Bundesrat **Drucksache 707/10**

04.11.10

EU - AS - FJ - G -
In - R - Wi

Unterrichtung
durch die Europäische Kommission

Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen:

Gesamtkonzept für den Datenschutz in der Europäischen Union

KOM(2010) 609 endg.

Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0720-2946

Der Bundesrat wird über die Vorlage gemäß § 2 EUZBLG auch durch die Bundesregierung unterrichtet.

Hinweis: vgl. Drucksache 690/90 = AE-Nrn. 902297 und 960499,
Drucksache 862/07 = AE-Nr. 070936 und
AE-Nr. 011577

EUROPÄISCHE KOMMISSION

Brüssel, den 4.11.2010
KOM(2010) 609 endgültig

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

Gesamtkonzept für den Datenschutz in der Europäischen Union

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

Gesamtkonzept für den Datenschutz in der Europäischen Union

1. NEUE HERAUSFORDERUNGEN FÜR DEN DATENSCHUTZ

Die Datenschutzrichtlinie von 1995[1] war ein Meilenstein in der Entwicklung der Datenschutzpolitik der Europäischen Union. Die Richtlinie bestätigt zwei der ältesten, gleichermaßen wichtigen Ziele des europäischen Integrationsprozesses: einerseits den Schutz der Grundrechte und der Grundfreiheiten des Einzelnen, insbesondere des Grundrechts auf Datenschutz, und andererseits die Vollendung des Binnenmarktes – in diesem Fall den freien Verkehr personenbezogener Daten.

Diese beiden Ziele sowie die Grundsätze der Richtlinie gelten fünfzehn Jahre später unverändert. **Die Welt um uns herum hat sich hingegen infolge der raschen technologischen Entwicklung und der Globalisierung tiefgreifend verändert, was den Datenschutz vor neue Herausforderungen stellt.**

Moderne Technologien ermöglichen es dem Einzelnen, in einem nie zuvor dagewesenen Ausmaß im Handumdrehen Informationen über seine Verhaltensweisen und Vorlieben weiterzugeben und sie öffentlich und weltweit zugänglich zu machen. Soziale Netzwerke, denen Hunderte Millionen Mitglieder aus aller Welt angehören, sind vielleicht das augenfälligste, aber nicht das einzige Beispiel für dieses Phänomen. „Cloud-Computing" – also die Datenverarbeitung über das Internet, bei der sich Software, Ressourcen und Informationen auf andernorts untergebrachten Servern („in the cloud", also „in der Wolke") befinden – könnte ebenfalls Datenschutzrisiken bergen: der Einzelne könnte die Kontrolle über potenziell sensible Informationen zu seiner Person verlieren, wenn er Daten mit Programmen abspeichert, die auf den Rechnern anderer Personen installiert sind. Einer aktuellen Studie zufolge besteht inzwischen unter den Datenschutzbehörden, Unternehmensverbänden und Verbraucherorganisationen weitgehend Einigkeit darüber, dass mit den Online-Aktivitäten zunehmende Risiken für den Schutz der Privatsphäre und personenbezogener Daten verbunden sind.[2]

Gleichzeitig **werden die Verfahren zur Erfassung personenbezogener Daten immer raffinierter und lassen sich immer schwerer aufspüren.** So können Unternehmen durch die Beobachtung des Verhaltens von Internetbenutzern mithilfe ausgeklügelter Programme Personen individuell ansprechen. Auch die zunehmende Verwendung von Verfahren, bei denen Daten automatisch erfasst werden, wie elektronische Fahrausweise, elektronische Straßengebührenerhebung oder elektronische Standortbestimmungsinstrumente, erleichtert die Bestimmung des Aufenthaltsortes einer Person, weil diese einen mobilen Datenträger oder

---

1 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).

2 Siehe *Study on the economic benefits of privacy enhancing technologies,* London Economics, Juli 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf), S. 14.

ein mobiles Gerät mit sich führt. Zudem verwenden die Behörden u. a. über ihre elektronischen Verwaltungssysteme zunehmend personenbezogene Daten für verschiedene Zwecke, wie zur Auffindung von Personen beim Ausbruch einer ansteckenden Krankheit, zur wirksameren Terrorismus- und Verbrechensbekämpfung, zur Verwaltung von Sozialversicherungssystemen und zur Steuererhebung.

Das führt unausweichlich zu der Frage, ob die geltenden Datenschutzbestimmungen der EU diesen Herausforderungen standhalten.

Zur Beantwortung dieser Frage leitete die Kommission im Mai 2009 mit einer hochrangigen Konferenz zunächst eine Überprüfung der bestehenden Datenschutzregelung ein. Im Anschluss daran führte sie bis Ende 2009 eine öffentliche Konsultation durch.[3] Außerdem wurden mehrere Studien in Auftrag gegeben.[4]

Die Ergebnisse bestätigen, dass die wesentlichen Grundsätze der Richtlinie nach wie vor Gültigkeit haben und ihre Technikneutralität beibehalten werden sollte. Allerdings wurde auch festgestellt, dass einige Aspekte problematisch sind und spezifische Probleme aufwerfen. Hierzu gehören:

- *Beherrschung der Auswirkungen neuer Technologien*

Aus den Antworten im Rahmen der Konsultation sowohl von Privatpersonen als auch von Organisationen konnte gefolgert werden, dass die Anwendung der Datenschutzgrundsätze auf neue Technologien präzisiert und spezifiziert werden muss, um sicherzustellen, dass personenbezogene Daten unabhängig von der zur Datenverarbeitung verwendeten Technologie wirksam geschützt werden, und dass sich die für die Verarbeitung Verantwortlichen der Auswirkungen neuer Technologien auf den Datenschutz voll und ganz bewusst sein müssen. Die Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation)[5], die die Bestimmungen der allgemeinen Datenschutzrichtlinie auf den Bereich der elektronischen Kommunikation überträgt und ergänzt[6], regelt diese Aspekte teilweise.

---

3 Zu den Antworten der Teilnehmer an der öffentlichen Konsultation der Kommission siehe: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm. 2010 wurden gezieltere Konsultationen interessierter Kreise durchgeführt. Außerdem fand am 5. Oktober 2010 in Brüssel ein hochrangiges Treffen mit interessierten Kreisen statt, bei dem Vizepräsidentin Viviane Reding den Vorsitz führte. Die Kommission konsultierte darüber hinaus die Datenschutzgruppe, die einen umfassenden Beitrag zur Konsultation von 2009 vorlegte (WP 168) und im Juli 2010 eine Stellungnahme speziell zum Grundsatz der Rechenschaftspflicht **(„accountability")** abgab (WP 173).

4 Neben der *Study on the economic benefits of privacy enhancing technologies* (siehe Fußnote 2) siehe auch *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, vom Januar 2010 (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf). Darüber hinaus wird zur Zeit eine Folgenabschätzung für die künftige EU-Datenschutzregelung durchgeführt.

5 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), (ABl. L 201 vom 31.7.2002, S. 37).

6 Die Datenschutzrichtlinie 95/46/EG legt Datenschutzstandards für sämtliche EU-Rechtsakte fest, darunter auch für die Datenschutzrichtlinie 2002/58/EG für elektronische Kommunikation (geändert durch die Richtlinie 2009/136/EG, ABl. L 337 vom 18.12.2009, S. 11). Letztere Richtlinie gilt für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher

- *Binnenmarktdimension des Datenschutzes*

Ein Aspekt, der vielen Befragten, besonders multinationalen Unternehmen, die meisten Probleme bereitet, ist die trotz der gemeinsamen EU-Regelung unzureichende Harmonisierung der verschiedenen Datenschutzvorschriften der Mitgliedstaaten. Nach Ansicht der Befragten müssen die Rechtssicherheit erhöht, der Verwaltungsaufwand verringert und gleiche Bedingungen für die Unternehmen und die anderen für die Datenverarbeitung Verantwortlichen gewährleistet werden.

- *Umgang mit der Globalisierung und Verbesserung internationaler Datentransfers*

Mehrere Beteiligte wiesen darauf hin, dass durch die zunehmende Praxis der Vergabe von Datenverarbeitungsaufträgen, sehr oft an Auftragnehmer außerhalb der EU, Unklarheiten bezüglich des für die Verarbeitung geltenden Rechts und der Zuweisung der Verantwortung zutage treten. Viele Organisationen gaben an, dass die derzeitigen Regelungen unzulänglich seien, dass sie überarbeitet und miteinander abgestimmt werden müssten, um internationale Datentransfers einfacher und weniger aufwändig zu machen.

- *Verstärkter institutioneller Rahmen für die wirksame Durchsetzung der Datenschutzvorschriften*

Alle Beteiligten sind sich darüber einig, dass die Datenschutzbehörden mehr Befugnisse erhalten sollten, damit die Einhaltung der Datenschutzvorschriften besser durchgesetzt werden kann. Einige Organisationen forderten auch mehr Transparenz in der Tätigkeit der Datenschutzgruppe (*vgl. 2.5*) und klare Informationen über deren Aufgaben und Befugnisse.

