KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN

Brüssel, den 2.5.2007
KOM(2007) 228 endgültig

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre

(Text von Bedeutung für den EWR)

1. EINLEITUNG

Dank der intensiven und nachhaltigen Entwicklung von Informations- und Kommunikationstechnologien (IKT) werden ständig neue Dienstleistungen zur Verbesserung des täglichen Lebens angeboten. Die Interaktion im Internet fußt weitgehend auf personenbezogenen Daten, die beim Erwerb von Waren und Dienstleistungen, bei der Herstellung und Pflege von Kontakten oder bei der Verbreitung persönlicher Ideen im Internet preisgegeben werden. Neben den Vorteilen, die diese Entwicklung mit sich bringt, entstehen allerdings auch neue Risiken wie Identitätsdiebstahl, diskriminierende Profilerstellung, fortwährende Überwachung oder Betrugsdelikte.

In Artikel 8 der Charta der Grundrechte der Europäischen Union wird das Recht auf den Schutz personenbezogener Daten anerkannt. Näher konkretisiert wird dieses Grundrecht durch einen europäischen Rechtsrahmen zum Schutz personenbezogener Daten, der sich insbesondere aus der Datenschutzrichtlinie 95/46/EG[1] und der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG[2] als auch aus der Verordnung (EG) 45/2001 zur Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft[3] zusammensetzt. In diesen Rechtsvorschriften werden wesentliche Pflichten des für die Datenverarbeitung Verantwortlichen festgelegt und Rechte der Betroffenen anerkannt. In diesen werden gleichfalls Sanktionen und gerichtliche Überprüfungsmöglichkeiten bei Datenschutzverletzungen sowie wirksame Durchsetzungsmaßnahmen festgelegt.

Dieser Rahmen kann sich gleichwohl als unzureichend erweisen, wenn personenbezogene Daten weltweit in IKT-Netzen verbreitet werden und die Bearbeitung der Daten unterschiedlicher, oftmals außerhalb der EU liegender gerichtlicher Zuständigkeiten unterliegt. Zwar darf davon ausgegangen werden, dass die geltenden Vorschriften auch diese Fälle erfassen und eine eindeutige rechtliche Würdigung gestatten. Darüber hinaus wird die Ermittlung der für die Durchsetzung dieser Vorschriften zuständigen Behörde ermöglicht.

---

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 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).

3 Verordnung (EG) 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr; (ABl. L 8 vom 12.1.2001, S. 1–22).

Gleichwohl können der Durchsetzung in der Praxis mitunter große Hindernisse im Weg stehen. Letztere beruhen auf Schwierigkeiten, welche sich beim Einsatz von Technologien zur Datenverarbeitung durch unterschiedliche Stellen an unterschiedlichen Orten und bei der Durchsetzung nationaler Verwaltungsvorschriften und Gerichtsentscheide in anderen Zuständigkeitsbereichen (und besonders in Nicht-EU-Ländern) ergeben können.

Wenngleich streng genommen für die Einhaltung der Datenschutzvorschriften allein die für die Datenverarbeitung Verantwortlichen zuständig sind, tragen, gesellschaftlich oder ethisch-moralisch betrachtet, auch andere eine gewisse Verantwortung für den Schutz personenbezogener Daten. Dazu gehören unter anderem diejenigen, die technische Spezifikationen ausarbeiten bzw. Datenverarbeitungsprogramme oder Betriebssysteme entwickeln.

Artikel 17 der Datenschutzrichtlinie sieht vor, dass der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen ergreifen muss, die einen der Art der Daten und den bei der Datenverarbeitung bestehenden Risiken angemessenen Schutz gewährleisten. Der Einsatz von technischen Maßnahmen zur Einhaltung von Rechtsvorschriften (und insbesondere der Datenschutzvorschriften) ist zum Teil bereits in der Datenschutzrichtlinie für elektronische Kommunikation[4] vorgesehen.

Eine weitere Möglichkeit zur Erreichung des durch den Rechtsrahmen vorgegebenen Ziels, die Verarbeitung personenbezogener Daten auf das erforderliche Mindestmaß zu beschränken und nach Möglichkeit anonyme oder pseudonymisierte Daten zu verwenden, wäre ein Rückgriff auf Technologien zum Schutz der Privatsphäre, die sicherstellen, dass Verstöße gegen Datenschutzvorschriften und persönliche Rechte nicht nur unter Strafe gestellt, sondern auch technisch erschwert werden.

In dieser an den ersten Bericht über die Durchführung der Datenschutzrichtlinie[5] anschließenden Mitteilung werden die Vorteile von Technologien zum Schutz der Privatsphäre erläutert, die von der Kommission verfolgten Ziele zur Förderung von Technologien zum Schutz der Privatsphäre festgelegt und diesbezüglich konkrete Maßnahmen zur Entwicklung von Technologien zum Schutz der Privatsphäre und ihrer Verwendung von den für den Datenschutz Verantwortlichen sowie von den Verbrauchern vorgestellt.

