Dokumentenband 2009: Zum Abschnitt Internationale Konferenz der Datenschutzbeauftragten

Entschließung der 31. Konferenz vom 4.-6. November 2009 in Madrid über Internationale Standards zum Schutz der Privatsphäre

-Übersetzung -

Berücksichtigend, dass:

- die 30. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre in Strassburg einstimmig den Beschluss über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen und die Ausarbeitung einer gemeinsamen Entschließung zur Abfassung Internationaler Richtlinien zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten fasste;
- die Konferenz die "Agencia Española de Protección de Datos" (im Folgenden: die spanische Datenschutzbehörde, d. Übers.) in ihrer Eigenschaft als Koordinatorin der 31. Internationalen Konferenz damit beauftragte, eine Arbeitsgruppe, die sich aus den interessierten Datenschutzbehörden zusammensetzen sollte, mit dem Ziel zu bilden, einen Gemeinsamen Vorschlag zur Abfassung Internationaler Standards zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten auszuarbeiten;
- die spanische Datenschutzbehörde gemäß diesem Auftrag eine Arbeitsgruppe bildete und die Arbeiten zur Erstellung eines Gemeinsamen Vorschlags für die Abfassung Internationaler Standards zum Schutz der Privatsphäre und der personenbezogenen Daten förderte und koordinierte;
- die Arbeitsgruppe den Gemeinsamen Vorschlag zur Abfassung Internationaler Standards zum Schutz der Privatsphäre und der personenbezogenen Daten insbesondere auf der Grundlage der Gemeinsamkeiten verschiedener juristischer Texte, Standards und Empfehlungen mit internationaler Reichweite, die in unterschiedlichen geografischen, wirtschaftlichen oder rechtlichen Anwendungsgebieten auf einen breiten Konsens gestoßen waren, entwickelte;
- bei der Erarbeitung des Gemeinsamen Vorschlags davon ausgegangen wurde, dass diese gemeinsamen Prinzipien und Ansätze Wertvolles zur Förderung des Schutzes der Privatsphäre und der persönlichen Information beitragen könnten und dass die Arbeitsgruppe die Erweiterung dieser Ansätze durch spezifische Lösungen und Standards anstrebte, die trotz der bestehenden Differenzen zwischen den vorhandenen Modellen zum Datenschutz und zum Schutz der Privatsphäre als anwendbar betrachtet wurden.

Im Einklang damit beschließt die Konferenz Folgendes:

1. Sie begrüßt den Gemeinsamen Vorschlag zur Abfassung der Internationalen Standards zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung von personenbezogenen Daten, die diesem Beschluss als Anlage beiliegt. Der Gemeinsame Vorschlag belegt zum angemessenen Zeitpunkt die Möglichkeit der Festlegung solcher Standards als einen neuen Schritt in Richtung auf die Ausarbeitung eines international verbindlichen Instruments.

2. Sie bestätigt, dass der Gemeinsame Vorschlag Grundsätze, Rechte, Verpflichtungen und Verfahrensweisen enthält, die zum Datenschutz und zum Schutz der Privatsphäre von allen Rechtssystemen angestrebt werden sollten. Auf diese Weise könnte die Verarbeitung

personenbezogener Daten im öffentlichen und privaten Sektor weltweit einheitlicher erfolgen, und zwar:

a. fair, rechtmäßig und angemessen im Hinblick auf bestimmte explizite und legitime Zwecke;
b. auf der Grundlage einer transparenten Politik, mit angemessenen Informationen für die Interessierten und ohne willkürliche Diskriminierungen, die diesen Grundsätzen widersprächen;
c. die Genauigkeit, Vertraulichkeit und Sicherheit der Daten sowie die Legitimität der Datenverarbeitung und die Rechte der Betroffenen auf Einsehen, Richtigstellung und Löschung der Daten sowie auf Widerspruch gegen eine bestimmte Datenverarbeitung gewährleistend;
d. unter Anwendung des Haftungsprinzips, einschließlich der Schadenshaftung, was auch die Datenverarbeitung durch Dienstleistungserbringer, die im Auftrag des Verantwortlichen handeln, einschließt;
e. mit geeigneteren Garantien, wenn es sich um sensible Daten handelt;
f. mit der Gewährleistung, dass international übertragene Daten unter dem in den genannten Standards vorgesehenen Schutz stehen;
g. indem die Datenverarbeitung unter die Kontrolle von unabhängigen und unparteiischen Aufsichtsbehörden gestellt wird, die über die angemessenen Befugnisse und Ressourcen verfügen müssen und zur Zusammenarbeit verpflichtet sind;
h. durch die Schaffung eines neuen und modernen Bezugsrahmens proaktiver Maßnahmen, deren Ziel insbesondere die Vorbeugung und Feststellung von Verstößen ist und die auf der Ernennung von Beauftragten für den Datenschutz und den Schutz der Privatsphäre, wirksamen Audits und Datenschutz-Folgenabschätzungen beruhen.

