ARTIKEL-29-DATENSCHUTZGRUPPE

01197/11/DE
WP187

Stellungnahme 15/2011 zur Definition von Einwilligung

Angenommen am 13. Juli 2011

Zusammenfassung

Die vorliegende Stellungnahme bietet eine gründliche Analyse des Konzepts der Einwilligung, wie es derzeit in der Datenschutzrichtlinie und in der Datenschutzrichtlinie für elektronische Kommunikation verwendet wird. Ausgehend von den Erfahrungen der Mitglieder der Artikel-29-Datenschutzgruppe werden in der Stellungnahme zahlreiche Beispiele für gültige und ungültige Einwilligungen gegeben, wobei der Schwerpunkt auf die Schlüsselelemente der Einwilligung wie die Bedeutung von „Willensbekundung", „ohne jeden Zwang", „für den konkreten Fall", „ohne jeden Zweifel", „ausdrücklich", „in Kenntnis der Sachlage" usw. gelegt wird. Die Stellungnahme stellt auch einige Aspekte in Bezug auf den Begriff „Einwilligung" klar, beispielsweise den Zeitpunkt, zu dem die Einwilligung vorliegen muss, die Unterschiede zwischen Widerspruchsrecht und Einwilligung usw.

Die Einwilligung ist eine von mehreren Rechtsgrundlagen für die Verarbeitung personenbezogener Daten. Sie spielt zwar eine wichtige Rolle, schließt aber je nach Kontext nicht aus, dass möglicherweise andere Rechtsgrundlagen sowohl aus der Sicht des für die Datenverarbeitung Verantwortlichen als auch aus der Sicht der betroffenen Person geeigneter sind. Wenn die Einwilligung richtig genutzt wird, ermöglicht sie der betroffenen Person die Kontrolle über die Verarbeitung ihrer personenbezogenen Daten. Wird sie nicht richtig angewendet, wird eine Kontrolle durch die betroffene Person illusorisch und die Einwilligung ist dann keine angemessene Grundlage für die Verarbeitung mehr.

Die vorliegende Stellungnahme wird teilweise auf Grund einer Anfrage der Kommission im Zusammenhang mit der gerade stattfindenden Überprüfung der Datenschutzrichtlinie verfasst. Deshalb enthält sie Empfehlungen, die bei der Überprüfung erwogen werden sollten. Dazu zählen unter anderem:

(i) Die Bedeutung von Einwilligung „ohne jeden Zweifel" sollte klargestellt werden und es sollte erklärt werden, dass nur eine Einwilligung, die auf Erklärungen oder Handlungen beruht, mit denen die Zustimmung zum Ausdruck gebracht wird, eine gültige Einwilligung darstellt.

(ii) Die für die Datenverarbeitung Verantwortlichen sollten zur Einführung von Mechanismen verpflichtet werden, mit denen die Einwilligung dargelegt wird (im Rahmen einer allgemeinen Rechenschaftspflicht).

(iii) Es sollte eine ausdrückliche Vorschrift bezüglich der Qualität und Zugänglichkeit der Informationen eingefügt werden, die die Grundlage für die Einwilligung bilden.

(iv) Eine Reihe von Vorschlägen in Bezug auf Minderjährige und sonstige Personen ohne Rechts- und Geschäftsfähigkeit.

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,

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

gestützt auf ihre Geschäftsordnung,

HAT FOLGENDES DOKUMENT ANGENOMMEN:

I. Einleitung

Die Einwilligung der betroffenen Person war immer ein Schlüsselbegriff des Datenschutzes. Es ist jedoch nicht immer klar, wann eine Einwilligung erforderlich ist und welche Bedingungen erfüllt sein müssen, damit die Einwilligung gültig ist. Das kann in den einzelnen Mitgliedstaaten zu verschiedenen Ansätzen und unterschiedlichen Ansichten über die bewährten Methoden führen, was wiederum die Stellung der betroffenen Personen schwächen kann. Dieses Problem hat mehr Gewicht bekommen, da die Verarbeitung personenbezogener Daten in der modernen Gesellschaft sowohl in der Online- als auch der Offline-Umgebung eine immer größere Rolle spielt und häufig verschiedene Mitgliedstaaten betroffen sind. Deshalb hat sich die Artikel-29-Datenschutzgruppe im Rahmen ihres Arbeitsprogramms für 2010-2011 entschieden, dieses Thema zu untersuchen.

Die Einwilligung ist auch einer der Bereiche, in dem die Kommission im Zusammenhang mit der Überprüfung der Richtlinie 95/46/EG um Anregungen gebeten hat. In der Mitteilung der Kommission „Gesamtkonzept für den Datenschutz in der Europäischen Union“[1] steht: *„Die Kommission wird prüfen, wie die Bestimmungen über die Einwilligung präzisiert und gestärkt werden können.“* Die Mitteilung erklärt[2] dies folgendermaßen:

> *„Wenn die Einwilligung in Kenntnis der Sachlage verlangt wird, muss die betroffene Person nach geltendem Recht ihren Willen zur Verarbeitung ihrer Daten „ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage“ bekunden; sie akzeptiert dadurch, dass die sie betreffenden personenbezogenen Daten verarbeitet werden. Diese Bedingungen werden allerdings derzeit in den Mitgliedstaaten unterschiedlich ausgelegt. Manche verlangen generell eine schriftliche Einwilligung, andere gehen sogar so weit, die stillschweigende Einwilligung zuzulassen.“*

---

1 KOM(2010) 609 endgültig vom 4.11.2010.

2 Der erste Bericht der Kommission über die Durchführung der Datenschutzrichtlinie (95/46/EG) (KOM(2003) 265 endgültig), erwähnte bereits auf Seite 17: „Der Begriff der Einwilligung „ohne jeden Zweifel“ (Artikel 7 Buchstabe a) muss näher erläutert werden und eine einheitlichere Auslegung erhalten insbesondere im Vergleich zu dem Begriff der „ausdrücklichen“ Einwilligung in Artikel 8. Die Beteiligten müssen wissen, was eine gültige Einwilligung ist, insbesondere bei Online-Szenarios.“

„Darüber hinaus ist es in der Online-Umgebung – wegen der Undurchsichtigkeit der einschlägigen Datenschutzgrundsätze – oft für Einzelne besonders schwer, ihre Rechte zu kennen und eine Einwilligung in Kenntnis der Sachlage zu erteilen. Erschwerend kommt hinzu, dass es in manchen Fällen nicht einmal klar ist, was unter einer ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage gegebenen Einwilligung zur Datenverarbeitung zu verstehen ist. Ein Beispiel hierfür ist die verhaltensorientierte Internetwerbung, bei der die jeweiligen Einstellungen des Internet-Browsers nach Meinung einiger, aber nicht aller, die Einwilligung des Nutzers zum Ausdruck bringen."

„Daher sollte geklärt werden, wann die Bedingungen für die Einwilligung des Betroffenen erfüllt sind, um zu garantieren, dass diese stets in Kenntnis der Sachlage gegeben wird und dass der Betroffene – wie Artikel 8 der Charta der Grundrechte der Europäischen Union verlangt – genau weiß, dass er seine Einwilligung zur Datenverarbeitung erteilt und was diese Verarbeitung genau beinhaltet. Wenn die wesentlichen Konzepte klar sind, kann dies auch Anreiz für Initiativen zur Selbstregulierung geben, so dass praktische Lösungen gefunden werden können, die mit dem EU-Recht vereinbar sind."

Die Artikel-29-Datenschutzgruppe hat sich zur Ausarbeitung einer Stellungnahme verpflichtet, um der Bitte der Kommission um Anregungen nachzukommen und ihr Arbeitsprogramm für 2010-2011 zu erfüllen. Mit der Stellungnahme soll für Klarheit gesorgt werden, damit ein einheitliches Verständnis des bestehenden Rechtsrahmens sichergestellt werden kann. Gleichzeitig greift sie die Logik früherer Stellungnahmen zu anderen Schlüsselbestimmungen der Richtlinie auf[3]. Mögliche Änderungen des bestehenden Rechtsrahmens benötigen Zeit, so dass die Klärung des derzeitigen Begriffs der „Einwilligung" und der wichtigsten Aspekte der Einwilligung Vorteile mit sich bringt. Eine Klärung der bestehenden Bestimmungen hilft auch zu zeigen, welche Bereiche einer Verbesserung bedürfen. Aufbauend auf der Analyse wird sich die Stellungnahme also bemühen, Politikempfehlungen auszusprechen, um so die Kommission und die Entscheidungsträger bei ihren Überlegungen bezüglich der Änderungen an dem anzuwendenden Datenschutzrechtsrahmen zu unterstützen.

Die Stellungnahme hat im Wesentlichen folgenden Inhalt: Nach einem kurzen Überblick über die rechtliche Entstehungsgeschichte und der Rolle der Einwilligung in den Datenschutzvorschriften werden die unterschiedlichen Aspekte und Erfordernisse untersucht, damit eine Einwilligung nach dem anwendbaren Recht gültig ist. Es werden auch einige einschlägige Teile der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) untersucht. Die Analyse wird mit praktischen Beispielen illustriert, die auf nationalen Erfahrungen basieren. Damit werden die Empfehlungen im letzten Teil der vorliegenden Stellungnahme gestützt, denen zufolge bestimmte Elemente vorhanden sein müssen, damit im Sinne der Richtlinie eine gültige Einwilligung eingeholt und erhalten werden kann. Sie enthält auch Politikempfehlungen für die Entscheidungsträger, die diese im Zusammenhang mit der Überprüfung der Richtlinie 95/46/EG berücksichtigen sollten.

[3] Wie Stellungnahme 8/2010 zum anwendbaren Recht, angenommen am 16.12.2010 (WP179) und Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", angenommen am 16.02.2010 (WP169).

II. Allgemeine Bemerkungen und politische Aspekte

II.1. Vorgeschichte

Während einige der nationalen Gesetze zum Datenschutz/der Privatsphäre, die in den siebziger Jahren angenommen wurden, die Einwilligung als eine der Rechtsgrundlagen für die Verarbeitung personenbezogener Daten angesehen haben[4], hat sich dies nicht in dem Übereinkommen 108 des Europarates[5] niedergeschlagen. Es gibt keinen ersichtlichen Grund dafür, dass die Einwilligung keine größere Rolle in dem Übereinkommen spielt[6].

