

Nichtamtliche Übersetzung

**EUROPARAT
MINISTERKOMITEE**

EMPFEHLUNG NR. R (99) 5

**DES MINISTERKOMITEES AN DIE MITGLIEDSTAATEN
ÜBER DEN SCHUTZ DES PRIVATLEBENS IM INTERNET**

**LEITLINIEN ZUM PERSONENSCHUTZ IM HINBLICK AUF DIE ERHEBUNG UND
VERARBEITUNG VON PERSONENDATEN AUF DEN "DATENAUTOBAHNEN"**

*(genehmigt vom Ministerkomitee, am 23. Februar 1999,
anlässlich der 660. Sitzung der Ministerdelegierten)*

Präambel

Das Ministerkomitee, gestützt auf Artikel 15.b der Satzung des Europarates,

In Erwägung, dass es das Ziel des Europarates ist, eine engere Verbindung zwischen seinen Mitgliedern herzustellen;

In Anbetracht der Entwicklung neuer Technologien und neuer Kommunikations- und Online-Informationendienste;

Bewusst, dass diese Entwicklung das Funktionieren der Gesellschaft allgemein und die Beziehungen zwischen den Menschen beeinflussen wird, insbesondere durch die erweiterten Möglichkeiten der Kommunikation und des Informationsaustauschs auf nationaler und internationaler Ebene;

Bewusst der Vorteile, welche die Benutzer der neuen Technologien aus dieser Entwicklung ziehen können;

In der Meinung, dass die technologische Entwicklung und die breite Anwendung der Erhebung und Verarbeitung von Personendaten auf den "Datenautobahnen" Risiken für das Privatleben der Menschen mit sich bringt;

In der Meinung, dass die technologische Entwicklung auch erlaubt, zur Achtung der Grundrechte und Grundfreiheiten beizutragen, insbesondere des Privatlebens bei der Verarbeitung von Personendaten natürlicher Personen;

Bewusst, dass Techniken entwickelt werden müssen, welche die Anonymität der betroffenen Personen und die Vertraulichkeit der auf den "Datenautobahnen" ausgetauschten Daten garantieren und zugleich die Achtung der Rechte und Grundfreiheiten anderer und der Werte einer demokratischen Gesellschaft schützen;

Bewusst, dass auch die Kommunikation mit Hilfe der neuen Informationstechnologien der Achtung der Menschenrechte und Grundfreiheiten untersteht, insbesondere der Achtung des Privatlebens und des Briefgeheimnisses, wie sie in Artikel 8 der Europäischen Menschenrechtskonvention garantiert werden;

Anerkennend, dass Erhebung, Verarbeitung und insbesondere Bekanntgabe von Personendaten über neue Informationstechnologien, insbesondere über die "Datenautobahnen", erfasst sind von den Bestimmungen des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Strassburg, 1981, Reihe Europäischer Staatsverträge Nr. 108) sowie den sektoriellen Empfehlungen zum Datenschutz, insbesondere der Empfehlung Nr. R (90) 19 zum Schutz personenbezogener Daten für Zahlungszwecke und andere verwandte Operationen, der Empfehlung Nr. R (91) 10 über die Bekanntgabe von personenbezogenen Daten im Besitze öffentlicher Stellen an Dritte und der Empfehlung Nr. R (95) 4 zum Schutz personenbezogener Daten im Bereich der Fernmeldedienste, namentlich im Hinblick auf die Telefondienste;

In der Meinung, dass die Benutzer und die Anbieter von Internetdiensten für die Umsetzung der allgemeinen Be-

stimmungen des weiter oben erwähnten Übereinkommens im Hinblick auf die Erhebung und Verarbeitung von Personendaten auf den "Datenautobahnen" sensibilisiert werden müssen,

Empfiehl den Regierungen der Mitgliedstaaten, die Leitlinien im Anhang zu dieser Empfehlung zu verbreiten, insbesondere an die Benutzer und die Anbieter von Internetdiensten, sowie an alle nationalen Behörden, die mit der Überwachung der Einhaltung der Datenschutzbestimmungen beauftragt sind.