3. Sie ermutigt die bei der Internationalen Konferenz akkreditierten Beauftragten für den Datenschutz und den Schutz der Privatsphäre zur Verbreitung des Gemeinsamen Vorschlags zur Abfassung Internationaler Standards zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten.

4. Sie beauftragt die für die Organisation der 31. und 32. Internationalen Konferenzen Verantwortlichen mit dem Aufbau einer Kontaktgruppe, an der die interessierten Beauftragten für den Datenschutz und den Schutz der Privatsphäre teilnehmen sollen. Diese Gruppe soll folgende Aufgaben in Angriff nehmen:

a. Die Förderung und die Verbreitung des Gemeinsamen Vorschlags unter privaten Instanzen, Experten sowie in- und ausländischen öffentlichen Stellen, insbesondere unter den in der Erklärung von Montreux aufgeführten Institutionen und Organisationen als Grundlage für die zukünftige Arbeit an einem verbindlichen universellen Abkommen; sowie
b. die Untersuchung und Information über weitere Möglichkeiten der Verwendung des Gemeinsamen Vorschlags als Grundlage für die Entwicklung eines weltweiten Verständnisses und einer internationalen Kooperation im Bereich des Datenschutzes und des Schutzes der Privatsphäre, insbesondere im Kontext der internationalen Übertragung personenbezogener Daten, bei der die Rechte und Freiheiten der Individuen geschützt werden müssen.

5. Die Kontaktgruppe soll:

a. ihre Arbeit mit der Steuerungsgruppe der Konferenz koordinieren und über ihre Vertretung auf Sitzungen internationaler Organisationen entscheiden, sowie
b. die 32. Internationale Konferenz über ihre Fortschritte informieren, damit die Aufmerksamkeit dauerhaft auf das Thema des vorliegenden Beschlusses gerichtet wird.

Erläuterung

Die 30. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre fasste in Strassburg einstimmig die **Entschließung über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen und die Ausarbeitung einer gemeinsamen Entschließung zur Abfassung Internationaler Standards zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten**. Diese wurde gemeinsam von den Datenschutzbehörden der Schweiz und Spaniens vorgelegt und von zwanzig weiteren Behörden unterstützt.

In dieser Entschließung erinnert die Konferenz daran, dass diverse Erklärungen und Beschlüsse in den letzten zehn Jahren darauf abzielten, den universellen Charakter des Rechts auf Datenschutz und auf den Schutz der Privatsphäre zu stärken und zur Erstellung eines universellen Übereinkommens zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten aufzurufen.

Außerdem betont der Beschluss, dass die Internationale Konferenz der Ansicht ist, das Recht auf Datenschutz und den Schutz der Privatsphäre sei ein Grundrecht der Menschen, unabhängig von ihrer Staatsangehörigkeit und ihrem Wohnsitz. Gleichzeitig stellt sie fest, dass die anhaltenden Disparitäten im Bereich des Datenschutzes und der Achtung der Privatsphäre weltweit, insbesondere wegen des Fehlens von Garantien in mehreren Staaten, dem Austausch personenbezogener Daten und der Schaffung eines effizienten, globalen Datenschutzes schaden.

Deshalb wird in dem Beschluss die Überzeugung der Konferenz zum Ausdruck gebracht, dass die Anerkennung dieser Rechte die Verabschiedung eines universellen, zwingenden Rechtsinstruments erfordert, das die in den verschiedenen bestehenden Instrumenten festgeschriebenen gemeinsamen Prinzipien des Datenschutzes und der Achtung der Privatsphäre bestätigt, auflistet und ergänzt und die internationale Zusammenarbeit zwischen Datenschutzbehörden verstärkt.

In diesem Sinne unterstützt der Beschluss der Internationalen Konferenz die Anstrengungen des Europarats, die Grundrechte auf den Datenschutz und den Schutz der Privatsphäre zu fördern und sie fordert die Staaten - unabhängig davon, ob sie Mitglieder dieser Organisation sind oder nicht - auf, das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und das Zusatzprotokoll zu ratifizieren. Gleichzeitig unterstützt die Konferenz die Initiativen der APEC, der OECD sowie anderer regionaler Organisationen und internationaler Foren, wirksame Mittel zur Förderung besserer internationaler Standards für den Datenschutz und den Schutz der Privatsphäre zu entwickeln.

Die Konferenz beauftragte die spanische Datenschutzbehörde in ihrer Eigenschaft als Koordinatorin der 31. Internationalen Konferenz, eine Arbeitsgruppe zu bilden, die sich aus den interessierten Datenschutzbehörden zusammensetzen soll, und deren Ziel es ist, einen Gemeinsamen Vorschlag zur Abfassung Internationaler Standards zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten zu entwickeln.

Der Beschluss enthält eine Reihe von Kriterien, die den Prozess zur Ausarbeitung dieses gemeinsamen Vorschlags lenken, insbesondere, dass öffentliche und private Organisationen und Instanzen zu einer breiten Beteiligung ermutigt werden sollen, um zu einem möglichst umfassenden institutionellen und gesellschaftlichen Konsens zu gelangen.

