5020/01/DE/endg.
WP 43

EMPFEHLUNG

zu einigen Mindestanforderungen für die Online-Erhebung personenbezogener Daten in der Europäischen Union

Angenommen am 17. Mai 2001

Die Datenschutzgruppe wurde durch Artikel 29 der Richtlinie der 95/46/EG eingesetzt. Sie ist das unabhängige EU-Beratungsgremium in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG festgelegt, ferner in Artikel 14 der Richtlinie 97/66/EG. Als Sekretariat fungiert folgender Dienst:

Europäische Kommission, GD Binnenmarkt, Funktionieren und Auswirkungen des Binnenmarktes - Koordinierung - Datenschutz
Rue de la Loi 200, B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Belgien - Büro: C100-6/136
Internet-Adresse: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN,

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 und Artikel 30 Absatz 1 Buchstabe a und Absatz 3 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung, insbesondere Artikel 12 und 14,

hat folgende Empfehlung angenommen:

I. Einführung

1. In ihrem Arbeitsdokument „Privatsphäre im Internet - Ein integrierter EU-Ansatz zum Online-Datenschutz" vom 21. November 2000[2] hatte die Datenschutzgruppe darauf hingewiesen, wie wichtig es ist, dass Mittel bereitgestellt werden, die garantieren, dass die Internet-Nutzer alle Informationen erhalten, die sie benötigen, um in Kenntnis der Sachlage entscheiden zu können, ob die Websites, zu denen sie Verbindung aufnehmen wollen, vertrauenswürdig sind, und ob sie ggf. bestimmte in den einschlägigen europäischen Rechtsvorschriften verankerte Rechte in Anspruch nehmen möchten. Das ist um so wichtiger, als die Nutzung des Internet immer mehr Möglichkeiten zur Erhebung personenbezogener Daten schafft und damit die Bedrohung der Grundrechte und -freiheiten der Bürger, insbesondere ihrer Privatsphäre, verstärkt. In ihrer Stellungnahme 4/2000 vom 16. Mai 2000 über „das Datenschutzniveau, das die Grundsätze des sicheren Hafens bietet" hat die Gruppe die Kommission ersucht, die Einführung eines EU-Gütesiegels für Websites auf der Grundlage einheitlicher Datenschutzkriterien, welche auf Gemeinschaftsebene festgelegt werden könnten, als dringlich zu behandeln.

   Die vorliegende Empfehlung ist eine konsequente Fortsetzung der Überlegungen in den beiden vorgenannten Unterlagen. Sie soll dazu beitragen, dass die einzelstaatlichen Vorschriften zur Umsetzung der Richtlinien über den Schutz personenbezogener Daten[3] wirksam und einheitlich angewandt werden. Zu diesem Zweck sollen praktische Orientierungshilfen dafür gegeben werden, wie die in den Richtlinien festgeschriebenen Regeln auf die gängigsten Verarbeitungen im Internet

---

1 Amtsblatt L 281 vom 23.11.1995, S. 31, verfügbar unter: http://europa.eu.int/comm/internal_market/de/media/dataprot/index.htm

2 WP 37 (5063/00): Arbeitsdokument - Privatsphäre im Internet - Ein integrierter EU-Ansatz zum Online-Datenschutz, angenommen am 21. November 2000. Verfügbar unter: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp37en.htm

3 Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und Richtlinie 97/66/EG vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation. Verfügbar unter http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp37de.pdf

anzuwenden sind. Diese werden insbesondere beim „ersten Kontakt" zwischen Internet-Nutzer und Website durchgeführt, unabhängig davon, ob er nur zu Informationszwecken oder aber zum Zwecke einer geschäftlichen Transaktion erfolgt; die jeweiligen Zwischenstufen sind hier eingeschlossen.

Die Orientierungshilfen betreffen im wesentlichen die Erhebung personenbezogener Daten im Web; sie sollen Auskunft darüber geben, welche Maßnahmen die einzelnen Beteiligten ergreifen müssen, um zu gewährleisten, dass die Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden (Anwendung der Artikel 6, 7, 10 und 11 der Richtlinie 95/46/EG). Sie erläutern im wesentlichen, wann und wie den einzelnen Nutzern Auskunft erteilt werden muss und auf welche Weise dies erfolgen muss, geben aber auch praktische Hinweise zu einzelnen Rechten und Pflichten, die sich aus den Richtlinien ergeben.