- *Kohärentere Regelung für den Datenschutz*

Im Zuge der öffentlichen Konsultation vertraten alle beteiligten Kreise die Ansicht, dass es einer übergreifenden Regelung bedarf, die für die Datenverarbeitung in sämtlichen Sektoren und Politikbereichen der Union gilt. So ließe sich ein einheitlicher Ansatz und ein nahtloser, kohärenter und wirksamer Schutz gewährleisten.[7]

Die vorstehend aufgeführten Herausforderungen **verlangen von der EU ein umfassendes, kohärentes Konzept,** das die **lückenlose Einhaltung des Grundrechts des Einzelnen auf Schutz seiner Daten in der EU und anderswo garantiert.** Mit dem Vertrag von Lissabon wurden in der EU zusätzliche Instrumente eingeführt, mit denen dies erreicht werden kann. Die EU-Charta der Grundrechte, in deren Artikel 8 das Recht jeder Person auf Schutz der sie betreffenden Daten anerkannt wird, wurde rechtsverbindlich. Außerdem wurde eine neue Bestimmung eingeführt[8], die die Grundlage für die Schaffung einer umfassenden, kohärenten Regelung der EU zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr bildet. Gestützt auf die neue Rechtsgrundlage kann die EU den Datenschutz einheitlich regeln, auch in den Bereichen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. Die Gemeinsame Außen- und Sicherheitspolitik

---

elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen. Sie setzt die Grundsätze der Datenschutzrichtlinie in Bestimmungen speziell für den Bereich der elektronischen Kommunikation um. Die Richtlinie 95/46/EG gilt u. a. für nicht öffentliche Kommunikationsdienste.

7 Allerdings haben Europol und Eurojust in gesonderten Beiträgen, die nach Ablauf der öffentlichen Konsultation eingereicht wurden, dafür plädiert, dass den Besonderheiten ihrer Tätigkeit hinsichtlich der Koordinierung von Strafverfolgung und Kriminalitätsprävention Rechnung getragen wird.

8 Siehe Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV).

fällt nur teilweise unter Artikel 16 AEUV, da die Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung von Daten durch die Mitgliedstaaten für diesen Bereich durch einen Beschluss des Rates erlassen werden müssen, der sich auf eine andere Rechtsgrundlage stützt.[9]

Die Kommission wird diese neuen rechtlichen Möglichkeiten nutzen und dabei der Beachtung des Grundrechts auf Datenschutz in der gesamten EU und in der gesamten Politik der EU höchste Priorität einräumen. Gleichzeitig wird sie der Binnenmarktdimension mehr Gewicht geben und den freien Verkehr personenbezogener Daten fördern. Bei der Gewährleistung des Grundrechts auf den Schutz personenbezogener Daten ist auch weiteren einschlägigen Grundrechten der Charta und weiteren Zielen der Verträge umfassend Rechnung zu tragen.

In der vorliegenden Mitteilung legt die Kommission ihr Konzept für eine Reform der EU-Vorschriften für den Schutz personenbezogener Daten in sämtlichen Tätigkeitsbereichen der EU unter besonderer Berücksichtigung der Herausforderungen der Globalisierung und der neuen Technologien dar, damit auch weiterhin ein *hohes Schutzniveau* für den Einzelnen bei der Verarbeitung personenbezogener Daten in sämtlichen Tätigkeitsbereichen der EU gewährleistet ist. So wird die EU treibende Kraft bei den Bemühungen um hohe Datenschutzstandards weltweit bleiben können.

2. HAUPTZIELE DES GESAMTKONZEPTS FÜR DEN DATENSCHUTZ

2.1. Stärkung der Rechte des Einzelnen

2.1.1. Angemessener Schutz des Einzelnen in allen Situationen

Die derzeit geltende Datenschutzregelung der EU zielt darauf ab, **die Achtung der Grundrechte natürlicher Personen, insbesondere des Grundrechts auf den Schutz personenbezogener Daten zu garantieren**, wie es die EU-Charta der Grundrechte vorsieht.[10]

Der Begriff „personenbezogene Daten“ ist ein Schlüsselkonzept der geltenden Datenschutzvorschriften der EU zum Schutz von Privatpersonen. Aus diesem Konzept leiten sich die Verpflichtungen ab, die den für die Datenverarbeitung Verantwortlichen und den Auftragsverarbeitern auferlegt wurden.[11] Der Begriff „personenbezogene Daten“ soll sämtliche Informationen im direkten oder indirekten Zusammenhang mit einer identifizierten oder identifizierbaren Person erfassen. Um festzustellen, ob eine Person identifizierbar ist, sollten „alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen“[12]. Dieser vom Gesetzgeber bewusst gewählte Ansatz

---

9 Siehe Artikel 16 Absatz 2 letzter Unterabsatz AEUV und Artikel 39 des Vertrags über die Europäische Union (EUV).

10 Siehe Gerichtshof der Europäischen Union, Rechtssachen C-101/01, *Bodil Lindqvist*, Slg. 2003, I-1297, Rdnrn. 96, 97, und C-275/06, *Productores de Música de España (Promusicae) gegen Telefónica de España SAU*, Slg. 2008, I-271. Siehe auch Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte, z. B. in den Rechtssachen: S. und Marper gegen das Vereinigte Königreich, 4.12.2008 (Beschwerden Nrn. 30562/04 und 30566/04) sowie Rotaru gegen Rumänien, 4.5.2000; Nr. 28341/95, Rdnr. 55, EGMR 2000-V.

11 Die Begriffe „für die Verarbeitung Verantwortlicher“ und „Auftragsverabeiter“ sind in der Richtlinie 95/46/EG Artikel 2 Buchstaben d und e definiert.

12 Siehe Erwägungsgrund 26 der Richtlinie 95/46/EG.

zeichnet sich durch seine Flexibilität aus: Er lässt sich auf verschiedene Situationen und Entwicklungen anwenden, die sich auf Grundrechte auswirken, auch auf solche, die bei Annahme der Richtlinie nicht vorhersehbar waren. Dieser hat jedoch auch dazu geführt, dass in vielen Fällen Unklarheit darüber besteht, wie die Richtlinie genau umzusetzen ist, ob Privatpersonen Anspruch auf Datenschutz haben und ob die Verantwortlichen für die Datenverarbeitung die durch die Richtlinie auferlegten Pflichten einzuhalten haben.[13]

In bestimmten Situationen werden bei einer Verarbeitung spezifische Daten verwendet, für die nach EU-Recht zusätzliche Maßnahmen erforderlich wären. Solche Maßnahmen wurden in einigen Fällen bereits eingeführt. So ist die Speicherung von Daten in Endgeräten (z. B. Mobiltelefonen) nur unter der Voraussetzung erlaubt, dass der Betroffene seine Zustimmung zur Verarbeitung seiner Daten gegeben hat. Eine entsprechende Regelung muss möglicherweise auf EU-Ebene eingeführt werden, beispielsweise auch für verschlüsselte Daten, Standortdaten, Datamining-Verfahren, bei denen Daten aus verschiedenen Quellen gleichzeitig verwendet werden, oder für Fälle, in denen die Vertraulichkeit und Integrität informationstechnischer Systeme[14] gewährleistet werden muss.

Alle diese Aspekte müssen sorgfältig geprüft werden.

Die Kommission wird prüfen, **wie eine kohärente Anwendung der Datenschutzvorschriften sichergestellt werden kann unter Berücksichtigung der Auswirkungen neuer Technologien auf die Rechte und Freiheiten von Personen mit dem Ziel, den freien Verkehr personenbezogener Daten im Binnenmarkt zu gewährleisten**.

2.1.2. Mehr Transparenz für die von der Verarbeitung Betroffenen

Transparenz ist eine Grundvoraussetzung dafür, dass der Einzelne die Kontrolle über seine personenbezogenen Daten hat und ein wirksamer Datenschutz gewährleistet werden kann. Daher müssen die Betroffenen von den für die Verarbeitung Verantwortlichen **umfassend, klar und in transparenter Weise darüber informiert** werden, wie, von wem und aus welchem Grund ihre Daten erfasst und verarbeitet werden, wie lange sie aufbewahrt werden und ob sie Zugriff auf ihre Daten haben und die Berichtigung oder Löschung der Daten verlangen können. Die Bestimmungen über die Informationen, die dem von der Verarbeitung Betroffenen erteilt werden müssen[15], reichen nicht aus.

