

## **EUROPARAT MINISTERKOMITEE**

### **EMPFEHLUNG Rec (2002) 9**

#### **DES MINISTERKOMITEES AN DIE MITGLIEDSTAATEN ÜBER DEN SCHUTZ VON ZU VERSICHERUNGSZWECKEN ERHOBENEN UND VERARBEITETEN PERSONENBEZOGENEN DATEN**

*(angenommen vom Ministerkomitee am 18. September 2002  
anlässlich der 808. Sitzung der Ministerdelegierten)*

#### Präambel

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

1. In Erwägung, dass es das Ziel des Europarates ist, eine engere Verbindung zwischen seinen Mitgliedern zu schaffen;
2. Die allgemeinen Grundsätze betreffend den Datenschutz in Erinnerung rufend, wie sie im Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (STE Nr. 108) niedergelegt sind, namentlich in Artikel 6, der bestimmt, dass sensible personenbezogene Daten nicht verarbeitet werden dürfen, ausser das innerstaatliche Recht gewährleiste einen geeigneten Schutz;
3. Im Bewusstsein, dass die automatisierte Verarbeitung von personenbezogenen Daten zu Versicherungszwecken immer mehr verbreitet ist, nicht nur zum Zweck der Vorbereitung, des Abschlusses, der Inkraftsetzung und der Aufhebung der Versicherung, sondern auch zum Zweck einer zweckmässigen und wirtschaftlichen Verwaltung der Versicherung sowie des Kampfes gegen den Versicherungsbetrug;
4. Im Bewusstsein, dass Versicherungen von einer Vielfalt von wirtschaftlichen Akteuren angeboten werden, insbesondere von Versicherungsunternehmen;
5. Überzeugt von der Bedeutung, die Qualität, Integrität und Verfügbarkeit der personenbezogenen Daten für die versicherten Personen haben;
6. Feststellend, dass fast die gesamte Bevölkerung der Mitgliedstaaten von einer oder mehreren Versicherungen betroffen ist und dass die Berufsleute der Versicherungsbranche deshalb über eine grosse Menge von personenbezogenen Daten verfügen, von denen gewisse sensibel sind;
7. Überzeugt davon, dass es wünschenswert ist, die Erhebung und Verarbeitung von personenbezogenen Daten zu Versicherungszwecken zu regeln, deren vertraulicher Charakter und die Datensicherheit zu gewährleisten und darüber zu wachen, dass bei ihrer Benutzung die Grundrechte und die

Grundfreiheiten der Einzelpersonen, namentlich ihr Recht auf Privatsphäre, geachtet werden;

8. Der Tatsache Rechnung tragend, dass die Mobilität der Einzelpersonen und die Globalisierung der Märkte und des Handels auch im Versicherungssektor den grenzüberschreitenden Austausch von Informationen notwendig machen und in allen Mitgliedstaaten des Europarates einen gleichwertigen Datenschutz erfordern,

Empfiehl den Regierungen der Mitgliedstaaten:

1. Massnahmen zu treffen, damit sich die im Anhang dieser Empfehlung enthaltenen Grundsätze in ihrem Recht und ihrer Praxis niederschlagen;
2. sicherzustellen, dass die im Anhang zu dieser Empfehlung enthaltenen Grundsätze bei den Personen, den Behörden und den öffentlichen oder privaten Organisationen, die personenbezogene Daten zu Versicherungszwecken erheben und verarbeiten, sowie bei den für den Datenschutz zuständigen Instanzen weite Verbreitung finden;
3. die Annahme und Inkraftsetzung der im Anhang zu dieser Empfehlung aufgeführten Grundsätze und Richtlinien zu fördern, namentlich indem gesetzliche Bestimmungen angenommen oder das Erstellen ethischer Richtlinien unterstützt werden.