Gemäß diesem Auftrag bildete die spanische Datenschutzbehörde die Arbeitsgruppe, auf die sich der Beschluss bezieht, und förderte und koordinierte die Arbeiten zur Erstellung eines gemeinsamen Vorschlags zur Abfassung internationaler Standards.

Die spanische Datenschutzbehörde lud alle bei der Internationalen Konferenz akkreditierten Behörden für den Datenschutz und den Schutz der Privatsphäre zur Teilnahme ein. Die im Anhang II aufgeführten Instanzen bekundeten ihren Willen, an dieser Arbeitsgruppe teilzunehmen und versammelten sich daraufhin.

Die Arbeitsgruppe kam im Januar und Juni 2009 zusammen. Auf der ersten Sitzung wurde die Vorgehensweise zur Abfassung des Gemeinsamen Vorschlags und dessen inhaltliche Reichweite

beschlossen und auf der zweiten Sitzung wurde eine fortgeschrittene Entwurfsversion besprochen, die später an die 31. Internationale Konferenz weitergeleitet werden sollte.

Die spanische Datenschutzbehörde leistete auf der Grundlage des Straßburger Beschlusses und der in der Arbeitsgruppe festgelegten Kriterien und Arbeitsmethoden eine gründliche Arbeit: Es wurde eine Reihe von Arbeitspapieren verfasst, an deren Ausarbeitung Beauftragte für den Datenschutz und den Schutz der Privatsphäre und andere mit dem Datenschutz verbundene öffentliche Instanzen sowie Experten aus privaten Unternehmen, Juristen, Wissenschaftler sowie internationale Organisationen und Nicht-Regierungs-Organisationen beteiligt waren.

Insbesondere entwickelte die Arbeitsgruppe den Gemeinsamen Vorschlag zur Abfassung Internationaler Standards zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten auf der Grundlage der Gemeinsamkeiten verschiedener juristischer Texte, Standards oder Empfehlungen mit internationaler Reichweite, die in unterschiedlichen geografischen, wirtschaftlichen oder rechtlichen Anwendungsgebieten auf einen breiten Konsens gestoßen waren.

Bei der Erarbeitung des Gemeinsamen Vorschlags wurde davon ausgegangen, dass diese gemeinsamen Prinzipien und Ansätze Wertvolles zur Förderung des Schutzes der Privatsphäre und der persönlichen Information beitragen. Ziel der Arbeitsgruppe war die Erweiterung dieser Ansätze durch spezifische Lösungen und Standards, die aber trotz der bestehenden Differenzen zwischen den vorhandenen Modellen zum Datenschutz und zum Schutz der Privatsphäre anwendbar sind.

Anlage

Gemeinsamer Vorschlag zur Erstellung internationaler Standards zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten

Teil I: Allgemeine Bestimmungen

1. Ziel

Das Ziel des vorliegenden Dokuments ist:

a) Die Definition einer Reihe von Grundsätzen und Rechten, die den tatsächlichen und einheitlichen Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten weltweit garantieren; und

b) die Erleichterung des internationalen Flusses von personenbezogenen Daten – das ist eine Notwendigkeit in einer globalisierten Welt.

2. Definitionen

Das vorliegende Dokument versteht unter:

a) „Personenbezogenen Daten“: Jegliche Information bezüglich einer identifizierten natürlichen Person bzw. einer natürlichen Person, die mit den vernünftigerweise einzusetzenden Mitteln identifiziert werden kann.

b) „Verarbeitung“: Jeglicher Vorgang oder eine Reihe von Vorgängen, die automatisiert sein können oder nicht, und die auf personenbezogene Daten angewendet werden, das betrifft insbesondere deren Erhebung, Aufbewahrung, Enthüllung oder Löschung.

c) „Betroffener“: Eine natürliche Person, deren personenbezogene Daten verarbeitet werden.

d) „Verantwortliche Person“: Eine natürliche oder juristische Person, öffentlich oder privat, die allein oder in Zusammenarbeit mit anderen über die Verarbeitung entscheidet.

e) „Dienstleistungserbringer“: Eine natürliche oder juristische Person, die nicht die verantwortliche Person ist und die personenbezogenen Daten im Auftrag der besagten verantwortlichen Person verarbeitet.

3. Anwendungsbereich

1. Das vorliegende Dokument gilt für jegliche Verarbeitung personenbezogener Daten, die voll- oder teilautomatisch oder andernfalls in strukturierter Form im öffentlichen oder im privaten Sektor vollzogen wird.

2. Die jeweilige nationale Gesetzgebung kann festlegen, dass die Bestimmungen des vorliegenden Dokuments nicht auf die Verarbeitung personenbezogener Daten anzuwenden ist, wenn diese von einer natürlichen Person im Rahmen von ausschließlich privaten bzw. familiären Tätigkeiten ausgeführt wird.

