RAT DER EUROPÄISCHEN UNION

Brüssel, den 27. Januar 2012 (30.01)
(OR. en)

5852/12

DATAPROTECT 8
JAI 43
MI 57
DRS 10
DAPIX 11
FREMP 6

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	27. Januar 2012
Empfänger:	der Generalsekretär des Rates der Europäischen Union, Herr Uwe CORSEPIUS
Nr. Komm.dok.:	KOM(2012) 9 endgültig
Betr.:	Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen Der Schutz der Privatsphäre in einer vernetzten Welt Ein europäischer Datenschutzrahmen für das 21. Jahrhundert

Die Delegationen erhalten in der Anlage das Kommissionsdokument KOM(2012) 9 endgültig.

Anl.: KOM(2012) 9 endgültig

EUROPÄISCHE KOMMISSION

Brüssel, den 25.1.2012
KOM(2012) 9 endgültig

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

Der Schutz der Privatsphäre in einer vernetzten Welt
Ein europäischer Datenschutzrahmen für das 21. Jahrhundert

(Text von Bedeutung für den EWR)

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

Der Schutz der Privatsphäre in einer vernetzten Welt
Ein europäischer Datenschutzrahmen für das 21. Jahrhundert

(Text von Bedeutung für den EWR)

1. AKTUELLE HERAUSFORDERUNGEN IM BEREICH DES DATENSCHUTZES

Die Geschwindigkeit des technologischen Wandels und der Globalisierung hat die Art und Weise, in der die ständig anwachsende Menge personenbezogener Daten erfasst, abgerufen, verwendet und übermittelt wird, zutiefst verändert. Neue Methoden des Informationsaustauschs durch soziale Netze und die Fernspeicherung großer Datenmengen gehören für viele der 250 Millionen Internetnutzer in Europa inzwischen zum Alltag. Zugleich stellen personenbezogene Daten heutzutage für viele Unternehmen einen Vermögenswert dar. Die Erfassung, Zusammenstellung und Analyse von Daten potenzieller Kunden ist oft ein wichtiger Teil ihrer Geschäftstätigkeit[1].

In dieser neuen digitalen Umgebung **muss jeder seine persönlichen Informationen wirksam kontrollieren können.** Der Schutz personenbezogener Daten ist in Europa als Grundrecht in Artikel 8 der Charta der Grundrechte der Europäischen Union und in Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) verankert und entsprechend geschützt.

Fehlendes Vertrauen lässt Verbraucher zögern, online zu kaufen und neue Dienstleistungen in Anspruch zu nehmen. Ein hohes Datenschutzniveau ist daher auch unentbehrlich, um das Vertrauen in Online-Dienste zu stärken, das Potenzial der digitalen Wirtschaft auszuschöpfen und auf diese Weise **Wirtschaftswachstum und Wettbewerbsfähigkeit der EU** zu steigern.

In der EU bedarf es moderner, kohärenter Regeln für den freien Datenverkehr zwischen den Mitgliedstaaten. Unternehmen brauchen klare und einheitliche Vorschriften, die ihnen Rechtssicherheit geben und den Verwaltungsaufwand auf ein Mindestmaß begrenzen. Dies ist für das reibungslose Funktionieren des Binnenmarkts und die **Ankurbelung des Wirtschaftswachstums, die Schaffung neuer Arbeitsplätze und die Unterstützung von Innovationen** unverzichtbar[2]. Die Modernisierung der Datenschutzvorschriften der EU im Sinne einer Stärkung ihrer

---

[1] Der Markt für die Analyse sehr großer Datensätze steigt jährlich weltweit um 40 %: http://www.mckinsey.com/mgi/publications/big_data/.

[2] Siehe auch die Schlussfolgerungen des Europäischen Rates vom 23. Oktober 2011, in denen die Schlüsselrolle des Binnenmarkts für Wachstum und Beschäftigung sowie die Notwendigkeit der Vollendung des digitalen Binnenmarkts bis 2015 hervorgehoben wird.

Binnenmarktdimension stellt ein hohes Datenschutzniveau für den Einzelnen sicher und fördert Rechtssicherheit, Klarheit und Kohärenz. Daher spielt sie eine zentrale Rolle im Aktionsplan der Europäischen Kommission zur Umsetzung des Stockholmer Programms[3], in der Digitalen Agenda für Europa[4] und darüber hinaus für die Wachstumsstrategie der EU (Europa 2020)[5].

Die EU-Richtlinie von 1995[6], das zentrale Rechtsinstrument für den Schutz personenbezogener Daten in Europa, war ein Meilenstein in der Geschichte des Datenschutzes. Ihre Ziele, ein gut funktionierender Binnenmarkt und der wirksame Schutz der Grundrechte und -freiheiten der Menschen, gelten unvermindert. Allerdings wurde sie vor 17 Jahren angenommen, als das Internet noch in den Kinderschuhen steckte. In der heutigen neuen, dynamischen digitalen Umgebung bieten die bestehenden Regeln weder den erforderlichen Harmonisierungsgrad noch die notwendige Wirksamkeit, um das Recht auf den Schutz personenbezogener Daten zu garantieren. Aus diesem Grund schlägt die Europäische Kommission eine grundlegende Reform des EU-Datenschutzrechts vor.