2. WAS SIND TECHNOLOGIEN ZUM SCHUTZ DER PRIVATSPHÄRE?

Es gibt eine Reihe von Definition von Technologien zum Schutz der Privatsphäre, die von der akademischen Gemeinschaft und im Rahmen von einschlägigen Pilotprojekten verwendet werden. Im Rahmen des von der Gemeinschaft finanzierten Projekts „PISA“ beispielsweise versteht man hierunter ein kohärentes System von IKT-Maßnahmen zum Schutz der Privatsphäre durch Eliminierung oder Verminderung personenbezogener Daten oder durch Vermeidung einer unnötigen und/oder unerwünschten Verarbeitung von personenbezogenen Daten ohne Verlust der Funktionalität des betreffenden Informationssystems. Die Verwendung von Technologien zum Schutz der Privatsphäre kann dabei helfen, Informations- und Kommunikationssysteme und -dienstleistungen so zu konzipieren, dass nur so wenig wie

---

4 Siehe Erwägungsgrund 46 und Artikel 14 Absatz 3 der Richtlinie 2002/58/EG.

5 KOM (2003) 265/1 vom 15.5.2003 (http://eurlex.europa.eu/LexUriServ/site/de/com/2003/com2003_0265de01.pdf)

nötig personenbezogene Daten gesammelt und verwendet werden müssen und die Einhaltung der Datenschutzbestimmungen erleichtert wird. Die Kommission hat diesbezüglich in ihrem ersten Bericht über die Durchführung der Datenschutzrichtlinie betont: *„Die Kommission hält den Einsatz geeigneter technologischer Maßnahmen für eine unverzichtbare Ergänzung rechtlicher Maßnahmen und ist der Auffassung, dass sie integraler Bestandteil jeglicher Bemühungen um einen ausreichendes Datenschutzniveau sein sollten."* Durch die Verwendung von Technologien zum Schutz der Privatsphäre sollte es möglich sein, Verstöße gegen bestimmte Datenschutzvorschriften zu erschweren und/oder leichter aufzudecken.

Die Wirksamkeit, die die verschiedenen Technologien zum Schutz der Privatsphäre in Bezug auf diesen Schutz und die Einhaltung der Datenschutzbestimmungen entfalten können, ist aufgrund der Dynamik der IKT unterschiedlich und ändert sich mit der Zeit. Auch bestehen Unterschiede in Bezug auf ihre Typologie. So kann es sich hierbei um Einzelhilfsmittel handeln, die entweder das aktive Mitwirken der Verbraucher (Erwerb und Installation auf ihrem PC) erfordern oder aber bereits „ab Werk" in der Architektur von Informationssystemen integriert sind. Hierfür lassen sich mehrere Beispiele nennen.

- Automatische Datenanonymisierung nach einer bestimmten Zeit fußt auf dem Grundsatz, dass die verarbeiteten Daten in einer Form vorgehalten werden sollten, die die Identifizierung der Betroffenen nur für einen so langen Zeitraum ermöglicht, wie er für die Zwecke, zu denen die Daten ursprünglich gesammelt wurden, notwendig ist.

- Verschlüsselungsanwendungen, die ein unrechtmäßiges Auslesen von Daten bei deren Übermittlung im Internet verhindern, erleichtern es dem für die Datenverarbeitung Verantwortlichen, seiner Pflicht nachzukommen, geeignete Maßnahmen zum Schutz personenbezogener Daten vor einer unrechtmäßigen Verarbeitung zu ergreifen .

- Hilfsprogramme („cookie cutters"), die verhindern, dass Profildateien („cookies") auf den PC des Verbrauchers geladen werden und dort ohne Wissen des Benutzers bestimmte Vorgänge in Gang setzen, sind ein nützliches Mittel zur Einhaltung der Vorgabe, dass personenbezogene Daten nach Treu und Glauben und auf rechtmäßige Weise verarbeitet werden müssen und der Betroffene über die laufende Verarbeitung in Kenntnis gesetzt werden muss.

- Die „Platform for Privacy Preferences" (P3P), die Internetnutzern Einblick in die Datenschutzpolitik von Webseitenbetreibern und den Vergleich ihrer Präferenzen in Bezug auf die von ihnen freigegebenen Informationen mit den diesbezüglichen Vorlieben anderer Internetnutzer ermöglicht, trägt ebenfalls dazu bei, dass es sich bei der Zustimmung der Betroffenen zur Verarbeitung ihrer Daten um eine fundierte Entscheidung handelt.