Anhang zu Empfehlung Nr. R (99) 5 des Ministerkomitees
an die Mitgliedstaaten über den Schutz des Privatlebens im Internet

Leitlinien zum Personenschutz im Hinblick auf die Erhebung und Verarbeitung von Personendaten auf den "Datenautobahnen", die in Verhaltenskodizes integriert oder ihnen beigefügt werden können

I. Einführung

Diese Leitlinien nennen die Grundsätze für ein loyales Verhalten der Benutzer und der Anbieter von Internetdiensten ^{Fussnote 1} betreffend den Schutz des Privatlebens. Diese Grundsätze können in Verhaltenskodizes aufgenommen werden.

Die Benutzer sollten sich der Verantwortlichkeiten der Anbieter von Internetdiensten bewusst sein und umgekehrt. Deshalb wird den Benutzern und den Anbietern von Internetdiensten empfohlen, diesen Text vollständig zu lesen, auch wenn er zur einfachen Benutzung in verschiedene Abschnitte gegliedert ist. Es ist möglich, dass Sie von einem oder gleichzeitig von mehreren Abschnitten dieses Textes betroffen sind.

Mit der Benutzung des Internets sind Verantwortung für jede einzelne Handlung und Risiken für das Privatleben verbunden. Das Verhalten sollte darauf ausgerichtet sein, sich selber zu schützen und gute Beziehungen mit anderen zu fördern. Diese Leitlinien nennen einige praktische Lösungen zum Schutz des Privatlebens, entbinden jedoch nicht davon, die eigenen Rechte und Pflichten zu kennen.

Denken Sie daran, dass die Achtung des Privatlebens ein Grundrecht jedes Menschen ist, das zudem durch Datenschutzgesetze geschützt werden kann. Überprüfen Sie auf alle Fälle Ihre rechtliche Situation.

II. Für die Benutzer

1. Denken Sie daran, dass das Internet nicht sicher ist. Es gibt indes bereits verschiedene Mittel, andere werden noch entwickelt, mit denen Sie den Schutz Ihrer Daten ^{Fussnote 2} verbessern können. Nutzen Sie deshalb jedes verfügbare Mittel, um Ihre Daten und Mitteilungen zu schützen, zum Beispiel die gesetzeskonform verfügbare Verschlüsselung der vertraulichen elektronischen Post sowie Zugriffsschlüssel für Ihren PC ^{Fussnote 3}.

2. Denken Sie daran, dass jede ausgeführte Transaktion, jeder Besuch einer Internetsite Spuren hinterlässt. Mit diesen "elektronischen Spuren" kann ohne Ihr Wissen ein Profil Ihrer Person und Ihrer Interessen erstellt werden. Wenn Sie dies nicht wollen, empfehlen wir Ihnen, die neuesten technischen Mittel zu nutzen, womit Sie jedes Mal, wenn Sie Spuren hinterlassen, informiert werden und die Aufzeichnung dieser Spuren ablehnen können. Sie können auch Auskunft verlangen über die von den jeweiligen Programmen und Sites zum Schutz des Privatlebens festgehaltenen Regeln, und sich für diejenigen entscheiden, die wenige Daten registrieren oder anonym zugänglich sind.

3. Anonym zugängliche und nutzbare Dienste und Zahlungsmethoden schützen das Privatleben am besten. Informieren Sie sich über die technischen Möglichkeiten der Wahrung Ihrer Anonymität, wo dies geeignet ist ^{Fussnote 4}.

4. Absolute Anonymität kann aus Gründen gesetzlicher Einschränkungen nicht angemessen sein. Erlaubt es das Gesetz, können Sie in diesem Fall jedoch ein Pseudonym verwenden, so dass nur Ihr Anbieter von Internetdiensten Ihre wahre Identität kennt.

