheit und dem Schutz der Privatsphäre und von personenbezogenen Daten erforderlich ist. Es hat verschiedene Entschlüsse zu diesen heiklen Themen angenommen, insbesondere in Bezug auf die Profilerstellung anhand der ethnischen Zugehörigkeit, den Prüm-Ratsbeschluss zur grenzüberschreitenden Zusammenarbeit bei der Bekämpfung von Terrorismus und grenzüberschreitenden Verbrechen, den Einsatz von Körperscannern zur Verbesserung der Flugsicherheit, biometrische Daten in Pässen sowie die Gemeinsame Konsularische Instruktion, Grenzmanagement, das Internet und „Data Mining“.

Das Parlament hat im Februar 2010 im Rahmen des Zustimmungsverfahrens die vorläufige Anwendung des Programms zum Aufspüren der Finanzierung des Terrorismus (TFTP; vormals SWIFT-Abkommen) abgelehnt, das der Weiterleitung von Daten zu Finanztransaktionen an die Vereinigten Staaten zum Zweck der Terrorismusbekämpfung diene. Nach der Annahme der Entschlüsse des Europäischen Parlaments vom 8. Juli 2010 trat das TFTP-Abkommen im August 2010 in Kraft. Im Juli 2011 legte die Kommission eine Mitteilung zu den wichtigsten Optionen für die Schaffung eines Systems zum Aufspüren der Terrorismusfinanzierung (EU TFTS) vor, hinsichtlich der das Parlament jedoch Bedenken äußerte. Im November 2013 gab die Kommission bekannt, dass sie derzeit keinen Vorschlag für ein EU TFTS vorzulegen gedenkt.

Ein weiteres Thema von großer Bedeutung ist das PNR-Abkommen zwischen der EU und den Vereinigten Staaten über die Verarbeitung und Weitergabe von Fluggastdatensätzen zwischen Luftfahrtgesellschaften und an das US-Heimatschutzministerium. Nachdem das Parlament seine Zustimmung erteilt hatte, nahm der Rat im April 2012 einen Beschluss über den Abschluss des neuen Abkommens an, das an die Stelle des früheren PNR-Abkommens mit den Vereinigten Staaten trat, welches seit 2007 vorläufig in Kraft war.

Im Februar 2011 legte die Kommission einen Vorschlag für eine Richtlinie zur Verwendung von Fluggastdatensätzen zum Zwecke der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität (EU PNR) vor. Im Juni 2013 beschloss das Plenum des Parlaments die Rücküberweisung der Angelegenheit an den Ausschuss für bürgerliche Freiheiten,



Justiz und Inneres (LIBE), der den Vorschlag zu EU-Fluggastdatensätzen aufgrund von Zweifeln an dessen Verhältnismäßigkeit und Grundrechtskonformität im April 2013 abgelehnt hatte. Nach den Terroranschlägen in Paris von 2015 und aufgrund neuer Bedenken hinsichtlich möglicher Bedrohungen der inneren Sicherheit der EU durch „ausländische Kämpfer“ ist die Diskussion über den Vorschlag zu EU-Fluggastdatensätzen neu entfacht. Im Dezember 2015 verständigten sich das Parlament und der Rat auf einen Kompromiss in dieser heiklen Angelegenheit. Die Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität sollte bis zum 25. Mai 2018 in innerstaatliches Recht umgesetzt werden.