Transparenz setzt voraus, dass die **Informationen leicht zugänglich, verständlich sowie klar und einfach abgefasst sind**. Das ist für die Online-Umgebung besonders relevant, wo die Datenschutzhinweise oft unklar, schwer zu finden, wenig transparent[16] und nicht immer mit den geltenden Vorschriften vereinbar sind. Als Beispiel könnte die verhaltensorientierte Internetwerbung angeführt werden, bei der sowohl die große Zahl der Beteiligten als auch die Komplexität der dazu nötigen Technik es dem Einzelnen schwer machen zu wissen und nachzuvollziehen, ob, von wem und zu welchem Zweck seine Daten erfasst werden.

---

13 Siehe beispielsweise die Frage der IP-Adressen, mit der sich die Datenschutzgruppe in ihrer Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“ (WP 136) befasst hat.

14 Siehe beispielsweise Entscheidung des deutschen Bundesverfassungsgerichts vom 27. Februar 2008, 1 BvR 370/07.

15 Siehe Artikel 10 und 11 der Richtlinie 95/46/EG.

16 Bei einer Eurobarometer-Umfrage von 2009 gab etwa die Hälfte der Befragten an, dass Datenschutzhinweise auf Websites „sehr“ oder „recht unklar“ sind (siehe Flash Eurobarometer N° 282 : http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

Kinder müssen dabei besonderen Schutz genießen, da sie sich der Risiken, Folgen, Garantien und Rechte bei der Verarbeitung personenbezogener Daten weniger bewusst sein dürften.[17]

Die Kommission wird folgende Maßnahmen in Erwägung ziehen:

- Einführung eines **allgemeinen Transparenzgrundsatzes für die Verarbeitung** personenbezogener Daten in der Datenschutzregelung;

- Einführung **besonderer Pflichten** für die Verantwortlichen für die Verarbeitung, was die Art der Informationen und die **Modalitäten** der Bereitstellung dieser Informationen anbelangt, auch in Bezug auf **Kinder**;

- Erstellung eines oder mehrerer **EU-Standardmuster** („**Datenschutzhinweise"**), die die für die Verarbeitung Verantwortlichen zu verwenden haben.

Wichtig ist auch, dass Personen informiert werden, wenn ihre Daten versehentlich oder unrechtmäßig gelöscht oder geändert wurden, wenn sie verlorengegangen sind oder wenn Unbefugte darauf zugegriffen oder sie weitergegeben haben. Bei der kürzlich vorgenommenen Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation wurde die **Mitteilung einer Verletzung des Datenschutzes** zur Pflicht gemacht, allerdings nur für den Bereich der Telekommunikation. Da aber auch in anderen Sektoren (z. B. Finanzsektor) die Gefahr der Verletzung des Datenschutzes besteht, wird die Kommission prüfen, inwiefern die Pflicht zur Mitteilung einer Verletzung des Datenschutzes auch für andere Sektoren eingeführt werden kann. Die Kommission hatte dies 2009 in einer Erklärung vor dem Europäischen Parlament im Zusammenhang mit der Reform des Rechtsrahmens für elektronische Kommunikationsnetze und –dienste bereits angesprochen.[18] Die Datenschutzrichtlinie für elektronische Kommunikation, die spätestens am 25. Mai 2011 in innerstaatliches Recht umgesetzt sein muss[19], wird nicht in diese Prüfung einbezogen. Auch für diese Aspekte bedarf es eines konsequenten kohärenten Ansatzes.

Die Kommission wird

- die Modalitäten für die Einführung einer **allgemeinen Anzeigepflicht für Datenschutzverstöße** in der allgemeinen Datenschutzregelung prüfen, einschließlich der Adressaten solcher Anzeigen und der Umstände, die eine Anzeigepflicht begründen.

---

17 Siehe Studie zum Kinder- und Jugendschutz im Internet, bei der es um die Altersgruppen der 9 bis 10-Jährigen und 12 bis 14-Jährigen ging und die zeigte, dass Kinder die Risiken der Internetnutzung oft unterschätzen und sich der Schwere der Folgen ihres riskanten Verhaltens nicht bewusst sind (die Studie ist abrufbar auf http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

18 „Die Kommission nimmt den Willen des Europäischen Parlaments zur Kenntnis, dass die Verpflichtung zur Benachrichtigung über die Verletzung des Schutzes personenbezogener Daten nicht auf den Bereich der elektronischen Kommunikation beschränkt sein sollte, sondern auch für Stellen wie Erbringer von Diensten der Informationsgesellschaft gelten sollte […]. Die Kommission wird daher unverzüglich die entsprechenden vorbereitenden Arbeiten, einschließlich der Anhörung der beteiligten Kreise, einleiten, um gegebenenfalls bis Ende 2011 Vorschläge in diesem Bereich vorzulegen […]", abrufbar auf http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//DE. Siehe auch Erwägungsgrund 59 der Richtlinie 2009/136/EG zur Änderung der Datenschutzrichtlinie 2002/58/EG für elektronische Kommunikation: „Das Interesse der Nutzer an der Benachrichtigung ist ersichtlich nicht auf den Bereich der elektronischen Kommunikation beschränkt, so dass ausdrückliche Anzeigepflichten vorrangig in allen Wirtschaftsbereichen auf Gemeinschaftsebene eingeführt werden sollten."

19 Artikel 4 der Richtlinie 2009/136/EG.

2.1.3. Bessere Kontrolle des Betroffenen über seine Daten

Zwei wichtige Voraussetzungen für ein hohes Datenschutzniveau sind, dass **der für die Datenverarbeitung Verantwortliche Daten nur zu ganz bestimmten Zwecken verarbeiten darf (Prinzip der Datensparsamkeit)** und der von der Verarbeitung Betroffene **weiterhin die Kontrolle über seine eigenen Daten hat**. In Artikel 8 Absatz 2 der Charta heißt es: „Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken." Jede Person sollte stets auf seine Daten zugreifen, sie berichtigen, löschen oder sperren können, wenn es keine legitimen gesetzlichen Gründe gibt, die dagegen sprechen. Diese Rechte sind bereits in der geltenden Regelung garantiert. Jedoch ist die Wahrnehmung dieser Rechte in der Praxis nicht einheitlich geregelt; in einigen Mitgliedstaaten ist es einfacher, diese Rechte auszuüben, als in anderen. Darüber hinaus wird die Gewährleistung dieser Rechte besonders in der Online-Umgebung immer schwieriger, weil die Daten dort oft ohne Wissen und/oder ohne Zustimmung des Betroffenen gespeichert werden.

Vor allem sind in diesem Zusammenhang die sozialen Online-Netzwerke anzuführen, da die Frage der Kontrolle des Einzelnen über seine personenbezogenen Daten hier besonders problematisch ist. Einige Personen haben sich an die Kommission gewandt und sich darüber beklagt, dass es ihnen nicht immer gelang, ihre personenbezogenen Daten (beispielsweise Bilder) von Online-Diensteanbieter zurückzuerhalten, und dass sie daher ihr Recht auf Zugang zu ihren Daten, auf deren Berichtigung und Löschung nicht wahrnehmen konnten.

Solche Rechte sollten daher expliziter und klarer formuliert und gegebenenfalls gestärkt werden.

Die Kommission wird daher Möglichkeiten prüfen, um

- das **Prinzip der Datensparsamkeit** zu stärken;

- die **Modalitäten** für die **Wahrnehmung der Rechte auf Zugang zu Daten, auf deren Berichtigung, Löschung oder Sperrung** zu verbessern (z. B. durch Einführung einer Antwortfrist für diesbezügliche Anträge, durch Zulassung technischer Lösungen, mit denen die Rechte auf elektronischem Weg wahrgenommen werden können, oder durch eine Vorschrift, wonach das Zugriffsrecht grundsätzlich gebührenfrei zu gewähren ist);

- das sogenannte **Recht auf Vergessen („right to be forgotten")** zu präzisieren, also das Recht von Personen, dass ihre Daten nicht länger verarbeitet und gelöscht werden, wenn sie nicht mehr für einen rechtmäßigen Zweck gebraucht werden. Dies ist beispielsweise der Fall, wenn die Verarbeitung auf der Grundlage der Zustimmung einer Person zur Verarbeitung erfolgt und wenn diese Person ihre Zustimmung zurückzieht oder wenn die Vorhaltefrist abgelaufen ist;

- die Rechte des von der Verarbeitung Betroffenen zu erweitern, in dem die „**Datenübertragbarkeit"** sichergestellt wird, also das Recht des Einzelnen, seine Daten (z. B. Fotos oder Freundeverzeichnisse) auf einer Anwendung oder einem Dienst zurückzuholen und die zurückgeholten Daten auf eine andere Anwendung oder einen anderen Dienst zu übertragen, sofern dies technisch möglich ist, ohne von dem für die Verarbeitung Verantwortlichen daran gehindert zu werden.