4. Zusätzliche Maßnahmen

1. Die Staaten können das in dem vorliegenden Dokument definierte Schutzniveau um zusätzliche Maßnahmen, die einen besseren Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten garantieren, ergänzen.

2. Die Bestimmungen des vorliegenden Dokuments bilden eine geeignete Grundlage für die grenzüberschreitende Übermittlung personenbezogener Daten, wenn dies gemäß den Vorgaben des Artikels 15 des vorliegenden Dokuments geschieht.

5. Ausnahmen

Die Staaten können die Reichweite der in den Artikeln 7 bis 10 und 16 bis 18 enthaltenen Bestimmungen einschränken, wenn dies in einer demokratischen Gesellschaft notwendig ist, um die nationale Sicherheit, die öffentliche Sicherheit, den Schutz der öffentlichen Gesundheit oder den Schutz der Rechte und Freiheiten anderer zu gewährleisten. Solche Einschränkungen müssen im nationalen Recht ausdrücklich vorgesehen sein, das heißt, ihre Grenzen müssen festgelegt werden und es muss angemessene Garantien zum Schutz der Rechte der Betroffenen geben.

Teil II: Grundlegende Prinzipien

6. Prinzipien der Rechtmäßigkeit und Fairness

1. Die Verarbeitung personenbezogener Daten muss fair ausgeführt werden, wobei die anwendbare nationale Gesetzgebung sowie die Rechte und Freiheiten der Menschen im Einklang mit den Inhalten des vorliegenden Dokuments und den Zielen und Grundsätzen der Allgemeinen Erklärung der Menschenrechte und dem Internationalen Pakt über bürgerliche und politische Recht eingehalten werden müssen

2. Insbesondere eine Verarbeitung personenbezogener Daten, die eine ungerechte oder willkürliche Diskriminierung der Betroffenen darstellt, wird als unredlich angesehen.

7. Prinzip der Zweckgebundenheit

1. Die Verarbeitung personenbezogener Daten muss sich auf die Erfüllung bestimmter, expliziter und legitimer Zwecke, die die verantwortliche Person verfolgt, beschränken.

2. Die verantwortliche Person darf keine Verarbeitungen durchführen, die nicht den Zwecken, für die die personenbezogenen Daten erhoben wurden, entsprechen, außer sie verfügt über das eindeutige Einverständnis des Betroffenen.

8. Verhältnismäßigkeitsprinzip

1. Die Verarbeitung der personenbezogenen Daten muss sich auf solche beschränken, die für die im vorherigen Absatz beschriebenen Zwecke angemessen, relevant und nicht exzessiv sind.

2. Insbesondere muss die verantwortliche Person angemessene Anstrengungen leisten, um die verarbeiteten personenbezogenen Daten auf ein notwendiges Mindestmaß zu reduzieren.

9. Qualitätsprinzip

1. Die verantwortliche Person muss jederzeit sicherstellen, dass die personenbezogenen Daten exakt sind und dass sie so vollständig und aktuell gehalten werden, wie es für die Erfüllung der Zwecke, für die sie verarbeitet werden, notwendig ist.

2. Die verantwortliche Person muss die Aufbewahrungszeit der verarbeiteten personenbezogenen Daten auf die erforderliche Mindestzeit beschränken. Wenn also die personenbezogenen Daten für die Erfüllung der Zwecke, die ihre Verarbeitung legitimierten, nicht mehr notwendig sind, müssen sie gelöscht oder anonymisiert werden.

10. Transparenzprinzip

1. Jede verantwortliche Person muss die von ihr durchgeführte Verarbeitung personenbezogener Daten in einer Datenschutzerklärung transparent machen.

2. Die verantwortliche Person muss dem Betroffenen zumindest über ihre Identität, den Zweck, zu dem sie die Verarbeitung auszuführen beabsichtigt, die Adressaten, an die sie die personenbezogenen Daten weiterzuleiten gedenkt und die Art, auf die der Betroffene seine in dem vorliegenden Dokument beschriebenen Rechte ausüben können, sowie alle weiteren Informationen, die die loyale Verarbeitung dieser personenbezogenen Daten gewährleistet, informieren.

3. Wenn die personenbezogenen Daten direkt von dem Betroffenen geliefert wurden, muss die Information zum Zeitpunkt der Datenerhebung gegeben werden, falls sie nicht schon vorher erteilt wurde.

4. Falls die personenbezogenen Daten nicht direkt vom Betroffenen stammen, muss die Information innerhalb eines angemessenen Zeitraums erbracht werden, obwohl sie auch durch alternative Maßnahmen ersetzt werden kann, falls die Erfüllung dieser Vorgabe unmöglich ist oder von der verantwortlichen Person einen unverhältnismäßigen Aufwand verlangt.

5. Alle Informationen, die dem Betroffenen gegeben werden, müssen verständlich und in einer eindeutigen und einfachen Sprache abgefasst sein, was insbesondere für solche Verarbeitungen gilt, die sich speziell an Minderjährige richten.