3. DIE KOMMISSION FÖRDERT TECHNOLOGIEN ZUM SCHUTZ DER PRIVATSPHÄRE

Aufgrund der obigen Überlegungen ist die Kommission der Auffassung, dass die Technologien zum Schutz der Privatsphäre weiterentwickelt werden und breitere Verwendung erfahren sollten – und zwar insbesondere in den Fällen, in denen personenbezogene Daten in IKT-Netzen verarbeitet werden. Von einer breiteren Verwendung von Technologien zum Schutz der Privatsphäre verspricht sich die Kommission sowohl einen besseren Schutz der Privatsphäre als auch eine einfachere Einhaltung der Datenschutzbestimmungen. Der Einsatz von Technologien zum Schutz der Privatsphäre wäre eine sinnvolle Ergänzung zum geltenden Rechtsrahmen und seinen Durchführungsvorschriften.

Daher hat die Kommission in ihrer Mitteilung „Eine Strategie für eine sichere Informationsgesellschaft – Dialog, Partnerschaft und Delegation der Verantwortung“ (KOM (2006) 251 vom 31. Mai 2006) insbesondere den Privatsektor aufgefordert, „*den Einsatz die Sicherheit erhöhender Produkte, Verfahren und Dienste anzuregen, um Identitätsdiebstahl und andere Angriffe auf die Privatsphäre zu verhindern und zu bekämpfen*". Zudem ist laut dem von der Kommission vorgelegten Fahrplan für die Schaffung eines gesamteuropäischen eIDM-Rahmens bis zum Jahr 2010[6] eines der zentralen Grundsätze der elektronischen Identitätsverwaltung, dass das betreffende System sicher sein, die zum Schutz der Privatsphäre des Nutzers erforderlichen Sicherheitsvorkehrungen treffen und eine Anpassung seiner Verwendung an örtliche Interessen und Tätigkeiten ermöglichen muss.

Da unterschiedliche Akteure bei der Datenverarbeitung mitwirken und unterschiedliche nationale Gerichtsbarkeiten zuständig sind, kann sich die Durchsetzung des geltenden Rechtsrahmens als schwierig erweisen. Demgegenüber könnten Technologien zum Schutz der Privatsphäre sicherstellen, dass bestimmte Verstöße gegen die Datenschutzvorschriften, die Eingriffe in Grundrechte einschließlich des Rechts auf Privatsphäre zur Folge haben, vermieden werden könnten, da sie technisch erschwert würden. Die Kommission ist sich bewusst, dass technische Mittel zwar einen wesentlichen Beitrag zum Schutz der Privatsphäre leisten können, aber allein nicht für einen sicheren Schutz ausreichen. Der Einsatz von Technologien zum Schutz der Privatsphäre muss daher nach Maßgabe eines Regelwerks erfolgen, das sich aus durchsetzbaren Datenschutzbestimmungen zusammensetzt, welche einen flexibel festlegbaren Schutz der Privatsphäre des Einzelnen ermöglichen. Die Verwendung von Technologien zum Schutz der Privatsphäre bedeutet nicht, dass die betreffenden Betreiber von bestimmten ihnen obliegenden Pflichten (wie der Pflicht, den Nutzern Zugang zu ihren Daten zu gewähren) befreit werden können.

Ferner könnte wichtigen öffentlichen Interessen besser gedient werden. Der rechtliche Rahmen zum Datenschutz sieht Einschränkungen der allgemeinen Grundsätze zur Verwirklichung wichtiger öffentlicher Interessen wie der öffentlichen Sicherheit, der Verbrechensbekämpfung oder der öffentlichen Gesundheit sowie Eingriffe in die Rechte des Einzelnen vor. Die Bedingungen für diese Einschränkungen sind in Artikel 13 der Datenschutzrichtlinie und in Artikel 15 der Datenschutzrichtlinie für elektronische Kommunikation festgelegt. Sie entsprechen denen von Artikel 8 der Europäischen Menschenrechtskonvention (EMRK): Derartige Eingriffe müssen gesetzlich vorgesehen, verhältnismäßig und in einer demokratischen Gesellschaft erforderlich sein, um rechtmäßigen öffentlichen Zwecken zu dienen[7]. Durch den Einsatz von Technologien zum Schutz der Privatsphäre dürfen Strafverfolgungsbehörden oder andere zuständige Behörden nicht bei der Ausübung ihrer in einem wichtigen öffentlichen Interesse erfüllten Aufgaben wie der Bekämpfung von Internetkriminalität, des Terrorismus oder der Verhinderung der Ausbreitung ansteckender Krankheiten behindert werden. Um diesen Aufgaben nachzukommen, müssen die zuständigen Behörden in Übereinstimmung mit den gesetzlich festgelegten Verfahren, Voraussetzungen und Garantien erforderlichenfalls Zugriff auf personenbezogene Daten nehmen können.