5. Geben Sie Ihrem Anbieter von Internetdiensten und jeder anderen Person nur die Daten an, die für den bestimmten Zweck, der Ihnen genannt wurde, notwendig sind. Seien Sie besonders vorsichtig mit Kreditkarten- und Kontonummern, die im Rahmen des Internets sehr leicht – missbräuchlich – verwendet werden können.

6. Denken Sie daran, dass Ihre elektronische Adresse eine persönliche Angabe ist, welche andere möglicherweise zu verschiedenen Zwecken wie die Aufnahme in Verzeichnisse oder Benutzerlisten benutzen wollen. Zögern Sie nicht, nach dem Zweck dieser Verzeichnisse oder anderer solcher Verwendungen zu fragen. Sie können verlangen, dass Ihre Adresse gelöscht wird, wenn Sie nicht in diesen Verzeichnissen oder Listen aufgeführt sein wollen.

7. Seien Sie vorsichtig bei Sites, die mehr als die für den Zugang zur Site oder eine Transaktion erforderlichen Daten verlangen oder nicht angeben, warum sie alle diese Daten von Ihnen benötigen.

8. Denken Sie daran, dass Sie für die Datenverarbeitung rechtlich verantwortlich sind, zum Beispiel wenn Sie illegal Daten hinauf- oder herunterladen, und dass man Sie identifizieren kann, auch wenn Sie ein Pseudonym verwenden.

9. Senden Sie keine boshaften Mitteilungen; dies könnte sich gegen Sie kehren und rechtliche Folgen haben.

10. Ihr Anbieter von Internetdiensten ist für die korrekte Datenverwendung verantwortlich. Fragen Sie ihn, welche Daten er wie und zu welchen Zwecken erhebt, verarbeitet und aufbewahrt. Wiederholen Sie diese Frage von Zeit zu Zeit. Fordern Sie, dass er die Daten berichtigt, wenn sie ungenau sind, oder sie löscht, wenn sie in übertriebenem Ausmass vorhanden, nicht mehr aktuell oder nicht mehr nötig sind. Verlangen Sie, dass er die Änderung an alle Parteien weitergibt, denen er Ihre Daten ^{Fussnote 5} mitgeteilt hat.

11. Falls Sie mit der Art, wie Ihr Anbieter von Internetdiensten Ihre Daten erhebt, verarbeitet, aufbewahrt oder mitteilt, nicht zufrieden sind und wenn er sich weigert, sein Vorgehen zu ändern, überlegen Sie sich einen Wechsel des Anbieters. Sind Sie der Ansicht, dass Ihr Anbieter von Internetdiensten die Datenschutzvorschriften nicht einhält, können Sie die zuständigen Behörden damit befassen oder gerichtlich vorgehen.

12. Informieren Sie sich über die Risiken für das Privatleben und die Sicherheit im Internet sowie die verfügbaren Mittel zur Verringerung dieser Risiken.

13. Falls Sie Daten in ein anderes Land schicken wollen, müssen Sie sich bewusst sein, dass diese Daten dort möglicherweise weniger geschützt sind. Handelt es sich um Ihre eigenen Daten, sind Sie natürlich frei, sie trotzdem zu übermitteln. Bevor Sie jedoch Daten anderer Personen in ein anderes Land schicken, informieren Sie sich zum Beispiel bei Ihren Behörden, ob diese Übermittlung ^{Fussnote 6} zulässig ist. Gegebenenfalls müssen Sie vom Datenempfänger fordern, dass er um die unerlässlichen Vorkehrungen ^{Fussnote 7} für die Sicherstellung des Datenschutzes besorgt ist.

III. Für die Anbieter von Internetdiensten

1. Wenden Sie – die vorzugsweise zertifizierten – Verfahren und verfügbaren Technologien an, um den Schutz des Privatlebens der betroffenen Personen (auch wenn sie nicht Internetbenutzer sind) und insbesondere die Integrität und die Vertraulichkeit der Daten sowie die physische und logische Sicherheit des Netzes und der im Netz angebotenen Dienste zu gewährleisten.