6. Wenn die personenbezogenen Daten online über elektronische Kommunikationsnetze erhoben werden, können die in diesem Artikel enthaltenen Verpflichtungen erfüllt werden, indem die Datenschutzpolitik leicht zugänglich und erkennbar veröffentlicht wird, wobei alle oben aufgeführten Punkte eingehalten werden müssen.

11. Verantwortlichkeitsprinzip

Die verantwortliche Person muss:

a) Die notwendigen Maßnahmen zur Erfüllung der in dem vorliegenden Dokument und in der anzuwendenden nationalen Gesetzgebung aufgeführten Grundsätze und Verpflichtungen ergreifen; und

b) die erforderlichen Nachweise über die Erfüllung der o.g. Vorgaben erbringen, und zwar sowohl gegenüber dem Betroffenen als auch gemäß Artikel 23 gegenüber den zuständigen Aufsichtsbehörden.

Teil III: Rechtfertigung der Verarbeitung

12. Allgemeines Rechtfertigungsprinzip

1. Als allgemeine Regel gilt, dass personenbezogene Daten nur dann verarbeitet werden dürfen, wenn einer der folgenden Punkte erfüllt wird:

a) nach Erhalt des freien, eindeutigen und informierten Einverständnisses des Betroffenen;

b) wenn ein legitimes Interesse der verantwortlichen Person die Verarbeitung rechtfertigt, vorausgesetzt, dass die legitimen Interessen, Rechte oder Freiheiten des Betroffenen keinen Vorrang haben;

c) wenn die Verarbeitung für die Aufrechterhaltung oder Erfüllung eines Rechtsverhältnisses zwischen der verantwortlichen Person und dem Betroffenen erforderlich ist;

d) wenn die Verarbeitung für die Erfüllung einer Verpflichtung, die der verantwortlichen Person von der anzuwendenden nationalen Gesetzgebung auferlegt wird, notwendig ist oder wenn

sie von einer öffentlichen Behörde, die diese für die legitime Erfüllung ihrer Zuständigkeiten benötigt, ausgeführt wird;

e) wenn außergewöhnliche Umstände auftreten, die das Leben, die Gesundheit oder die Sicherheit des Betroffenen oder einer anderen Person gefährden.

2. Die verantwortliche Person muss den Betroffenen einfache, schnelle und wirksame Verfahren bereitstellen, damit diese ihr Einverständnis jederzeit zurücknehmen können. Diese Verfahren dürfen weder Verzögerungen noch ungerechtfertigte Kosten für die Betroffenen noch Einkünfte der verantwortlichen Person verursachen.

13. Sensitive Daten

1. Als sensitiv werden folgende personenbezogenen Daten betrachtet:

a) Solche, die die Intimsphäre des Interessierten betreffen; oder

b) wenn deren ungerechtfertigte Verwendung

i. eine gesetzwidrige oder willkürliche Diskriminierung verursacht; oder

ii. ein schwerwiegendes Risiko für den Betroffenen darstellt.

2. Insbesondere werden solche personenbezogenen Daten als sensibel eingestuft, die Aufschluss über Aspekte wie die rassische oder ethnische Herkunft, politische Einstellungen, religiöse oder philosophische Überzeugungen geben, sowie Daten, die sich auf die Gesundheit oder die Sexualität beziehen. Falls die Umstände, auf die der vorhergehende Artikel sich bezieht, auftreten, kann die anzuwendende nationale Gesetzgebung weitere Kategorien für sensitive Daten vorsehen.

3. In der jeweiligen nationalen Gesetzgebung müssen die notwendigen Garantien zum Schutz der Rechte der Betroffenen festgeschrieben werden. Diese müssen zusätzliche Bedingungen für die Verarbeitung sensibler personenbezogener Daten enthalten.

14. Datenverarbeitung im Auftrag

Die verantwortliche Person kann die Verarbeitung von personenbezogenen Daten von verschiedenen Auftragnehmern durchführen lassen. In diesem Fall verpflichtet sie sich zur:

a) Kontrolle, dass jeder Auftragnehmer sicherstellt, dass zumindest das in dem vorliegenden Dokument und in der anzuwendenden nationalen Gesetzgebung vorgeschriebene Schutzniveau eingehalten wird; und

b) Verbindlichmachung der Rechtsbeziehung mittels eines Vertrags oder eines anderen Rechtsakts, der das Vorhandensein, die Reichweite und den Inhalt des Rechtsverhältnisses nachweist und den Auftragnehmer zur Einhaltung dieser Garantien und zur Gewährleistung, dass die personenbezogenen Daten gemäß der Anweisungen der verantwortlichen Person verarbeitet werden, verpflichtet.

15. Internationaler Datenverkehr

1. Als allgemeine Regel gilt, dass personenbezogene Daten grenzüberschreitend übermittelt werden können, wenn der Staat, in den diese Daten übertragen werden, zumindest das in dem vorliegenden Dokument vorgesehene Schutzniveau bietet.