Auf EU-Ebene war die Einwilligung als Kriterium für die Legitimierung der Verarbeitung personenbezogener Daten seit Beginn des Rechtsetzungsprozesses vorgesehen, der mit der Annahme der Richtlinie 95/46/EG endete. Artikel 12 des Vorschlags der Kommission[7] von 1990 legte fest, welche Eigenschaften eine Einwilligung haben musste, damit die Verarbeitung personenbezogener Daten rechtmäßig ist: Sie musste *„ausdrücklich"* und *„für den konkreten Fall"* erfolgen. Gemäß Artikel 17 zu sensiblen Daten muss die Einwilligung *„ausdrücklich und schriftlich"* sein. „Der geänderte Vorschlag der Kommission[8] führte 1992 eine Textpassage ein, die der Definition der „Einwilligung der betroffenen Person" in dem heutigen Artikel 2 Buchstabe h ähnelt und den ursprünglichen Artikel 12 ersetzt. Es wurde festgelegt, dass die Einwilligung *„ohne Zwang, für den konkreten Fall"* erfolgen musste. Der Verweis auf *„ausdrücklich erteilt"* wurde durch Einwilligung als *„ausdrückliche Willensbekundung (der betroffenen Person)"* ersetzt. Die zu dem geänderten Vorschlag von 1992[9] gehörende Begründung legte fest, dass die Einwilligung entweder mündlich oder schriftlich erteilt werden konnte. In Bezug auf sensible Daten blieb die Forderung nach einer *„schriftlichen"* Einwilligung bestehen. 1992 strukturierte der geänderte Vorschlag der Kommission den vorangegangenen Vorschlag um und fügte Artikel 7 über die Rechtsgrundlagen für die Verarbeitung ein. Artikel 7 Buchstabe a legte fest, dass die Verarbeitung durchgeführt werden kann, wenn *„die betroffene Person zugestimmt hat"*. Die ursprüngliche Liste enthielt, wie heute auch, fünf zusätzliche Rechtsgrundlagen (zusätzlich zur Einwilligung), die zur Legitimierung der Datenverarbeitung herangezogen werden können.

---

4 Siehe beispielsweise Artikel 31 des französischen Gesetzes Nummer 78-17 vom 6. Januar 1978 „relative a l'informatique, aux fichiers et aux libertés".

5 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (bezeichnet als „Übereinkommen 108"). Es trat am 1. Oktober 1985 in Kraft.

6 Das Übereinkommen 108 führte die Begriffe „rechtmäßige Verarbeitung" und „rechtmäßiger Zweck" (Artikel 5) ein, ohne jedoch wie die Richtlinie 95/46/EG eine Liste der Kriterien für die rechtmäßige Datenverarbeitung zu bieten. Die Einwilligung der betroffenen Person spielte lediglich im Zusammenhang mit der gegenseitigen Hilfeleistung (Artikel 15) eine Rolle. Das Erfordernis der „Einwilligung" wurde jedoch später wiederholt in verschiedenen Empfehlungen des Ministerkomitees genannt.

7 Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, KOM(90) 314 endg., SYN 287 und 288, Brüssel, 13. September 1990.

8 Geänderter Vorschlag für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, KOM(92) 422 endg. - SYN 287, Brüssel, 15. Oktober 1992.

9 Siehe Seite 11 des geänderten Vorschlags für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, KOM(92) 422 endg. - SYN 287, Brüssel, 15. Oktober 1992.

Der Gemeinsame Standpunkt des Rates[10] von 1995 führte die endgültige (heutige) Definition von Einwilligung ein. Sie wurde definiert als *„jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden“*. Als wichtigste Änderung gegenüber dem Standpunkt der Kommission von 1992 wurde das Wort „*ausdrücklich*“ gestrichen, welches zuvor vor dem Wort „*Bekundung*“ stand. Gleichzeitig wurde Artikel 7 Buchstabe a durch „ohne jeden Zweifel“ ergänzt. Er lautet jetzt: *„Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben”*. Die Forderung nach einer schriftlichen Einwilligung in Bezug auf sensible Daten wurde durch *„ausdrückliche Einwilligung“* ersetzt.

In der Begründung des Rates[11] werden diese Änderungen nicht ausdrücklich erklärt. Auf Seite 4 steht jedoch: *„… dienen zahlreiche Änderungen ... einer Flexibilisierung; hierdurch wird … ein gleichwertiges Schutzniveau gewährleistet, ohne dass es zu einer Absenkung des Schutzniveaus kommen dürfte, da diese Flexibilität unter Berücksichtigung des extrem weiten Spektrums der ... Verarbeitung personenbezogener Daten eine effiziente und unbürokratische Anwendung der allgemeinen Grundsätze ermöglicht.“*

Die Bedeutung der Einwilligung wurde in der Charta der Grundrechte der Europäischen Union in Bezug auf den Schutz personenbezogener Daten ausdrücklich anerkannt. Artikel 8 Absatz 2 legt fest, dass personenbezogene Daten *„mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage“* verarbeitet werden können. Folglich wird die Einwilligung als grundlegender Aspekt des Grundrechts auf Schutz der personenbezogenen Daten anerkannt. Gleichzeitig ist die Einwilligung im Sinne der Charta nicht die einzige Rechtsgrundlage, mit der die Einwilligung in die Verarbeitung personenbezogener Daten ermöglicht wird, sondern die Charta erkennt ausdrücklich an, dass Rechtsvorschriften – wie bei der Richtlinie 95/46/EG der Fall – sonstige legitime Grundlagen festlegen können.

Zusammenfassend zeigt die Entstehungsgeschichte, dass die Einwilligung insbesondere in der EU eine wichtige Rolle für das Verständnis von Datenschutz und Privatsphäre gespielt hat. Gleichzeitig zeigt sich auch, dass die Einwilligung nicht als einzige Rechtsgrundlage für die Legitimierung der Datenverarbeitung angesehen wurde. Die Entstehungsgeschichte der Richtlinie 95/46/EG zeigt einen relativen Konsens zu den Bedingungen einer gültigen Einwilligung, nämlich: *ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage*. Sie zeigt jedoch auch eine gewisse Unsicherheit in Bezug darauf, wie eine Einwilligung zum Ausdruck gebracht werden kann – ob sie ausdrücklich erfolgen muss, in Schriftform usw. Das wird nachfolgend analysiert.

[10] Gemeinsamer Standpunkt des Rates zu einem Vorschlag für eine Richtlinie des Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, (00/287) COD, angenommen am 15.03.95.

[11] Siehe Seite 4 des Gemeinsamen Standpunkts.

II.2. Das Konzept: Rechtsgrundlage

Allgemeine/spezifische Rechtsgrundlage:

In der Richtlinie wird die Einwilligung sowohl als allgemeine (Artikel 7), als auch als spezifische Rechtsgrundlage für einige besondere Situationen (Artikel 8 Absatz 2 Buchstabe a, Artikel 26 Absatz 1 Buchstabe a) verwendet. Artikel 7 nennt die Einwilligung als erste von sechs verschiedenen Grundlagen für die Legitimierung der Verarbeitung personenbezogener Daten, während Artikel 8 die Möglichkeit bietet, die Einwilligung zur Legitimierung besonderer Kategorien (sensibler) Daten zu nutzten, die ansonsten verboten wären. In diesem letztgenannten Fall sind die Anforderungen an die Einwilligung höher, da sie hier über „ausdrücklich" hinausgehen muss.

Die Richtlinie ermöglicht darüber hinaus das Zusammenspiel mit anderen Rechtsvorschriften, wie in Erwägungsgrund 23 erwähnt: „*Die Mitgliedstaaten können den Schutz von Personen sowohl durch ein allgemeines Gesetz zum Schutz von Personen bei der Verarbeitung personenbezogener Daten als auch durch gesetzliche Regelungen für bestimmte Bereiche ... sicherstellen.*" Dieses System ist in der Praxis sehr komplex: Die Mitgliedstaaten haben eigene Ansätze gewählt und in manchen Fällen hat dies zu Diversität geführt.

Das Konzept der Einwilligung wurde auf nationaler Ebene nicht immer Wort für Wort umgesetzt. In den französischen Datenschutzvorschriften beispielsweise ist die Einwilligung als allgemeines Konzept nicht definiert, ihre Bedeutung wurde aber im Sinne der Definition in der Datenschutzrichtlinie genau und konsequent in der Rechtslehre des Datenschutzbehörde (CNIL) erklärt. Im Vereinigten Königsreich wurde das Konzept der Einwilligung unter Bezugnahme auf den Wortlaut der Richtlinie im Common Law entwickelt. Außerdem wurde die Einwilligung manchmal in bestimmten Bereichen ausdrücklich definiert, beispielsweise im Zusammenhang mit ePrivacy, eGovernment oder eHealth. Das in spezifischen Rechtsvorschriften entwickelte Konzept interagiert folglich mit dem in den allgemeinen Datenschutzvorschriften entwickelten Konzept.

Einwilligung ist ein Grundbegriff, der auch in anderen Rechtsgebieten genutzt wird, insbesondere im Vertragsrecht. In diesem Zusammenhang werden andere als die in der Richtlinie genannten Kriterien herangezogen, um sicherzustellen, dass ein Vertrag rechtsgültig ist, beispielsweise das Alter, unzulässige Beeinflussung usw. Hier liegt kein Widerspruch vor, sondern eine Überschneidung zwischen dem Anwendungsbereich des Zivilrechts und der Richtlinie: Die Richtlinie spricht die allgemeinen Bedingungen für die Gültigkeit einer Einwilligung im Zivilrecht nicht an, schließt sie aber auch nicht aus. Das bedeutet beispielsweise, dass zur Bewertung der Gültigkeit eines Vertrags im Zusammenhang mit Artikel 7 Buchstabe b der Richtlinie zivilrechtliche Anforderungen berücksichtigt werden müssen. Zusätzlich zur Anwendung der allgemeinen Voraussetzungen für die Gültigkeit der Einwilligung im Sinne des Zivilrechts muss die gemäß Artikel 7 Buchstabe a geforderte Einwilligung auch unter Berücksichtigung von Artikel 2 Buchstabe h der Richtlinie ausgelegt werden.

Dieses Zusammenspiel mit anderen Rechtsvorschriften ist nicht nur auf nationaler Ebene, sondern auch auf EU-Ebene sichtbar. Die Bestimmungen der Richtlinie wurden

auch in anderem Zusammenhang ähnlich ausgelegt, wie ein Urteil des Gerichtshofs im Bereich des Arbeitsrechts zeigt[12]: die Einwilligung wurde im Zusammenhang mit der Aufgabe eines sozialen Rechts erforderlich. Das Gericht legte den Begriff der Einwilligung im Zusammenhang mit der Richtlinie 93/104 über bestimmte Aspekte der Arbeitszeitgestaltung aus. Es stellte fest, dass „die Zustimmung des Arbeitnehmers" der Einwilligung des Arbeitnehmers (und nicht einer Gewerkschaft für den Arbeitnehmer) bedarf und interpretierte „Zustimmung" (….) als Zustimmung ohne Zwang und in Kenntnis der Sachlage. Der Gerichtshof vertrat auch die Ansicht, dass die Tatsache, dass ein Arbeitnehmer einen Arbeitsvertrag unterzeichnet, der auf einen Tarifvertrag verweist, der die Überschreitung dieser Arbeitszeit zulässt, nicht die Forderung der ausdrücklichen und freien Zustimmung unter Kenntnis aller Fakten erfüllt. Diese Auslegung der Zustimmung in einem spezifischen Zusammenhang ist sehr eng an den Wortlaut der Richtlinie 95/46/EG angelehnt.

Einwilligung ist nicht die einzige Rechtsgrundlage

Die Richtlinie stellt die Einwilligung eindeutig als eine von mehreren Rechtsgrundlagen dar. Einige Mitgliedstaaten sehen sie jedoch als bevorzugte Grundlage an, manchmal ähnlich eines Verfassungsgrundsatzes, der mit dem Status des Datenschutzes als Grundrecht verbunden ist. Andere Mitgliedstaaten sehen sie als eine von sechs Möglichkeiten an, ein operatives Erfordernis, das nicht wichtiger ist als die anderen Möglichkeiten. Eine Klarstellung der Bedeutung der Einwilligung in Bezug auf andere Rechtsgrundlagen – beispielsweise auf Verträge, Aufgaben öffentlichen Interesses oder rechtmäßige Interessen des für die Datenverarbeitung Verantwortlichen und das Widerspruchsrecht - wird helfen, die Rolle der Einwilligung in speziellen Fällen zu unterstreichen.