Darüber hinaus wurde mit dem Vertrag von Lissabon in Artikel 16 AEUV eine neue Rechtsgrundlage für ein moderneres und umfassendes Konzept für den Datenschutz und den freien Verkehr personenbezogener Daten geschaffen, das auch den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen abdeckt[7]. Seine Entsprechung findet dieses Konzept in den Mitteilungen der Europäischen Kommission zum Stockholmer Programm und zum Aktionsplan zur Umsetzung des Stockholmer Programms[8], wonach „die Union eine umfassende Regelung zum Schutz personenbezogener Daten schaffen muss, die für sämtliche Zuständigkeitsbereiche der Union gleichermaßen gilt“ und dass sie „für eine konsequente Anwendung des Grundrechts auf Datenschutz sorgen“ muss.

Um die Reform des EU-Datenschutzrahmens auf transparente Weise vorzubereiten, hat die Kommission seit 2009 öffentliche Anhörungen zum Datenschutz[9] veranstaltet und intensive Gespräche mit Interessenvertretern geführt[10]. Am 4. November 2010 veröffentlichte die Kommission eine Mitteilung über ein Gesamtkonzept für den Datenschutz in der Europäischen Union[11], in der die wichtigsten Themen der Reform skizziert werden. Zwischen September und Dezember 2011 erörterte die Kommission in ausführlichen Gesprächen mit den nationalen Datenschutzbehörden in der EU und mit dem Europäischen Datenschutzbeauftragten die Möglichkeiten,

---

3 KOM(2010) 171 endg.

4 KOM(2010) 245 endg.

5 KOM(2010) 2020 endg.

6 Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31.

7 Im Bereich der Gemeinsamen Außen- und Sicherheitspolitik wird die Verarbeitung von Daten durch die Mitgliedstaaten in einem Ratsbeschluss auf der Grundlage von Artikel 39 AEUV geregelt.

8 KOM(2009) 262 und KOM(2010) 171.

9 Es wurden zwei öffentliche Anhörungen zur Reform des Datenschutzes eingeleitet, eine erste von Juli bis Dezember 2009 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm) und eine zweite von November 2010 bis Januar 2011 (http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm).

10 2010 fanden Anhörungen mit den Behörden der Mitgliedstaaten und dem privaten Sektor statt. Im November 2010 veranstaltete die für Justiz zuständige EU-Kommissarin Viviane Reding einen Runden Tisch zur Datenschutzreform. 2011 fanden zusätzlich Workshops und Seminare zu Einzelthemen (z.B. Meldung von Datenschutzverstößen) statt.

11 KOM(2010) 609.

wie in den EU-Mitgliedstaaten eine einheitlichere Anwendung der Datenschutzvorschriften erreicht werden kann[12].

Aus diesen Gesprächen ging eindeutig hervor, dass sowohl Bürger als auch Unternehmen eine umfassende Reform der EU-Datenschutzvorschriften durch die Kommission wünschten. Nach Abschätzung der Folgen verschiedener Optionen[13] schlägt die Europäische Kommission jetzt einen **soliden und kohärenten politikübergreifenden Rechtsrahmen vor, mit dem die Rechte der Menschen gestärkt, die Binnenmarktdimension des Datenschutzes gefördert und der Verwaltungsaufwand für Unternehmen verringert wird**[14]. Dem Vorschlag der Kommission zufolge soll dieser Rechtsrahmen aus zwei Teilen bestehen:

– einer **Verordnung** (die die Richtlinie 95/46/EG ersetzt), mit der ein allgemeiner EU-Datenschutzrahmen geschaffen wird[15],

– und einer **Richtlinie** (die den Rahmenbeschluss 2008/977/JI[16] ersetzt) mit Regeln für den Schutz personenbezogener Daten, die zum Zweck der **Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten und für damit verbundene justizielle Tätigkeiten** verarbeitet werden.

Diese Mitteilung gibt einen Überblick über die wichtigsten Aspekte der Reform des EU-Datenschutzrechts.

2. DAFÜR SORGEN, DASS DER EINZELNE DIE KONTROLLE ÜBER SEINE PERSONENBEZOGENEN DATEN HAT

Im Rahmen der Richtlinie 95/46/EG – der bis heute wichtigsten Datenschutzregelung der EU – ist die Art und Weise, in der die Menschen ihr Recht auf Datenschutz wahrnehmen können, über die Grenzen der Mitgliedstaaten hinweg nicht ausreichend vereinheitlicht. Auch sind die Kompetenzen der für den Datenschutz zuständigen nationalen Behörden nicht soweit harmonisiert, dass die einheitliche und wirksame Anwendung der Vorschriften gewährleistet wäre. Das bedeutet, dass die Ausübung dieser Rechte – vor allem online - in einigen Mitgliedstaaten schwieriger ist als in anderen.

---

12 Siehe Schreiben der EU-Justizkommissarin Viviane Reding vom 19. September 2011 an die Mitglieder der Datenschutzgruppe, veröffentlicht unter http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm.

13 Siehe Folgenabschätzung (SEK(2012) 72.

14 Dazu gehören zu einem späteren Zeitpunkt Änderungen zur Anpassung spezifischer sektorenbezogener Instrumente, z. B. der Verordnung (EG) Nr. 45/2001, ABl. L 8 vom 12.1.2001, S. 1.

15 Die Verordnung enthält auch einige technische Anpassungen der Datenschutzrichtlinie im Bereich der elektronischen Kommunikation (Richtlinie 2002/58/EG, zuletzt geändert durch die Richtlinie 2009/136/EG – ABl. L 337 vom 18.12.2009, S. 11), mit denen der Umwandlung der Richtlinie 95/46/EG in eine Verordnung Rechnung getragen wird. Die rechtlichen Folgen der neuen Verordnung und der neuen Richtlinie für die Datenschutzrichtlinie für elektronische Kommunikation werden zu gegebener Zeit Gegenstand einer Überprüfung der Kommission sein, in die das Ergebnis der Verhandlungen über die derzeitigen Vorschläge mit dem Europäischen Parlament und dem Rat eingeht.