2. Informieren Sie die Benutzer, bevor sie sich anmelden oder die Dienste zu benutzen beginnen, über die Risiken, welche die Benutzung des Internets für das Privatleben beinhaltet. Es kann sich um Risiken bezüglich der Integrität oder Vertraulichkeit der Daten, der Sicherheit des Netzes oder anderer mit dem Privatleben verbundener Risiken handeln, wie der Erhebung oder Registrierung von Daten ohne Wissen der Benutzer.

3. Informieren Sie die Benutzer über die erlaubten technischen Mittel wie die Verschlüsselung und die gesetzlich verfügbaren elektronischen Unterschriften, um die Risiken bezüglich Sicherheit der Daten und der Mitteilungen zu verringern. Bieten Sie diese technischen Mittel zu einem Preis an, der kostenorientiert und nicht abschreckend ist.

4. Bevor Sie Abonnemente annehmen und Benutzer mit dem Internet verbinden, informieren Sie sie über anonyme Möglichkeiten, die Dienste zu benutzen und zu bezahlen (zum Beispiel mit Prepaid-Zugangskarten). Absolute Anonymität kann aus Gründen gesetzlicher Einschränkungen nicht angemessen sein. Bieten Sie in diesem Fall die Möglichkeit an, Pseudonyme zu verwenden, wenn das Gesetz es erlaubt. Informieren Sie die Benutzer über Programme, die anonymes Suchen und Surfen im Internet ermöglichen. Bauen Sie Ihr System so auf, dass die Verwendung von Personendaten vermieden oder doch auf das unerlässliche Minimum beschränkt wird.

5. Lesen, ändern oder löschen Sie keine an andere gesandten Mitteilungen.
6. Lassen Sie keinerlei Einmischung in den Inhalt der Mitteilungen zu, ausser dies sei gesetzlich vorgesehen und werde von einer öffentlichen Behörde vorgenommen.
7. Erheben, verarbeiten und bewahren Sie die Daten der Benutzer nur auf, wenn dies für eindeutige, genau angegebene und zulässige Zwecke unbedingt erforderlich ist.
8. Geben Sie keine Daten an Drittpersonen weiter, ausser die Weitergabe sei gesetzlich vorgesehen ^{Fussnote 8}.
9. Bewahren Sie Daten nicht länger auf, als es für den Zweck der Verarbeitung ^{Fussnote 9} unbedingt erforderlich ist.
10. Verwenden Sie Daten nur dann zu Promotions- oder Marketingzwecken Ihrer eigenen Dienste, wenn die Person, nachdem sie informiert wurde, keine Einwände erhoben hat, oder, soweit es um die Verarbeitung von Verkehrs- oder sensiblen Daten geht, ausdrücklich zugestimmt hat.
11. Sie sind verantwortlich für die korrekte Verwendung der Daten. Geben Sie auf Ihrer Homepage klar und deutlich ersichtlich Ihre Politik betreffend den Schutz des Privatlebens an. Dieser Hinweis sollte mit einem „Hypertext-Link“ zu einer detaillierten Erläuterung Ihrer Praxis in Bezug auf den Schutz des Privatlebens führen. Informieren Sie den Benutzer, bevor er die Dienste zu benutzen beginnt, wenn er Ihre Site besucht und jedesmal, wenn er hierum er sucht, über Ihre Identität und darüber, welche Daten Sie erheben, verarbeiten und aufbewahren und wie, wofür und wie lange Sie sie aufbewahren. Verlangen Sie erforderlichenfalls seine Einwilligung. Berichtigen Sie falsche Daten auf Verlangen der betroffenen Person unverzüglich, löschen Sie sie, wenn sie in übertriebenem Ausmass vorhanden, nicht mehr aktuell oder nicht mehr nötig sind, und beenden Sie die Verarbeitung der Daten, wenn der Benutzer Einwände erhebt. Teilen Sie Drittpersonen, denen Sie die Daten weitergegeben haben, jede Änderung mit. Vermeiden Sie jede Erhebung von Daten, die ohne Wissen der betroffenen Person geschieht.
12. Die Information an den Benutzer muss korrekt und aktuell sein.
13. Überlegen Sie zweimal, bevor Sie Daten auf Ihrer Site veröffentlichen! Eine solche Veröffentlichung könnte das Privatleben anderer Menschen beeinträchtigen und überdies gesetzlich verboten sein.
14. Bevor Sie Daten in ein anderes Land schicken, informieren Sie sich zum Beispiel bei Ihren Behörden über die Zulässigkeit der Übermittlung ^{Fussnote 10}. Gegebenenfalls müssen Sie vom Datenempfänger fordern, dass er für die zur Sicherstellung des Datenschutzes unerlässlichen Vorkehren ^{Fussnote 11} besorgt ist.