Die Reihenfolge, in der die Rechtsgrundlagen in Artikel 7 genannt werden, ist wichtig. Sie bedeutet jedoch nicht, dass die Einwilligung immer die geeignetste Grundlage für die Legitimierung der Verarbeitung personenbezogener Daten ist. Artikel 7 beginnt mit der Einwilligung und listet dann die anderen Grundlagen auf, einschließlich Verträgen und rechtlichen Verpflichtungen und geht langsam über zum Ausgleich der Interessen. Es ist anzumerken, dass bei den anderen fünf Grundlagen nach der Einwilligung die „Notwendigkeit" geprüft werden muss. Dadurch wird der Zusammenhang, in dem sie angewendet werden können, sehr eingeschränkt. Das heißt aber nicht, dass das Erfordernis der Einwilligung mehr Spielraum als die anderen in Artikel 7 genannten Rechtsgrundlagen lässt.

Die Einholung der Einwilligung befreit den für die Datenverarbeitung Verantwortlichen darüber hinaus nicht von seinen Pflichten gemäß Artikel 6 in Bezug auf Gerechtigkeit, Notwendigkeit und Verhältnismäßigkeit sowie Datenqualität. So wäre beispielsweise die Erhebung von personenbezogenen Daten trotz der Einwilligung des Nutzers in die Verarbeitung der Daten nicht zulässig, wenn sie über die Zwecke hinausgeht, für die die Daten erhoben wurden.

Das Einholen der Einwilligung gestattet auch nicht das Umgehen anderer Bestimmungen, wie beispielsweise Artikel 8 Absatz 5. Die Einwilligung kann eine

[12] Urteil des Gerichtshofs (Große Kammer) vom 5. Oktober 2004, Pfeiffer, Roith, Süß, Winter, Nestvogel, Zeller, Döbele in den verbundenen Rechtssachen C-397/01 bis C-403/01.

normalerweise verbotene Verarbeitung von Daten nur unter sehr eingeschränkten Umständen legitimieren. Dies gilt insbesondere in Beziehung auf die Verarbeitung einiger sensibler Daten (Artikel 8) oder auf die Genehmigung der Nutzung personenbezogener Daten für die weitere Verarbeitung, unabhängig davon, ob sie mit dem ursprünglichen Zweck vereinbar ist oder nicht. Prinzipiell darf die Einwilligung nicht als Befreiung von den anderen Datenschutzgrundsätzen gesehen werden, sondern als Schutz. Sie ist in erster Linie eine Rechtsgrundlage und befreit nicht von der Anwendung der anderen Grundsätze.

Die Wahl der passendsten Rechtsgrundlage ist nicht immer einfach, insbesondere die Wahl zwischen Artikel 7 Buchstabe a und Artikel 7 Buchstabe b. Gemäß Artikel 7 Buchstabe b muss die Verarbeitung erforderlich sein für die Erfüllung eines Vertrags oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen. Das sind alle Bereiche. Ein für die Datenverarbeitung Verantwortlicher, der Artikel 7 Buchstabe b als Rechtsgrundlage im Zusammenhang mit dem Schließen eines Vertrags nutzt, kann den Artikel nicht ausweiten, um die Verarbeitung von Daten zu rechtfertigen, die über das erforderliche Maß hinausgeht: er muss die darüber hinaus gehende Verarbeitung durch eine besondere Einwilligung legitimieren, auf die die Anforderungen von Artikel 7 Buchstabe a Anwendung finden. Dies zeigt das Erfordernis der Granularität in Vertragsklauseln. In der Praxis heißt das, dass die Einwilligung möglicherweise als zusätzliche Voraussetzung für einen Teil der Verarbeitung erforderlich ist. Entweder ist die Verarbeitung notwendig für die Erfüllung eines Vertrags oder die Einwilligung (ohne Zwang) muss eingeholt werden.

Bei einigen Transaktionen könnten gleichzeitig eine Reihe von Rechtsgrundlagen Anwendung finden. Anders ausgedrückt heißt das, dass die Datenverarbeitung stets mit mindestens einer Rechtsgrundlage im Einklang stehen muss. Das schließt die gleichzeitige Anwendung mehrerer Rechtsgrundlagen nicht aus, vorausgesetzt, sie werden im richtigen Zusammenhang genutzt. Einige Datenerhebungen und Weiterverarbeitungen sind möglicherweise gemäß dem Vertrag mit der betroffenen Person erforderlich – Artikel 7 Buchstabe b; andere Verarbeitungen können als Ergebnis einer rechtlichen Verpflichtung notwendig sein - Artikel 7 Buchstabe c; die Erhebung zusätzlicher Informationen kann eine gesonderte Einwilligung erfordern - Artikel 7 Buchstabe a; noch andere Verarbeitungen können auch unter dem Ausgleich der Interessen zulässig sein - Artikel 7 Buchstabe f.

Beispiel: Kauf eines Autos
Der für die Datenverarbeitung Verantwortliche kann zur Verarbeitung personenbezogener Daten für verschiedene Zwecke und aufgrund unterschiedlicher Rechtsgrundlagen befugt sein:
- Daten, die für den Kauf des Fahrzeuges erforderlich sind: Artikel 7 Buchstabe b
- Daten zur Bearbeitung der Autopapiere: Artikel 7 Buchstabe c
- Daten für das Kundenmanagement (damit das Auto beispielsweise bei verschiedenen Tochtergesellschaften innerhalb der EU zum Kundendienst gebracht werden kann): Artikel 7 Buchstabe f
- für die Übermittlung der Daten an Dritte für deren eigene Werbeaktivitäten: Artikel 7 Buchstabe a.

II.3. Verwandte Begriffe

Kontrolle

Der Begriff der Einwilligung ist traditionell mit der Idee verknüpft, dass die betroffene Person die Kontrolle über die Verwendung ihrer Daten haben sollte. Aus der Perspektive der Grundrechte ist die durch die Einwilligung ausgeübte Kontrolle ein wichtiges Konzept. Gleichzeitig und auch im Hinblick auf die Grundrechte sollte die Entscheidung einer Person, in die Datenverarbeitung einzuwilligen, strengen Anforderungen unterliegen, wobei insbesondere berücksichtigt werden sollte, dass die betroffene Person dabei möglicherweise auf ein Grundrecht verzichtet.

Auch wenn die Einwilligung wichtig ist, um den betroffenen Personen die Möglichkeit der Kontrolle zu geben, ist sie hierfür nicht die einzige Möglichkeit. Die Richtlinie stellt noch weitere Kontrollmöglichkeiten bereit, insbesondere das Widerspruchsrecht. Das ist jedoch ein anderes Instrument, das während einer anderen Phase der Verarbeitung einzusetzen ist, d.h. nachdem die Verarbeitung begonnen hat. Es basiert auch auf einer anderen Rechtsgrundlage.

Die Einwilligung ist verwandt mit dem Konzept der informationellen Selbstbestimmung. Die Autonomie der betroffenen Person ist sowohl eine Voraussetzung als auch eine Folge der Einwilligung: sie gibt der betroffenen Person Einfluss über die Verarbeitung der Daten. Wie jedoch in dem nächsten Kapitel dargelegt wird, hat dieses Mittel Grenzen und es gibt immer Fälle, in denen die betroffene Person nicht dazu in der Lage ist, eine wirkliche Entscheidung zu treffen. Der für die Datenverarbeitung Verantwortliche möchte die Einwilligung der betroffenen Person möglicherweise dazu nutzen, seine Verantwortung auf sie zu übertragen. Durch ihre Einwilligung in die Veröffentlichung personenbezogener Daten im Internet oder in die Übermittlung der Daten an eine zweifelhafte Rechtspersönlichkeit in einem dritten Staat, erleidet die betroffene Person z.B. möglicherweise einen Schaden und der für die Datenverarbeitung Verantwortliche kann dann argumentieren, dass die betroffene Person genau in diese Veröffentlichung oder Übermittlung eingewilligt hat. Folglich muss daran erinnert werden, dass eine in vollem Maße gültige Einwilligung den für die Datenverarbeitung Verantwortlichen nicht von seinen Pflichten befreit und dass sie nicht eine Verarbeitung zulässig macht, die ansonsten gemäß Artikel 6 der Richtlinie nicht gerechtfertigt wäre.

Das Konzept der Kontrolle stützt sich auch darauf, dass die betroffene Person die Möglichkeit haben sollte, ihre Einwilligung zu widerrufen. Ein Widerruf ist nicht rückwirkend, sondern sollte grundsätzlich jede weitere Verarbeitung der Daten der betroffenen Person durch den für die Datenverarbeitung Verantwortlichen verhindern. Es wird nachfolgend untersucht, wie das in der Praxis funktioniert (Kapitel III).

Transparenz

Eine zweite Dimension der Einwilligung bezieht sich auf die Information: Transparenz gegenüber der betroffenen Person. Kontrolle und eine gültige Einwilligung setzen Transparenz voraus. Transparenz an sich reicht nicht aus, um die Verarbeitung personenbezogener Daten zu legitimieren, aber sie ist eine wesentliche Bedingung um sicherzustellen, dass die Einwilligung gültig ist.

Um gültig zu sein, muss die Einwilligung in Kenntnis der Sachlage erfolgen. Das bedeutet, dass alle erforderlichen Informationen dann zu erteilen sind, wenn die Einwilligung gefordert wird und dass sie alle wesentlichen Aspekte der Verarbeitung ansprechen, die durch die Einwilligung legitimiert werden sollen. Das würde normalerweise alle Informationen abdecken, die in Artikel 10 der Richtlinie aufgeführt sind. Es hängt aber auch davon ab, wann und unter welchen Umständen die Einwilligung gefordert wird.

Unabhängig davon, ob die Einwilligung gegeben wird oder nicht, ist die Transparenz der Datenverarbeitung eine Bedingung der Fairness, die auch nach Bereitstellung der anfänglichen Informationen ihren Wert hat.

Handlung/Zeitablauf: Wege der Einwilligung

Diese dritte Dimension bezieht sich auf den Weise, auf die Kontrolle ausgeübt wird: wie kann die Einwilligung zum Ausdruck gebracht werden und wann sollte sie eingeholt werden, um sicherzustellen, dass tatsächlich eine Einwilligung vorliegt? Diese Fragen haben eine entscheidende Auswirkung auf die Weise, in der eine Einwilligung erteilt und ausgelegt wird.

Auch wenn in der Richtlinie nicht festgelegt wird, zu welchem Zeitpunkt die Einwilligung eingeholt werden sollte, wird durch die Ausdrucksweise in den verschiedenen Bestimmungen eindeutig impliziert, dass die Einwilligung vor Beginn der Verarbeitung einzuholen ist[13]. Das Einholen der Einwilligung vor Beginn der Datenverarbeitung ist eine wesentliche Bedingung der Legitimierung der Datenverarbeitung. Dieser Punkt wird in Kapitel III.B in Bezug auf die Datenschutzrichtlinie für elektronische Kommunikation weiter ausgearbeitet.