2.1.4. Bewusstsein fördern

Transparenz ist gewiss von wesentlicher Bedeutung, doch ist es darüber hinaus erforderlich, die Allgemeinheit, insbesondere junge Leute, besser über die Risiken der Verarbeitung personenbezogener Daten aufzuklären. Eine Eurobarometer-Umfrage von 2008 in den EU-Mitgliedstaaten erbrachte, dass es nach Meinung der großen Mehrheit der Bevölkerung in ihrem Land an Datenschutzbewusstsein mangelt.[20] Daher sollte die Aufklärung von verschiedenen Seiten verstärkt gefördert und propagiert werden, beispielsweise durch Behörden der Mitgliedstaaten, insbesondere Datenschutzbehörden und für Bildung zuständige Stellen, sowie durch die für die Verarbeitung Verantwortlichen und Verbände der Zivilgesellschaft. In diesem Zusammenhang sollten auch nichtlegislative Maßnahmen ergriffen werden wie Informationskampagnen in den Print- und den Online-Medien und die Bereitstellung leserfreundlicher Informationen auf Websites, aus denen die Rechte der von der Verarbeitung Betroffenen und die Pflichten der für die Verarbeitung Verantwortlichen klar ersichtlich sind.

Die Kommission wird Folgendes sondieren:

- die Möglichkeit der **Kofinanzierung von Aufklärungsmaßnahmen zum Thema Datenschutz** mit Mitteln aus dem EU-Haushalt;

- die Notwendigkeit einer einschlägigen Verpflichtung in der Datenschutzregelung zu **Aufklärungsmaßnahmen** und die Möglichkeiten, die die Regelung dazu bietet.

2.1.5. Gewährleistung der Einwilligung ohne Zwang und in Kenntnis der Sachlage

Wenn die Einwilligung in Kenntnis der Sachlage verlangt wird, muss die betroffenen Person nach geltendem Recht ihren Willen zur Verarbeitung ihrer Daten „ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage“ bekunden; sie akzeptiert dadurch, dass die sie betreffenden personenbezogenen Daten verarbeitet werden.[21] Diese Bedingungen werden allerdings derzeit in den Mitgliedstaaten unterschiedlich ausgelegt. Manche verlangen generell eine schriftliche Einwilligung, andere gehen sogar so weit, die stillschweigende Einwilligung zuzulassen.

Darüber hinaus ist es in der Online-Umgebung – wegen der Undurchsichtigkeit der einschlägigen Datenschutzgrundsätze – oft für Einzelne besonders schwer, ihre Rechte zu kennen und eine Einwilligung in Kenntnis der Sachlage zu erteilen. Erschwerend kommt hinzu, dass es in manchen Fällen nicht einmal klar ist, was unter einer ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage gegebenen Einwilligung zur Datenverarbeitung zu verstehen ist. Ein Beispiel hierfür ist die verhaltensorientierte Internetwerbung, bei der die jeweiligen Einstellungen des Internet-Browsers nach Meinung einiger, aber nicht aller, die Einwilligung des Nutzers zum Ausdruck bringen.

Daher sollte geklärt werden, wann die Bedingungen für die Einwilligung des Betroffenen erfüllt sind, um zu garantieren, dass diese stets in Kenntnis der Sachlage gegeben wird und dass der Betroffene – wie Artikel 8 der Charta der Grundrechte der Europäischen Union verlangt – genau weiß, dass er seine Einwilligung zur Datenverarbeitung erteilt und was diese

---

[20] Siehe Flash Eurobarometer Nr. 225 – Data Protection in the European Union (Datenschutz in der Europäischen Union): http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

[21] Siehe Artikel 2 Buchstabe h der Richtlinie 95/46/EG.

Verarbeitung genau beinhaltet. Wenn die wesentlichen Konzepte klar sind, kann dies auch Anreiz für Initiativen zur Selbstregulierung geben, so dass praktische Lösungen gefunden werden können, die mit dem EU-Recht vereinbar sind.

Die Kommission wird prüfen, wie **die Bestimmungen über die Einwilligung präzisiert und gestärkt werden können**.

2.1.6. Schutz sensibler Daten

Die Verarbeitung sensibler Daten, also von Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben, ist - mit wenigen Ausnahmen unter bestimmten Bedingungen und mit angemessenen Garantien - derzeit bereits generell verboten.[22] Angesichts der technologischen und gesellschaftlichen Entwicklungen müssen jedoch die Bestimmungen über den Schutz sensibler Daten insbesondere daraufhin überprüft werden, ob dies auch für andere Datenkategorien gelten sollte und ob die Voraussetzungen für die Datenverarbeitung präzisiert werden sollten. Das betrifft beispielsweise Gendaten, die bisher nicht ausdrücklich als sensible Datenkategorie eingestuft sind.

Die Kommission wird prüfen,

- ob andere Datenkategorien, beispielsweise **Gendaten**, als **sensible Daten** eingestuft werden sollten;

- ob die **Voraussetzungen** für die Zulassung der Verarbeitung bestimmter Kategorien sensibler Daten **präzisiert und harmonisiert** werden sollten.

2.1.7. Wirksamere Rechtsbehelfe und Sanktionen

Für eine wirksame Durchsetzung der Datenschutzvorschriften bedarf es **wirksamer Bestimmungen über Rechtsbehelfe und Sanktionen.** Viele Fälle, in denen die Datenschutzrechte einer Person verletzt wurden, betreffen auch viele andere Personen in einer ähnlichen Situation.

Die Kommission wird

- prüfen, ob die **Befugnis zur Klage bei nationalen Gerichten** auch auf Datenschutzbehörden und Verbände der Zivilgesellschaft sowie andere **Verbände, die die Interessen der von der Verarbeitung Betroffenen vertreten**, ausgedehnt werden kann;

- untersuchen, ob die **bestehenden Sanktionsregelungen verschärft** werden sollten, beispielsweise durch strafrechtliche Sanktionen bei ernsten Datenschutzverletzungen, damit die Sanktionen mehr Wirkung zeigen.

[22] Siehe Artikel 8 der Richtlinie 95/46/EG.

2.2. Stärkung der Binnenmarktdimension

2.2.1. Mehr Rechtssicherheit und gleiche Bedingungen für die Verantwortlichen für die Datenverarbeitung

Der Datenschutz in der EU hat eine **ausgeprägte Binnenmarktdimension**, d. h. im Binnenmarkt muss der freie Verkehr personenbezogener Daten zwischen den Mitgliedstaaten sichergestellt werden. Daher beschränkt sich die Richtlinie nicht auf eine Mindestharmonisierung der einzelstaatlichen Datenschutzvorschriften, sondern zielt vielmehr auf eine vollständige Harmonisierung.[23]

Gleichzeitig lässt die Richtlinie den Mitgliedstaaten in bestimmten Bereichen einen gewissen Spielraum und erlaubt ihnen, für bestimmte Situationen ihre Sonderbestimmungen beizubehalten oder solche einzuführen.[24] Dies und die Tatsache, dass die Richtlinie von manchen Mitgliedstaaten nicht ordnungsgemäß umgesetzt wurde, hat zu **divergierenden Rechtsvorschriften in den Mitgliedstaaten geführt, die einem der Hauptziele der Richtlinie entgegenstehen, nämlich der Gewährleistung des freien Verkehrs personenbezogener Daten im Binnenmarkt**. Das trifft auf viele Sektoren und Situationen zu, beispielsweise auf die Verarbeitung personenbezogener Daten im Personalwesen oder zum Zweck des Gesundheitsschutzes. Die mangelnde Harmonisierung ist in der Tat eines der Hauptprobleme, auf die private interessierte Gruppen, besonders Unternehmen, immer wieder hinweisen, weil ihnen dadurch Zusatzkosten und Verwaltungsaufwand entstehen. Besonders betroffen sind für die Verarbeitung Verantwortliche, die in mehreren Mitgliedstaaten Niederlassungen haben und sich an die Vorschriften und Praktiken aller dieser Staaten halten müssen. Darüber hinaus führen Unterschiede bei der Umsetzung der Richtlinie in den Mitgliedstaaten nicht nur für die Verantwortlichen für die Verarbeitung zu Rechtsunsicherheit, sondern auch für die von der Verarbeitung Betroffenen, wodurch ein gleichwertiger Schutz, den die Richtlinie eigentlich sicherstellen soll, möglicherweise nicht mehr gewährleistet werden kann.

Die Kommission wird Ansätze für eine **weitere Harmonisierung der Datenschutzbestimmungen auf EU-Ebene** prüfen.

2.2.2. Verringerung des Verwaltungsaufwands

Die Gewährleistung gleicher Bedingungen bedeutet, dass der für die Verarbeitung Verantwortliche mit weniger divergierenden einzelstaatlichen Bestimmungen konfrontiert ist, was den Verwaltungsaufwand für ihn erheblich reduzieren wird. Ein weiterer konkreter Schritt zur Verminderung der Verwaltungslasten und der Kosten für diesen Personenkreis bestünde in der **Änderung und Vereinfachung der derzeitigen Melderegelung.**[25] Die für die Verarbeitung Verantwortlichen sind sich darüber einig, dass die derzeitige allgemeine Pflicht zur Meldung sämtlicher Verarbeitungsvorgänge bei den Datenschutzbehörden eine relativ hohe Belastung darstellt und nicht nennenswert zum Schutz personenbezogener Daten beiträgt. Darüber hinaus ist die Meldepflicht ein Beispiel der Bestimmungen, bei denen die Richtlinie den Mitgliedstaaten einen gewissen Spielraum bei Entscheidungen über Ausnahmen und Vereinfachungen sowie bei der Wahl der anzuwendenden Verfahren lässt.