16 Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeiten werden (ABl. L 350 vom 30.12.2008, S. 60). Als Teil des Datenschutz-Reformpakets wird auch ein Bericht über die Umsetzung des Rahmenbeschlusses (KOM(2012) 12) angenommen.

Dies ist nicht zuletzt auch auf die schiere Menge der täglich erfassten Daten und darauf zurückzuführen, dass sich die Benutzer häufig nicht in vollem Umfang dessen bewusst sind, dass ihre Daten erfasst werden. Zwar sind viele Europäer der Meinung, dass die Weitergabe personenbezogener Daten immer mehr zum modernen Leben gehört[17], doch haben 72 % der Internetbenutzer in Europa Vorbehalte, wenn sie online nach zu vielen personenbezogenen Daten gefragt werden[18]. Sie haben den Eindruck, dass sie keine Kontrolle über ihre Daten haben. Sie werden nicht richtig informiert, was mit ihren persönlichen Informationen geschieht und an wen und zu welchem Zweck sie weitergeleitet werden. Häufig wissen sie nicht, wie sie ihre Rechte online wahrnehmen können.

„Recht auf Vergessenwerden"

Ein europäischer Student, der Mitglied eines sozialen Online-Netzes ist, beschließt, Auskunft über alle personenbezogenen Daten seiner selbst zu verlangen, über die dieses Netz verfügt. Dabei stellt er fest, dass das Netz sehr viel mehr Daten speichert, als er angenommen hatte, und dass einige personenbezogene Daten, die er für gelöscht hielt, immer noch gespeichert sind.

Die Reform der EU-Datenschutzvorschriften wird auf folgendem Wege sicherstellen, dass so etwas nicht mehr passiert:

- Soziale Online-Netze (und alle anderen für die Verarbeitung Verantwortlichen) werden ausdrücklich verpflichtet, die Menge der erfassten und verarbeiteten personenbezogenen Daten der Benutzer auf ein Mindestmaß zu begrenzen.

- Aufgrund der Standardeinstellungen muss sichergestellt sein, dass Daten nicht veröffentlicht werden.

- Die für die Verarbeitung Verantwortlichen werden ausdrücklich verpflichtet, die personenbezogenen Daten zu löschen, wenn die betroffene Person das Löschen ausdrücklich verlangt und kein anderer legitimer Grund vorliegt, die Daten aufzubewahren.

Im genannten Fall würde das den Anbieter des sozialen Netzes verpflichten, die Daten des Studenten unverzüglich und vollständig zu löschen.

Wie in der Digitalen Agenda für Europa hervorgehoben wird, zählen Vorbehalte in Bezug auf den Schutz der Privatsphäre zu den häufigsten Gründen, warum Menschen keine Waren und Dienstleistungen online kaufen. In Anbetracht des Beitrags des Informations- und Kommunikationstechnologiesektors (IKT) zum Gesamtproduktivitätswachstum in Europa – 20 % des IKT-Sektors unmittelbar und 30 % aufgrund von IKT-Investitionen[19] – ist das Vertrauen zu solchen Diensten zur Ankurbelung des Wirtschaftswachstums in der EU und der Wettbewerbsfähigkeit der europäischen Industrie unverzichtbar.

Meldung von Datenschutzverstößen

Ein Anbieter von Glücksspielen, dessen Zielgruppe Benutzer in der EU sind, wurde von Hackern angegriffen. Der Datenschutzverstoß betraf Datenbanken, die personenbezogene Daten von Millionen

---

17 Siehe Eurobarometer Spezial 359 – „*Attitudes on Data Protection and Electronic Identity in the European Union*", Juni 2011, S. 23.

18 S. o. S. 54.

19 Eine Digitale Agenda für Europa, s. o., S. 4.

von Benutzern weltweit enthielten (u.a. Namen, Adressen und möglicherweise Kreditkartendaten). Der Anbieter ließ eine Woche verstreichen, bevor er die betroffenen Kunden benachrichtigte.

Durch die Reform der EU-Datenschutzvorschriften wird sichergestellt, dass so etwas nicht mehr passiert. Die neuen Vorschriften verpflichten die Unternehmen,

- ihre Sicherheitsmaßnahmen zu verstärken, damit solche Verstöße unterbunden werden,

- Datenschutzverstöße unverzüglich sowohl der nationalen Datenschutzbehörde – möglichst binnen 24 Stunden nach ihrer Entdeckung - als auch den betroffenen Personen mitzuteilen.

Ziel der von der Kommission vorgeschlagenen neuen Vorschriften ist es, die Rechte zu stärken, den Menschen wirkungsvolle Mittel an die Hand zu geben, die sicherstellen, dass sie vollständig darüber im Bilde sind, was mit ihren personenbezogenen Daten geschieht, und die sie in die Lage zu versetzen, ihre Rechte wirksamer wahrzunehmen.