Einwilligung als Zustimmung der natürlichen Person in die Verarbeitung ihrer personenbezogenen Daten kann auf unterschiedliche Weise ausgedrückt werden: Artikel 2 Buchstabe h bezieht sich auf jede „Bekundung“; sie muss ohne jeden Zweifel sein (Artikel 7 Buchstabe a) und ausdrücklich in Bezug auf sensible Daten (*im Sinne von* Artikel 8) erfolgen. Es muss jedoch unbedingt betont werden, dass sich die Einwilligung vom Widerspruchsrecht gemäß Artikel 14 unterscheidet. Während der für die Datenverarbeitung Verantwortliche gemäß Artikel 7 Buchstabe a die Daten erst dann verarbeiten kann, wenn er die Einwilligung der betroffenen Person erhalten hat, kann er sie gemäß Artikel 7 Buchstabe f vorbehaltlich bestimmter Voraussetzungen und Schutzbestimmungen verarbeiten, sofern die betroffene Person der Verarbeitung der Daten nicht widersprochen hat. In dem Arbeitspapier 114 der Datenschutzgruppe steht:

[13] Zur Veranschaulichung: in der deutschen Version der Richtlinie (und im Bundesdatenschutzgesetz) wird der Begriff „Einwilligung“ verwendet. Dieser Begriff wird im deutschen Zivilrecht als „vorherige Zustimmung“ definiert.

„Dadurch dass eine ausdrückliche vorherige Willensbekundung verlangt wird, wird faktisch eine Regelung ausgeschlossen, bei der sich eine Person erst gegen die Übermittlung aussprechen kann, nachdem sie bereits stattgefunden hat.“[14].

Aus diesen Gründen sollte das Widerspruchsrecht *im Sinne von* Artikel 14 der Richtlinie nicht mit Einwilligung verwechselt werden. Einwilligung ist eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten gemäß Artikel 7 Buchstabe a, Artikel 8 Absatz 2 Buchstabe a, Artikel 26 Absatz 1 und wird in verschiedenen Bestimmungen der Richtlinie 2002/58/EG vorgesehen.

II.4. Angemessene Nutzung der Einwilligung als Rechtsgrundlage

Es muss betont werden, dass die Einwilligung nicht immer das erste Mittel oder das Mittel der ersten Wahl bei der Legitimierung der Verarbeitung personenbezogener Daten ist.

Die Einwilligung ist manchmal eine schwache Grundlage für die Rechtfertigung der Verarbeitung personenbezogener Daten und sie verliert ihren Wert, wenn sie ausgedehnt oder beschnitten wird, um sie Situationen anzupassen, für die sie niemals gedacht war. Die Verwendung der Einwilligung „im richtigen Zusammenhang“ ist wesentlich. Wenn sie unter Umständen genutzt wird, für die sie nicht geeignet ist, da das Vorliegen der für eine gültige Einwilligung erforderlichen Elemente unwahrscheinlich ist, würde dies die Einwilligung sehr anfällig machen. In der Praxis würde das die Position der betroffenen Person *schwächen*.

Dieser Ansatz wurde bereits von der Datenschutzgruppe und dem EDSP in ihren Beiträgen zu den Diskussionen um die neue Datenschutzrichtlinie dargelegt. Es wurde insbesondere Folgendes festgestellt: *„… ist nicht immer klar, wodurch sich eine echte, eindeutige Einwilligung auszeichnet. Bestimmte für die Verarbeitung Verantwortliche nutzen diese Ungewissheit aus und stützen sich auf Methoden, die für die Erteilung einer echten, eindeutigen Einwilligung nicht geeignet sind*“[15] und verstoßen so gegen die Bestimmungen im Sinne von Artikel 6 der Richtlinie. Entsprechend hat die Artikel-29-Datenschutzgruppe Folgendes angemerkt: *„In vielen Fällen jedoch übersteigt die Komplexität von Datenerhebungsverfahren, Wirtschaftsmodellen, Käufer-Verkäuferbeziehungen und technologischen Anwendungen die Fähigkeit oder Bereitschaft des Einzelnen, aktiv über die Verwendung und gemeinsame Nutzung der Informationen zu entscheiden.“*[16]

Folglich ist es wichtig, die Grenzen der Einwilligung klarzustellen und sicherzustellen, dass nur eine Einwilligung, die nach dem Gesetz ausgelegt wird, auch als solche angesehen wird.[17]

---

[14] WP114 – Arbeitspapier der Artikel-29-Datenschutzgruppe über eine Gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995.

[15] Stellungnahme des Europäischen Datenschutzbeauftragten vom 14. Januar 2011 zur Mitteilung der Kommission „Gesamtkonzept für den Datenschutz in der Europäischen Union“.

[16] „Die Zukunft des Datenschutzes: Gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten”, 1. Dezember 2009, WP 168.

[17] Stellungnahme des Europäischen Datenschutzbeauftragten vom 14. Januar 2011, op.cit.

III. Analyse von Vorschriften

In Kapitel III.A liegt der Schwerpunkt dieser Analyse auf der Richtlinie 95/46/EG. In Kapitel III.B werden einige wichtige Teile der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) analysiert. Es sollte angemerkt werden, dass sich die beiden Richtlinien nicht ausschließen. Die allgemeinen Bedingungen für die Zulässigkeit der Einwilligung, wie sie in Richtlinie 95/46/EG vorgesehen sind, finden sowohl in der Offline- als auch in der Online-Umgebung Anwendung. Richtlinie 2002/58/EG spezifiziert diese Bedingungen für einige ausdrücklich identifizierte Online-Dienste. Sie tut dies immer angesichts der allgemeinen Bedingungen der Datenschutzrichtlinie.

III.A Richtlinie 95/46/EG

Das Konzept der „Einwilligung der betroffenen Person" wird in Artikel 2 Buchstabe h definiert und im Folgenden in den Artikeln 7, 8 und 26 verwendet. Die Funktion der Einwilligung wird auch in den Erwägungsgründen 30 und 45 genannt. Diese Bestimmungen und alle einschlägigen Details werden in diesem Abschnitt gesondert diskutiert.

III.A.1. Artikel 2 Buchstabe h

Gemäß Artikel 2 Buchstabe h bedeutet die Einwilligung der betroffenen Person *„jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden."* Diese Definition enthält verschiedene Schlüsselelemente, die nachfolgend besprochen werden.

„… jede Willensbekundung …"

Prinzipiell gibt es keine Einschränkung in Bezug auf die Form, die eine Einwilligung annehmen kann. Damit die Einwilligung gemäß der Richtlinie gültig ist, sollte sie jedoch eine Willensbekundung sein. Selbst wenn sie „jede" Form der Willensbekundung sein kann, sollte klar sein, was genau unter die Definition von Willensbekundung fällt.

Die Form der Willensbekundung (d.h. wie der Wille ausgedrückt wird) ist in der Richtlinie nicht definiert. Aus Gründen der Flexibilität wurde die „schriftliche" Einwilligung nicht in den endgültigen Text übernommen. Es sollte betont werden, dass die Richtlinie „jede" Willensbekundung umfasst. Dies ermöglicht eine breite Auslegung der Geltung einer solchen Willensbekundung. Die minimale Willensbekundung könnte eine Art von Zeichen sein, das ausreichend klar ist, um die Wünsche der betroffenen Person zum Ausdruck zu bringen und für den für die Datenverarbeitung Verantwortlichen verständlich zu sein. „Willensbekundung" deutet darauf hin, dass eine Handlung nötig ist (im Gegensatz zu einer Situation, in der eine Einwilligung aus dem Ausbleiben einer Handlung gefolgert werden kann).

Eine Einwilligung sollte jede Willensbekundung umfassen, mit der die betroffene Person ihre Zustimmung *zum Ausdruck bringt*: sie könnte eine handschriftliche Unterschrift am Ende eines Papiervordrucks darstellen. Sie könnte aber auch eine mündliche Erklärung der Zustimmung oder ein Verhalten sein, aus dem zu Recht die

Einwilligung geschlossen werden kann. Über das klassische Beispiel einer Unterschrift hinaus, könnte es also durchaus in den Bereich der Definition fallen, wenn man eine Geschäftskarte in eine Glasschale fallen lässt. Dasselbe gilt auch, wenn eine natürliche Person ihren Namen und ihre Anschrift an eine Organisation sendet, um Informationen über diese zu erhalten. In diesem Fall kann die Handlung so verstanden werden, dass in die Verarbeitung der Daten insoweit eingewilligt wird, als diese zur Bearbeitung und Beantwortung der Anfrage erforderlich ist.

In ihrer Stellungnahme zur Nutzung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen (WP115) hat die Datenschutzgruppe bewertet, wie es natürlichen Personen ermöglicht werden soll, in die Bereitstellung eines Dienstes einzuwilligen, der die automatische Standortbestimmung einer Person erfordert (z.B. die Möglichkeit, eine bestimmte Nummer anzurufen, um eine Wettervorhersage für den jeweiligen Standort zu erhalten). In diesem Fall wurde Folgendes anerkannt: sofern die Nutzer im Voraus vollständige Informationen über die Verarbeitung ihrer Standortdaten erhalten, würde das Anrufen der entsprechenden Nummer bedeuten, dass die Einwilligung zur Standortbestimmung erteilt wird.

Beispiel: Bluetooth Werbetafeln
Derzeit wird ein Werbemittel entwickelt, das aus Tafeln besteht, die Nachrichten senden und den Aufbau einer Bluetooth-Verbindung erbitten, um den vorbeigehenden Personen Anzeigen zu schicken. Die Nachrichten werden an die Personen geschickt, die die Bluetooth-Funktion ihres Handys aktiviert haben. Lediglich die Aktivierung der Bluetooth-Funktion stellt keine gültige Einwilligung dar (die Bluetooth-Funktion könnte nämlich auch für andere Zwecke aktiviert sein). Wenn andererseits eine Person über diese Leistung informiert ist und sich mit ihrem Handy dieser Tafel bis auf ein paar Zentimeter nähert, ist das normalerweise eine Willensbekundung: so wird gezeigt, welche Personen wirklich daran interessiert sind, die Anzeigen zu erhalten. Man sollte nur bei diesen Personen von einer Einwilligung ausgehen und nur diesen Personen sollten die Nachrichten auf das Handy geschickt werden.

Es ist fraglich, ob das Fehlen einer Handlung – oder besser gesagt: ein passives Verhalten – auch als eine Willensbekundung unter sehr spezifischen Umständen angesehen werden kann (d.h. in einem vollkommen eindeutigen Zusammenhang). Der Begriff „Willensbekundung“ ist dehnbar, aber er scheint eine Handlung zu fordern. Andere Elemente der Definition von Einwilligung und die zusätzliche Anforderung von Artikel 7 Buchstabe a, dass die Einwilligung ohne jeden Zweifel erfolgen muss, stützen diese Auslegung. Das Erfordernis, dass die betroffene Person ihre Einwilligung „zum Ausdruck bringen“ muss, scheint darauf hinzudeuten, dass eine einfache Untätigkeit nicht ausreicht und dass irgendeine Art von Handlung für die Einwilligung erforderlich ist. Es sind jedoch verschiedene Handlungen möglich, die „im jeweiligen Zusammenhang“ bewertet werden müssen.