### **Anhang zur Empfehlung Rec (2002) 9**

#### 1. Definitionen

In dieser Empfehlung bedeuten die Ausdrücke:

- a. "Personenbezogene Daten": jede Information, die eine bestimmte oder bestimmbar natürliche Person betrifft (betroffene Person). Eine natürliche Person wird nicht als „bestimmbar“ angesehen, wenn diese Bestimmung einen ausserordentlich hohen Aufwand an Zeit und Arbeit erfordert.
- b. "Sensible Daten": personenbezogene Daten, welche über die rassische Herkunft, politische Meinungen, religiöse oder andere Überzeugungen Auskunft geben, sowie personenbezogene Daten in bezug auf Gesundheit und Geschlechtsleben. Sind ebenfalls sensible Daten über Strafverfolgungen und strafrechtliche Verurteilungen sowie andere vom innerstaatlichen Recht als sensible bezeichnete Daten.
- c. "Zu Versicherungszwecken": alle Handlungen der Erhebung oder Verarbeitung von personenbezogenen Daten in Zusammenhang mit der Abdeckung eines Risikos, namentlich auf Grund eines Vertrages oder einer Versicherungspolice.
- d. "Verarbeitung": jede Handlung oder Gesamtheit von Handlungen, die teilweise oder ganz unterstützt von automatischen Verfahren ausgeführt und auf personenbezogene Daten angewendet wird, wie Registrierung, Aufbewahrung, oder Veränderung, Auszug, Einsicht, Verwendung, Bekanntgabe, Vergleich oder Verbindung sowie Löschung oder Vernichtung.

e. "Bekanntgabe": die Handlung, die zum Zugang für Dritte zu personenbezogenen Daten führt, unabhängig von Mitteln oder Geräten, die dazu verwendet werden.

f. "Verarbeitungsverantwortlicher": natürliche oder juristische Person, öffentliche Behörde, Institution oder jede andere Stelle, die allein oder in Zusammenarbeit mit anderen, Ziele und Mittel der Erhebung und der Verarbeitung von personenbezogenen Daten festlegt.

g. „Auftragsverarbeiter“: natürliche oder juristische Person, öffentliche Behörde, Institution oder jede andere Stelle, die personenbezogene Daten im Auftrag des Verarbeitungsverantwortlichen verarbeitet.

## 2. Geltungsbereich

2.1. Diese Empfehlung gilt für die Erhebung und die automatische Verarbeitung von personenbezogenen Daten für Versicherungszwecke. Sie gilt nicht für die Erhebung und die Verarbeitung von personenbezogenen Daten, die für Zwecke der sozialen Sicherheit verwendet werden.

2.2. Die Mitgliedstaaten werden angeregt, den Geltungsbereich dieser Empfehlung auf die nicht automatische Verarbeitung von personenbezogenen Daten für Versicherungszwecke auszudehnen.

2.3. Es dürfte keine Verarbeitung von personenbezogenen Daten auf nicht automatische Weise durchgeführt werden, um die Bestimmungen dieser Empfehlung zu umgehen.

2.4. Die Mitgliedstaaten können den Geltungsbereich der in dieser Empfehlung erwähnten Grundsätze auch auf die Erhebung und Verarbeitung von Daten erweitern, die Personengruppen, Vereine, Stiftungen, Gesellschaften, Korporationen oder jede andere Institution betreffen, die direkt oder indirekt natürliche Personen versammelt und Rechtspersönlichkeit hat oder nicht hat.

2.5. Die Mitgliedstaaten können die Grundsätze dieser Empfehlung auf den Schutz von personenbezogenen Daten ausdehnen, die für Zwecke der sozialen Sicherheit verwendet werden.

## 3. Achtung der Privatsphäre

3.1. Die Achtung der Rechte und Grundfreiheiten, insbesondere des Rechts auf einen Persönlichkeitsbereich, muss bei der Erhebung und Verarbeitung von personenbezogenen Daten für Versicherungszwecke gewährleistet werden.

3.2. Das innerstaatliche Recht und die interne Praxis müssen Personen, die in Zusammenhang mit einer Tätigkeit im Versicherungsbereich Kenntnis von personenbezogenen Daten erlangen, Vorschriften bezüglich der Vertraulichkeit unterstellen. Die Erhebung und Verarbeitung medizinischer Daten dürfen zudem nur von Berufsleuten des Gesundheitswesens vorgenommen werden oder nur unter Einhaltung der Vertraulichkeitsvorschriften, die mit denjenigen des Berufspersonals des Gesundheitswesens vergleichbar sind, oder mit gleichen Wirksamkeitsgarantien, die das innerstaatliche Recht vorsieht.