Um das Recht des Einzelnen auf den Schutz seiner Daten zu stärken, schlägt die Kommission neue Vorschriften vor, die Folgendes bewirken:

Verbesserte Möglichkeiten für den Einzelnen, seine Daten zu kontrollieren, indem

- sichergestellt wird, dass falls es einer **Einwilligung** bedarf, diese freiwillig und **ausdrücklich gegeben werden muss, d. h. durch eine Erklärung oder eine bestätigende Handlung der betroffenen Person**

- Internetbenutzer ein wirksames **Recht auf Vergessenwerden** in der Online-Umgebung erhalten: das Recht auf Löschen ihrer Daten, wenn sie ihre Einwilligung zurückziehen und keine anderen legitimen Gründe für die Aufbewahrung dieser Daten vorliegen

- den Personen **leichter Zugang zu ihren eigenen Daten** sowie das **Recht auf Datenübertragbarkeit** garantiert wird, d. h. das Recht, vom für die Verarbeitung Verantwortlichen eine Kopie der gespeicherten Daten zu erhalten und diese ungehindert von einem Diensteanbieter auf einen anderen zu übertragen

- das **Recht auf Information** gestärkt wird, damit der Einzelne in vollem Umfang versteht, wie seine personenbezogenen Daten behandelt werden, insbesondere, wenn die Verarbeitung **Kinder** betrifft

Verbesserte Möglichkeiten für den Einzelnen, seine Rechte wahrzunehmen, indem

- die **Befugnisse und die Unabhängigkeit der nationalen Datenschutzbehörden** gestärkt werden, damit sie wirksam Beschwerden nachgehen können; dazu gehört die Befugnis, Ermittlungen durchzuführen, rechtsverbindliche Beschlüsse zu fassen und wirksame, abschreckende Sanktionen zu verhängen

- verstärkte **administrative und justizielle Abhilfen** für den Fall der Verletzung von Datenschutzrechten geschaffen werden. Insbesondere erhalten

Datenschutzverbände das Recht, im Namen einer natürlichen Personen Klage vor Gericht zu erheben

<u>eine verstärkte Datensicherheit</u>, <u>indem</u>

- der Einsatz von **Technologien zum Schutz der Privatsphäre** (Technologien, die Informationen schützen, indem sie die Speicherung personenbezogener Daten auf ein Mindestmaß begrenzen), **datenschutzgerechte Standardeinstellungen** und **Datenschutz-Zertifizierungsregeln** gefördert werden

- eine **allgemeine Verpflichtung**[20] der für die Verarbeitung Verantwortlichen eingeführt wird, **Datenschutzverstöße unverzüglich** den Datenschutzbehörden (d. h. nach Möglichkeit binnen 24 Stunden) und den betroffenen Personen **zu melden**

<u>eine verschärfte Rechenschaftspflicht der Datenverarbeiter,</u> <u>indem</u>

- diese verpflichtet werden, in Unternehmen mit mehr als 250 Beschäftigten und in Unternehmen, die mit Datenverarbeitungen betraut sind, die aufgrund ihrer Art, ihrer Tragweite oder ihrer Zweckbestimmung besondere Risiken für die Rechte und Freiheiten der betroffenen Personen mit sich bringen („risikobehaftete Datenverarbeitung“) einen **Datenschutzbeauftragten** zu benennen

- der **Grundsatz des „Datenschutzes durch Technik“** (Privacy by Design) eingeführt wird, um sicherzustellen, dass der Datenschutz schon bei der Planung von Verfahren und Systemen berücksichtigt wird

- für Unternehmen, die mit risikobehafteter Datenverarbeitung betraut sind, die Verpflichtung zur Durchführung von **Datenschutz-Folgenabschätzungen** eingeführt wird.

3. DATENSCHUTZVORSCHRIFTEN FÜR DEN DIGITALEN BINNENMARKT

Trotz der Zielsetzung der geltenden Richtlinie, in der EU ein gleichmäßiges Datenschutzniveau zu gewährleisten, sind die Vorschriften der Mitgliedstaaten nach wie vor sehr uneinheitlich. Infolgedessen müssen sich die für die Verarbeitung Verantwortlichen unter Umständen auf 27 unterschiedliche nationale Regelungen und Anforderungen einstellen. Die dadurch bedingte **Zersplitterung des Rechtsrahmens** hat zu **Rechtsunsicherheit** und einem uneinheitlichen Schutz des Einzelnen geführt. Für die Wirtschaft ist dies mit **unnötigen Kosten und übertriebenem Verwaltungsaufwand** verbunden, und es könnte im Binnenmarkt tätige Unternehmen von einer Geschäftsausweitung über die Grenzen hinweg abhalten.

Darüber hinaus gibt es erhebliche Unterschiede zwischen den Mitgliedstaaten, was die Ressourcen und Befugnisse der für den Datenschutz zuständigen nationalen

---

[20] Bisher besteht diese Verpflichtung aufgrund der Datenschutzrichtlinie für die elektronische Kommunikation nur im Telekommunikationssektor.

Behörden anbelangt[21]. In manchen Fällen sind sie nicht in der Lage, ihrem Durchsetzungsauftrag angemessen nachzukommen. Die Zusammenarbeit zwischen den Behörden auf europäischen Ebene – im Wege der bestehenden beratenden Gruppe (der so genannten Artikel-29-Datenschutzgruppe)[22] – gewährleistet nicht immer, dass die Bestimmungen einheitlich angewandt werden, und muss also verbessert werden.

Einheitliche Durchsetzung von Datenschutzvorschriften in Europa

Ein multinationales Unternehmen mit mehreren Niederlassungen in der EU bringt ein Online-Kartierungssystem für ganz Europa heraus, mit dem Bilder aller privaten und öffentlichen Gebäude und möglicherweise auch Bilder von Menschen auf der Straße erfasst werden. In einem Mitgliedstaat wurde die Aufnahme nicht unkenntlich gemachter Bilder von Personen, die nicht wissen, dass sie fotografiert werden, als rechtswidrig betrachtet, während dies in anderen Mitgliedstaaten keinen Verstoß gegen die Datenschutzvorschriften darstellte. Folglich reagierten die nationalen Datenschutzbehörden in dieser Situation unterschiedlich.