Eine bessere Einhaltung der Datenschutzbestimmungen würde sich auch positiv auf das Vertrauen der Verbraucher (insbesondere im Internet) auswirken. Eine Reihe viel

---

6 http://ec.europa.eu/information_society/activities/egovernment_research/doc/eidm_roadmap_paper.pdf

7 Europäischer Gerichthof, Urteil vom 20. Mai 2003, Verb. Rechtssachen C-465/00, C-138/01 und C-139/01 „Österreichischer Rundfunk u.a." ("Rechnungshof“), Slg. 2003, I-04989, Randnr. 71 und 72;

versprechender und nützlicher Dienste, die auf der Übertragung von personenbezogenen Daten in IT-Netzen beruhen, beispielsweise „E-Lernen“, „E-Verwaltung“, „E-Gesundheit“, „E-Bankverkehr“, „E-Handel“ oder intelligente Kfz-Systeme, würden sicher davon profitieren. Die Nutzer könnten sicher sein, dass die Daten, die sie preisgeben, um sich auszuweisen, Dienste in Anspruch zu nehmen oder Zahlungen zu leisten, nur zu legitimen Zwecken verwendet werden und dass sie für ihr Mitwirken in der digitalen Gemeinschaft nicht auf ihre dem Einzeln zustehenden Rechte verzichten müssen.

4. FERTIGGESTELLTE ARBEITEN UND WEITERES VORGEHEN

Um die angestrebte Verbesserung des Schutzes der Privatsphäre und des Datenschutzes in der Gemeinschaft unter anderem durch die Förderung der Entwicklung und des Einsatzes von Technologien zum Schutz der Privatsphäre zu erreichen, beabsichtigt die Kommission die nachfolgend genannten Maßnahmen zu ergreifen, welche ein Vielzahl von Akteuren einschließlich ihrer eigenen Dienststellen, nationaler Behörden, Unternehmen und Verbraucher betreffen.

In den diesbezüglichen Diskussionen sollte die besondere Lage der kleinen und mittleren Unternehmen (KMU), ihrer Einsatzmöglichkeiten für Technologien zum Schutz der Privatsphäre und entsprechende Anreize beachtet werden. Die Kommission hat daneben die Punkte Vertrauen und Sensibilisierung zu berücksichtigen, die gleichfalls von besonderer Bedeutung für KMU sind.

4.1. Erstes Ziel: Unterstützung der Entwicklung von Technologien zum Schutz der Privatsphäre

Wenn Technologien zum Schutz der Privatsphäre breite Verwendung finden sollen, müssen sie zunächst konzipiert, entwickelt und hergestellt werden. Obwohl all dies bereits in gewissem Umfang im Rahmen von Forschungsmaßnahmen des öffentlichen und des privaten Sektors geschieht, ist die Kommission der Auffassung, dass diese Tätigkeit intensiviert werden sollte. Dafür sollten zunächst der Bedarf an Technologien zum Schutz der Privatsphäre und ihre technischen Anforderungen ermittelt und im Rahmen von Maßnahmen auf dem Gebiet der Forschung und technologischen Entwicklung die entsprechenden Werkzeuge entwickelt werden.

4.1.1. Maßnahme 1.1.: Ermittlung des Bedarfs an Technologien zum Schutz der Privatsphäre und ihrer technischen Anforderungen

Technologien zum Schutz der Privatsphäre hängen stark von der Entwicklung von IKT ab. Sobald die durch technologische Entwicklungen verursachten Gefahren ermittelt sind, müssen die Anforderungen an eine entsprechende technische Lösung ermittelt werden.

Die Kommission wird verschiedene beteiligte Gruppen ermutigen, gemeinsam über Technologien zum Schutz der Privatsphäre zu diskutieren. Zu diesen beteiligten Gruppen zählen insbesondere Vertreter des IKT-Sektors, Entwickler von Technologien zum Schutz der Privatsphäre, Datenschutzbehörden, Strafverfolgungsbehörden, Technologiepartner einschließlich Sachverständige aus den betroffenen Bereichen wie „E-Gesundheit“ und Informationssicherheit, sowie Verbraucher und Bürgerrechtsverbände. Diese solchermaßen Beteiligten sollen die technische Entwicklung regelmäßig überprüfen, die von ihr ausgehenden Gefahren für die Grundrechte und den Datenschutz zu ermitteln und die

technischen Anforderungen einer auf Technologien zum Schutz der Privatsphäre beruhenden Lösung festzustellen. Dies kann auch eine Feinabstimmung der technischen Maßnahmen auf die unterschiedlichen Risiken und Daten und Berücksichtigung der zu wahrenden öffentlichen Interessen wie der öffentlichen Sicherheit mitumfassen.