---

[23] Gerichtshof der Europäischen Union, Rechtssache C-101/01, *Bodil Lindqvist,* Slg. [2003], I-1297, Rdnrn. 96, 97.

[24] A.a.O. Rdnr. 97. Siehe auch Erwägungsgrund 9 der Richtlinie 95/46/EG.

[25] Siehe Artikel 18 der Richtlinie 95/46/EG.

Eine harmonisierte vereinfachte Regelung würde die Kosten wie auch den Verwaltungsaufwand vermindern, vor allem für die multinationalen Unternehmen, die in mehreren Mitgliedstaaten Niederlassungen haben.

Die Kommission wird verschiedene Möglichkeiten für eine **Vereinfachung und Harmonisierung der derzeitigen Melderegelung** prüfen, darunter die Einführung eines **EU-weit einheitlichen Registrierungsformulars**.

2.2.3. Klärung der Bestimmungen über das anwendbare Recht und der Verantwortung der Mitgliedstaaten

Bereits 2003 hatte die Kommission in ihrem ersten Bericht über die Durchführung der Datenschutzrichtlinie[26] darauf hingewiesen, dass die Bestimmungen über das anwendbare Recht[27] „in mehreren Fällen fehlerhaft [sind], wodurch genau die Art von Konflikten auftreten könnten, die durch diesen Artikel verhindert werden sollen“. Dies ist seitdem nicht besser geworden. Wenn mehrere Mitgliedstaaten betroffen sind, ist es daher den für die Verarbeitung Verantwortlichen und den Datenschutzbehörden nicht immer klar, welcher Mitgliedstaat verantwortlich und welches Recht anwendbar ist. Dies ist vor allem dann der Fall, wenn der für die Verarbeitung Verantwortliche nicht übereinstimmende Bestimmungen verschiedener Mitgliedstaaten beachten muss, wenn ein multinationales Unternehmen Niederlassungen in mehreren Mitgliedstaaten hat oder wenn der für die Verarbeitung Verantwortliche nicht in der EU niedergelassen ist, aber Dienste für in der EU Ansässige erbringt.

Auch die Globalisierung und die technologische Entwicklung tragen zu mehr Komplexität bei: Die für die Verarbeitung Verantwortlichen, die oft rund um die Uhr Dienste und Unterstützungsleistungen anbieten, sind zunehmend in mehreren Mitgliedstaaten und Rechtsordnungen tätig. Das Internet erleichtert es ihnen, auch von außerhalb des Europäischen Wirtschaftsraums (EWR)[28] aus großer Entfernung Dienstleistungen zu erbringen und personenbezogene Daten in der Online-Umgebung zu verarbeiten. Oft ist es sogar schwer, zu einem bestimmten Zeitpunkt personenbezogene Daten und die jeweils verwendeten Anlagen zu orten (z. B. bei Cloudcomputing-Anwendungen und -Diensten).

Nach Meinung der Kommission sollte die Tatsache, dass personenbezogene Daten von für die Datenverarbeitung verantwortlichen Personen verarbeitet werden, die in einem Drittland niedergelassen sind, den Betroffenen nicht den Schutz entziehen, auf den sie kraft der Grundrechtecharta und der EU-Datenschutzvorschriften Anspruch haben.

Die Kommission wird prüfen, wie die geltenden **Vorschriften über das anwendbare Recht** sowie die Kriterien zu dessen Bestimmung **geändert und präzisiert** werden können, um für mehr Rechtssicherheit zu sorgen, die Zuständigkeit der Mitgliedstaaten für die Anwendung der Datenschutzvorschriften zu klären und letztlich den von der Verarbeitung Betroffenen in der EU unabhängig vom geografischen Standort des für die Verarbeitung Verantwortlichen stets ein gleiches Schutzniveau zu garantieren.

---

[26] Bericht der Kommission - Erster Bericht über die Durchführung der Datenschutzrichtlinie (95/46/EG) - (KOM(2003) 265).

[27] Siehe Artikel 4 der Richtlinie 95/46/EG.

[28] Norwegen, Liechtenstein und Island sind Teil des Europäischen Wirtschaftsraums.

2.2.4. Mehr Verantwortung der für die Verarbeitung Verantwortlichen

Die verwaltungstechnische Vereinfachung sollte nicht dazu führen, dass **die für die Verarbeitung Verantwortlichen insgesamt weniger Verantwortung für den Datenschutz tragen**. Nach Meinung der Kommission sollten die Pflichten vielmehr stärker rechtlich verankert werden, darunter auch durch Vorschriften über interne Kontrollverfahren und die Zusammenarbeit mit den Datenschutzbehörden. Darüber hinaus sollte sichergestellt werden, dass eine solche Verantwortung auch für die für die Verarbeitung Verantwortlichen, die beruflichen Geheimhaltungspflichten unterliegen (z. B. Anwälte), sowie in den immer häufigeren Fällen besteht, in denen für die Verarbeitung Verantwortliche Unteraufträge über die Datenverarbeitung vergeben (beispielsweise an Auftragsverarbeiter).

Die Kommission wird daher Möglichkeiten ausloten, wie **sichergestellt werden kann, dass die für die Verarbeitung Verantwortlichen wirksame Maßnahmen und Verfahren einführen, mit denen die Einhaltung der Datenschutzvorschriften gewährleistet werden kann.** Dabei wird sie der aktuellen Debatte über die mögliche Einführung des Rechenschaftsgrundsatzes **(„accountability")** Rechnung tragen.[29] Das sollte nicht zu einem zusätzlichen Verwaltungsaufwand für die Verantwortlichen für die Verarbeitung führen, da es darum geht, Garantien und Verfahren festzulegen, die die Einhaltung der Datenschutzbestimmungen erleichtern und gleichzeitig bestimmte Formalitäten abschaffen oder vereinfachen, beispielsweise die Meldeformalitäten (*vgl. 2.2.2*).

Die Technologien zum Schutz der Privatsphäre, für deren Förderung sich die Kommission bereits 2007 in einer Mitteilung ausgesprochen hat, sowie die Anwendung des Konzepts „Privacy by Design" („mit eingebautem Datenschutz") könnten hierbei und für die Datensicherheit eine wichtige Rolle spielen.[30]

---

29 Siehe insbesondere Stellungnahme der Datenschutzgruppe vom 13. Juli 2010, 3/2010.

30 Zu Technologien zum Schutz der Privatsphäre siehe: Mitteilung der Kommission an das Europäische Parlament und den Rat über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre, KOM(2007) 228. Das Konzept „Privacy by Design" bedeutet, dass der Schutz der Privatsphäre und der Datenschutz in den gesamten Technologie-Lebenszyklus integriert werden, vom frühen Entwurfsstadium bis zu deren Einführung, Nutzung und letztendlichen Außerbetriebnahme. Nachzulesen ist dieses Konzept u. a. in der Mitteilung der Kommission „Eine Digitale Agenda für Europa", KOM(2010) 245.

Die Kommission wird folgende Maßnahmen prüfen, um die Verantwortung der für die Verarbeitung Verantwortlichen zu stärken:

– verpflichtende Benennung eines unabhängigen **Datenschutzbeauftragten** und Harmonisierung der Bestimmungen über dessen Aufgaben und Zuständigkeiten[31], wobei zur Vermeidung eines übermäßigen Verwaltungsaufwands vor allem für kleine und kleinste Unternehmen angemessene Schwellen in Erwägung zu ziehen wären;

– Einführung – in der Datenschutzregelung – der Pflicht der für die Verarbeitung Verantwortlichen zur Durchführung einer **Datenschutzfolgenabschätzung** in bestimmten Fällen, wenn beispielsweise sensible Daten verarbeitet werden oder wenn die jeweilige Verarbeitung mit besonderen Risiken verbunden ist, insbesondere beim Einsatz bestimmter Technologien, Systeme und Verfahren, darunter bei der Erstellung von Profilen oder Videoüberwachung;

– weitere Förderung von Technologien zum Schutz der Privatsphäre und der Möglichkeiten für die konkrete Umsetzung des **Privacy-by-Design-**Konzepts.