Durch die Reform der Datenschutzvorschriften der EU wird auf folgende Weise sichergestellt, dass so etwas nicht mehr passiert:

- In der EU-Verordnung werden Datenschutzanforderungen und –garantien mit unmittelbarer Anwendung in der gesamten Union festgelegt.

- Nur die Datenschutzbehörde des Staates, in dem das Unternehmen seinen Hauptsitz hat, wird darüber beschließen können, ob das Unternehmen rechtmäßig handelt.

- Angesichts der Tatsache, dass die nationalen Datenschutzbehörden für Personen in verschiedenen Mitgliedstaaten zuständig sind, wird eine zügige und wirksame Abstimmung zwischen ihnen dazu beitragen, dass die neuen EU-Datenschutzvorschriften in allen Mitgliedstaaten einheitlich angewandt und durchgesetzt werden.

Die nationalen Behörden müssen gestärkt und ihre Zusammenarbeit muss intensiviert werden, damit eine einheitliche Anwendung und Durchsetzung der Vorschriften in der EU gewährleistet ist.

Ein straffer, eindeutiger und einheitlicher rechtlicher Rahmen auf EU-Ebene wird dazu beitragen, das Potenzial des digitalen Binnenmarkts freizusetzen und Wirtschaftswachstum, Innovation und Beschäftigung zu fördern. Eine Verordnung wird die gesetzlichen Regelungen in den 27 Mitgliedstaaten vereinheitlichen und die Hindernisse für den Marktzutritt überwinden, was ganz besonders für kleinste, kleine und mittlere Unternehmen von Bedeutung ist.

Die neuen Vorschriften verschaffen den Unternehmen aus der EU ferner einen Vorteil im globalen Wettbewerb. Aufgrund des neuen Rechtsrahmens werden sie ihren Kunden zusichern können, dass wichtige personenbezogene Informationen mit der notwendigen Sorgfalt behandelt werden. Das Vertrauen in einen kohärenten EU-Rechtsrahmen ist ein entscheidender Vorteil für Diensteanbieter und ein Anreiz für Investoren, die bei der Standortsuche nach optimalen Bedingungen Ausschau halten.

---

21 Weitere Einzelheiten hierzu siehe in der den Legislativvorschlägen beiliegenden Folgenabschätzung SEK(2012) 72.

22 Die Arbeitsgruppe wurde 1996 auf der Grundlage von Artikel 29 der Richtlinie 95/46/EG mit beratender Funktion eingesetzt. Ihr gehören Vertreter der nationalen Datenschutzbehörden sowie der Europäische Datenschutzbeauftragte und die Kommission an. Weitere Informationen zur Tätigkeit der Datenschutzgruppe unter http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

Um die **Binnenmarktdimension des Datenschutzes** zu stärken, schlägt die Kommission vor,

- auf EU-Ebene mit einer **unmittelbar in allen Mitgliedstaaten anwendbaren Verordnung**[23] Datenschutzvorschriften zu erlassen, die der gleichzeitigen Anwendung unterschiedlicher nationaler Datenschutzgesetze ein Ende setzt; dies wird allein **aufgrund des entfallenden Verwaltungsaufwands für die Unternehmen Nettoeinsparungen in Höhe von rund 2,3 Mrd. EUR jährlich** bedeuten

- den **rechtlichen Rahmen durch eine drastische Verringerung des Verwaltungsaufwands zu vereinfachen** und **Formalitäten** wie allgemeine Meldepflichten aufzuheben (was aufgrund des entfallenden Verwaltungsaufwands Nettoeinsparungen von jährlich 130 Mio. EUR bewirkt). In Anbetracht ihrer Bedeutung für die Wettbewerbsfähigkeit der Europäischen Wirtschaft wird den spezifischen Erfordernissen der kleinsten, kleinen und mittleren Unternehmen besonders Rechnung getragen

- **die Unabhängigkeit der nationalen Datenschutzbehörden zu stärken und ihre Befugnisse auszubauen**, damit sie Ermittlungen vornehmen, verbindliche Beschlüsse fassen und wirksame abschreckende Sanktionen erlassen können, und die Mitgliedstaaten zu verpflichten, sie mit **ausreichenden Ressourcen** auszustatten

- **eine zentrale Kontaktstelle für den Datenschutz in der EU einzurichten:** In der EU werden sich die für die Verarbeitung Verantwortlichen nur an **eine Datenschutzbehörde**, und zwar diejenige des Mitgliedstaats, in dem sich die Hauptniederlassung des Unternehmens befindet, wenden müssen

- die Rahmenbedingungen für eine **reibungslose und effiziente Zusammenarbeit zwischen den nationalen Datenschutzbehörden** zu schaffen, was auch die Verpflichtung für die Datenschutzbehörden einschließt, auf Antrag für eine andere Datenschutzbehörde Ermittlungen durchzuführen und die von einer anderen Behörde gefassten Beschlüsse anzuerkennen

- auf EU-Ebene **ein Verfahren zur Gewährleistung einer einheitlichen Rechtsanwendung (Kohärenz-Verfahren) einzuführen**, mit dem sichergestellt wird, dass von einer Datenschutzbehörde gefasste Beschlüsse, die weitergehende Auswirkungen in Europa haben, die Sichtweise anderer betroffener Datenschutzbehörden in vollem Umfang berücksichtigen und mit dem Recht der EU vereinbar sind

- die Datenschutzgruppe nach Artikel 29 zu einem **unabhängigen Europäischen Datenschutzausschuss** auszubauen, der besser zu einer kohärenten Anwendung der Datenschutzvorschriften beitragen kann und eine solide Grundlage für die Zusammenarbeit der Datenschutzbehörden sowie des Europäischen Datenschutzbeauftragten bietet. Im Sinne der Synergie- und Effizienzförderung soll

---

[23] Um Regeln für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (siehe unten Abschnitt 4) festzulegen, wird eine Richtlinie vorgeschlagen, die den Mitgliedstaaten in diesem spezifischen Bereich mehr Flexibilität einräumt.

das Sekretariat dieses Europäischen Datenschutzausschusses vom Europäischen Datenschutzbeauftragten übernommen werden.