Diese Empfehlung ist mithin primär als praktische Handreichung für die Umsetzung der allgemeinen Grundsätze der Richtlinie gedacht. Die Datenschutzgruppe betrachtet diese Empfehlung als ersten Schritt zur Festlegung von Mindestanforderungen auf europäischer Ebene, die die für die Verarbeitung Verantwortlichen (also die natürlichen oder juristischen Personen, die im Zusammenhang mit einer Website für die Verarbeitung personenbezogener Daten verantwortlich sind[4]) beim Betrieb ihrer Website problemlos erfüllen können; gegebenenfalls müssen diese Mindestanforderungen durch ausführlichere Angaben und Fachinformationen ergänzt werden[5]. Das entbindet die für die Verarbeitung Verantwortlichen keineswegs von ihrer Pflicht zu prüfen, ob bei ihren Verarbeitungen sämtliche Anforderungen und Bedingungen erfüllt werden, an die die geltenden nationalen Rechtsvorschriften die Rechtmäßigkeit der Verarbeitung knüpfen.

Die vorliegende Empfehlung gilt, wenn der für die Verarbeitung Verantwortliche in einem der Mitgliedstaaten der Europäischen Union ansässig ist. In diesem Fall ist das nationale Recht des betreffenden Mitgliedstaates auf die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit der jeweiligen Niederlassung anwendbar. Die Empfehlung gilt auch in den Fällen, in denen der für die Verarbeitung Verantwortliche nicht auf dem Gebiet der Gemeinschaft ansässig ist, aber zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder sonstige

---

4 Zum besseren Verständnis sei darauf hingewiesen, dass Artikel 2 der Richtlinie 95/46/EG den Begriff „für die Verarbeitung Verantwortlicher“ definiert als „die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten in einzelstaatlichen oder gemeinschaftlichen Rechts- und Verwaltungsvorschriften festgelegt, so können der für die Verarbeitung Verantwortliche bzw. die spezifischen Kriterien für seine Benennung durch einzelstaatliche oder gemeinschaftliche Rechtsvorschriften bestimmt werden“

5 Die Empfehlungen in dieser Unterlage sind Mindestanforderungen in dem Sinne, dass es außer ihnen noch weitere Anforderungen gibt. Sie müssen zu einem späteren Zeitpunkt vervollständigt werden durch ergänzende Empfehlungen zur Verarbeitung von personenbezogenen Daten, die sensiblerer Natur sind, wie z. B. die, die auf Websites, welche Gesundheitsinformationen bieten oder sich an Kinder richten, oder auf Webportalen bereitgestellt werden. Bezüglich anderer spezifischer Verarbeitungen, wie der Verbreitung personenbezogener Daten auf einer Website oder die Speicherung von Verkehrsdaten durch Internet Service Provider oder Anbieter von Internetinhalten und -diensten, sei auf die Empfehlungen der Datenschutzgruppe in der in Fußnote 1 genannten Unterlage sowie auf weitere relevante Stellungnahmen der Gruppe hingewiesen, z. B. WP 25 (5085/99): Empfehlung 3/99 zur Aufbewahrung von Verkehrsdaten durch Internet-Dienstanbieter für Strafverfolgungszwecke, angenommen am 7. September 1999. WP 18 (5005/99): Empfehlung 2/99 zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs, angenommen am 3. Mai 1999. WP 17 (5093/98): Empfehlung 1/99 über die unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet durch Software und Hardware, angenommen am 23. Februar 1999. Alle Unterlagen sind unter der in Fußnote 1 genannten Adresse verfügbar.

Mittel zurückgreift, die sich auf dem Hoheitsgebiet eines der Mitgliedstaaten der EU befinden. Solche Verarbeitungen fallen unter das nationale Recht des Mitgliedstaats, in dessen Hoheitsgebiet die technischen Einrichtungen oder Mittel belegen sind[6].