Das Parlament war (im Rahmen des Zustimmungsverfahrens) an der Genehmigung eines rechtsverbindlichen Rahmenabkommens mit den Vereinigten Staaten über den Austausch von Informationen und Datenschutz (sog. „Umbrella Agreement“) beteiligt. Ziel ist ein hohes Niveau des Schutzes von personenbezogenen Informationen, die im Zuge der transatlantischen Zusammenarbeit bei der Bekämpfung des Terrorismus und der organisierten Kriminalität übermittelt werden. Durch die Unterzeichnung des Gesetzes über den Rechtsbehelf („Judicial Redress Act“) durch Präsident Obama im Februar 2016 wurde der Weg frei für die Unterzeichnung des Rahmenabkommens zwischen der EU und den Vereinigten Staaten am 2. Juni 2016. Parallel dazu wurde der „EU-US-Datenschutzschild“ eingeführt, mit dem ein hohes Datenschutzniveau für die Übermittlung von Geschäftsdaten sichergestellt werden sollte. Der „Datenschutzschild“ spiegelt die vom Gerichtshof der Europäischen Union in seinem Urteil vom Oktober 2015 festgelegten Auflagen wider, in dem der EuGH den „Safe Harbour“-Rahmen (freiwillige Datenschutzstandards für Unternehmen aus Drittländern, die personenbezogene Daten von EU-Bürgern in die Vereinigten Staaten übermitteln) für ungültig erklärte. Die Kommission nahm am 12. Juli 2016 den Durchführungsbeschluss gemäß der Richtlinie 95/46/EG über die Angemessenheit des vom „EU-US-Datenschutzschild“ gebotenen Schutzes an, der unmittelbar in Kraft trat. Seit dem 1. August 2016 können Unternehmen dem „Datenschutzschild“ mit dem US-Handelsministerium beitreten, das dann überprüft, ob ihre Datenschutzbestimmungen den gemäß dem „Datenschutzschild“ erforderlichen hohen Datenschutzstandards entsprechen. Das Parlament begrüßte in seiner Entschließung vom 26. Mai 2016 zur transatlantischen Datenübermittlung die Bemühungen, beim „Datenschutzschild“ wesentliche Verbesserungen im Vergleich zur „Safe Harbour“-Entscheidung – die dadurch ersetzt wurde – zu erreichen, und übte an einigen Punkten Kritik. In seiner Entschließung vom 6. April 2017 zur Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes<sup>[1]</sup> forderte das Parlament die Kommission auf, eine ordentliche Beurteilung durchzuführen und sicherzustellen, dass der EU-US-Datenschutzschild für zu gewerblichen Zwecken übermittelte Daten einen ausreichenden Schutz der personenbezogenen Daten von EU-Bürgern bietet, um der Charta der Grundrechte der EU und den neuen EU-Datenschutzvorschriften zu entsprechen.

---

[1] Angenommene Texte, [P8\\_TA\(2017\)0131](#).



Am 12. März 2014 nahm das Parlament eine Entschließung zu dem Überwachungsprogramm der Nationalen Sicherheitsagentur der Vereinigten Staaten, den Überwachungsbehörden in mehreren Mitgliedstaaten und den entsprechenden Auswirkungen auf die Grundrechte der EU-Bürger und die transatlantische Zusammenarbeit im Bereich Justiz und Inneres<sup>[2]</sup> an. Diese Entschließung beendete eine sechsmonatige parlamentarische Untersuchung über die elektronische Massenüberwachung von EU-Bürgern, die infolge der Enthüllungen vom Juni 2013 über mutmaßliche Ausspähungen durch die Vereinigten Staaten und einige EU-Mitgliedstaaten eingeleitet worden war. In dieser Entschließung forderte das Parlament die Aussetzung der „Safe Harbour“-Grundsätze zum Datenschutz und des Programms zum Aufspüren der Terrorismusfinanzierung. Am 29. Oktober 2015 nahm das Parlament eine Entschließung zur Weiterbehandlung seiner Entschließung vom 12. März 2014 zur elektronischen Massenüberwachung der Unionsbürger<sup>[3]</sup> an, in der es seine Forderung nach Aussetzung der „Safe Harbour“-Entscheidung und des Programms zum Aufspüren der Terrorismusfinanzierung bekräftigte.

Das Parlament war im Rahmen des ordentlichen Gesetzgebungsverfahrens an der Genehmigung der Datenschutzreform beteiligt (siehe vorangegangener Abschnitt). Durch die neuen Datenschutzbestimmungen werden die Grundrechte der Bürger im digitalen Zeitalter gestärkt und der Geschäftsverkehr erleichtert, indem die Vorschriften für Unternehmen im digitalen Binnenmarkt vereinfacht werden.

Kristiina Milt  
10/2018

---

[2] Angenommene Texte, [P7\\_TA\(2014\)0230](#).

[3] Angenommene Texte, [P8\\_TA\(2015\)0388](#).