2.2.5. Förderung von Initiativen zur Selbstregulierung und Möglichkeit der Zertifizierung durch die EU

Die Kommission ist nach wie vor der Meinung, dass **Initiativen** der für die Verarbeitung Verantwortlichen **zur Selbstregulierung zu einer besseren Durchsetzung der Datenschutzvorschriften beitragen können.** Bisher wurden die Bestimmungen der Datenschutzrichtlinie über die Selbstregulierung, die die Erstellung von Verhaltenskodizes vorsehen[32], selten angewandt und werden von den privaten Gruppen als unzureichend gewertet.

Die Kommission wird zudem sondieren, ob **EU-Zertifizierungsregelungen (z. B. Datenschutzsiegel)** für Verfahren, Technologien, Produkte und Dienste, die hinsichtlich des Datenschutzes unbedenklich sind, eingeführt werden sollten.[33] Dies wäre nicht nur für Nutzer dieser Technologien, Produkte und Dienste eine Hilfe, sondern hätte auch Vorteile für die für die Verarbeitung Verantwortlichen: Durch die Wahl zertifizierter Technologien, Produkte und Dienste könnten sie nachweisen, dass sie ihren Pflichten nachgekommen sind (*vgl. 2.2.3*). Selbstverständlich müsste unbedingt die **Zuverlässigkeit solcher Datenschutzsiegel gewährleistet** und geprüft werden, ob sie mit den rechtlichen Pflichten und internationalen Techniknormen vereinbar sind.

Die Kommission wird

- Möglichkeiten zur **verstärkten Förderung von Initiativen zur Selbstregulierung** prüfen, darunter die aktive Förderung von Verhaltenskodizes.

- die Möglichkeit der Einführung von **EU-Zertifizierungsregelungen** für den Schutz der Privatsphäre und den Datenschutz sondieren.

---

31 Bisher ist vorgesehen, dass ein unabhängiger Datenschutzbeauftragter benannt werden kann, der die Einhaltung der Datenschutzvorschriften der EU und der Mitgliedstaaten sicherstellt und an den sich die Betroffenen wenden können. Verschiedene Mitgliedstaaten haben eine solche Funktion bereits eingeführt (beispielsweise in Deutschland, wo es Beauftragte für den Datenschutz gibt, und in Frankreich, das über „Correspondants informatique et libertés (CIL)“ verfügt).

32 Siehe Artikel 27 der Richtlinie 95/46/EG.

33 Dazu siehe auch Mitteilung zu Technologien zum Schutz der Privatsphäre (Fußnote 29).

2.3. Änderung der Datenschutzvorschriften in den Bereichen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen

Die Datenschutzrichtlinie gilt für jegliche Verarbeitung personenbezogener Daten in den Mitgliedstaaten, und zwar sowohl für den öffentlichen als auch für den privaten Bereich. Ausgenommen ist jedoch die „Verarbeitung personenbezogener Daten, die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen", beispielsweise im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen.[34] Mit dem Vertrag von Lissabon wurde jedoch die frühere Säulenstruktur der EU abgeschafft und eine neue Rechtsgrundlage für den Schutz personenbezogener Daten in sämtlichen Politikbereichen der EU eingeführt.[35] Vor diesem Hintergrund und unter Berücksichtigung der EU-Grundrechtecharta hat die Kommission in ihren Mitteilungen über das Stockholmer Programm und den Aktionsplan zur Umsetzung des Stockholmer Programms herausgestellt, dass es einer „*einheitliche[n] Regelung zum Schutz personenbezogener Daten*" bedarf und die „*Position der EU bezüglich des Schutzes personenbezogener Daten bei allen EU-Maßnahmen, einschließlich jener in den Bereichen Strafverfolgung und Kriminalprävention*" gestärkt werden müsse.[36]

Im Unionsrecht ist der Schutz personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen im **Rahmenbeschluss 2008/977/JI**[37] geregelt. Der Rahmenbeschluss ist ein wichtiger Fortschritt in diesem Bereich, in dem gemeinsame Datenschutzstandards dringend erforderlich sind. Darüber hinaus müssen aber noch weitere Schritte ergriffen werden.

Der Rahmenbeschluss gilt nur für den grenzüberschreitenden Austausch von personenbezogenen Daten innerhalb der EU, nicht aber für die Datenverarbeitung innerhalb der Mitgliedstaaten. In der Praxis ist eine Trennung dieser Verarbeitungsvorgänge schwierig; sie kann die Umsetzung und Anwendung des Rahmenbeschlusses erschweren.[38]

Außerdem **lässt der Rahmenbeschluss zu viele Ausnahmen vom Zweckbindungsprinzip zu.** Darüber hinaus werden in den Bestimmungen Datenkategorien nicht nach ihrer sachlichen Richtigkeit und Zuverlässigkeit unterschieden. Auch sollten auf Fakten beruhende Daten anders behandelt werden als Daten, denen Meinungen und persönliche Einschätzungen zugrunde liegen,[39] und es sollte zwischen verschiedenen Gruppen der von der Verarbeitung Betroffenen (Straftäter, Verdächtigte, Opfer, Zeugen usw.) unterschieden werden, wobei für die Gruppe der Nichtverdächtigten besondere Garantien gelten müssten.[40]

---

34 Siehe Artikel 3 Absatz 2 erster Unterabsatz der Richtlinie 95/46/EG.

35 Siehe Artikel 16 AEUV.

36 Siehe KOM(2009) 262 vom 10.6.2009 und KOM(2010) 171 vom 20.4.2010.

37 Rahmenbeschluss 2008/977/JI des Rates vom 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30.12.2008, S. 60). Der Rahmenbeschluss zielt nur auf eine Mindestharmonisierung der Datenschutzstandards.

38 Eine solche Unterscheidung wird in den einschlägigen Instrumenten des Europarates nicht gemacht. Zu diesen Instrumenten gehören: Übereinkommen über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108), Zusatzprotokoll zu diesem Übereinkommen betreffend Kontrollstellen und grenzüberschreitenden Datenverkehr (SEV Nr. 181) und Empfehlung R (87) 15 des Ministerkomitees des Europarates an die Mitgliedstaaten zur Regelung der Benutzung personenbezogener Daten durch die Polizei vom 17. September 1987.

39 Gemäß dem Grundsatz 3.2 der Empfehlung R (87) 15.

40 Entgegen dem Grundsatz 2 der Empfehlung R (87) 15 und den Bewertungsberichten dazu.

Zudem ersetzt der **Rahmenbeschluss nicht die auf EU-Ebene erlassenen sektorspezifischen Vorschriften über die polizeiliche und justizielle Zusammenarbeit in Strafsachen,**[41] insbesondere nicht die Rechtsakte über Europol, Eurojust, das Schengener Informationssystem (SIS) und das Zollinformationssystem (ZIS)[42], die entweder spezielle Datenschutzvorschriften enthalten und/oder auf die Datenschutzübereinkommen des Europarates verweisen. Im Bereich der polizeilichen und justiziellen Zusammenarbeit haben alle Mitgliedstaaten zugesagt, die Empfehlung R (87) 15 des Ministerkomitees des Europarates zu beachten, die die Grundsätze der Konvention Nr. 108 auf polizeiliche Angelegenheiten überträgt. Sie ist jedoch nicht rechtsverbindlich.

Dieser Sachstand kann sich direkt auf die Möglichkeiten auswirken, die Einzelpersonen zur Wahrnehmung ihrer Datenschutzrechte in diesem Bereich haben (z. B. das Recht zu wissen, dass ihre Daten verarbeitet oder weitergegeben werden, wer dies tut und zu welchem Zweck, wie sie ihre Rechte, beispielsweise ihr Recht auf Zugriff auf ihre Daten, durchsetzen können).

Wenn das Ziel einer umfassenden und kohärenten Regelung der EU, die auch gegenüber Drittländern gilt, erreicht werden soll, **muss somit auch eine Änderung der geltenden Datenschutzregeln im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in Erwägung gezogen werden.** Die Kommission betont, dass eine umfassende Datenschutzregelung besondere Bestimmungen für die Bereiche Polizei und Justiz innerhalb der allgemeinen Regelung nicht ausschließt, die dem spezifischen Charakter dieser Bereiche gebührend Rechnung tragen, wie in Erklärung Nr. 21 im Anhang zum Vertrag von Lissabon zum Ausdruck gebracht wurde. Das bedeutet beispielsweise, dass geprüft werden muss, inwieweit die Wahrnehmung bestimmter Datenschutzrechte im Einzelfall die Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder die Vollstreckung strafrechtlicher Sanktionen beeinträchtigen würde.

---

41 Einen Überblick dieser Vorschriften gibt die Mitteilung der Kommission „Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht“, KOM(2010) 385.

42 Zur Überwachung des Datenschutzes wurden für die einzelnen Instrumente gemeinsame Kontrollinstanzen geschaffen. Daneben hat der Europäische Datenschutzbeauftragte aufgrund der Verordnung (EG) Nr. 45/2001 allgemeine Kontrollbefugnisse über die Einrichtungen sowie Ämter und Agenturen der EU.