4.1.2. Maßnahme 1.2.: Entwicklung von Technologien zum Schutz der Privatsphäre

Sobald der Bedarf an Technologien zum Schutz der Privatsphäre und ihre technologischen Anforderungen ermittelt sind, müssen konkrete Maßnahmen ergriffen werden, um ein gebrauchsfertiges Endprodukt zu erzeugen.

Die Kommission hat bereits hinsichtlich der Notwendigkeit von Technologien zum Schutz der Privatsphäre Maßnahmen ergriffen. Sie finanziert im Rahmen des 6. Rahmenprogramms das Projekt „PRIME“[8], bei dem es um Fragen der digitalen Identitätsverwaltung und des Datenschutzes in der Informationsgesellschaft geht. Das Projekt „OPEN-TC“[9] soll einen Schutz der Privatsphäre auf der Grundlage einer offenen, vertrauenswürdigen Datenverarbeitung ermöglichen, und im Rahmen des Projekts „DISCREET“[10] wird eine Verteilungsplattform („middleware“) zum Schutz der Privatsphäre bei fortgeschrittenen Netzdiensten entwickelt. Die Kommission beabsichtigt, im Rahmen des 7. Rahmenprogramms weitere FuE-Projekte sowie umfangreiche Pilotvorhaben zu fördern, um das Wissen über Technologien zum Schutz der Privatsphäre weiterzuentwickeln und zu verbessern. Dabei geht es darum, die Grundlage für Datenschutzdienste zu schaffen, die eine stärkere Einflussnahme der Benutzer ermöglichen und im Rahmen von Partnerschaften zwischen dem öffentlichen und dem privaten Sektor die bestehenden rechtlichen und technischen Unterschiede in Europa zu beseitigen versuchen.

Die Kommission fordert ferner die nationalen Behörden und den privaten Sektor auf, in die Entwicklung von Technologien zum Schutz der Privatsphäre zu investieren. Derartige Investitionen sind der Schlüssel für eine Vorreiterrolle der europäischen Wirtschaft in einem Sektor, der immer stärker wachsen wird, da diese Technologien zunehmend durch technologische Standards vorgeschrieben und von Verbrauchern, die sich der Notwendigkeit des Schutzes ihrer Rechte im Internet bewusst sind, gefordert werden.

4.2. Zweites Ziel: Förderung des Einsatzes verfügbarer Technologien zum Schutz der Privatsphäre durch die für die Datenverarbeitung Verantwortlichen

Technologien zum Schutz der Privatsphäre können ihren Nutzen nur dann entfalten, wenn sie einen effizienten Verbund mit entsprechender Hard- und Software für die Verarbeitung personenbezogener Daten bilden. Der Mitwirkung der Hersteller derartiger Ausrüstung und der für die Datenverarbeitung Verantwortlichen, die diese Ausrüstung zur Datenverarbeitung benutzen, kommt daher große Bedeutung zu.

4.2.1. Maßnahme 2.1.: Förderung des Einsatzes von Technologien zum Schutz der Privatsphäre in der Wirtschaft

Die Kommission ist davon überzeugt, dass alle an der Verarbeitung personenbezogener Daten beteiligten Akteure von eine breiteren Verwendung von Technologien zum Schutz der

---

8 https://www.prime-project.eu/

9 http://www.opentc.net/

10 http://www.ist-discreet.org/

Privatsphäre profitieren würden. Die IKT-Industrie als größter Entwickler und Bereitsteller von Technologien zum Schutz der Privatsphäre hat bei der Förderung dieser Technologien eine besonders wichtige Rolle zu spielen. Die Kommission fordert alle für die Datenverarbeitung Verantwortlichen auf, Technologien zum Schutz der Privatsphäre in größerem Umfang und intensiver in ihre Verfahren einzubinden. Zu diesem Zweck wird die Kommission Seminare für die wichtigsten Akteure der IKT-Industrie (und insbesondere Entwickler von Technologien zum Schutz der Privatsphäre) organisieren, um zu ermitteln, wie diese dazu beitragen können, dass die für die Datenverarbeitung Verantwortlichen stärkeren Gebrauch von Technologien zum Schutz der Privatsphäre machen.

Die Kommission wird ferner eine Studie über den wirtschaftlichen Nutzen von Technologien zum Schutz der Privatsphäre durchführen und ihre Ergebnisse veröffentlichen, um Unternehmen (und insbesondere KMU) zu ermuntern, diese Technologien einzusetzen.