2. Um die genannten Ziele zu erreichen, richtet sich die Empfehlung vor allem an:
   - die für die Verarbeitung von online erhobenen Daten Verantwortlichen, denen ein praktischer Leitfaden an die Hand gegeben wird, in dem die erforderlichen Mindestmaßnahmen beschrieben sind;
   - die Internet-Nutzer, damit sie ihre Rechte kennen und auch in Anspruch nehmen können;
   - die Stellen, die Gütesiegel vergeben wollen, welche die Konformität der Verarbeitungen mit den EU-Datenschutzrichtlinien bescheinigen; diesen Stellen werden Kriterien für die Vergabe eines solchen Gütesiegels geliefert; es versteht sich von selbst, dass bei der Vergabe auch noch andere, mit anderen Rechten und Pflichten zusammenhängende Kriterien zwingend berücksichtigt werden müssen; die Datenschutzgruppe wird sich zu einem späteren Zeitpunkt hierzu noch ausführlicher äußern;
   - die in Europa für den Schutz personenbezogener Daten zuständigen Kontrollstellen, damit sie ein einheitliches Instrument erhalten, auf das sie sich beziehen können, wenn sie ihre Aufgabe erfüllen, d. h., wenn sie dafür sorgen, dass die nationalen Rechtsvorschriften zur Umsetzung der genannten Richtlinien eingehalten werden.

3. Darüber hinaus ist die Datenschutzgruppe der Auffassung, dass diese Empfehlung auch bei der Entwicklung von Normen für Software und Hardware, die für die Erhebung und Verarbeitung personenbezogener Daten im Internet bestimmt sind, herangezogen werden sollte.

II. Empfehlungen zu den Informationen, die bei der Erhebung personenbezogener Daten im Gebiet der Mitgliedstaaten der Europäischen Union zu liefern sind

2.1. Welche Informationen wären den Betroffenen zu erteilen und wann?

4. Jegliche Erhebung personenbezogener Daten über eine Website setzt voraus, dass zunächst bestimmte Informationen geliefert werden. Inhaltlich bedeutet diese Informationspflicht folgendes:

[6] Siehe Artikel 4 Absatz 1 Buchstabe a und c der Richtlinie 95/46/EG. Dieser Sachverhalt ist deutlich zu unterscheiden von der Rechtmäßigkeit der Übermittlung personenbezogener Daten von der EU in ein Drittland. Diese Frage wird in den Artikeln 25 und 26 der Richtlinie 95/46/EG und den damit zusammenhängenden Entscheidungen der Europäischen Kommission über die Angemessenheit des Datenschutzes in bestimmten Drittländern behandelt. Wenn beispielsweise eine amerikanische Website in der EU befindliche Ausrüstungen benutzt, um personenbezogene Daten zu erheben und zu verarbeiten, dann sind die Rechtsvorschriften des betreffenden europäischen Landes auf die Erhebungen und die Verarbeitung unanwendbar, unabhängig davon, ob das betreffende Unternehmen einen angemessenen Datenschutzes im Sinne der Entscheidung der Kommission zum sicheren Hafen bietet oder nicht. Die Frage, ob ein Datenempfänger sich auf die Grundsätze des sicheren Hafens verpflichtet hat, ist nur für die Rechtmäßigkeit nachfolgender Übermittlungen personenbezogener Daten von einem in der EU ansässigen Unternehmen an das betreffende amerikanische Unternehmen von Belang.

5. Die Identität und die physische und elektronische Adresse des für die Verarbeitung Verantwortlichen sind anzugeben, ggf. auch die des von ihm gemäß Artikel 4 Absatz 2 der Richtlinie benannten Vertreters.

6. Der Zweck/die Zwecke der Verarbeitung von Daten, die der für die Verarbeitung Verantwortliche über eine Website erhebt, ist/sind deutlich anzugeben. Wenn beispielsweise Daten sowohl zur Ausführung eines Vertrags (Internet-Abonnement, Bestellung eines Produkts usw.) als auch für die Zwecke der Direktwerbung erhoben werden, muss der für die Verarbeitung Verantwortliche deutlich auf beide Zwecke hinweisen.