In der Praxis erschwert es das Fehlen eines aktiven Verhaltens von Seiten der betroffenen Person dem für die Datenverarbeitung Verantwortlichen, festzustellen, ob das Schweigen Zustimmung oder Einwilligung bedeutet. Der für die Datenverarbeitung Verantwortliche hat beispielsweise in dem folgenden Fall nicht die erforderliche Sicherheit, um eine Einwilligung zu vermuten: Stellen wir uns folgende Situation vor:

Auf einen Brief an die Kunden, in dem sie über einen geplanten Datentransfer informiert werden, wenn sie nicht innerhalb von zwei Wochen widersprechen, antworten nur 10% der Kunden. In diesem Beispiel ist es anfechtbar, dass die 90%, die nicht geantwortet haben, dem Datentransfer tatsächlich zustimmen. In solchen Fällen liegt dem für die Datenverarbeitung Verantwortlichen keine klare Willensbekundung der betroffenen Personen vor. Darüber hinaus hat er keinen Beweis und er kann folglich nicht nachweisen, dass er die Einwilligung erhalten hat. In der Praxis macht es die Mehrdeutigkeit einer passiven Antwort schwierig, die Erfordernisse der Richtlinie zu erfüllen.

„… ohne Zwang …“

Eine Einwilligung kann nur dann gültig sein, wenn die betroffene Person eine tatsächliche Wahlmöglichkeit hat und kein Risiko einer Täuschung, Einschüchterung, Nötigung oder beträchtlicher negativen Folgen besteht, wenn sie die Einwilligung nicht erteilt. Wenn die Folgen einer Einwilligung die Wahlfreiheit einer natürlichen Person einschränken, wäre die Einwilligung nicht ohne Zwang. Die Richtlinie selbst sieht in Artikel 8 Absatz 2 Buchstabe a vor, dass in einigen, von den Mitgliedstaaten festzulegenden Fällen, das Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten durch die Einwilligung der betroffenen Person nicht aufgehoben werden kann.

Ein Beispiel für oben Stehendes ist der Fall, in dem die betroffene Person unter dem Einfluss des für die Datenverarbeitung Verantwortlichen steht, beispielsweise wenn ein Arbeitsverhältnis vorliegt. In diesem Fall befindet sich die betroffene Person möglicherweise aufgrund der Art der Beziehung oder aufgrund spezieller Umstände in einem Abhängigkeitsverhältnis von dem für die Datenverarbeitung Verantwortlichen – auch wenn dies nicht immer der Fall ist – und befürchtet womöglich, bei einer Ablehnung der Datenverarbeitung anders behandelt zu werden.

Die Datenschutzgruppe hat in mehreren Stellungnahmen die Grenzen der Einwilligung in Fällen untersucht, in denen sie nicht ohne Zwang gegeben werden kann. Das war insbesondere der Fall in ihrer Stellungnahme zu elektronischen Patientenakten (WP131) zur Verarbeitung personenbezogener Daten von Beschäftigen (WP48) und zur Verarbeitung personenbezogener Daten durch die Welt-Anti-Doping-Agentur (WP162).

In WP131erwähnt die Datenschutzgruppe Folgendes: *„Ohne Zwang bedeutet, dass sich eine Person aus freien Stücken und im Vollbesitz ihrer geistigen Kräfte ohne jeglichen sozialen, finanziellen, psychologischen oder sonstigen Druck von außen entscheiden kann. Erfolgt die Einwilligung nur, weil mit Nichtbehandlung oder einer schlechteren medizinischen Behandlung gedroht wird, kann von einer Einwilligung aus freien Stücken nicht die Rede sein. ... Wenn eine medizinische Fachkraft aus medizinisch indizierten Gründen in einer bestimmten Situation nicht anders kann als personenbezogene Daten in einer elektronischen Patientenakte zu verarbeiten, ist es nach Meinung der Datenschutzgruppe irreführend, wenn sie dazu die Einwilligung des Betreffenden einholt, um die Verarbeitung zu legitimieren. Eine Einwilligung sollte auf die Fälle beschränkt werden, in denen die betreffende Person tatsächlich frei entscheiden kann und anschließend die Einwilligung ohne irgendwelche Nachteile zurückziehen kann.“*[18]

[18] WP162 zu WADA kommt zu derselben Schlussfolgerung: *„Aufgrund der Sanktionen und Konsequenzen, die verhängt werden können, wenn sich ein Teilnehmer weigert, den Verpflichtungen des Codes (zum Beispiel der Übermittlung von*

Wenn die Datenverarbeitung auf der Basis einer anderen Rechtsgrundlage fortgeführt wird, nachdem die Einwilligung zurückgezogen wurde, könnten Zweifel an der ursprünglichen Verwendung der Einwilligung als erste Rechtsgrundlage entstehen: wenn die Verarbeitung von Anfang an unter Verwendung der anderen Rechtsgrundlage erfolgen konnte, könnte es als irreführend oder grundsätzlich ungerecht angesehen werden, die Person mit einer Situation zu konfrontieren, in der sie um die Einwilligung in die Datenverarbeitung gebeten wird. Das wäre bei einer Änderung der Umstände etwas anderes, beispielsweise wenn eine neue Rechtsgrundlage im Verlauf der Verarbeitung entstehen würde, wie ein neues Gesetz, das die betroffene Datenbank reguliert. Wenn diese neue Rechtsgrundlage rechtsgültig auf die Datenverarbeitung angewendet werden kann, kann die Verarbeitung fortgesetzt werden. In der Praxis treten solche Fälle jedoch nur selten auf. Prinzipiell kann die Einwilligung als unzureichend angesehen werden, wenn kein wirkungsvoller Widerruf gestattet ist.

Die Datenschutzgruppe hat in Bezug auf die Auslegung der Einwilligung ohne Zwang durch Beschäftigte deutlich Stellung bezogen:[19] *„Wird eine Einwilligung vom Beschäftigten erbeten und ist die Nichteinwilligung mit tatsächlichen oder potenziellen Nachteilen für ihn verbunden, so ist eine solche Einwilligung … nicht gültig im Sinne von Artikel 7 oder Artikel 8, da sie nicht freiwillig erfolgt. Wenn der Arbeitnehmer keine Möglichkeit zur Ablehnung hat, kann nicht von Einwilligung gesprochen werden … Probleme entstehen dort, wo die Einwilligung Einstellungsvoraussetzung ist. Der Arbeitnehmer hat theoretisch das Recht, die Einwilligung zu verweigern, aber er muss in diesem Fall damit rechnen, dass er die Chance auf eine bestimmte Stelle verliert. Unter solchen Umständen wird die Einwilligung nicht freiwillig erteilt und ist daher nicht gültig. Noch eindeutiger ist die Situation wenn, wie es häufig der Fall ist, alle Arbeitgeber die gleichen oder ähnliche Einstellungsvoraussetzungen festlegen.“*

Beispiel: Bilder im Intranet

Das folgende Beispiel zeigt, dass die Einwilligung von Beschäftigten gültig sein kann: Ein Unternehmen entschließt sich zur Einrichtung eines Intranets, in dem die Namen und wichtigsten Funktionen der Beschäftigten aufgeführt sind. Jeder Beschäftigte wird gefragt, ob er zusammen mit seinem Namen ein Bild hochgeladen haben möchte. Diejenigen, die ihr Bild im Intranet wollen, werden dazu aufgefordert, an eine bestimmte Adresse ein Bild zu schicken. Nach Erhalt der entsprechenden Informationen wird es als Einwilligung angesehen, wenn eine Person ein Bild sendet. Wenn das Unternehmen digitale Fotos aller Beschäftigten hat und jeden um die Einwilligung bittet, sein Foto für die oben genannten Zwecke hochladen zu dürfen, wird bei jedem Beschäftigen, der eine Schaltfläche anklickt, um seine Einwilligung zum Ausdruck zu bringen, von einer gültigen Einwilligung ausgegangen. In beiden Fällen wird die Entscheidung der Beschäftigten, ob ihre Bilder im Intranet erscheinen oder nicht, vollumfänglich respektiert.

Daten über den Aufenthaltsort und die Erreichbarkeit) nachzukommen, gelangt die Arbeitsgruppe zu dem Schluss, dass die Zustimmung keineswegs ohne Zwang gegeben wird.“

[19] WP48 zur Verarbeitung personenbezogener Daten von Beschäftigten. WP114 – Arbeitspapier der Artikel-29-Datenschutzgruppe über eine Gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995 ist hier ebenfalls einschlägig.

Das Umfeld Beschäftigung bedarf besonderer Diskussionen: die kulturellen und sozialen Aspekte des Beschäftigungsverhältnisses spielen hier genauso eine Rolle wie die Art und Weise, in der die Datenschutzprinzipien mit anderen Rechtsvorschriften zusammenspielen. In Bezug auf die Beschäftigung können personenbezogene Daten für verschiedene Zwecke verarbeitet werden:

- Daten, die für die Erfüllung der Aufgaben durch den Beschäftigten erforderlich sind: Anwendung von Artikel 7 Buchstabe b - Notwendigkeit für den Vertrag
- Zur Ermittlung des Aktienbezugsrechts des Beschäftigten: die Verarbeitung kann entweder auf der Grundlage der Einwilligung erfolgen - Artikel 7 Buchstabe a, oder sie wird als den verwaltungstechnischen Aspekten der vertraglichen Arbeitsbeziehungen innewohnend angesehen - Artikel 7 Buchstabe b
- Verarbeitung der Sozialversicherungsnummer für Sozialversicherungszwecke: Artikel 7 Buchstabe c – rechtliche Verpflichtung oder möglicherweise Artikel 8 Buchstabe b – Pflichten auf dem Gebiet des Arbeitsrechts
- Verarbeitung ethnischer Daten: in einigen Ländern könnte dies auch eine Pflicht aus dem Arbeitsrecht sein - Artikel 8 Buchstabe b, während sie in anderen Ländern strikt verboten ist.

Auch wenn stark vermutet werden kann, dass die Einwilligung in solchen Zusammenhängen eine schwache Rechtsgrundlage ist, schließt dies ihre Anwendung dennoch nicht vollständig aus, vorausgesetzt, es liegen ausreichend Garantien vor, dass die Einwilligung wirklich ohne Zwang erfolgt.

Während eine Situation der Abhängigkeit oft der wichtigste Grund ist, der eine Einwilligung ohne Zwang verhindert, können auch andere vertragliche Elemente die Entscheidung der betroffenen Person beeinflussen. Diese Elemente können beispielsweise eine finanzielle, emotionale oder praktische Dimension aufweisen. Die betroffene Person kann auch durch die Tatsache beeinflusst werden, dass die Datenerhebung von einer öffentlichen Stelle durchgeführt wird. Es kann jedoch schwierig sein, zu entscheiden, ob etwas nur ein einfacher Anreiz ist oder sich tatsächlich auf die Wahlfreiheit der betroffenen Person auswirkt. Anhand der nachfolgenden Beispiele soll aufgezeigt werden, welche Anstrengungen oder Kosten die Entscheidungen der betroffenen Personen beeinflussen könnten.