4.2.2. Maßnahme 2.2.: Sicherstellung der Einhaltung geeigneter Normen zum Schutz personenbezogener Daten durch Technologien zum Schutz der Privatsphäre

Während eine weit reichende Förderung die aktive Mitwirkung der IKT-Industrie als Hersteller von Technologien zum Schutz der Privatsphäre erfordert, sind zur Sicherstellung der Einhaltung geeigneter Normen Maßnahmen erforderlich, die über eine Selbstregulierung oder den guten Willen der Akteure hinausgehen. Die Kommission wird anhand entsprechender Folgenabschätzungen prüfen, inwieweit es notwendig ist, Normen für die Verarbeitung personenbezogener Daten durch Technologien zum Schutz der Privatsphäre zu entwickeln. Nach Maßgabe der Ergebnisse dieser Folgenabschätzungen könnten sodann folgende weitere Maßnahmen ergriffen werden:

- *Maßnahme 2.2.a) Normung*

Die Kommission wird prüfen, inwieweit die Notwendigkeit der Einhaltung der Datenschutzbestimmungen bei der Normung zu berücksichtigten ist. Die Kommission wird sich bemühen, den Beiträgen der von den Beteiligten geführten Debatte über Technologien zum Schutz der Privatsphäre bei der Vorbereitung entsprechender Maßnahmen der Kommission und der Arbeiten der europäischen Normungseinrichtungen Rechnung zu tragen. Besonders wichtig wird dies für aus der Debatte hervorgegangene Datenschutzstandards sein, die die Einbindung und Verwendung bestimmter Technologien zum Schutz der Privatsphäre erfordern.

Die Kommission wird möglicherweise die europäischen Normungseinrichtungen (CEN, CENELEC und ETSI) ersuchen, spezifische europäische Anforderungen zu ermitteln und diese anschließend durch Anwendung der geltenden Abkommen zwischen europäischen und internationalen Normungseinrichtungen auf die internationale Ebene zu bringen. Die europäischen Normungseinrichtungen sollten gegebenenfalls ein spezifisches Normungsprogramm für die europäischen Anforderungen aufstellen, um die auf internationaler Ebene laufenden Arbeiten zu ergänzen.

- *Maßnahme 2.2.b) Koordinierung der technischen nationalen Vorschriften über Sicherheitsvorkehrungen bei der Datenverarbeitung*

Die zur Umsetzung der Datenschutzrichtlinie[11] erlassenen einzelstaatlichen Rechtsvorschriften ermöglichen den nationalen Datenschutzbehörden einen gewissen Einfluss auf die Ermittlung der genauen technischen Anforderungen (z.B. Leitlinien für die für die Datenverarbeitung Verantwortlichen, Prüfung der eingerichteten Systeme und technische Vorgaben). Nationale Datenschutzbehörden könnten auch Anforderungen für die Einbindung und Verwendung bestimmter Technologien zum Schutz der Privatsphäre in Fällen aufstellen, in denen die Verarbeitung der betreffenden personenbezogenen Daten dies erfordert. Die Kommission ist der Auffassung, dass durch die Koordinierung der nationalen Praktiken in diesem Bereich ein positiver Beitrag zur Förderung der Verwendung von Technologien zum Schutz der Privatsphäre geleistet werden könnte. Insbesondere die Arbeitsgruppe nach Artikel 29[12] sollte durch die Förderung einer einheitlichen Anwendung der gemäß der Richtlinie angenommenen nationalen Maßnahmen dazu beitragen. Die Kommission fordert daher die Artikel-29-Datenschutzgruppe auf, in ihr Arbeitsprogramm für diesen Bereich als Dauertätigkeit die Prüfung der Notwendigkeit der Einbindung von Technologien zum Schutz der Privatsphäre in Datenverarbeitungsvorgänge als wirksames Mittel zur Sicherstellung der Einhaltung der Datenschutzvorschriften aufzunehmen. Im Rahmen dieser Arbeiten sollten sodann Leitlinien für Datenschutzbehörden entwickelt werden, die diese auf nationaler Ebene im Wege einer koordinierten Annahme der geeigneten Instrumente umsetzen müssten.

4.2.3. Maßnahme 2.3.: Förderung des Einsatzes von Technologien zum Schutz der Privatsphäre in Behörden

Eine beständige Zahl von personenbezogene Daten betreffenden Verarbeitungsvorgängen wird von öffentlichen Behörden im Rahmen ihrer Zuständigkeiten auf nationaler und auf Gemeinschaftsebene durchgeführt. Öffentliche Einrichtungen sind verpflichtet, ihrerseits die Grundrechte einschließlich des Rechts auf den Schutz personenbezogener Daten zu wahren und dafür Sorge zutragen, dass diese auch von Dritten gewahrt werden. Daher sollten sie mit gutem Beispiel vorangehen.