Die Kommission wird

- die **Einbeziehung der Bereiche der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in den Anwendungsbereichs der allgemeinen Datenschutzbestimmungen** prüfen, und zwar auch bei einer rein innerstaatlichen Verarbeitung, gegebenenfalls bei gleichzeitiger Einführung harmonisierter **Einschränkungen** bestimmter Datenschutzrechte von Personen, z. B. hinsichtlich des Zugriffsrechts oder des Transparenzprinzips;

- prüfen, ob die neue allgemeine Datenschutzregelung **besondere, harmonisierte Vorschriften** enthalten sollte, beispielsweise für den Datenschutz bei der Verarbeitung von **Gendaten** zu strafrechtlichen Zwecken, oder unterschiedliche Vorschriften für verschiedene Gruppen von Betroffenen (Zeugen, Verdächtigte usw.) im Bereich der Zusammenarbeit zwischen den Polizeibehörden und der justiziellen Zusammenarbeit in Strafsachen;

- 2011 eine **Konsultation** aller interessierten Kreise durchführen, um ihre Meinung zu den bestehenden Verfahren zur **Änderung des derzeitigen Kontrollsystems im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen** einzuholen und so eine wirksame, kohärente Datenschutzkontrolle in den Einrichtungen, Ämtern und Agenturen der EU sicherzustellen;

- prüfen, ob die **in einzelnen Rechtsakten enthaltenen sektorspezifischen EU-Vorschriften für die polizeiliche und justizielle Zusammenarbeit in Strafsachen** langfristig an die neue allgemeine Datenschutzregelung **angepasst** werden sollten.

2.4. Die globale Dimension des Datenschutzes

2.4.1. Klärung und Vereinfachung der Bestimmungen über internationale Datentransfers

Der Transfer personenbezogener Daten in Länder außerhalb der EU und des EWR kann u. a. nach einer **Angemessenheitsprüfung** erlaubt werden. Die Angemessenheit des Datenschutzes in einem Drittland, also die Frage, ob das Drittland einen Schutz gewährleistet, den die EU als angemessen betrachtet, kann von der Kommission oder von den Mitgliedstaaten geprüft werden.

Bescheinigt die Kommission die Angemessenheit des Datenschutzes, dürfen personenbezogene Daten unbeschränkt und ohne weitere Garantien von den 27 EU-Mitgliedstaaten und den drei EWR-Staaten an dieses Land weitergegeben werden. Die Anforderungen für die Anerkennung eines angemessenen Datenschutzniveaus durch die Kommission sind allerdings bisher in der Datenschutzrichtlinie nicht genau genug geregelt. Darüber hinaus ist im Rahmenbeschluss eine solche Entscheidung der Kommission nicht vorgesehen.

In manchen Mitgliedstaaten wird beispielsweise die Angemessenheit von dem für die Verarbeitung Verantwortlichen, der die personenbezogenen Daten in ein Drittland übermittelt, geprüft, manchmal nimmt die Datenschutzbehörde eine Ex-post-Kontrolle vor. Dies kann dazu führen, dass bei der Prüfung der Angemessenheit des Datenschutzes in Drittländern oder in internationalen Organisationen unterschiedlich vorgegangen wird **mit der Folge, dass der Schutz, der den von der Verarbeitung Betroffenen in einem Drittland gewährt wird, von Mitgliedstaat zu Mitgliedstaat unterschiedlich beurteilt wird.** Auch enthalten die geltenden Rechtsakte keine genauen harmonisierten Bestimmungen darüber, welche Transfers als rechtmäßig einzustufen sind. Das führt zu einer uneinheitlichen Vorgehensweise in den Mitgliedstaaten.

Hinzu kommt, dass die Standardklauseln der Kommission für den Transfer personenbezogener Daten an für die Verarbeitung Verantwortliche[43] und an Auftragsverarbeiter[44] in Drittländern, die keinen angemessenen Schutz gewährleisten, nicht auf Situationen anwendbar sind, die nicht durch Verträge geregelt sind, und beispielsweise für den Transfer zwischen Behörden nicht verwendet werden können.

Außerdem sehen internationale Abkommen, die die EU oder ihre Mitgliedstaaten schließen, oft die Einführung von Datenschutzgrundsätzen und spezifischen Bestimmungen vor. Das kann zu abweichenden, inkohärenten Bestimmungen und Unterschieden bei den Rechten führen, die zum Nachteil der von der Verarbeitung Betroffenen unterschiedlich ausgelegt werden können. Daher wird die Kommission, wie angekündigt, wesentliche Datenschutzbestimmungen für Abkommen zwischen der EU und Drittländern über die Strafverfolgung erarbeiten.[45]

Auch andere Methoden, die als Form der Selbstregulierung entwickelt wurden, wie verbindliche unternehmensinterne Vorschriften,[46] können nützliche Hilfsmittel für den rechtmäßigen Transfer personenbezogener Daten zwischen den einzelnen Unternehmen eines Konzerns sein. Bei der Konsultation wurde jedoch die Meinung vertreten, dass dieses Verfahren noch verbessert und seine Anwendung erleichtert werden könnte.

Zur Behebung der ermittelten Probleme **müssen die bestehenden Verfahren für internationale Transfers personenbezogener Daten allgemein verbessert werden.** Gleichzeitig muss sichergestellt werden, dass die personenbezogenen Daten beim Transfer und bei der Verarbeitung außerhalb der EU und des EWR angemessen geschützt werden.

Die Kommission wird prüfen, wie

- die **bestehenden Verfahren** für den internationalen Datentransfer, darunter rechtsverbindliche Instrumente und verbindliche unternehmensinterne Vorschriften, **verbessert und koordiniert** werden können, um ein **einheitlicheres und kohärenteres Vorgehen der EU** gegenüber Drittländern und internationalen Organisationen sicherzustellen;

---

43 Entscheidung 2001/497/EG der Kommission vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG (ABl. L 181 vom 4.7.2001, S. 19); Entscheidung 2002/16/EG der Kommission vom 27. Dezember 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (ABl. L 6 vom 10.1.2002, S. 52); Entscheidung 2004/915/EG der Kommission vom 27. Dezember 2004 zur Änderung der Entscheidung 2001/497/EG bezüglich der Einführung alternativer Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (ABl. L 385 vom 29.12.2004, S. 74).

44 Beschluss 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (ABl. L 39 vom 12.2.2010, S. 5).

45 Aktionsplan zur Umsetzung des Stockholmer Programms, siehe Fußnote 36.

46 Verbindliche unternehmensinterne Vorschriften (BCR – Binding Corporate Rules) sind Verhaltenskodizes auf der Grundlage europäischer Datenschutzstandards, die von multinationalen Unternehmen aufgestellt und freiwillig befolgt werden, um angemessene Garantien für den Transfer personenbezogener Daten oder Transferkategorien zwischen Unternehmen eines Konzerns, die konzerninterne Regeln zu befolgen haben, zu gewährleisten. Siehe: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

- das **Verfahren der Kommission zur Prüfung der Angemessenheit präzisiert** und geeignete **Kriterien und Anforderungen** für die Bewertung des Datenschutzniveaus in einem Drittland oder in einer internationalen Organisation festgelegt werden können;

- wie die **zentralen Elemente des Datenschutzes** zu definieren sind, die für alle Arten von internationalen Übereinkommen verwendet werden können.

2.4.2. Förderung universeller Grundsätze

Die Datenverarbeitung ist globalisiert. Daher müssen universell gültige Grundsätze für den Schutz von Personen bei der Verarbeitung personenbezogener Daten festgelegt werden.

Die Datenschutzregelung der EU war oft **Vorbild für Drittländer, die ebenfalls Datenschutzbestimmungen einführen wollten**. Durch ihre Geltung und ihre Auswirkungen in der EU und anderswo setzt sie maßgebende Standards. Die **Europäische Union muss daher weiterhin treibende Kraft bei der Entwicklung und Förderung internationaler rechtlicher und technischer Normen im Bereich des Schutzes personenbezogener Daten** sein, die sich auf die einschlägigen Rechtsinstrumente der EU und der EU-Mitgliedstaaten zum Datenschutz stützen sollten. Dies ist im Rahmen der Erweiterungspolitik der EU besonders wichtig.

Die Kommission ist der Meinung, dass ihre künftige Regelung und die internationalen technischen Normen von Normungsorganisationen unbedingt aufeinander abgestimmt werden müssen, um in der Praxis eine kohärente Anwendung der Datenschutzbestimmungen durch die für die Verarbeitung Verantwortlichen zu gewährleisten.