#### 4. Erhebung und Verarbeitung von personenbezogenen Daten für Versicherungszwecke

##### *Wesentliche Voraussetzungen für die Erhebung und Verarbeitung personenbezogener Daten*

4.1. Die Erhebung und Verarbeitung (einschliesslich der Bekanntgabe) personenbezogener Daten sollte nach Treu und Glauben und unter Beachtung der Rechtmässigkeit sowie zu bestimmten und rechtmässigen Zwecken erfolgen.

Die personbezogenen Daten sollten:

- den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein und nicht darüber hinausgehen;
- sachlich richtig und wenn nötig auf den neuesten Stand gebracht sein.

##### *Herkunft der personenbezogenen Daten*

4.2. Personenbezogene Daten, die zu Versicherungszwecken erhoben und verarbeitet werden, sollten grundsätzlich bei der betroffenen Person oder ihrem gesetzlichen Vertreter erhoben werden.

##### *Rechtmässigkeit*

4.3. Personenbezogene Daten können zu Versicherungszwecken erhoben und verarbeitet werden:

- a. wenn es das Gesetz vorsieht;
- b. im Hinblick auf die Erfüllung eines Versicherungsvertrages, bei dem die betroffene Person Partei ist, oder die Vorbereitung eines solchen Vertrages auf Antrag der betroffenen Person;
- c. wenn die betroffene Person oder ihr gesetzlicher Vertreter oder eine Behörde oder eine vom Gesetz vorgesehene Person oder Instanz im Sinne von Kapitel 6 eingewilligt hat;
- d. wenn die Daten für die Verfolgung des berechtigten Interesses des Verantwortlichen notwendig sind, vorausgesetzt, dass das Interesse der betroffenen Person nicht überwiegt.

##### *Zweck*

4.4. Unter Vorbehalt der Bestimmungen der Grundsätze 4.6 - 4.8, 8.1 und 13.1 dürfen personenbezogene Daten nur zu folgenden Zwecken erhoben und verarbeitet werden:

- a. Vorbereitung und Abschluss einer Versicherung;
- b. Prämienforderung und andere Rechnungstellungen;
- c. Regelung von Entschädigungsansprüchen und andere Leistungen;
- d. Rückversicherung;
- e. Mitversicherung;

- f. Verhütung, Aufdeckung und/oder Strafverfahren im Falle eines Versicherungsbetrugs;
- g. Feststellung, Geltendmachung oder Verteidigung eines rechtlichen Anspruchs;
- h. Erfüllen einer anderen spezifischen gesetzlichen oder vertraglichen Pflicht;
- i. Erschliessung neuer Versicherungsmärkte;
- j. interne Verwaltung;
- k. versicherungsmathematische Aktivitäten.

Diese Daten dürfen nachträglich nicht zu Zwecken verarbeitet werden, die mit dem ursprünglichen Zweck der Erhebung nicht vereinbar sind.

#### *Ungeborene Kinder*

4.5. Personenbezogene Daten über ein ungeborenes Kind sollten den gleichen Schutz geniessen wie die personenbezogenen Daten eines Minderjährigen.

Wenn das innerstaatliche Recht nichts anderes vorsieht, kann der Inhaber der elterlichen Gewalt als juristisch befugte Person für ein ungeborenes Kind handeln.