2. Übermittlungen personenbezogener Daten in Staaten, die das in dem vorliegenden Dokument vorgesehene Schutzniveau nicht bieten, sind möglich, wenn derjenige, der die Daten zu übertragen beabsichtigt, garantiert, dass der Empfänger dieses Schutzniveau sicherstellt. Diese Garantie kann sich beispielsweise aus geeigneten vertraglichen Klauseln ableiten. Insbesondere, wenn die Datenübermittlung im Rahmen multinationaler Organisationen oder Unternehmensgruppen erfolgt,

kann diese Garantie durch interne Datenschutzbestimmungen, deren Einhaltung rechtsverbindlich ist, geleistet werden.

3. Wenn die Übermittlung im Rahmen einer Vertragsbeziehung zugunsten des Betroffenen, zum Schutz eines lebenswichtigen Interesses des Betroffenen bzw. einer anderen Person oder zur Erfüllung einer gesetzlichen Verpflichtung zur Wahrung eines wichtigen öffentlichen Interesses erforderlich ist, kann die für den Datenexporteur geltende nationale Gesetzgebung die Übermittlung der personenbezogenen Daten in Staaten zulassen, die das im vorliegenden Dokument vorgesehene Schutzniveau nicht bieten.

4. Die anzuwendende nationale Gesetzgebung kann die in Artikel 23 genannten Aufsichtsbehörden, die im Absatz 23 vorgesehen sind, zur vorherigen Genehmigung aller oder einiger grenzüberschreitender Übermittlungen von personenbezogenen Daten ermächtigen, die von ihrem Zuständigkeitsbereich aus erfolgen. Auf jeden Fall muss derjenige, der die personenbezogenen Daten ins Ausland übermitteln will, nachweisen, dass die Übermittlung die im vorliegenden Dokument vorgesehenen Garantien erfüllt, insbesondere wenn dies von den Aufsichtsbehörden in Ausübung ihrer im Artikel 23.2 vorgesehenen Zuständigkeiten gefordert wird.

Teil IV: Die Rechte des Betroffenen

16. Recht auf Einsicht

1. Der Betroffene hat das Recht, bei der verantwortlichen Person Informationen über die konkreten, zu verarbeitenden, personenbezogenen Daten sowie über die Herkunft dieser Daten, die Zwecke ihrer Verarbeitung und die Empfänger bzw. Empfängerkategorien zu verlangen, an die diese Daten weitergeleitet werden bzw. werden sollen.

2. Alle Informationen, die dem Betroffenen zugänglich gemacht werden, müssen in einer verständlichen, klaren und einfachen Sprache gehalten sein.

3. Die anzuwendende nationale Gesetzgebung kann die wiederholte Ausübung dieser Rechte, die die verantwortliche Person dazu veranlassen würde in kurzen Zeitabständen eine Vielzahl von Anträgen zu beantworten, einschränken, außer in den Fällen, in denen der Betroffene in seinem Antrag ein berechtigtes Interesse nachweist.

17. Recht auf Berichtigung und Löschung

1. Der Betroffene hat das Recht, bei der verantwortlichen Person die Berichtigung oder Löschung unvollständiger, ungenauer, unnötiger oder übermäßiger personenbezogener Daten zu beantragen.

2. Wenn dieser Fall eintritt, muss die verantwortliche Person die personenbezogenen Daten antragsgemäß berichtigen oder löschen. Er muss dies außerdem den Dritten, an die er die personenbezogenen Daten weitergeleitet hat, mitteilen, falls er diese kennt.

3. Die Löschung erfolgt nicht, wenn die personenbezogenen Daten entsprechend einer der verantwortlichen Person von der nationalen Gesetzgebung auferlegten Verpflichtung oder infolge der Vertragsbeziehungen zwischen der verantwortlichen Person und dem Betroffenen aufbewahrt werden müssen.

18. Widerspruchsrecht

1. Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten widersprechen, wenn er einen berechtigten Grund aufgrund seiner konkreten persönlichen Situation vorbringt.

2. Dieses Widerspruchsrecht kann nicht ausgeübt werden, wenn die Verarbeitung der personenbezogenen Daten der verantwortlichen Person von der nationalen Gesetzgebung vorgeschrieben ist.

3. Jeder Betroffene kann gleichfalls solchen Entscheidungen widersprechen, die allein auf der automatischen Verarbeitung der personenbezogenen Daten beruhende Rechtsfolgen nach sich ziehen, es sei denn die Entscheidung wurde von dem Betroffenen ausdrücklich beantragt oder sie ist für den Abschluss, die Aufrechterhaltung oder Erfüllung einer Rechtsbeziehung zwischen der verantwortlichen Person und dem Betroffenen erforderlich. In diesem letzten Fall muss der Betroffene zur Verteidigung seines Rechts oder Interesses die Möglichkeit zur Geltendmachung seiner Sichtweise haben.