Die Kommission wird

- sich weiterhin **für die Festlegung hoher rechtlicher und technischer Datenschutzstandards** in Drittländern und auf internationaler Ebene **einsetzen**;

- sich auf internationaler Ebene für den **Grundsatz der Gegenseitigkeit des Schutzes** einsetzen, vor allem beim Export von Daten der von der Verarbeitung Betroffenen aus der EU in Drittländer;

- **dazu enger mit Drittländern und internationalen Organisationen zusammenarbeiten**, darunter mit der OECD, dem Europarat, den Vereinten Nationen und anderen regionalen Organisationen;

- **die Entwicklung internationaler technischer Normen durch Normungsorganisationen** wie CEN und ISO **aufmerksam verfolgen**, um sicherzustellen, dass diese die Rechtsvorschriften sinnvoll ergänzen und die Umsetzung und wirksame Anwendung der wichtigsten Datenschutzvorschriften gewährleisten helfen.

2.5. Verstärkter institutioneller Rahmen für eine bessere Durchsetzung der Datenschutzvorschriften

Die Um- und Durchsetzung der grundlegenden Datenschutzbestimmungen und –regeln ist für den Schutz der Rechte des Einzelnen von grundlegender Bedeutung.

Dabei kommt den **Datenschutzbehörden eine wesentliche Aufgabe zu**. Sie sind unabhängige Hüter der Grundrechte und Grundfreiheiten im Bereich des Datenschutzes, auf die die Einzelnen vertrauen für die Gewährleistung des Schutzes ihrer personenbezogenen

Daten und die Rechtmäßigkeit der Datenverarbeitung. Aus diesem Grund sollte deren Rolle nach Dafürhalten der Kommission besonders in Anbetracht der jüngsten ständigen Rechtsprechung des EuGH zu deren Unabhängigkeit[47] gestärkt werden, und sie sollten die nötigen Befugnisse und Ressourcen erhalten, um ihren Auftrag in ihren Ländern und bei der Zusammenarbeit mit anderen Datenschutzbehörden erfüllen zu können.

Nach Meinung der Kommission sollten die **Datenschutzbehörden** außerdem **enger zusammenarbeiten und ihre Tätigkeiten besser miteinander abstimmen**, besonders dann, wenn sie mit Angelegenheiten befasst sind, die ihrer Natur nach grenzüberschreitenden Charakter haben. Das ist vor allem dann der Fall, wenn multinationale Unternehmen in mehreren Mitgliedstaaten Niederlassungen haben und in allen diesen Ländern aktiv sind oder wenn die Überwachungstätigkeiten mit dem Europäischen Datenschutzbeauftragten koordiniert werden müssen.[48]

Dabei **kann die Datenschutzgruppe eine wichtige Rolle spielen**[49]; neben ihrer Beratungsfunktion[50] muss sie bereits jetzt sicherstellen helfen, dass die EU-Datenschutzvorschriften auf nationaler Ebene einheitlich angewendet werden. Da die EU-Bestimmungen von den Datenschutzbehörden allerdings weiterhin unterschiedlich angewandt und ausgelegt werden, auch wenn die Datenschutzproblematik in der gesamten EU die Gleiche ist, sollte die Rolle der Datenschutzgruppe bei der Koordinierung der Standpunkte der Datenschutzbehörden gestärkt werden, damit eine einheitlichere Anwendung auf Ebene der Mitgliedstaaten und somit ein einheitliches Datenschutzniveau gewährleistet werden kann.

Die Kommission wird prüfen,

- wie die **Rechtsstellung und die Befugnisse der nationalen Datenschutzbehörden** in der neuen Regelung **gestärkt, präzisiert und harmonisiert** werden können, darunter auch durch die uneingeschränkte Durchsetzung des Grundsatzes der völligen Unabhängigkeit;[51]

- wie die **Zusammenarbeit und Abstimmung zwischen den Datenschutzbehörden verbessert** werden kann**;**

- wie eine kohärentere Anwendung der Datenschutzvorschriften der EU im gesamten Binnenmarkt sichergestellt werden kann. Beispielsweise kommen folgende Maßnahmen in Frage: **Stärkung der Rolle der nationalen Datenschutzbeauftragten, bessere Koordinierung ihrer Tätigkeiten über die Datenschutzgruppe (die transparenter werden sollte) und Einführung eines Verfahrens zur Sicherstellung einer einheitlichen Praxis im Binnenmarkt unter der Zuständigkeit der Europäischen Kommission**.

---

47 EuGH-Urteil vom 9.3.2010, Kommission gegen Deutschland, Rechtssache C-518/07.

48 Das ist derzeit für IT-Großanlagen erforderlich, z. B. für das SIS II (siehe Artikel 46 der Verordnung (EG) Nr. 1987/2006, ABl. L 318 vom 28.12.2006, S. 4) und das VIS (siehe Artikel 43 der Verordnung (EG) Nr. 767/2008, ABl. L 218 vom 13.8.2008, S. 60).

49 Die Datenschutzgruppe ist ein Beratungsgremium, das sich aus je einem Vertreter der Datenschutzbehörden der Mitgliedstaaten, dem Europäischen Datenschutzbeauftragten und einem Vertreter der Kommission (ohne Stimmrecht) zusammensetzt. Die Kommission stellt das Sekretariat. Siehe: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm .

50 Die Datenschutzgruppe berät die Kommission über das Schutzniveau in der EU und in Drittländern und über Maßnahmen im Bereich der Verarbeitung personenbezogener Daten.

51 Siehe EuGH-Urteil vom 9.3.2010, Kommission gegen Deutschland, Rechtssache C-518/07.

3. SCHLUSSFOLGERUNG: DAS WEITERE VORGEHEN

Mit der Technologie verändert sich auch die Art und Weise, wie personenbezogene Daten in unserer Gesellschaft verwendet und übermittelt werden. Das stellt die Gesetzgeber vor die Herausforderung, eine Regelung einzuführen, die solche Veränderungen überdauert. Nach der Reform sollten die europäischen Datenschutzvorschriften nach wie vor ein hohes Schutzniveau gewährleisten und gleichzeitig Privatpersonen, Behörden und Unternehmen im Binnenmarkt dauerhaft Rechtssicherheit bieten. Wie komplex die Situation und wie ausgeklügelt eine Technik auch sein mag, es muss klar sein, welches Recht und welche Standards die nationalen Behörden durchzusetzen und die Unternehmen und Entwickler neuer Technologien einzuhalten haben. Auch natürliche Personen müssen Klarheit über ihre Rechte haben.

Das **umfassende Konzept der Kommission** zur Lösung der Probleme und zur Erreichung der zentralen Ziele, die in dieser Mitteilungen dargelegt wurden, wird als Grundlage für die Diskussionen mit den anderen EU-Organen und interessierten Kreisen dienen und zu gegebener Zeit in konkrete Vorschläge und Maßnahmen legislativer und nichtlegislativer Art einfließen. Daher wünscht sich die Kommission Rückmeldung zu den in der Mitteilung angesprochenen Aspekten.

Auf dieser Grundlage wird die Kommission **2011** nach Durchführung einer Folgenabschätzung und unter Berücksichtigung der EU-Grundrechtecharta **Rechtsvorschriften vorschlagen**, um die Datenschutzvorschriften im Sinne des Anliegens der EU zu ändern, dass der Schutz personenbezogener Daten in allen Politikbereichen, auch bei der Strafverfolgung und der Kriminalitätsprävention, deren Besonderheiten zu berücksichtigen sind, gewährleistet wird. Gleichzeitig sind nichtlegislative Maßnahmen geplant. Beispielsweise soll die Selbstregulierung gefördert und die mögliche Einführung von EU-Datenschutzsiegeln geprüft werden.

In einem zweiten Schritt wird die Kommission prüfen, **ob andere Rechtsakte** an die neue allgemeine Datenschutzregelung **angepasst werden müssen**. An erster Stelle betrifft dies die Verordnung (EG) Nr. 45/2001, deren Vorschriften an diese neue Regelung angepasst werden müssten. Später müssen dann auch die Auswirkungen auf andere sektorspezifische Vorschriften sorgfältig geprüft werden.

Die Kommission wird zudem weiterhin für die zuverlässige Überwachung der Umsetzung des Unionsrechts in diesem Bereich **sorgen** und ihr **Vertragsverletzungsinstrumentarium** einsetzen, wenn die EU-Datenschutzbestimmungen nicht ordnungsgemäß umgesetzt und angewandt werden. Die derzeit laufende Überprüfung der Datenschutzbestimmungen berührt nicht die Verpflichtung der Mitgliedstaaten zur Umsetzung und Gewährleistung der ordnungsgemäßen Anwendung des geltenden Datenschutzrechts.[52]

Ein hohes einheitliches Datenschutzniveau in der EU ist die beste Methode zur Unterstützung und Verbreitung der EU-Datenschutzstandards auf internationaler Ebene.

---

[52] Das gilt auch für den Rahmenbeschluss 2008/977/JI des Rates: Die Mitgliedstaaten müssen die erforderlichen Maßnahmen treffen, um dem Rahmenbeschluss vor dem 27. November 2010 nachzukommen.