#### *Sensible Daten*

4.6. Die Erhebung und Verarbeitung von sensiblen Daten sollte verboten sein, ausser zu einem der in den Grundsätzen 4.4, 4.8, 8.1 und 13.1 erwähnten Zwecken:

- a. wenn die betroffene Person oder ihr gesetzlicher Vertreter oder eine Behörde oder eine andere vom Gesetz bestimmte Person oder Instanz im Sinne vom Kapitel 6 ausdrücklich eingewilligt hat; oder
- b. wenn das Gesetz es erlaubt und
  - i. unter Vorbehalt angemessener Sicherheitsmassnahmen, wenn die Verarbeitung zum Zweck der Erfüllung anderer spezifischer gesetzlicher oder vertraglicher Pflichten des Verantwortlichen notwendig ist; oder
  - ii. wenn die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht notwendig ist; oder
  - iii. wenn die Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person oder eines Dritten notwendig ist, sofern die Person aus physischen oder rechtlichen Gründen ausserstande ist, ihre Einwilligung zu geben;
- c. wenn die Erhebung und Verarbeitung unter Vorbehalt angemessener Garantien aus Gründen eines wichtigen öffentlichen Interesses aufgrund eines Gesetz oder eines Beschlusses einer Behörde im Sinne von Grundsatz 15.1. vorgesehen ist.

## *Strafrechtliche Daten*

4.7. In Abweichung vom Grundsatz 4.6 kann die Erhebung und Verarbeitung von personenbezogenen Daten über Strafverfolgungen und strafrechtliche Verurteilungen zu Versicherungszwecken nur erfolgen, wenn das innerstaatliche Recht angemessene und spezifische Garantien vorsieht und wenn die Daten notwendig sind, um den Versicherungsbetrug zu bekämpfen, um Versicherungsschutz zu gewähren oder um eine Entschädigung oder eine andere Leistung auszus zahlen.

## *Direct Marketing*

4.8. Vorausgesetzt, dass die betroffene Person informiert wurde und nicht widersprochen hat, kann der Verantwortliche die zu Versicherungszwecken erhobenen und registrierten Daten zum Zweck der Vermarktung und Anpreisung seiner Dienstleistungspalette benutzen. Betrifft die Verarbeitung indessen sensible Daten, ist, soweit das innerstaatliche Recht nicht dagegen spricht, die ausdrückliche Einwilligung der betroffenen Person notwendig.

Die betroffene Person sollte darüber informiert werden, dass die Tatsache, dass sie ihre Einwilligung verweigert oder der Benutzung ihrer Daten zum Zweck der Vermarktung und Anpreisung widerspricht, den Entscheid, ob ihr Versicherungsschutz gewährt wird oder ob sie auf Grund einer bereits gewährten Versicherung Deckung erhält, nicht beeinflussen wird.

## 5. Information der betroffenen Person

5.1. Die betroffenen Personen sollten über folgende Elemente informiert werden:

- a. den Zweck oder die Zwecke, für die die Daten jetzt oder später verarbeitet werden;
- b. die Identität des Verantwortlichen;
- c. jede andere Information, die notwendig ist, um bei der Erhebung Treu und Glauben zu wahren, wie:
  - die Kategorien der erhobenen oder zu erhebenden Daten;
  - die Kategorien von Personen oder Organisationen, denen die Daten bekanntgegeben werden können und der Zweck dieser Bekanntgabe;
  - die Möglichkeit, dass die betroffenen Personen ihre Einwilligung allenfalls verweigern oder widerrufen können, sowie die Folgen eines solchen Widerrufs;
  - die Bedingungen für die Ausübung des Auskunfts- und Berichtigungsrechts;
  - die Personen oder Organisation, bei denen die Daten jetzt oder in Zukunft erhoben werden;

- den obligatorischen oder fakultativen Charakter der Antwort auf die Fragen, die Gegenstand der Erhebung sind, und die Folgen einer fehlerhaften Antwort für die Person;

5.2. Wenn die Daten bei der betroffenen Person erhoben werden, informiert der Verantwortliche diese spätestens zum Zeitpunkt der Erhebung über die im Grundsatz 5.1 aufgelisteten Elemente, ausser die Person sei schon informiert worden.

5.3. Wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, sollte diese vom Verantwortlichen über die im Grundsatz 5.1 aufgelisteten Elemente informiert werden, sobald die Daten registriert worden sind; falls die Bekanntgabe der Daten an einen Dritten vorgesehen ist, sollte diese Information spätestens bei der ersten Bekanntgabe der Daten erfolgen.