IV. Klärung und Hilfe

1. Wo in diesem Text der Begriff "Anbieter von Internetdiensten" verwendet wird, ist er gegebenenfalls auch auf andere Akteure im Internet anwendbar, wie die Zugangs-, Inhalts- und Netz-Anbieter, die Hersteller von Navigationssoftware, die Koordinatoren von Foren oder "Info-Kiosken" usw.
2. Es ist wichtig, dass Sie sich der Achtung Ihrer Rechte versichern. Die Feedback-Mechanismen, welche die Internet-Foren, die Verbände der Anbieter von Internetdiensten, die Datenschutzbehörden oder andere Instanzen anbieten, sind wichtige Mittel, um die Beachtung dieser Leitlinien sicherzustellen. Nehmen Sie mit ihnen Kontakt auf, wenn Sie Klärung oder Hilfe brauchen.
3. Diese Leitlinien sind auf jede Art von "Datenautobahn" anwendbar.

1 Siehe Teil IV, Abschnitt 1.

2 Der Begriff "Daten" bezieht sich auf Personendaten und bedeutet jede Information, die Sie selbst oder andere Personen betrifft.

3 Verwenden Sie zum Beispiel Passwörter und wechseln Sie sie regelmässig.

4 Zum Beispiel indem Sie öffentliche Internet-Kioske oder Prepaid-Zugangskarten und Zahlungskarten benutzen.

5 Die Datenschutzgesetze ebenso wie Artikel 5 des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten machen den Datenverarbeiter für die Korrektheit und Aktualisierung der Daten verantwortlich.

6 Die Gesetzgebung zahlreicher Länder Europas verbietet die Weitergabe in Länder, die kein gleichwertiges Datenschutzniveau wie Ihr Land aufweisen. Allerdings sind Ausnahmen vorgesehen, insbesondere wenn die betroffene Person sich einverstanden erklärt hat.

7 Diese Vorkehrungen können insbesondere in einem Vertrag über den grenzüberschreitenden Datenverkehr entwickelt und/oder aufgeführt werden.

8 Im Allgemeinen erlauben Datenschutzgesetze unter bestimmten Bedingungen die Bekanntgabe folgender Daten an Drittpersonen, insbesondere:

- von sensiblen und der Verkehrsdaten, vorausgesetzt, dass die betroffene Person ausdrücklich eingewilligt hat;

- von anderen Daten, wenn die Bekanntgabe nötig ist, um einen zulässigen Zweck zu erfüllen, oder wenn die betroffene Person, nachdem sie informiert wurde, keine Einwände erhoben hat.

9 Bewahren Sie zum Beispiel die Rechnungsdaten nicht auf, ausser wenn dies gesetzlich vorgesehen ist.

10 Siehe Fussnote 6.

11 Siehe Fussnote 7.