19. Ausübung dieser Rechte

1. Die in den Artikeln 16 bis 18 des vorliegenden Dokuments aufgeführten Rechte können folgendermaßen ausgeübt werden:

a) direkt vom Interessierten, der sich gegenüber der verantwortlichen Person angemessen ausweisen muss.

b) über einen Vertreter, der diese Eigenschaft gegenüber der verantwortlichen Person entsprechend nachweisen muss.

2. Die verantwortliche Person muss Verfahren vorsehen, die es den Betroffenen ermöglichen, die in den Absätzen 16 bis 18 des vorliegenden Dokuments vorgesehenen Rechte einfach, schnell und wirksam auszuüben. Diese Verfahren dürfen weder Verzögerungen noch ungerechtfertigte Kosten für den Betroffenen noch Einkünfte für die verantwortliche Person verursachen.

3. Wenn die verantwortliche Person der Ansicht ist, dass im Einklang mit der anzuwendenden nationalen Gesetzgebung die Ausübung der in diesem Teil aufgeführten Rechte nicht angebracht ist, muss er den Betroffenen vollständig über seine Gründe informieren.

Teil V: Sicherheit

20. Sicherheitsmaßnahmen

1. Sowohl die verantwortliche Person als auch die Auftragnehmer müssen die personenbezogenen Daten, die sie verarbeiten, mit den zu dem jeweiligen Zeitpunkt geeigneten technischen und organisatorischen Mitteln schützen, um ihre Vollständigkeit, Vertraulichkeit und Verfügbarkeit zu gewährleisten. Diese Maßnahmen hängen vom bestehenden Risiko, den möglichen Folgen für die Betroffenen, der Sensitivität der personenbezogenen Daten, dem technischen Zustand und dem Kontext, in dem die Verarbeitung erfolgt, sowie von der jeweiligen nationalen Gesetzgebung ab.

2. Die Betroffenen müssen von denjenigen, die an irgendeiner der Verarbeitungsschritte beteiligt sind, über alle Sicherheitsverstöße, die ihre Vermögens- und Nichtvermögensrechte wesentlich beeinträchtigen könnten, sowie über die ergriffenen Lösungsversuche informiert werden. Diese Information muss früh genug erteilt werden, damit die Betroffenen genügend Zeit haben, zur Verteidigung ihrer Rechte darauf zu reagieren.

21. Datengeheimnis

Die verantwortliche Person und diejenigen, die an irgendeiner der Verarbeitungsschritte der personenbezogenen Daten beteiligt sind, müssen darüber Verschwiegenheit bewahren. Diese Verpflichtung besteht auch dann noch, wenn die Beziehungen mit dem Betroffenen oder der verantwortlichen Person bereits abgeschlossen sind.

Teil VI: Einhaltung und Überwachung

22. Proaktive Maßnahmen

Die Staaten müssen über ihr innerstaatliches Recht Anreize für Maßnahmen schaffen, die eine bessere Einhaltung der Gesetzgebung zum Datenschutz durch diejenigen fördern, die an den unterschiedlichen Verarbeitungsschritten beteiligt sind. Zu diesen Maßnahmen können unter anderem Folgende zählen:

a) Die Einführung von Verfahren zur Vorbeugung und Feststellung von Verstößen, die auf standardisierten Modellen zur Steuerung und/oder für das Management der Informationssicherheit beruhen.

b) Die Ernennung eines oder mehrerer Beauftragter für den Schutz der Privatsphäre oder des Datenschutzes, die für die Wahrnehmung ihrer Aufsichtsfunktionen über ausreichende Qualifikationen, Ressourcen und Kompetenzen verfügen müssen.

c) Die regelmäßige Durchführung von Programmen zur Bewusstseinsbildung, Aus- und Weiterbildung der Mitglieder der Organisation zur Verbesserung ihrer Kenntnisse der auf den Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten anzuwendende Gesetzgebung sowie der von der Organisation zu diesem Zweck eingerichteten Verfahren.

d) Die regelmäßige Durchführung von transparenten Audits durch qualifizierte und vorzugsweise unabhängige Personen, bei denen die Einhaltung der auf den Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten anzuwendenden Gesetzgebung sowie der von der Organisation zu diesem Zweck eingerichteten Verfahren geprüft wird.

e) Die Anpassung der Informationssysteme und/oder Informationstechnologien, die der Verarbeitung personenbezogener Daten dienen, an die auf den Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten anzuwendende Gesetzgebung, insbesondere wenn es darum geht, Entscheidungen über technische Merkmale, die technische Entwicklung und Implementierung zu treffen.

f) Die Praxisumsetzung von Datenschutz-Folgenabschätzungen vor der Implementierung neuer Informationssysteme und/oder Informationstechnologien, die der Verarbeitung personenbezogener Daten dienen, sowie die Praxisumsetzung neuer Arten der Verarbeitung personenbezogener Daten vor der Einführung wesentlicher Veränderungen der Verarbeitungspraxis.

g) Die Annahme von Verhaltensregeln, deren Einhaltung verpflichtend ist und die es ermöglichen, ihre Wirksamkeit in Bezug auf die Befolgung und den Grad des Schutzes der personenbezogenen Daten zu messen und die wirkungsvolle Maßnahmen im Fall der Nichterfüllung festlegen.

h) Die Einführung von Eventualfallplänen, die Handlungsanweisungen für den Fall festlegen, dass eine Nichtbefolgung der auf den Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten anzuwendende Gesetzgebung festgestellt wird, und die zumindest die Verpflichtung enthalten, die Ursache und Reichweite der eingetretenen Vorschriftsverletzung zu bestimmen, ihre negativen Auswirkungen zu beschreiben und die erforderlichen Maßnahmen zu ergreifen, damit das zukünftig nicht noch einmal geschieht.