Die neue EU-Verordnung gewährleistet zuverlässigen Schutz des Grundrechts auf Datenschutz in der gesamten Europäischen Union und stärkt das reibungslose Funktionieren des Binnenmarkts. Zugleich enthält die Verordnung angesichts der Tatsache, dass , wie vom Gerichtshof der Europäischen Union[24] hervorgehoben wurde, das Recht auf den Schutz der personenbezogenen Daten keine uneingeschränkte Geltung beanspruchen kann, sondern im Hinblick auf seine gesellschaftliche Funktion gesehen werden[25] und mit anderen Grundrechten im Einklang mit dem Grundsatz der Verhältnismäßigkeit[26] ausbalanciert werden muss, Bestimmungen, die die Wahrung anderer Grundrechte - Freiheit der Meinungsäußerung und Informationsfreiheit, Recht auf Verteidigung sowie auf Wahrung des Berufsgeheimnisses (z. B. für Rechtsberufe) – sicherstellen, den Status der Kirchen im Recht der Mitgliedstaaten aber unberührt lassen.

4. VERWENDUNG VON DATEN IM RAHMEN DER POLIZEILICHEN UND JUSTIZIELLEN ZUSAMMENARBEIT IN STRAFSACHEN

Das Inkrafttreten des Vertrags von Lissabon und vor allem die Einführung einer neuen Rechtsgrundlage (Artikel 16 AEUV) bietet Gelegenheit, einen umfassenden Rechtsrahmen für den Datenschutz zu schaffen, mit dem für personenbezogene Daten ein hohes Schutzniveau sichergestellt und zugleich der Besonderheit des Bereichs der polizeilichen und justiziellen Zusammenarbeit in Strafsachen Rechnung getragen wird. Insbesondere wird ermöglicht, dass der überarbeitete EU-Datenschutzrahmen sowohl für die grenzübergreifende als auch für die innerstaatliche Verarbeitung personenbezogener Daten gilt. Dies würde die Unterschiede in den Rechtsvorschriften der Mitgliedstaaten verringern und voraussichtlich dem umfassenden Schutz personenbezogener Daten zugute kommen. Ferner könnte es zu einem flüssigeren Informationsaustausch zwischen den Polizei- und Justizbehörden der Mitgliedstaaten führen und somit die Zusammenarbeit im Bereich der Bekämpfung schwerer Kriminalität in Europa verbessern. Für die Verarbeitung von Daten durch Polizei- und Justizbehörden im strafrechtlichen Bereich gilt derzeit in erster Linie der Rahmenbeschluss 2008/977/JI, der vor Inkrafttreten des Vertrags von Lissabon erlassen wurde. Da es sich um einen Rahmenbeschluss handelt, ist die Kommission nicht befugt, diese Vorschriften durchzusetzen, was zu einer uneinheitlichen Umsetzung beigetragen hat. Außerdem ist der Anwendungsbereich des Rahmenbeschlusses auf die grenzübergreifende

---

24 EuGH, Urteil vom 9.11.2010, verbundene Rechtssachen C-92/09 und C-93/09 Volker und Markus Schecke und Eifert, noch nicht veröffentlicht.

25 Gemäß Artikel 52 Absatz 1 der Grundrechtecharta müssen Einschränkungen der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten gesetzlich vorgesehen sein, den Wesensgehalt dieser Rechte und Freiheiten achten und dürfen unter Wahrung des Grundsatzes der Verhältnismäßigkeit nur vorgenommen werden, wenn sie notwendig sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

26 EuGH, Urteil vom 6.11.2003 in der Rs. C-101/01 Lindqvist, Slg. 2003, I-12971, Rdnrn. 82-90; Urteil vom 16.12.2008 in der Rs. C-73/07 Satamedia, Slg. 2008, I-9831, Rdnrn. 50-62.

Datenverarbeitung beschränkt[27]. Das bedeutet, dass personenbezogene Daten, die nicht Gegenstand solcher Übermittlungen waren, derzeit nicht unter die EU-Datenverarbeitungsvorschriften fallen, die das Grundrecht auf den Schutz dieser Daten absichern. Dies schafft in einigen Fällen praktische Probleme für Polizei- und andere Behörden, für die womöglich nicht zu erkennen ist, ob die Datenverarbeitung nur das eigene Land betrifft oder grenzübergreifend ist, oder ob „inländische" Daten zu einem späteren Zeitpunkt Gegenstand eines grenzübergreifenden Austauschs werden[28].

Der reformierte EU-Datenschutzrahmen zielt somit darauf ab, ein einheitliches, hohes Datenschutzniveau zu garantieren, **um das Vertrauen zwischen den Polizei- und Justizbehörden verschiedener Mitgliedstaaten zu stärken und damit zu einem freien Datenverkehr und einer wirksamen Zusammenarbeit zwischen den Polizei- und Justizbehörden beizutragen**.