Die Verpflichtung, die betroffene Person zu informieren, fällt dahin, wenn

- a. die betroffene Person schon informiert wurde;
- b. das Erteilen der Information sich als unmöglich erweist oder unverhältnismässigen Arbeitsaufwand bedingt;
- c. die Verarbeitung oder Bekanntgabe von Daten zu Versicherungszwecken im innerstaatlichen Recht ausdrücklich vorgesehen ist.

In den Fällen von Abschnitt *b* und *c* müssen angemessene Garantien vorgesehen sein.

5.4. Die Information der betroffenen Person muss angemessen sein und den Umständen Rechnung tragen.

5.5. Sind die betroffenen Personen handlungsunfähig und nicht in der Lage, sich frei zu äussern, und gestattet das innerstaatliche Recht ihnen nicht, in ihrem eigenen Namen zu handeln, muss die Information an diejenigen Personen abgegeben werden, die vor dem Gesetz im Interesse der betroffenen Personen handeln können.

5.6. Die Information der betroffenen Personen kann eingeschränkt werden, wenn ein Gesetz es vorsieht und eine notwendige Massnahme zur Prävention, Untersuchung oder Bekämpfung einer Straftat oder zum Schutz der Rechte und Freiheiten Dritter darstellt.

## 6. Einwilligung

6.1. Wenn die Einwilligung der betroffenen Person verlangt wird, muss diese freiwillig, spezifisch und in Kenntnis der Sachlage erfolgen. Sie muss ausserdem eindeutig und im Falle von sensiblen Daten ausdrücklich sein.

Es kann indessen Fälle geben, in denen das innerstaatliche Recht die Einwilligung nicht als genügende Grundlage für die Rechtmässigkeit der Erhebung oder der Verarbeitung anerkennt.

6.2. Wenn die personenbezogenen Daten handlungsunfähige Personen betreffen und das innerstaatliche Recht der betroffenen Person nicht erlaubt, in ihrem eigenen Namen zu handeln, ist die Einwilligung des gesetzlichen

Vertreters oder einer Behörde oder einer anderen vom Gesetz bestimmten Person oder Instanz notwendig.

6.3. Wenn gemäss Grundsatz 5.5 die nicht handlungsfähigen Personen darüber informiert worden sind, dass ihre personenbezogenen Daten erhoben und verarbeitet werden sollen, könnte ihr Wille berücksichtigt werden, wenn das innerstaatliche Recht nicht dagegen spricht.

## 7. Erhebung und Verarbeitung durch einen Auftragsverarbeiter

7.1. In Übereinstimmung mit dem innerstaatlichen Recht können die Verantwortlichen Dritte mit der Erhebung und Verarbeitung von personenbezogenen Daten zu einem bestimmten Zweck beauftragen, vorausgesetzt sie sind rechtlich befugt, diese Daten zu erheben und zu verarbeiten und der Auftragsverarbeiter verpflichtet sich, nur auf alleinige Weisung des Verantwortlichen zu handeln und die Bestimmungen des innerstaatlichen Rechts, die Kapitel 11 des Anhangs zur Empfehlung Rechtswirkung verleihen, zu beachten.

7.2. Die Verantwortlichen sollten Auftragsverarbeiter auswählen, die in Bezug auf die technischen und organisatorischen Massnahmen für die durchzuführende Verarbeitung ausreichende Gewähr bieten. Sie müssen sich vergewissern, dass die Massnahmen eingehalten werden und insbesondere dass die Verarbeitung gemäss ihren Weisungen erfolgt.

7.3. Die Erhebung und Verarbeitung von personenbezogenen Daten durch einen Auftragsverarbeiter sollte durch einen Vertrag oder einen Rechtsakt geregelt sein, der den Auftragsverarbeiter an den Verantwortlichen bindet und der namentlich festhält, dass der Auftragsverarbeiter nur im Rahmen des Auftrags, den der Verantwortliche erteilt hat, sowie der Bestimmungen des innerstaatlichen Rechts betreffend die Pflichten des Verantwortlichen handelt.