Beispiel – elektronische Patientendaten
In vielen Mitgliedstaaten werden elektronische Zusammenfassungen der Patientenakten erstellt. Diese ermöglichen dem Erbringer von Gesundheitsleistungen den Zugriff auf Schlüsselinformationen, wo auch immer der Patient eine Behandlung benötigt.
- Im ersten Szenario ist die Erstellung der Zusammenfassung vollständig freiwillig und der Patient wird auch dann noch behandelt, wenn er dieser elektronischen Zusammenfassung nicht zugestimmt hat. In diesem Fall wird die Einwilligung in die Erstellung der Zusammenfassung ohne Zwang erteilt, da der Patient keine Nachteile erleidet, wenn er die Einwilligung nicht gibt oder ihr widerspricht.
- Im zweiten Fall gibt es einen kleinen finanziellen Anreiz, sich für die elektronische Patientenakte zu entscheiden. Patienten, die nicht einwilligen, erleiden keinen Nachteil, da sich die Kosten für sie nicht ändern. Auch hier kann man sagen, dass ihre Entscheidung für oder gegen das neue System ohne Zwang erfolgt.

- Im dritten Szenario müssen Patienten, die sich gegen die elektronische Patientenakte entscheiden, beträchtliche Zusatzkosten im Vergleich zu dem vorherigen Tarifsystem tragen. Außerdem werden ihre Akten deutlich langsamer bearbeitet. Das bedeutet für diejenigen, die ihre Einwilligung nicht erteilen, einen klaren Nachteil. Ziel ist es, alle Bürger bis zu einem bestimmten Stichtag in dem elektronischen Gesundheitssystem zusammenzufassen. Die Einwilligung ist folglich nicht in ausreichendem Maße ohne Zwang. Deshalb sollte auch nach anderen Rechtsgrundlagen für die Verarbeitung der personenbezogenen Daten gesucht werden oder die Anwendung von Artikel 8 Absatz 3 der Richtlinie 95/46/EG geprüft werden.

Beispiel: Körperscanner

In einigen öffentlichen Bereichen kommt es zum Einsatz von Körperscannern, insbesondere in Flughäfen im Zugang zum Abfertigungsbereich. Angesichts der Tatsache, dass die Passagierdaten zum Zeitpunkt des Scannens verarbeitet werden[20], muss die Verarbeitung eine der Rechtsgrundlagen gemäß Artikel 7 erfüllen. Manchmal wird es so dargestellt, als ob die Passagiere die Wahlmöglichkeit hätten, durch Körperscanner zu gehen oder nicht. Das impliziert, dass die Verarbeitung durch ihre Einwilligung gerechtfertigt sein könnte. Wenn sich ein Passagier jedoch weigert, durch den Körperscanner zu gehen, wird er womöglich verdächtigt oder es werden weitere Kontrollen durchgeführt, wie beispielsweise eine Leibesvisitation. Viele Passagiere werden in das Scannen einwilligen, weil sie dadurch mögliche Probleme oder Verzögerungen vermeiden. Denn ihr vorrangiges Ziel ist es, ihren Flug rechtzeitig zu erreichen. Eine solche Einwilligung erfolgt nicht in ausreichendem Maße ohne Zwang. Da nachgewiesen werden muss, dass eine solche Verarbeitung erforderlich ist (aus Gründen der öffentlichen Sicherheit), sollte die Rechtsgrundlage nicht in Artikel 7 Absatz a gesucht werden, sondern in einer Rechtsvorschrift des Gesetzgebers – Artikel 7 Buchstabe c oder e – die die Passagiere zur Kooperation verpflichtet. Die Grundlage für ein Screening mit Körperscannern sollte also eine Rechtsvorschrift sein: Diese Rechtsvorschrift könnte immer noch die Wahl zwischen dem Scannen und einem Abtasten bieten, allerdings würde diese Wahl dem Einzelnen nur als Ergänzung im Rahmen von zusätzlichen Maßnahmen angeboten werden.

Die Natur des für die Datenverarbeitung Verantwortlichen kann bei der Wahl der Rechtsgrundlage für die Verarbeitung personenbezogener Daten ebenfalls entscheidend sein. Dies gilt insbesondere für für die Datenverarbeitung Verantwortliche im öffentlichen Sektor, wo die Verarbeitung personenbezogener Daten normalerweise mit der Ausübung einer rechtlichen Verpflichtung gemäß Artikel 7 Buchstabe c oder der Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt (Artikel 7 Buchstabe e), verbunden ist. Folglich ist die Einwilligung der betroffenen Person zur Legitimierung der Datenverarbeitung nicht die angemessene Rechtsgrundlage. Dies ist besonders eindeutig im Fall der Verarbeitung personenbezogener Daten durch öffentliche Behörden, die mit maßgeblichen Befugnissen ausgestattet sind, wie beispielsweise Strafverfolgungsbehörden, die gemäß

[20] Siehe den Brief des Vorsitzenden der Artikel-29-Datenschutzgruppe vom 11. Februar 2009 an Herrn Daniel CALLEJA CRESPO, Direktor der GD TREN über Körperscanner, als Antwort auf die Konsultation der Kommission zu „den Auswirkungen der Verwendung von Körperscannern im Bereich der Flugsicherheit auf die Menschenrechte, die Privatsphäre, die menschliche Würde, die Gesundheit und den Datenschutz“. Verfügbar unter: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2009-others_en.htm.

ihren Aufgaben im Bereich der polizeilichen und justiziellen Tätigkeiten handeln. Polizeibehörden können sich nicht auf die Einwilligung der betroffenen Personen in Maßnahmen verlassen, die nicht vorgesehen sind oder die ansonsten nicht gesetzlich zugelassen wären.

Es sollte dennoch anerkannt werden, dass der Einzelne nicht immer zur Mitarbeit verpflichtet ist, auch wenn die Staaten möglicherweise gesetzlich zur Verarbeitung der personenbezogenen Daten verpflichtet sind. Es mag Fälle geben, in denen betroffenen Personen „Dienste mit Zusatznutzen" zur Verfügung gestellt werden, die sie nutzen können oder nicht. In den meisten Fällen ist die Verarbeitung aber tatsächlich verpflichtend. Es ist häufig nicht so einfach, zu unterscheiden, ob sich die Verarbeitung personenbezogener Daten durch öffentliche Stellen rechtmäßig auf die Einwilligung des Einzelnen stützt. Die Verarbeitung personenbezogener Daten im öffentlichen Sektor umfasst also häufig Mischformen, die zu Unsicherheit und Missbrauch führen können, wenn sie fälschlicherweise durch eine Einwilligung gerechtfertigt werden.

In Ausnahmefällen kann die Einwilligung eine gültige Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Staaten sein. Es sollte dennoch von Fall zu Fall entscheiden werden, ob die Einwilligung wirklich in ausreichendem Maße ohne Zwang erfolgt. Die nachfolgenden Beispiele zeigen, dass die Rechtsgrundlage für die Legitimierung der Verarbeitung eher die Einhaltung einer rechtlichen Verpflichtung gemäß Artikel 7 Buchstabe c ist oder die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt (Artikel 7 Buchstabe e), als die Einwilligung, wenn es sich bei dem für die Datenverarbeitung Verantwortlichen um eine öffentliche Stelle handelt.

Beispiel: e-Government
In den Mitgliedstaaten werden neue Personalausweise entwickelt, bei denen in einem Chip weitere Funktionen eingebettet sind. Es ist möglicherweise nicht verpflichtend, die elektronischen Leistungen der Karte zu aktivieren. Eine fehlende Aktivierung könnte den Nutzer aber vom Zugang zu bestimmten Verwaltungsdienstleistungen ausschließen, die schwierig auf einem anderen Weg zu erhalten sind (Online-Transfer mancher Dienste, kürzere Öffnungszeiten). Die Einwilligung kann nicht als Rechtsgrundlage für die Legitimierung der Verarbeitung angegeben werden. In diesem Fall sollte das Gesetz über die Entwicklung der elektronischen Dienste zusammen mit den entsprechenden Sicherheitsvorkehrungen die Grundlage sein.

Beispiel: PNR-Daten
Es wurde die Frage diskutiert, ob die Einwilligung von Passagieren rechtsgültig zur Legitimierung der Übermittlung von Buchungsdaten („PNR-Daten") von europäischen Fluggesellschaften an die US-Behörden herangezogen werden kann. Die Datenschutzgruppe ist der Ansicht, dass die Einwilligung der Passagiere nicht ohne Zwang erfolgen kann, da die Fluggesellschaften dazu verpflichtet sind, die Daten vor Abflug zu übermitteln. Folglich haben die Fluggäste keine wirkliche Wahl, wenn sie fliegen möchten.[21] Die Rechtsgrundlage ist in diesem Fall nicht die Einwilligung der Passagiere, sondern stattdessen gemäß Artikel 7 Buchstabe c die Verpflichtung aus dem internationalen Abkommen zwischen der EU und den USA über die Verarbeitung und Übermittlung von Passagierdatensätzen (PNR Daten).

[21] Siehe die Stellungnahme 6/2002 der Artikel-29-Datenschutzgruppe zur Übermittlung von Informationen aus Passagierlisten und anderen Daten von Fluggesellschaften an die Vereinigten Staaten.

Beispiel: Volkszählung
Im Rahmen einer Volkszählung wird die Bevölkerung zur Beantwortung einer Reihe von Fragen zu ihrer persönlichen und beruflichen Situation aufgefordert. Die Beantwortung dieser Fragen ist verpflichtend. Darüber hinaus wird bei der Volkszählung auch eine Frage gestellt, deren Beantwortung eindeutig als freiwillig gekennzeichnet ist. Sie bezieht sich auf das von der Person genutzte Transportmittel. Auch wenn eindeutig keine zwangsfreie Einwilligung für den größten Teil der Volkszählung vorliegt, gibt es die freie Wahl für die Beantwortung dieser letzten freiwilligen Frage. Das sollte nicht die Tatsache verschleiern, dass der Hauptzweck, den die Staaten mit dieser Art Fragebogen verfolgen, das Einholen von Antworten ist. Allgemein gesprochen ist die Einwilligung in diesem Zusammenhang keine gültige Rechtsgrundlage.

„… für den konkreten Fall …"

Damit eine Einwilligung gültig ist, muss sie für den konkreten Fall erfolgen. Das heißt mit anderen Worten, dass eine pauschale Einwilligung ohne Angabe des genauen Zwecks der Verarbeitung nicht zulässig ist.

Damit sie für den konkreten Fall ist, muss die Einwilligung verständlich sein: sie sollte sich eindeutig und genau auf den Anwendungsbereich und die Folgen der Datenverarbeitung beziehen. Sie kann nicht für Verarbeitungsaktivitäten gelten, die in keinster Weise eingegrenzt sind. Das heißt mit anderen Worten, dass der Kontext, in dem die Einwilligung gilt, eingeschränkt ist.

Die Einwilligung muss in Bezug auf die verschiedenen, klar herausgestellten Aspekte der Verarbeitung gegeben werden. Dazu gehört insbesondere eine Angabe der zu verarbeitenden Daten und der Zweck der Verarbeitung. Diese Einigung sollte auf den angemessenen Erwartungen der Parteien basieren. Die „Einwilligung für den konkreten Fall" ist folglich untrennbar mit der Tatsache verbunden, dass die Einwilligung in Kenntnis der Sachlage erfolgen muss. Es gibt die Anforderung der Granularität der Einwilligung in Bezug auf die verschiedenen Elemente, die die Datenverarbeitung ausmachen. Sie kann nicht „alle rechtmäßigen Zwecke" abdecken, die der für die Datenverarbeitung Verantwortliche verfolgt. Die Einwilligung sollte sich auf die Verarbeitung beziehen, die in Bezug auf den Zweck angemessen und erforderlich ist.