Um ein hohes Schutzniveau für personenbezogene Daten im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen zu gewährleisten und zugleich die Übermittlung personenbezogener Daten zwischen den Polizei- und Justizbehörden der Mitgliedstaaten zu erleichtern, schlägt die Kommission als Teil des Datenschutz-Reformpakets eine Richtlinie vor, die Folgendes vorsieht:

- die **Anwendung allgemeiner Datenschutzgrundsätze** auf die polizeiliche und justizielle Zusammenarbeit in Strafsachen unter Berücksichtigung des spezifischen Charakters dieser Bereiche[29]

- die Einführung eines **Mindestmaßes an harmonisierten Kriterien und Bedingungen für mögliche Beschränkungen** der allgemeinen Vorschriften. Dies betrifft insbesondere die Rechte der Person, informiert zu werden, wenn Polizei- und Justizbehörden auf ihre Daten zugreifen oder diese bearbeiten. Solche Beschränkungen sind für die wirkungsvolle Prävention, Untersuchung, Aufdeckung oder Verfolgung von Straftaten unerlässlich

- die Einführung **spezifischer Regeln, mit denen dem besonderen Charakter der Strafverfolgung**, u.a. hinsichtlich der **Unterscheidung verschiedener Gruppen von betroffenen Personen** mit möglicherweise unterschiedlichen Rechten (z. B. Zeugen und Verdächtige) Rechnung getragen wird.

5. DATENSCHUTZ IN EINER GLOBALISIERTEN WELT

Die Rechte natürlicher Personen müssen auch dann gewahrt werden, wenn personenbezogene Daten von der EU in Drittländer übermittelt werden und wenn Daten von Personen in den Mitgliedstaaten durch Diensteanbieter in Drittländern

---

27 Der Rahmenbeschluss gilt für personenbezogene Daten, die zwischen Mitgliedstaaten oder zwischen Mitgliedstaaten und EU-Organen oder -Einrichtungen übermittelt oder bereitgestellt werden oder wurden (siehe Artikel 1 Absatz 2).

28 Dies wurde von einigen Mitgliedstaaten in ihrer Antwort auf den Fragebogen der Kommission zum Bericht über die Umsetzung des Rahmenbeschlusses (KOM(2012) 12) bestätigt.

29 Siehe Erklärung Nr. 21 zum Schutz personenbezogener Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit im Anhang zur Schlussakte der Regierungskonferenz, die den Vertrag von Lissabon annahm.

verwendet oder analysiert werden. Das bedeutet, dass die Datenschutzstandards der EU unabhängig vom Standort des Unternehmens oder seiner Datenverarbeitungseinrichtungen gelten müssen.

In der heutigen globalisierten Welt werden personenbezogene Daten über immer mehr virtuelle und geografische Grenzen hinweg übermittelt und auf Servern in unterschiedlichen Ländern gespeichert. Immer zahlreichere Unternehmen bieten Cloud-Computing-Dienste an, die es Kunden ermöglichen, Daten auf andernorts untergebrachten Servern zu speichern und auf sie zuzugreifen. Diese Faktoren erfordern eine Verbesserung des bisherigen Systems der Datenübermittlung in Drittländer. Dazu gehören Angemessenheitsbeschlüsse – d.h. Beschlüsse, mit denen „angemessene" Datenschutzstandards in Drittländern bescheinigt werden - und geeignete Garantien, wie standardisierte Vertragsklauseln oder verbindliche unternehmensinterne Datenschutzregelungen[30], mit dem Ziel, ein hohes Datenschutzniveau bei internationalen Verarbeitungsvorgängen zu gewährleisten und zugleich den grenzübergreifenden Datenverkehr zu erleichtern.

Verbindliche unternehmensinterne Datenschutzregelungen

Eine Unternehmensgruppe muss regelmäßig personenbezogene Daten von ihren Tochtergesellschaften in der EU an ihre Tochtergesellschaften in Drittländern übermitteln. Die Unternehmensgruppe möchte verbindliche unternehmensinterne Datenschutzregelungen einführen, um den EU-Vorschriften zu entsprechen und zugleich den Verwaltungsaufwand für jede einzelne Übermittlung zu begrenzen. In der Praxis stellen solche unternehmensinternen Datenschutzregelungen sicher, dass im ganzen Konzern statt verschiedener interner Anweisungen ein einheitliches Regelwerk gilt.

Nach der bisherigen im Rahmen der Datenschutzgruppe vereinbarten Vorgehensweise setzt die Feststellung, dass die verbindlichen unternehmensinternen Datenschutzregelungen angemessene Garantien bieten, eine gründliche Überprüfung durch drei nationale Datenschutzbehörden (eine „leitende" und zwei „überprüfende" Behörden) voraus; darüber hinaus können auch andere Datenschutzbehörden Stellung nehmen. Die Vorschriften zahlreicher Mitgliedstaaten schreiben außerdem zusätzliche nationale Genehmigungen für die unter die verbindlichen unternehmensinternen Datenschutzregelungen fallenden Übermittlungen vor, was das Verfahren aufwändig, kostspielig, lang und umständlich macht.

Die Datenschutzreform wird Folgendes bewirken:

- Das Verfahren wird vereinfacht und gestrafft.

- Verbindliche unternehmensinterne Datenschutzregelungen werden nur durch eine Datenschutzbehörde beurteilt, wobei sichergestellt wird, dass andere betroffene Datenschutzbehörden zügig einbezogen werden.

- Sobald eine Datenschutzbehörde die verbindlichen unternehmensinternen Datenschutzregelungen genehmigt hat, gilt diese Genehmigung für die gesamte EU ohne zusätzliche Genehmigungen auf nationaler Ebene.