## 8. Bekanntgabe der Daten zu anderen Zwecken

8.1. Die Bekanntgabe von personenbezogenen Daten zu anderen Zwecken als den in Grundsatz 4.4 erwähnten kann nur erfolgen:

a. wenn die Bekanntgabe gesetzlich vorgesehen ist und in einer demokratischen Gesellschaft eine notwendige Massnahme zur Verhütung, Ermittlung oder Bekämpfung von Straftaten oder zur Wahrung eines anderen wichtigen öffentlichen Interesses bildet; oder

b. wenn die betroffenen Personen oder ihre rechtlichen Vertreter oder eine Behörde oder eine vom Gesetz bezeichnete Person oder Instanz in Übereinstimmung mit Kapitel 6 eingewilligt haben; oder

c. wenn die Bekanntgabe zum Zweck der Vermarktung erfolgt, vorausgesetzt die betroffene Person wurde informiert und hat nicht untersagt. Wenn die Bekanntgabe indessen sensible Daten betrifft, sollte in Übereinstimmung mit Kapitel 6 die ausdrückliche Einwilligung der betroffenen Person notwendig sein; oder

d. wenn die Daten für die Verfolgung des berechtigten Interesses des Verantwortlichen notwendig sind, vorausgesetzt, dass das Interesse der betroffenen Person nicht überwiegt. Wenn die Bekanntgabe indessen sensiblen Daten betrifft, sollte in Übereinstimmung mit Kapitel 6 die ausdrückliche Einwilligung der betroffenen Person notwendig sein.

## 9. Automatisierte Einzelentscheidungen

9.1. Versicherungsentscheide, die für die betroffene Person Rechtswirkung entfalten oder von denen sie wesentlich betroffen wird, sollten nicht einzig auf der Grundlage einer automatisierten Datenverarbeitung getroffen werden, die dazu dient, auf Grund vorher festgelegter Kriterien oder statistischer Resultate gewisse Persönlichkeitsaspekte der betroffenen Person zu bewerten.

9.2. Solche Entscheide können indessen getroffen werden, wenn sie auf Antrag der betroffenen Personen im Hinblick auf den Abschluss oder die Erfüllung eines Versicherungsvertrags erfolgen oder wenn die betroffenen Personen ihren Standpunkt geltend machen können, um ihr berechtigtes Interesse zu wahren. Solche Entscheide können ebenfalls getroffen werden, wenn sie durch ein Gesetz zugelassen werden, das Massnahmen vorsieht, die die Wahrung des berechtigten Interesses der betroffenen Person gewährleisten.

## 10. Auskunfts- und Berichtigungsrecht

10.1. Jeder Person sollte auf Anfrage die Bestätigung dafür erhalten können, dass es Verarbeitungen sie betreffender Daten gibt oder nicht gibt; sie sollte in verständlicher Form alle Daten, die sie betreffen, erhalten, ebenso wie Informationen zumindest über den Zweck der Verarbeitung, die verarbeiteten Datenkategorien, die Empfänger oder die Empfängerkategorien, denen die Daten bekanntgegeben werden, und die Herkunft der Daten. Sie sollte auch Auskunft über den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten erhalten, zumindest im Falle automatisierter Entscheidungen.

10.2. Das Auskunftsrecht der betroffenen Personen zu Daten, die sie betreffen, sollte nicht eingeschränkt werden, mit Ausnahme der Fälle, in denen es von Gesetzes wegen vorgesehen und notwendig ist

a. zur Verhütung, Ermittlung und Bekämpfung von Straftaten;

b. zur Wahrung der Rechte und Freiheiten der betroffenen Person oder Dritter.

In diesen Fällen darf die Einschränkung nur so lange andauern als der Grund dafür vorhanden ist.

10.3. Die betroffenen Personen sollten gegebenenfalls die Berichtigung, Vernichtung oder Sperre ihrer Daten verlangen können, wenn diese in Unkenntnis der Bestimmungen des innerstaatlichen Rechts, die den Grundsätzen der vorliegenden Empfehlung Rechtswirkung verleihen, erhoben oder verarbeitet wurden, namentlich wenn die Daten unrichtig, nicht zweckdienlich oder unverhältnismässig sind.