7. Es muss deutlich erkennbar sein, wo es sich um zwingende und wo um freiwillige Angaben handelt. Als zwingend sind die Daten zu betrachten, ohne deren Angabe die gewünschte Leistung nicht erbracht werden kann. Der Hinweis, ob es sich um zwingende oder freiwillige Angaben handelt, könnte durch Hinzufügen eines Sternchens erfolgen, mit dem die zwingenden Angaben gekennzeichnet werden, oder aber durch Hinzufügung eines Hinweises „freiwillig" dort, wo nicht zwingende Informationen erfragt werden. Es darf im übrigen niemandem zum Nachteil gereichen, wenn er auf freiwilliger Basis abgefragte Informationen nicht erteilt.

8. Es muss darauf aufmerksam gemacht werden, dass und unter welchen Voraussetzungen die betroffene Person ihre Zustimmung zur Verarbeitung ihrer personenbezogenen Daten geben muss bzw. sie verweigern kann[7], und dass sie ein Auskunftsrecht sowie das Recht auf Berichtigung und Löschung der Daten besitzt. Insbesondere zu nennen ist die Person oder die Stelle, an die man sich zur Ausübung seiner Rechte wenden muss; zudem muss auf die Möglichkeit hingewiesen werden, die Rechte sowohl online als auch an der physischen Adresse des für die Verarbeitung Verantwortlichen auszuüben.

9. Die Empfänger bzw. Kategorien von Empfängern der erhobenen Informationen sind zu nennen. Bei jeder Datenerhebung wäre auf der betreffenden Website anzugeben, ob die erhobenen Daten an Dritte - wie z. B. Geschäftspartner oder Tochtergesellschaften - weitergegeben werden und wozu (zu anderen Zwecken als zur Erbringung der gewünschten Leistung und zu Zwecken der Direktwerbung[8]).

---

[7] Eine Verarbeitung für einen bestimmten Zweck ist nur dann rechtmäßig, wenn sie aus einem der in Artikel 7 der Richtlinie 95/46/EG genannten Gründe erfolgt (u. a. wenn die betroffene Person ohne jeden Zweifel ihre Einwilligung gegeben hat, wenn die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich ist, wenn die Verarbeitung für die Erfüllung einer rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt, erforderlich ist, wenn sie erforderlich ist zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse der betroffenen Personen überwiegt.

Das Widerspruchsrecht (vgl. Artikel 14) müssen die Mitgliedstaaten in mindestens zwei in Artikel 7 genannten Fällen, einschließlich des letztgenannten Falls, anerkennen. Die betroffene Person kann jederzeit aus überwiegenden, schutzwürdigen, sich aus ihrer Situation ergebenden Gründen dagegen Widerspruch einlegen, dass die sie betreffenden Daten verarbeitet werden; dies gilt nicht bei einer im einzelstaatlichen Recht vorgesehenen entgegenstehenden Bestimmung. Der Widerspruch muss in jedem Fall auf Antrag kostenfrei möglich sein, wenn die betreffende Verarbeitung zum Zwecke der Direktwerbung erfolgen soll. Darüber hinaus muss die betroffene Person auch kostenfrei dagegen Widerspruch erheben können (nachdem sie informiert wurde und vor der ersten Weitergabe), dass sie betreffende personenbezogene Daten zu Zwecken der Direktwerbung an Dritte weitergegeben oder im Auftrag Dritter genutzt werden.

[8] Die Daten dürfen nur dann Dritten zur Verfügung gestellt werden, wenn dies mit den Zwecken, zu denen sie erhoben wurden, nicht unvereinbar ist und wenn die Verarbeitung aus einem der in Artikel 7 der Richtlinie 95/46/EG genannten Gründe erfolgt und von daher rechtmäßig ist.

Ist das der Fall, müssen die Internet-Nutzer effektiv die Möglichkeit haben, durch Anklicken eines entsprechenden Feldes bei der Online-Übermittlung der Daten Widerspruch dagegen zu erheben, dass die Daten zu anderen Zwecken als zur Erbringung der jeweiligen Leistung benutzt werden. Da es jederzeit möglich sein muss, das Widerspruchsrecht in Anspruch zu nehmen, sollte den Betroffenen außerdem mitgeteilt werden, dass das Widerspruchsrecht online ausgeübt werden kann. Die Datenschutzgruppe ist sich durchaus bewusst, dass die Bildschirme nicht mit Informationen überladen werden sollten, und vertritt deshalb die Auffassung, dass das Fehlen jeglichen Hinweises auf die Datenempfänger gleichbedeutend ist mit der Verpflichtung des für die Verarbeitung Verantwortlichen, die erhobenen Daten nicht an Dritte weiterzugeben oder gegenüber Dritten offenzulegen, deren Name und Anschrift nicht angegeben sind, es sei denn, die Identität des Dritten ist offenkundig und die Weitergabe der Daten an diesen ist unbedingt erforderlich, um die von dem Internet-Nutzer gewünschte Leistung zu erbringen.