---

30 Verbindliche unternehmensinterne Datenschutzregelungen (BCR – Binding Corporate Rules) sind Verhaltenskodizes auf der Grundlage europäischer Datenschutzstandards, die von Unternehmen aufgestellt und freiwillig befolgt werden, um angemessene Garantien für die Übermittlung personenbezogener Daten zwischen Unternehmen eines Konzerns zu geben, die konzerninterne Regeln zu befolgen haben. Sie werden nicht ausdrücklich in der Richtlinie 95/46/EG genannt, wurden aber aus praktischen Gründen von den nationalen Datenschutzbehörden mit Unterstützung der Datenschutzgruppe entwickelt.

Um die Herausforderungen der Globalisierung zu bestehen, bedarf es – insbesondere für weltweit tätige Unternehmen - flexibler Instrumente und Verfahren, die zugleich einen lückenlosen Schutz der personenbezogenen Daten garantieren. Die Kommission schlägt folgende Maßnahmen vor:

- Einführung **klarer Regeln**, in denen festgelegt ist, **wann die EU-Vorschriften auf die für die Datenverarbeitung Verantwortlichen in Drittländern anwendbar sind,** insbesondere durch die Regelung, **dass die EU-Vorschriften Anwendung finden,** wenn Personen in der EU Waren und Dienstleistungen angeboten werden oder ihr Verhalten im Netz beobachtet wird

- **Angemessenheitsbeschlüsse** werden auch im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen von der Europäischen Kommission auf der Grundlage expliziter und klarer Kriterien gefasst

- Rechtmäßiger Datenverkehr nach Drittländern wird durch eine Straffung und Vereinfachung der **Regeln für die internationale Datenübermittlung** in Länder, für die kein Angemessenheitsbeschluss gilt, einfacher; dies geschieht vor allem durch Modernisierung und häufigere Verwendung von Instrumenten wie **verbindlichen unternehmensinternen Datenschutzregeln**, die für **Auftragsverarbeiter** sowie in **Unternehmensgruppen** gelten und der insbesondere beim Cloud-Computing festzustellenden Vielzahl der an der Verarbeitung beteiligten Unternehmen Rechnung tragen

- Aufnahme von **Gesprächen** und gegebenenfalls **Verhandlungen** mit Drittländern – vor allem strategischen Partnern der EU und Ländern der Europäischen Nachbarschaftspolitik – und wichtigen internationalen Organisationen (z. B. Europarat, Organisation für wirtschaftliche Zusammenarbeit und Entwicklung, Vereinte Nationen), **um weltweit hohe interoperable Datenschutzstandards zu unterstützen**.

6. SCHLUSSFOLGERUNG

Die Reform der EU-Datenschutzvorschriften zielt darauf ab, einen **modernen, stabilen, kohärenten und umfassenden Datenschutz-Rechtsrahmen für die Europäische Union** bereitzustellen. Auf diese Weise wird dem Grundrecht des Einzelnen auf Datenschutz Geltung verschafft. Andere Rechte wie das Recht auf freie Meinungsäußerung, auf Information, die Rechte des Kindes, die unternehmerische Freiheit, das Recht auf ein faires Verfahren und die Wahrung des Berufsgeheimnisses (z. B. für Rechtsberufe) sowie der Status der Kirchen gemäß dem Recht der Mitgliedstaaten werden gewahrt.

Die Reform kommt in erster Linie dem Einzelnen zugute, da seine Datenschutzrechte ausgebaut und sein Vertrauen in die digitale Umgebung gestärkt werden. Ferner wird das rechtliche Umfeld für Unternehmen und den öffentlichen Sektor durch die Reform wesentlich vereinfacht, was die Entwicklung der digitalen Wirtschaft im EU-Binnenmarkt und darüber hinaus entsprechend den Zielen der Strategie Europa 2020 und der Digitalen Agenda für Europa anregen dürfte. Schließlich wird die Reform das Vertrauen der Strafverfolgungsbehörden untereinander stärken, damit der Datenaustausch zwischen ihnen erleichtert und die Zusammenarbeit bei der

Bekämpfung schwerer Kriminalität verbessert, zugleich aber ein hohes Schutzniveau für den Einzelnen garantiert wird.

Die Europäische Kommission wird eng mit dem Europäischen Parlament und dem Rat zusammenarbeiten, um bis Ende 2012 eine Einigung über den neuen EU-Datenschutzrahmen zu erreichen. Während des Gesetzgebungsverfahrens und darüber hinaus, vor allem bei der Umsetzung und Anwendung der neuen Rechtsinstrumente, wird die Kommission weiterhin **einen engen und transparenten Dialog mit allen Beteiligten,** d. h. auch den Vertretern des privaten und öffentlichen Sektors, pflegen. An diesen Gesprächen sollen Vertreter von Polizei und Justiz, Regulierungsstellen für elektronische Kommunikation, Organisationen der Zivilgesellschaft, Datenschutzbehörden und Wissenschaftler sowie Vertreter einschlägiger EU-Agenturen wie Eurojust, Europol, der Grundrechte-Agentur und der Agentur für Netz- und Informationssicherheit, beteiligt werden.

Im Umfeld sich ständig weiterentwickelnder Informationstechnologien und sich ändernden Sozialverhaltens sind solche Gespräche von größter Bedeutung, um die Beiträge zu nutzen, die notwendig sind, um für den Einzelnen ein hohes Datenschutzniveau, für die EU-Wirtschaft Wachstum und Wettbewerbsfähigkeit, ein reibungsloses Funktionieren des öffentlichen Sektors (einschließlich Polizei und Justiz) und einen geringen Verwaltungsaufwand zu gewährleisten.