23. Überwachung

1. In jedem Staat muss es eine oder mehrere Aufsichtsbehörden geben, die im Einklang mit dem innerstaatlichen Recht für die Überwachung der Einhaltung der in dem vorliegenden Dokument festgelegten Grundsätze verantwortlich sind.

2. Diese Aufsichtsbehörden müssen unparteiisch und unabhängig sein und sie müssen über eine angemessene technische Qualifikation, ausreichende Kompetenzen und die geeigneten Ressourcen verfügen, um über die Reklamationen, die die Interessenten an sie richten, entscheiden zu können und um die Untersuchungen und Eingriffe durchführen zu können, die die Befolgung der nationalen Gesetzgebung zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten gewährleisten.

3. Auf jeden Fall und unbeschadet der Einsprüche, die bei den genannten Aufsichtsbehörden eingelegt werden - was auch die gerichtliche Nachprüfung ihrer Entscheidungen einschließt - kann der Betroffene zur Geltendmachung seiner Rechte gemäß den Vorschriften der nationalen Gesetzgebung direkt den Rechtsweg beschreiten.

24. Kooperation und Koordination

1. Die im vorigen Artikel genannten Aufsichtsbehörden müssen bestrebt sein, im Interesse eines einheitlicheren Schutzes der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten sowohl im Inland als auch auf internationaler Ebene miteinander zu kooperieren. Um diese Kooperation zu vereinfachen, müssen die Staaten jederzeit die bei ihnen zuständigen Aufsichtsbehörden benennen können.

2. Diese Behörden bemühen sich insbesondere um die Erfüllung folgender Aufgaben:

a) den Austausch von Studien, Untersuchungsmethoden, Kommunikations- und Regelungsstrategien sowie von allen Informationen, die für eine wirksame Ausübung ihrer Funktionen hilfreich sind, insbesondere nachdem sie von einer anderen Aufsichtsbehörde im Rahmen einer Untersuchung oder Intervention um Unterstützung gebeten worden sind;

b) die Durchführung koordinierter Untersuchungen oder Interventionen - sowohl im Inland als auch auf internationaler Ebene – bei Angelegenheiten, bei denen das Interesse zweier oder mehrerer Aufsichtsbehörden zusammentreffen;

c) die Teilnahme an Verbänden, Arbeitsgruppen oder gemeinsamen Foren sowie Seminaren, Workshops oder Kursen, die dazu beitragen, gemeinsame Standpunkte zu entwickeln oder die technische Qualifizierung des Personals, das diesen Aufsichtsbehörden seine Dienste leistet, zu verbessern;

d) die Aufrechterhaltung einer angemessenen Vertraulichkeit der Informationen, die sie während ihrer Kooperation untereinander ausgetauscht hatten.

3. Die Staaten müssen die Schaffung von Kooperationsvereinbarungen zwischen regionalen, nationalen oder internationalen Aufsichtsbehörden, die zu einer wirksameren Einhaltung dieses Absatzes beitragen, fördern.

25. Haftung

1. Die verantwortliche Person haftet für solche Schäden - sowohl immaterieller als auch materieller Art - die dem Betroffenen durch die Verarbeitung personenbezogener Daten, bei der gegen die Datenschutzvorschriften verstoßen wurde, entstanden sind, es sei denn sie kann nachweisen, dass der Schaden ihr nicht anzulasten ist. Dies gilt unbeschadet des Rechtsanspruchs, den die verantwortliche Person gegenüber den Auftragnehmern, die an den einzelnen Verarbeitungsschritten teilhaben, geltend machen kann.

2. Die Staaten müssen geeignete Maßnahmen fördern, damit die Betroffenen Zugang zu den entsprechenden Gerichts- oder Verwaltungsverfahren haben, die ihnen die Wiedergutmachung der oben erwähnten Schäden ermöglichen.

3. Die in den vorherigen Absätzen vorgesehene Haftung gilt unbeschadet der strafrechtlichen, zivilrechtlichen und verwaltungsrechtlichen Ahndung der Verletzung der Gesetzgebung zum Datenschutz.

4. Das Ergreifen proaktiver Maßnahmen, wie sie im Artikel 22 beschrieben werden, muss bei der Feststellung der Haftung und der Verhängung der in diesem Artikel vorgesehenen Sanktionen berücksichtigt werden.