10. Wenn die Daten von dem für die Verarbeitung Verantwortlichen in ein Nicht-EU-Land übermittelt werden sollen, ist anzugeben, ob dort ein angemessenes Datenschutzniveau im Sinne von Artikel 25 der Richtlinie 95/46/EG gegeben ist oder nicht. Im letztgenannten Fall muss die Identität und die (physische und ggf. elektronische[9]) Adresse der Empfänger angegeben werden.

11. Des weiteren sind Name und (physische und elektronische) Adresse des Dienstes oder der Person anzugeben, die damit beauftragt ist, Fragen zum Schutz personenbezogener Daten zu beantworten.

12. Ferner ist auf die Verwendung automatisierter Datenerhebungsverfahren, wie z. B. Cookies, deutlich hinzuweisen, und zwar bevor eine Erhebung mit Hilfe dieser Verfahren erfolgt[10].

    Wenn solche Verfahren verwendet werden, müssen die betroffenen Personen die in dieser Unterlage genannten Informationen erhalten. Zudem muss dem Nutzer Folgendes mitgeteilt werden: Domain-Namen des Site-Servers, über den der Einsatz der automatisierten Erhebungsverfahren erfolgt; der Zweck dieser Verfahren; ihre Lebensdauer; Angaben darüber, ob die Einwilligung in den Einsatz dieser Verfahren Voraussetzung für den Besuch der Site sind; ein Hinweis auf die Möglichkeit für jeden Nutzer, sich dem Einsatz des jeweiligen Verfahrens zu widersetzen und schließlich Angaben darüber, welche Folgen es hat, wenn ein Verfahren deaktiviert wird. Wenn andere für die Verarbeitung Verantwortliche an der Erhebung personenbezogener Daten beteiligt sind, sollten die betroffenen Personen darüber informiert werden, wer jeweils verantwortlich ist, und für welchen Zweck die Daten jeweils verarbeitet werden.

---

[9] Informationen über Beschlüsse zur Angemessenheit des Datenschutzes sind auf der Website der Kommission unter folgender Adresse verfügbar:
http://europa.eu.int/comm/internal_market/de/media/dataprot/index.htm

[10] Die „unsichtbare“ automatische Verarbeitung personenbezogener Daten unterliegt denselben Bedingungen wie die andere Verarbeitungen personenbezogener Daten, und es müssen hierfür auch dieselben Garantien gegeben werden. Vgl. Empfehlung 1/99 über die unsichtbare und automatische Verarbeitung personenbezogener Daten im Internet durch Software und Hardware (vom 23. Februar 1999), verfügbar auf der in Fußnote 1 genannten Website.

Die Informationen und der Hinweis darauf, dass der Datenerhebung widersprochen werden kann, müssen jeweils vor Einsatz der automatisierten Verfahren angezeigt werden, die dem Nutzer-PC den Befehl geben, eine Verbindung zu einer anderen Website aufzubauen, beispielsweise wenn der Internet-Nutzer durch eine Website automatisch an eine andere Website weitergeleitet wird, damit er dort Bannerwerbung anschaut; damit wird vermieden, dass die zweite Site ohne Wissen des Nutzers Daten erheben kann.

Wenn beispielsweise der Server eines für die Verarbeitung Verantwortlichen ein Cookie setzt, muss dies mitgeteilt werden, bevor das Cookie auf der Festplatte des Nutzer-PC abgelegt wird, und zwar zusätzlich zu den Angaben, die bei der derzeit verwendeten Technik bereits erteilt werden; man beschränkt sich derzeit darauf, den Namen des Cookie-setzenden Webservers sowie die Lebensdauer des Cookie automatisch anzugeben.