In Bezug auf die nationalen Behörden stellt die Kommission fest, dass sich „E-Behörden"-Anwendungen als Werkzeug zur Steigerung der Effizienz öffentlicher Dienste immer stärker verbreiten. Sie hat in ihrer Mitteilung „*Die Rolle elektronischer Behördendienste (E-Government) für die Zukunft Europas*"[13] darauf hingewiesen, dass der Einsatz „datenschutzfreundlicher Technik" in elektronischen Behördendiensten erforderlich ist, um das für ihren Erfolg notwendige Vertrauen zu schaffen. Die Kommission ruft die Regierungen auf, dafür Sorge zu tragen, dass in„E-Behörden"-Anwendungen Datenschutzvorkehrungen integriert werden und bei der Auslegung und Implementierung dieser Anwendungen ein möglichst umfassender Rückgriff auf Technologien zum Schutz der Privatsphäre erfolgt.

Was die Gemeinschaftsorgane und -einrichtungen anbelangt, so wird die Kommission selbst dafür Sorge tragen, dass sie den Anforderungen der Verordnung (EG) Nr. 45/2001 erfüllt, insbesondere durch eine breitere Verwendung von Technologien zum Schutz der Privatsphäre bei der die Verarbeitung von personenbezogenen Daten einschließenden Implementierung

---

11 Beispielsweise gemäß Artikel 17.

12 Durch Artikel 29 der Richtlinie 95/46/EG eingesetzte Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten.

13 KOM (2003) 567 endg. vom 26.9.2003.

von IKT-Anwendungen. Gleichzeitig ruft die Kommission die anderen EU-Organe und -einrichtungen auf, ebenso zu verfahren. Der Europäische Datenschutzbeauftragte könnte die Gemeinschaftsorgane und -einrichtungen bei der Ausarbeitung interner Vorschriften über die Verarbeitung personenbezogener Daten beraten. Bei der Wahl neuer IKT-Anwendungen für den eigenen Gebrauch oder bei der Weiterentwicklung bestehender Anwendungen wird die Kommission die Möglichkeit der Einbindung von Technologien zum Schutz der Privatsphäre prüfen. Der Bedeutung von Technologien zum Schutz der Privatsphäre wird auch in der Strategie der Kommission für den IT-Bereich Rechnung getragen werden. Die Kommission wird ferner die Sensibilisierung ihres eigenen Personals vorantreiben. Die Umsetzung von Technologien zum Schutz der Privatsphäre in den IKT-Anwendungen der Kommission hängt jedoch von der Verfügbarkeit entsprechender Produkte ab und wird von Fall zu Fall nach Maßgabe des Entwicklungsstands der einzelnen Anwendungen zu prüfen sein.

4.3. Drittes Ziel: Anregung der Verbraucher zur Verwendung von Technologien zum Schutz der Privatsphäre

Es sind nach wie vor die Verbraucher, denen am meisten daran liegt, dass ihre personenbezogenen Daten ordnungsgemäß verarbeitet werden, dass Datenschutzvorschriften ordnungsgemäß angewandt werden, und dass die Wahrung ihrer Grundrechte durch effiziente Technologien zum Schutz der Privatsphäre sichergestellt wird.

Die Verbraucher sollten daher umfassend über die Vorteile aufgeklärt werden, die die Verwendung von Technologien zum Schutz der Privatsphäre mit sich bringen kann, wenn es darum geht, die bei der Verarbeitung ihrer personenbezogenen Daten bestehenden Risiken zu mindern. Auch sollten die Verbraucher, wenn sie IT-Geräte und Software erwerben oder elektronische Dienstleistungen in Anspruch nehmen, eine wohlüberlegte Wahl treffen können. Sie müssen sich der Risiken bewusst sein, insbesondere, ob Technologien zum Schutz der Privatsphäre einen angemessenen Schutz ermöglichen. Dazu müssen den Nutzern einfache, leicht verständliche Informationen über verfügbare technologische Hilfsmittel zum Schutz ihrer Privatsphäre an die Hand gegeben werden. Im Falle eines stärkeren Einsatzes von Technologien zum Schutz der Privatsphäre sowie einer stärkeren Inanspruchnahme elektronischer, auf Technologien zum Schutz der Privatsphäre basierender Dienstleistungen würde sich dies für solche Unternehmen wirtschaftlich lohnen, die Rückgriff auf diese Technologien genommen haben, was den Dominoeffekt haben könnte, wiederum andere Unternehmen dazu zu bewegen, größeren Wert auf die Einhaltung der Datenschutzbestimmungen zu legen. Um dies zu erreichen, sollten die nachfolgend behandelten Maßnahmen ergriffen werden.