10.4. Die Gründe für eine Einschränkung des Auskunftsrechts oder des Rechts, Daten berichtigen, vernichten oder sperren zu lassen, sollten schriftlich angegeben werden. Wenn das Auskunftsrecht oder das Recht der betroffenen

Person, eine Berichtigung, Vernichtung oder Sperre der Daten zu verlangen, eingeschränkt ist, sollte diese über ihr Recht informiert sein, bei der zuständigen Behörde eine Überprüfung der Rechtmässigkeit der Verarbeitung zu verlangen.

10.5. Dritten, denen die Daten bekanntgegeben wurden, sollte eine vorgenommene Berichtigung, Vernichtung oder Sperre mitgeteilt werden, ausser in Fällen, in denen sich dies als offensichtlich unangemessen oder unmöglich erweist.

10.6. Der Verantwortliche sollte der Person, die das Auskunftsrecht ausübt, in angemessenen Zeitabständen und ohne unverhältnismässigen Zeitaufwand und unverhältnismässige Kosten die personenbezogenen Daten, die sie betreffen, sowie alle in Grundsatz 10.1. erwähnten Informationen, über die Auskunft verlangt wird, mitteilen.

## 11. Datensicherheit

11.1. Zum Schutz der personenbezogenen Daten, die in Übereinstimmung mit den Bestimmungen des innerstaatlichen Rechts, die den Grundsätzen der vorliegenden Empfehlung Rechtswirkung verleihen, verarbeitet werden, vor (zufälliger oder unbefugter) Vernichtung und zufälligem Verlust, gegen den Zugriff, die Änderung, die Bekanntgabe und jede andere Form unbefugter Verarbeitung sollten geeignete technische und organisatorische Massnahmen getroffen werden.

Diese Massnahmen sollten einen angemessenen Sicherheitsgrad gewährleisten, indem sie einerseits dem Stand der Technik und andererseits der sensiblen Natur der zu Versicherungszwecken erhobenen und verarbeiteten Daten sowie der Evaluation potentieller Risiken Rechnung tragen. Sie sollten periodisch überprüft werden.

11.2. Um namentlich die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten sowie den Schutz der betroffenen Personen sicherzustellen, sollte der Verantwortliche angemessene Massnahmen treffen, um:

- a. jede unbefugte Person daran zu hindern, auf die zur Verarbeitung der personenbezogenen Daten verwendeten Einrichtungen zuzugreifen (Zugangskontrolle);
- b. zu verhindern, dass Datenträger von einer unbefugten Person gelesen, kopiert, geändert oder entfernt werden können (Datenträgerkontrolle);
- c. die unbefugte Eingabe von Daten in das Informationssystem sowie jegliche Einsichtnahme, Änderung und unbefugte Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle);
- d. zu verhindern, dass automatisierte Verarbeitungssysteme von unbefugten Personen mittels Einrichtungen zur Datenübertragung genutzt werden können (Benutzerkontrolle);
- e. einerseits im Sinne eines selektiven Datenzugriffs und andererseits um die Sicherheit der personenbezogenen Daten sicherzustellen, dass die Verarbeitung grundsätzlich so konzipiert wird, dass eine Trennung der folgenden Elemente möglich ist:

- Identifikationsdaten und Daten über die Identität der Personen,
- administrative Daten,
- sensible Daten (Zugriffskontrolle).

*f.* zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Personen oder welche Institutionen personenbezogene Daten mittels Einrichtungen bekanntgegeben werden können (Bekanntgabekontrolle);

*g.* zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, wer zum System Zugriff hatte und welche personenbezogenen Daten zu welcher Zeit und von welcher Person ins Informationssystem eingegeben wurden (Eingabekontrolle);

*h.* zu verhindern, dass bei der Bekanntgabe personenbezogener Daten sowie beim Transport von Datenträgern Daten unbefugt gelesen, kopiert, geändert oder gelöscht werden können (Transportkontrolle);

*i.* die Daten durch das Erstellen von Sicherheitskopien zu sichern (Verfügbarkeitskontrolle).