13. Es sind Angaben erforderlich über die in Anwendung des einzelstaatlichen Rechts ergriffenen Sicherheitsmaßnahmen, die die Authentizität der Website, die Integrität der Daten und die Vertraulichkeit der über das Netz übermittelten Daten gewährleisten[11].

14. Die Informationen sollten in allen Sprachen geliefert werden, die auf der Site benutzt werden, insbesondere dort, wo personenbezogene Daten erhoben werden sollen.

15. Die für die Verarbeitung Verantwortlichen sollten dafür sorgen, dass die Informationen in den einzelnen „Dokumenten" (Rubrik „Schutz personenbezogener Daten und Schutz der Privatsphäre", elektronische Formulare, Wortlaut der allgemeinen Geschäftsbedingungen und sonstiger kommerzieller Mitteilungen), die eine Verpflichtung des Website-Betreibers beinhalten, kohärent sind.

2.2. Wie sind die Betroffenen zu informieren?

16. Die Datenschutzgruppe ist der Auffassung, dass die nachfolgend aufgeführten Angaben direkt auf dem Bildschirm angezeigt werden sollten, bevor überhaupt Daten erhoben werden; damit würde garantiert, dass die Verarbeitung nach Treu und Glauben erfolgt. Es geht dabei um folgende:

- Identität des für die Verarbeitung Verantwortlichen;
- Zweck bzw. Zwecke der Verarbeitung;
- Angaben dazu, ob die erfragten Informationen zwingend oder freiwillig sind;
- Empfänger bzw. Kategorien von Empfängern der erhobenen Daten;
- Hinweis auf das Auskunftsrecht und das Recht auf Berichtigung;
- Hinweis auf das Recht, der Offenlegung der Daten gegenüber Dritten zu anderen Zwecken als zur Erbringung der gewünschten Leistung zu widersprechen, und Angaben dazu, wie dieses Recht wahrgenommen werden kann (z. B. durch Anzeige eines Felds, das angeklickt werden kann);
- Informationen, die im Falle der Verwendung automatisierter Erhebungsverfahren zu erteilen sind;
- Angaben zum Sicherheitsniveau in allen Phasen der Übermittlung, z. B. über Netze.

[11] Siehe die Vorschriften von Artikel 17 Absatz 1 und Absatz 3 zweiter Spiegelstrich der Richtlinie 95/46/EG.

In diesen Fällen sollten die Angaben interaktiv auf dem Bildschirm gemacht werden. Werden automatisierte Erhebungsverfahren eingesetzt, könnten die entsprechenden Hinweise, falls erforderlich, durch Öffnen eines „Pop-up-Fensters" erfolgen.

Informationen zur Sicherheit der Übermittlung von Daten vom Nutzer-PC zur Website könnten folgendermaßen aussehen: „Sie bauen jetzt eine sichere Sitzung auf", oder der Nutzer könnte über den Navigator automatisch informiert werden, beispielsweise durch Anzeigen eines Bildsymbols (Schlüssel oder Vorhängeschloss) auf dem Bildschirm.

17. Darüber hinaus vertritt die Datenschutzgruppe die Ansicht, dass vollständige Informationen über die Datenschutzpolitik (einschließlich Angaben über die Möglichkeit zur Ausübung des Auskunftsrechts) direkt auf der Homepage zugänglich sein sollten und überall dort, wo personenbezogene Daten online erfasst werden. Der Titel der anzuklickenden Rubrik sollte so deutlich hervorgehoben und aussagekräftig sein, dass sich der Internet-Nutzer ein genaues Bild von den Inhalten machen kann, zu denen die Verbindung hergestellt werden soll. Beispielsweise könnte folgender Hinweis gegeben werden „Wir erheben und verarbeiten Sie betreffende personenbezogene Daten. Klicken Sie hier, wenn Sie Näheres wissen möchten" oder „Personenbezogene Daten und Datenschutz". Die Inhalte, zu denen eine Verbindung aufgebaut wird, sollten ebenfalls ausreichend genau beschrieben sein.