Prinzipiell sollte es ausreichen, wenn der für die Datenverarbeitung Verantwortliche die Einwilligung einmal für verschiedene Verarbeitungstätigkeiten einholt, wenn die betroffene Person diese Tätigkeiten vernünftigerweise erwarten kann.

Kürzlich hat der Gerichtshof eine Vorabentscheidung[22] in Bezug auf Artikel 12 Absatz 2 der Datenschutzrichtlinie für elektronische Kommunikation erlassen, die sich auf die Notwendigkeit einer erneuten Zustimmung der Teilnehmer

[22] Urteil des Gerichtshofs vom 5. Mai 2011, Deutsche Telekom AG (Rechtssache C-543/09). Die Rechtssache begann mit der Anrufung des deutschen Bundesverwaltungsgerichts in Bezug auf Telefonverzeichnisse und insbesondere in Bezug auf die Auslegung von Artikel 25 Absatz 2 der Universaldienstrichtlinie (2002/22/EG) und Artikel 12 Absatz 2 der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG). Die Rechtssache hat eindeutig Bezug auf die Sonderrolle der Teilnehmerverzeichnisse in der Universaldienstrichtlinie.

bezieht, die bereits in die Veröffentlichung ihrer personenbezogenen Daten in einem Teilnehmerverzeichnis eingewilligt hatten, damit ihre Daten für die Veröffentlichung in einem anderen Teilnehmerverzeichnis übermittelt werden. Der Gerichtshof war der Ansicht, dass keine erneute Zustimmung des Teilnehmers in die Übermittlung derselben Daten erforderlich ist, sofern der Teilnehmer richtig darüber informiert wurde, dass seine personenbezogenen Daten an ein drittes Unternehmen übermittel werden können und der Teilnehmer bereits in die Veröffentlichung der Daten in einem solchen Verzeichnis zugestimmt hat und *sofern zum anderen gewährleistet ist, dass die betreffenden Daten nach ihrer Weitergabe nicht für andere Zwecke als diejenigen verwendet werden, für die sie im Hinblick auf ihre erste Veröffentlichung erhoben wurden (Randnummer 65).*

Es kann dennoch eine eindeutige Einwilligung erforderlich sein, wenn der für die Datenverarbeitung Verantwortliche die Daten für verschiedene Zwecke verarbeiten möchte. Eine Einwilligung könnte beispielsweise die Information sowohl über neue Produkte als auch über Sonderwerbeaktionen umfassen, da man davon ausgehen kann, dass das vernünftigerweise von der betroffenen Person erwartet wird. Es sollte jedoch eine gesonderte und zusätzliche Einwilligung eingeholt werden, um die Übermittelung der Daten der betroffenen Person an Dritte zu genehmigen. Die Notwendigkeit der Granularität bei der Einholung der Einwilligung sollte von Fall zu Fall bewertet werden und von dem Zweck/den Zwecken oder dem Datenempfänger abhängen.

Es sollte daran erinnert werden, dass die Verarbeitung verschiedene Rechtsgrundlagen haben kann: einige Daten werden möglicherweise verarbeitet, da sie im Rahmen eines Vertrags mit der betroffenen Person benötigt werden, beispielsweise im Rahmen von Product Fulfilment und Service Management. Eine gesonderte Einwilligung kann für die Verarbeitung erforderlich sein, die über das hinausgeht, was für die Erfüllung des Vertrags erforderlich ist, beispielsweise zur Bewertung der Zahlungskapazität (Kreditprüfung) der betroffenen Person.

Die Datenschutzgruppe hat diesen Aspekt der Einwilligung in WP131 zu elektronischen Patientenakten (EPA) geklärt: Die Einwilligung „für den konkreten Fall“ muss sich auf eine genau umrissene konkrete Situation beziehen, in der die Verarbeitung der medizinischen Daten erfolgen soll. Eine „pauschale Zustimmung“ der betroffenen Person beispielsweise zur Erfassung ihrer medizinischen Daten in einer elektronischen Patientenakte und zur anschließenden Weitergabe dieser medizinischen Daten an in die Behandlung eingebundene medizinische Fachkräfte wäre keine Einwilligung im Sinne von Artikel 2 Buchstabe h der Richtlinie.

Dieselbe Begründung wird in WP115 zur Nutzung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen zum Ausdruck gebracht: *„Mit dieser Definition wird ausdrücklich ausgeschlossen, dass die Einwilligung im Zuge der Annahme der allgemeinen Bedingungen für die Nutzung der angebotenen elektronischen Kommunikationsdienste erteilt wird. … Abhängig von der Art der angebotenen Dienste kann sich die Einwilligung jedoch auf einen spezifischen Vorgang beziehen oder sie kann die Zustimmung zu einer kontinuierlichen Standortbestimmung darstellen.“*

In der in Kapitel II unter „Rolle der Einwilligung“ genannten Gerichtsentscheidung wird in der Begründung auch auf der Notwendigkeit einer Einwilligung für den konkreten Fall bestanden, selbst wenn der Wortlaut „für den konkreten Fall“ nicht genutzt wurde:

„Es genügt (…) nicht, dass der Arbeitsvertrag des Betroffenen auf einen Tarifvertrag verweist, der eine solche Überschreitung erlaubt“.

Beispiel: soziale Netzwerke
Der Zugang zu sozialen Netzwerken hängt häufig von der Einwilligung in verschiedene Arten der Verarbeitung personenbezogener Daten ab.

Der Nutzer muss möglicherweise ohne nähere Spezifikationen oder Alternativmöglichkeiten in den Empfang von verhaltensorientierter Internetwerbung einwilligen, um sich bei einem sozialen Netzwerkdienst registrieren zu können. Angesichts der Bedeutung, die einige soziale Netzwerke haben, werden manche Kategorien von Nutzern (wie Jugendliche) den Empfang von verhaltensorientierter Internetwerbung akzeptieren, um das Risiko zu vermeiden, von manchen sozialen Interaktionen teilweise ausgeschlossen zu werden. Der Nutzer sollte in der Lage sein, in den Erhalt der verhaltensorientierten Internetnutzung ohne Zwang und für den konkreten Fall einzuwilligen und zwar unabhängig von seinem Zugang zu den sozialen Netzwerkdiensten. Es könnte ein Pop-Up-Feld verwendet werden, um dem Nutzer diese Möglichkeit zu geben.

Soziale Netzwerkdienste bieten die Möglichkeit, externe Anwendungen zu nutzen. In der Praxis wird der Nutzer häufig an der Nutzung einer Anwendung gehindert, wenn er nicht in die Übermittlung seiner Daten an den Entwickler der Anwendung einwilligt. Die Gründe für diese Übermittlung sind vielschichtig und umfassen verhaltensorientierte Internetwerbung und den Weiterverkauf an Dritte. Angesichts der Tatsache, dass die Anwendung läuft, ohne dass die Übermittlung von Daten an den Entwickler dieser Anwendung erforderlich ist, unterstützt die Datenschutzgruppe die Granularität bei der Einholung der Einwilligung der Nutzer. D.h., es wird eine gesonderte Einwilligung für die Übermittlung der Daten des Nutzers an den Entwickler für diese verschiedenen Zwecke eingeholt. Es könnten verschiedene Mechanismen, wie die Pop-Up-Felder genutzt werden, so dass der Nutzer auswählen kann, in welche Datennutzung er einwilligt (Übermittlung an den Entwickler, Dienste mit Zusatznutzen, verhaltensorientiert Internetwerbung, Übermittlung an Dritte usw.).

Einwilligung für den konkreten Fall bedeutet auch, dass der Nutzer über eine Änderung der Zwecke informiert werden muss, für die der für die Datenverarbeitung Verantwortliche die Daten verarbeitet. Er muss auch die Möglichkeit haben, in die neue Verarbeitung seiner Daten einzuwilligen. Die Informationen, die er erhält, müssen insbesondere die Folgen einer Ablehnung der vorgeschlagenen Änderungen aufzeigen.

„… in Kenntnis der Sachlage …“

Das letzte Element der Definition von Einwilligung – aber nicht die letzte Anforderung, wie nachfolgend gezeigt wird – ist, dass sie in Kenntnis der Sachlage erfolgen muss.

Artikel 10 und 11 der Richtlinie legen die Pflicht fest, die betroffenen Personen zu informieren. Die Informationspflicht ist folglich eine eigenständige Pflicht, die aber in vielen Fällen offensichtlich mit der Einwilligung verbunden ist. Während auf die Bereitstellung von Informationen nicht immer eine Einwilligung erfolgt (es kann eine

andere Rechtsgrundlage von Artikel 7 genutzt werden), kann vor der Bereitstellung von Informationen keine Einwilligung erteilt werden.

Das heißt in der Praxis, dass *„(die) Einwilligung der betroffenen Person nach der bewussten Erfassung und Würdigung der Fakten und Auswirkungen einer Handlung (erfolgen muss). Sie muss in klarer und verständlicher Form genau und umfassend über alle relevanten Aspekte, insbesondere die in den Artikeln 10 und 11 genannten wie Art und Zweckbestimmung der verarbeiteten Daten, Personen, an die die Daten möglicherweise weitergegeben werden, und ihre Rechte, aufgeklärt werden. Hierzu gehört auch die Aufklärung über die möglichen Folgen bei Verweigerung der Einwilligung zu der jeweiligen Verarbeitung*“[23].

In vielen Fällen wird die Einwilligung zum Zeitpunkt der Erhebung der personenbezogenen Daten erhalten, wenn die Verarbeitung beginnt. In diesem Fall stimmt die bereitzustellende Information mit den in Artikel 10 der Richtlinie aufgeführten Punkten überein. Die Einwilligung kann jedoch auch später eingeholt werden, wenn sich der Zweck der Verarbeitung ändert. In diesem Fall muss sich die bereitzustellende Information darauf konzentrieren, was in dem spezifischen Kontext in Bezug auf den Zweck erforderlich ist.

Einwilligung in Kenntnis der Sachlage ist in Bezug auf die Übermittlung von personenbezogene Daten an Drittländer insofern besonders wichtig, *„als damit verlangt wird, dass die betroffene Person über das konkrete Risiko der Übermittlung der Daten in ein Land ohne angemessenes Schutzniveau ordnungsgemäß in Kenntnis gesetzt werden muss.*“[24]

Es können zwei Arten von Anforderungen identifiziert werden, um eine angemessene Information zu gewährleisten:

- Qualität der Information – die Art und Weise, in der die Information erteilt wird (einfache Sprache, ohne die Verwendung von Jargon, verständlich, deutlich) ist ausschlaggebend, wenn bewertet werden soll, ob die Einwilligung „in Kenntnis der Sachlage“ erfolgt. Die Art und Weise, in der diese Informationen gegeben werden sollten, hängt von dem Kontext ab: ein regelmäßiger/durchschnittlicher Nutzer sollte dazu in der Lage sein, sie zu verstehen.