11.3. Die Verantwortlichen müssen in Übereinstimmung mit dem innerstaatlichen Recht und unter Berücksichtigung der erheblichen Grundsätze dieser Empfehlung ein angemessenes internes Reglement erstellen.

11.4. Wenn nötig, sollten die Verantwortlichen eine unabhängige Person bezeichnen, die für die Sicherheit der Informationssysteme und den Datenschutz verantwortlich ist und auf diesem Gebiet beraten kann.

## 12. Grenzüberschreitender Datenverkehr

12.1 Die Grundsätze dieser Empfehlung gelten für den grenzüberschreitenden Verkehr personenbezogener Daten, die zu Versicherungszwecken erhoben und verarbeitet werden.

12.2. Der grenzüberschreitende Verkehr personenbezogener Daten mit einem Staat, der das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (STE Nr. 108) ratifiziert hat und über eine Gesetzgebung verfügt, die einen gleichwertigen Schutz der Daten sicherstellt, sollte keinen besonderen Bedingungen zum Schutze der Privatsphäre unterstellt werden.

12.3. Beim grenzüberschreitenden Verkehr personenbezogener Daten mit einem Staat, der das Übereinkommen nicht ratifiziert hat, aber ein angemessenes Schutzniveau sicherstellt, sollte es keine Begrenzung geben.

12.4. Soweit das innerstaatliche Recht nichts anderes vorsieht, sollte der grenzüberschreitende Verkehr personenbezogener Daten mit einem Staat, der kein angemessenes Schutzniveau sicherstellt, grundsätzlich nicht stattfinden, ausser wenn

*a.* die betroffene Person ihre Einwilligung gemäss Kapitel 6 gegeben hat oder

*b.* notwendige Massnahmen, einschliesslich solche vertraglicher Art, zur Einhaltung des innerstaatlichen Rechts, das die Grundsätze der Konvention und

dieser Empfehlung verwirklicht, getroffen wurden und die betroffene Person die Möglichkeit hat, sich der Übermittlung entgegenzustellen.

### 13. Aufbewahrung der Daten

13.1. Wenn die personenbezogenen Daten für die Erreichung der Zwecke, für die sie durch den Verantwortlichen erhoben und verarbeitet wurden, nicht mehr notwendig sind, sollten sie vernichtet werden. Dieser Grundsatz findet auch Anwendung, wenn eine Versicherungsdeckung abgelehnt wird. Wenn indessen eine Aufbewahrung für Forschung, Statistik oder andere gesetzlich vorgesehene Zwecke notwendig ist, sollten sie getrennt aufbewahrt werden, und angemessene Schutzmassnahmen sollten sicherstellen, dass ein Zugriff nur für diese Zwecke möglich ist.

13.2. Bezüglich der Dauer der Aufbewahrung der Daten sollte namentlich der Notwendigkeit Rechnung getragen werden, Daten während des Zeitraums aufzubewahren, in dem es notwendig sein könnte, sich vor Gericht zu verteidigen, eine geschäftliche Tätigkeit zu beweisen oder die Ablehnung einer Versicherungsdeckung zu begründen.

### 14. Rechtsmittel

Das innerstaatliche Recht sollte bei Verletzung der Bestimmungen des innerstaatlichen Rechts, das die Grundsätze dieser Empfehlung verwirklicht, angemessene Sanktionen und Rechtsmittel vorsehen.

### 15. Gewährleistung der Beachtung der Grundsätze

15.1. Die Mitgliedstaaten beauftragen eine oder mehrere Behörden in völliger Unabhängigkeit mit der Aufsicht über die Einhaltung der Bestimmungen des innerstaatlichen Rechts, die die Grundsätze dieser Empfehlung verwirklichen.

15.2. Folgende Informationen sollten angemessen veröffentlicht werden und jedermann zugänglich sein:

a. Name und Adresse des Verantwortlichen und gegebenenfalls seines Vertreters;

b. Zweckbestimmung(en) der Verarbeitung;

c. Kategorie(n) der betroffenen Personen und der Daten;

d. Empfänger oder Kategorien von Empfängern, denen die Daten bekanntgegeben werden könnten;

e. geplanten Datenübermittlung nach Drittländern.