3. Empfehlungen bezüglich anderer Rechte und Pflichten

Die Datenschutzgruppe möchte die Aufmerksamkeit der Adressaten dieser Empfehlung noch auf einige andere Rechte der Betroffenen und Pflichten der für die Verarbeitung Verantwortlichen lenken, die sich aus den Richtlinien ergeben und die im Zusammenhang mit der Erhebung personenbezogener Daten über Websites besonders wichtig sind. Die Gruppe ist der Auffassung, dass die unten stehenden Empfehlungen ebenso wie die obigen Erläuterungen zu den Informationen sowohl für die für die Verarbeitung Verantwortlichen als auch für die Internetnutzer von unmittelbarem praktischem Nutzen sind.

18. Daten sollten nur insoweit erhoben werden, als sie zur Erreichung des angegebenen Zwecks erforderlich sind.

19. Es sollte gewährleistet werden, dass Daten nur verarbeitet werden, wenn dies im Sinne von Artikel 7 der Richtlinie 95/46/EG rechtmäßig ist.

20. Es sollte sichergestellt werden, dass das Auskunftsrecht und das Recht auf Berichtigung wirklich in Anspruch genommen werden können, und zwar sowohl über die physische Adresse des für die Verarbeitung Verantwortlichen als auch online. Es sollte Sicherheitsmaßnahmen geben, die garantieren, dass nur die betroffene Person online Zugang zu den sie betreffenden Daten hat.

21. Der Grundsatz der Zweckbestimmung sollte beachtet werden, d. h., personenbezogene Daten sollten nur benutzt werden, wenn dies für einen spezifischen Zweck erforderlich ist. Mit anderen Worten: Personenbezogene Daten dürfen nur für rechtmäßige Zwecke benutzt werden, und die betroffene Person muss

anonym bleiben (Artikel 6 Absatz 1 Buchstabe b der Richtlinie 95/46/EG). Dieser Grundsatz wird zuweilen auch als „Grundsatz der Datenminimierung“ bezeichnet.

22. In demselben Kontext (vgl. Ziff. 21) sollte es möglich sein, eine kommerzielle Website anonym abzufragen, ohne dass also der Benutzer sich zunächst durch Angabe von Namen, Vornamen, E-Mail-Adresse oder sonstige Angaben identifizieren muss; die Möglichkeit zur anonymen Abfrage sollte gefördert werden.

    Falls eine Verbindung zu einer bestimmten Person erforderlich ist, ohne dass eine vollständige Identifizierung nötig wäre, sollte die Verwendung von Pseudonymen aller Art angeboten und akzeptiert werden.

    Die Verwendung von Pseudonymen sollte selbst bei bestimmten Transaktionen gefördert und akzeptiert werden, sofern kein gesetzliches Erfordernis zur Identifizierung besteht. Ein Beispiel ist die Verwendung von Pseudonymen in Zertifikaten für elektronische Signaturen (vgl. Artikel 8 der Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen).

23. Es sollte festgelegt werden, wie lange die erhobenen Daten aufbewahrt werden dürfen. Die Daten dürfen nicht länger aufbewahrt werden, als es für die Realisierung der Zwecke, für die sie erhoben oder weiterverarbeitet werden, erforderlich ist (Artikel 6 der Richtlinie 95/46/EG und Artikel 6 der Richtlinie 97/66/EG).

24. Es sollten die Maßnahmen ergriffen werden, die notwendig sind, um die Sicherheit der Daten bei der Verarbeitung, einschließlich der Übermittlung, zu garantieren (z. B. Beschränkung und Festlegung des Personenkreises, der Zugang zu den Daten hat; Verwendung starker Verschlüsselungen; Artikel 17 der Richtlinie 95/46/EG).

25. Falls ein Auftragsverarbeiter beteiligt ist, beispielsweise als Hostserver für eine Website, sollte ein Vertrag geschlossen werden, in dem von dem Auftragsverarbeiter verlangt wird, dass er gemäß den Rechtsvorschriften des Mitgliedstaats, indem er ansässig ist, angemessene Sicherheitsmaßnahmen trifft und personenbezogene Daten nur entsprechend den Anweisungen des für die Verarbeitung Verantwortlichen verarbeitet.

26. Es sollte, entsprechend den nationalen Rechtsvorschriften, eine Meldung an die zuständige Kontrollstelle erfolgen (wenn der für die Website Verantwortliche in der Europäischen Union niedergelassen ist oder dort keine Niederlassung, aber einen Vertreter hat). Es wäre sinnvoll, wenn das Aktenzeichen der Meldung auf der Website in der Rubrik angegeben würde, die die Informationen zum Datenschutz enthält.