4.3.1. Maßnahme 3.1.: Aufklärung der Verbraucher

Es sollte eine konsequente Strategie zur Aufklärung der Verbraucher über die bei der Verarbeitung ihrer personenbezogenen Daten bestehenden Risiken und über die möglichen Lösungen durch die die bestehenden Garantien der Datenschutzvorschriften ergänzenden Technologien zum Schutz der Privatsphäre verabschiedet werden. Die Kommission beabsichtigt, eine Reihe EU-weiter Maßnahmen zur Aufklärung über Technologien zum Schutz der Privatsphäre in die Wege zu leiten.

Es ist in erster Linie die Aufgabe der nationalen Datenschutzbehörden, die bereits über einschlägige Erfahrungen auf diesem Gebiet verfügen, diese Maßnahme umzusetzen. Die Kommission fordert daher die nationalen Datenschutzbehörden auf, im Rahmen ihrer Maßnahmen zur Verbraucheraufklärung nach Möglichkeit auch über Technologien zum

Schutz der Privatsphäre zu informieren. Die Kommission fordert zudem die Artikel-29-Datenschutzgruppe auf, die einschlägigen nationalen Praktiken im Rahmen eines kohärenten Arbeitsplans zur Aufklärung über Technologien zum Schutz der Privatsphäre zu koordinieren und als Forum für den Austausch über auf nationaler Ebene bestehende bewährte Praktiken zu agieren. Beispielsweise könnten gemeinsam mit Verbraucherverbänden und sonstige Beteiligten wie das Netz der Europäischen Verbraucherzentren („ECC-Netz") als EU-weites Netz zur Beratung der Bürger über ihre Rechte als Verbraucher Aktionen zur Verbraucheraufklärung unternommen werden.

4.3.2. Maßnahme 3.2.: Erleichterung der von den Verbrauchern getroffenen Wahl: Datenschutzgütesiegel

Die Einführung und Verwendung von Technologien zum Schutz der Privatsphäre könnte gesteigert werden, wenn das Vorhandensein dieser Technologien in einem gegebenen Produkt und ihre wesentlichen Eigenschaften leicht erkennbar wären. Zu diesem Zweck plant die Kommission eine Machbarkeitsstudie über ein EU-weites System von Datenschutzgütesiegeln einschließlich einer Analyse seiner wirtschaftlichen und sozialen Auswirkungen. Zweck derartiger Datenschutzgütesiegel wäre es, die Verbraucher in die Lage zu versetzen, das Produkt leichter zu erkennen, dass sicherstellt oder dazu beiträgt, die Datenschutzvorschriften bei der Datenverarbeitung einzuhalten, insbesondere dank integrierter Technologien zum Schutz der Privatsphäre.

Damit Datenschutzgütesiegel ihren Zweck erfüllen können, müssten folgende Grundsätze eingehalten werden:

– Die Zahl der Datenschutzgütesiegelsysteme sollte so gering wie möglich gehalten werden. Ein Übermaß an Siegeln könnte die Verbraucher nur noch weiter verunsichern und ihr Vertrauen in sämtliche Siegel erschüttern. Daher sollte ermittelt werden, ob und inwieweit es angebracht wäre, ein europäisches Datenschutzgütesiegel in ein allgemeines Sicherheits-Zertifizierungsprogramm aufzunehmen[14].

– Datenschutzgütesiegel sollten nur vergeben werden, wenn ein Produkt bestimmte durch Datenschutzvorschriften vorgegebene Normen erfüllt. Diese Normen sollten nach Möglichkeit in der ganzen EU einheitlich sein.

– Öffentliche Behörden und vor allem die nationalen Datenschutzbehörden sollten durch ihre Mitwirkung bei der einschlägigen Normen- und Verfahrensfestlegung und der Überwachung der Funktionsfähigkeit des Datenschutzgütesiegelsystems eine wichtige Rolle in diesem System spielen.

Im Lichte dieser Überlegungen und der jüngsten Erfahrungen mit Gütesiegelprogrammen in anderen Bereichen (u.a. Umwelt, Landwirtschaft, Sicherheitszertifizierung für Produkte und Dienstleistungen) wird die Kommission in einen Dialog mit allen Betroffen (darunter nationale Datenschutzbehörden, Industrie- und Verbraucherverbände sowie Normungseinrichtungen) treten.

---

[14] Die Kommission hat den Privatsektor bereits in ihrer Mitteilung „Eine Strategie für eine sichere Informationsgesellschaft - Dialog, Partnerschaft und Delegation der Verantwortung" (KOM(2006) 251 vom 31. Mai 2006) aufgefordert, „auf erschwingliche Sicherheits-Zertifizierungsprogramme für Produkte, Verfahren und Dienste hinzuarbeiten, die bestimmte EU-Anforderungen abdecken (insbesondere in Bezug auf die Privatsphäre)".