27. Wenn Daten in ein Drittland übermittelt werden, in dem kein angemessener Datenschutz gewährleistet ist, sollte sichergestellt werden, dass die Übermittlung nur dann erfolgt, wenn sie unter eine der Ausnahmeregelungen des Artikels 26 der Richtlinie 95/46/EG fällt. In diesem Fall ist die betroffene Person davon zu unterrichten, dass angemessene Garantien für die Rechtmäßigkeit der Übermittlung gegeben wurden.

4. Erhebung von Adressen zum Zwecke der Direktwerbung per E-Mail und der Übersendung von Informationsschreiben

28. Direktwerbung per E-Mail:

- Die Datenschutzgruppe bekräftigt ihre Auffassung, dass E-Mail-Adressen, die im öffentlichen Bereich des Internet, beispielsweise in Newsgroups, erhoben wurden, ohne dass die betroffenen Personen davon Kenntnis hatten und sich dazu äußern konnten, als nicht rechtmäßig erhoben zu betrachten sind. Diese Adressen dürfen deshalb für keinen anderen Zweck benutzt werden als für den Zweck, zu dem sie veröffentlicht wurden, insbesondere nicht für die Zwecke der Direktwerbung[12].

- E-Mail-Adressen dürfen für Direktwerbung nur dann benutzt werden, wenn die Adressen nach Treu und Glauben und rechtmäßig erhoben wurden. Eine Erhebung in diesem Sinne setzt voraus, dass die Betroffenen von einer etwaigen Nutzung ihrer Daten zu Zwecken der kommerziellen Direktwerbung in Kenntnis gesetzt wurden und ihnen die Möglichkeit gegeben wurde, ihre Einwilligung zu einer solchen Nutzung zu geben, und zwar zum Zeitpunkt der Datenerhebung (Ankreuzfeld auf dem Bildschirm). Die Übermittlung von Werbe-E-Mails unter diesen Voraussetzungen muss auch mit der Möglichkeit verknüpft werden, sich online von der Liste der verwendeten E-Mail-Adressen streichen zu lassen[13].

29. Übermittlung von Informationsschreiben

- Es sollte jeweils sichergestellt werden, dass die Betroffenen vor der Übersendung eines Informationsschreibens ihre Einwilligung gegeben haben und dass sie jederzeit das betreffende Abonnement wirksam kündigen können. Um letzteres zu gewährleisten, müssen die Betroffenen bei jeder Übersendung einen diesbezüglichen Hinweis erhalten.

Die Datenschutzgruppe fordert den Rat, die Europäische Kommission, das Europäische Parlament und die Mitgliedstaaten auf, dieser Empfehlung Rechnung zu tragen.

Die Gruppe behält sich weitere Äußerungen zu diesem Thema vor.

---

12 Siehe WP 28 (5007/00): „Stellungnahme 1/2000 zu bestimmten Datenschutzaspekten des elektronischen Geschäftsverkehrs“, angenommen am 3.2.2000; WP 29 (5009/00) „Stellungnahme 2/2000 zur allgemeinen Neugestaltung des Rechtsrahmens für den Telekommunikationssektor“, angenommen am 3.2.2000, und insbesondere im Hinblick auf die Anwendung der Artikel 6 und 7 der Richtlinie 95/46/EG; WP 36 (5042/00): “Stellungnahme 7/2000 zum Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2000 - KOM (2000) 385”, angenommen am 2.11.2000, und WP 37 (5063/00): “Privatsphäre im Internet - Ein integrierter EU-Ansatz zum Online-Datenschutz”, angenommen am 21.11.2000.

13 Weitere Anforderungen im Zusammenhang mit nicht angeforderter kommerzieller Kommunikation in den Fällen, in denen ein Opt-out aufgrund der Richtlinie 97/66/EG möglich ist, sind in der Richtlinie zum elektronischen Geschäftsverkehr enthalten.

Geschehen zu Brüssel am 21. Mai 2001

Für die Datenschutzgruppe

Der Vorsitzende

Stefano RODOTA