- Zugänglichkeit und Sichtbarkeit der Informationen – Informationen müssen den Personen direkt gegeben werden. Es reicht nicht aus, dass die Informationen irgendwo „verfügbar“ sind. Der Gerichtshof hat in seinem Urteil von 2004[25] auf diesem Punkt bestanden, als er sich auf einen Arbeitsvertrag bezog, der Bedingungen enthielt, die in dem Vertrag nicht ausdrücklich niedergelegt waren, sondern auf die nur verwiesen wurde. Die Informationen müssen deutlich sichtbar sein (Art und Größe der Schrift), auffällig und verständlich. Dialogfenster können genutzt werden, um spezifische Informationen zu geben, wenn die Einwilligung erforderlich ist. Wie vorstehend in Bezug auf die „Einwilligung für den konkreten Fall“ erwähnt, sind Online-

[23] WP131 – Arbeitspapier - Verarbeitung von Patientendaten in elektronischen Patientenakten.

[24] WP12 - Arbeitsunterlage: Übermittlungen personenbezogener Daten an Drittländer : Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU. Siehe auch WP114 – Arbeitspapier der Artikel-29-Datenschutzgruppe über eine Gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995.

[25] Siehe Fußnote 12 (Kapitel II.2).

Informationsmittel besonders hilfreich in Bezug auf soziale Netzwerkdienste, um so eine ausreichende Granularität und Klarheit der Privatsphären-Einstellungen zu bieten. Auch mehrschichtige Hinweise können hier ein hilfreiches Mittel sein, da sie dazu beitragen, die richtigen Informationen auf eine einfach zugängliche Weise zu geben.

Mit dem Verstreichen der Zeit entstehen möglicherweise Zweifel, ob die Einwilligung, die ursprünglich auf gültigen, ausreichenden Informationen beruhte, immer noch gültig ist. Aus einer Vielzahl von Gründen ändern die Leute häufig ihre Meinung, weil ihre ursprünglichen Entscheidungen schlecht waren oder aufgrund einer Änderung der Umstände, beispielsweise wenn ein Kind reifer wird[26]. Deshalb sollten die für die Datenverarbeitung Verantwortlichen im Rahmen der bewährten Praktiken danach streben, die Wahl der Einzelpersonen nach einer Weile zu überprüfen. Hierzu können sie diese beispielsweise über ihre aktuelle Wahl informieren und ihnen die Möglichkeit anbieten, sie entweder zu bestätigen oder zu widerrufen[27]. Der jeweilige Zeitraum hängt natürlich von dem Kontext und den Umständen des Falls ab.

Beispiel: Verbrechenskartierung
Einige Polizeikräfte überlegen, Karten oder sonstige Daten zu veröffentlichen, die zeigen, wo ein bestimmtes Verbrechen verübt wurde. Normalerweise stellen in den Prozess integrierte Schutzmaßnahmen sicher, dass keine personenbezogenen Daten über das Opfer des Verbrechens veröffentlicht werden, da das Verbrechen nur mit relativ großen geographischen Regionen verknüpft wird. Einige Polizeikräfte wollen Verbrechen aber punktgenauer kennzeichnen, sofern das Opfer des Verbrechens einwilligt. Dann wird es möglich, die betroffene Person genauer mit dem Ort in Verbindung zu bringen, an dem das Verbrechen begangen wurde. Dem Opfer wird jedoch nicht mitgeteilt, dass identifizierbare Informationen über es offen im Internet veröffentlicht werden und wie diese Informationen genutzt werden können. Die Einwilligung ist in diesem Fall folglich nicht gültig, da das Opfer das Ausmaß, in dem Daten über es veröffentlicht werden, möglicherweise gar nicht versteht.

Je komplexer die Datenverarbeitung ist, desto mehr kann von dem für die Datenverarbeitung Verantwortlichen erwartet werden. Je schwieriger es für den Durchschnittsbürger wird, alle Elemente der Datenverarbeitung zu überblicken und zu verstehen, desto größer sollten die Anstrengungen des für die Datenverarbeitung Verantwortlichen sein, zu zeigen, dass die Einwilligung basierend auf verständlichen Informationen für den konkreten Fall erteilt wurde.

Eine Einwilligung im Sinne der Definition von Artikel 2 Buchstabe h sollte zusammen mit den weiteren Anforderungen gesehen werden, die später im Text der Richtlinie genannt werden. Artikel 7 fügt der Definition „ohne jeden Zweifel“ bei und Artikel 8 fügt das Wort „ausdrücklich“ hinzu, wenn sich die Verarbeitung auf besondere Kategorien personenbezogener Daten bezieht.

[26] Arbeitspapier 1/2008 zum Schutz der personenbezogenen Daten von Kindern, WP147, 18. Februar 2008.

[27] Die Artikel-29-Datenschutzgruppe hat in ihrer Stellungnahme 171 zur Werbung auf Basis von Behavioural Targeting, angenommen am 22.6.2010 eine ähnliche Empfehlung gemacht.

III.A.2. Artikel 7 Buchstabe a

Gemäß Artikel 7 Buchstabe a der Richtlinie stellt eine Einwilligung der betroffenen Person, die ohne jeden Zweifel erfolgt, eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten dar. Um gültig zu sein, muss die Einwilligung also zusätzlich zu den in Artikel 2 Absatz h genannten Kriterien auch *ohne jeden Zweifel* erfolgen.

Damit eine Einwilligung ohne jeden Zweifel erfolgt, darf das Verfahren zur Einholung und Erteilung der Einwilligung *keinen Zweifel* an der Einwilligungsabsicht der betroffenen Person lassen. Mit anderen Worten: die Willensbekundung, mit der die betroffene Person ihre Einwilligung zum Ausdruck bringt, darf keinen Zweifel an ihrer Absicht hinterlassen. Bei Vorliegen eines berechtigten Zweifels an der Absicht der Person liegt Mehrdeutigkeit vor.

Wie nachfolgend beschrieben, zwingt diese Anforderung die für die Datenverarbeitung Verantwortlichen zur Schaffung stabiler Verfahren, mit denen die betroffenen Personen ihre Einwilligung erteilen können. Die für die Datenverarbeitung Verantwortlichen können entweder eine klare, ausdrückliche Einwilligung anstreben oder sich auf Verfahren verlassen, die die eindeutige, konkludente Einwilligung der Person übermitteln. Der für die Datenverarbeitung Verantwortliche muss ausreichend sicher sein, dass die die Einwilligung gebende Person tatsächlich die betroffene Person ist. Dies ist insbesondere bei einer telefonischen Einwilligung oder einer Einwilligung per Internet von Bedeutung.

Ein verwandtes Thema ist der Nachweis der Einwilligung. Die für die Datenverarbeitung Verantwortlichen wollen oder müssen möglicherweise nachweisen, dass sie die Einwilligung erhalten haben, beispielsweise im Falle eines Streits mit der betroffenen Person. In einigen Fällen werden sie im Rahmen von Durchsetzungsmaßnahmen vielleicht wirklich um die Vorlage eines solches Beweises gebeten. Folglich und im Rahmen der bewährten Praktiken sollten für die Datenverarbeitung Verantwortliche einen Nachweis über die tatsächliche Erteilung der Einwilligung schaffen und aufbewahren. Das heißt, das Vorliegen der Einwilligung sollte nachprüfbar sein.

Nachfolgend werden die folgenden Methoden für die Erteilung der Einwilligung analysiert und es wird geprüft, ob sie eine Einwilligung ohne Zweifel darstellen.

Ausdrückliche Erklärungen, mit denen die Zustimmung zum Ausdruck gebracht wird, wie beispielsweise unterschriebene Abkommen oder schriftliche Erklärungen des Wunsches auf Einwilligung sind als Verfahren oder Mechanismen gut dazu geeignet, eine Einwilligung ohne jeden Zweifel zu erteilen. Gleichzeitig bieten sie grundsätzlich einen Nachweis für den für die Datenverarbeitung Verantwortlichen, dass er die Einwilligung erhalten hat.

Beispiel: Einwilligung in den Erhalt von Werbeinformationen per Post
Ein Hotel bittet Personen darum, ihre Anschrift auf einem Papierformular anzugeben, wenn sie Werbeinformationen per Post erhalten wollen. Wenn die Person das Formular nach Angabe der Anschrift unterzeichnet, um damit ihre Einwilligung zu zeigen, ist das eine Einwilligung ohne jeden Zweifel. In dem Fall ist die Einwilligung sowohl ausdrücklich als auch in Schriftform. Das Verfahren gibt dem für die

Datenverarbeitung Verantwortlichen einen angemessenen Nachweis über den Erhalt der Einwilligung des Kunden, sofern er die unterzeichneten Formulare aufbewahrt.

Nicht alle Formen der Einwilligung jedoch, die ausdrücklich zu sein scheinen, erteilen auch eine Einwilligung. Dieser Fall wurde in der kürzlich vor dem Gerichtshof anhängigen Rechtssache (Volker und Markus Schecke gegen Land Hessen) diskutiert, der sich auf die Veröffentlichung der Namen von Begünstigten verschiedener EU-Fonds[28] und auf die Nennung der von jedem Begünstigten erhaltenen Geldsumme bezog. Die Generalanwältin prüfte, ob die Voraussetzungen für eine Einwilligung ohne jeden Zweifel in einem Fall erfüllt wurden, in dem die Betroffenen ein Formular mit dem folgenden Hinweis unterzeichnet hatten: „Mir ist bekannt, dass nach Artikel 44 Buchstabe a der Verordnung … Nr. 1290/2005 vorgeschrieben ist, Informationen über die Empfänger von EGFL- und ELER-Mitteln sowie die Beträge, die jeder Begünstigte erhalten hat, zu veröffentlichen." Die Generalanwältin schlussfolgerte: *„Die Kenntnisnahme durch den vorherigen Hinweis, dass eine Veröffentlichung irgendwelcher Art erfolgen werde, ist nicht gleichzusetzen mit der Abgabe der Einwilligung „ohne jeden Zweifel" zu einer bestimmten Art der detaillierten Veröffentlichung. Sie kann auch nicht wirklich als eine Willensbekundung der Kläger angesehen werden, die im Sinne der in Artikel 2 Buchstabe h gegebenen Begriffsbestimmung der Einwilligung der betroffenen Person „ohne Zwang, für den konkreten Fall … erfolgt."* Sie äußerte daher die Ansicht, dass die Kläger keine Einwilligung in die Verarbeitung (d. h. hier, in die Veröffentlichung) ihrer Daten im Sinne von Artikel 7 Buchstabe a der Richtlinie 95/46/EG gegeben hatten.[29]

Auch Online kann eine ausdrückliche Einwilligung erteilt werden. Wie in der Offline-Welt gibt es auch Online sehr geeignete Mittel, mit denen eine Einwilligung ohne jeden Zweifel erteilt werden kann. Das wird in dem nachfolgenden Beispiel dargelegt:

Beispiel: Online-Einwilligung in die Einbindung in ein Treueprogramm
Die Website eines Hotels enthält ein Reservierungsformular, so dass Zimmer vorab elektronisch reserviert werden können. Das Online-Formular, in dem die Personen das gewünschte Datum und Informationen bezüglich der Zahlung eingeben, enthält auch eine sichtbare Schaltfläche, die von denjenigen Personen angeklickt werden kann, die wollen, dass ihre Daten in ein Treueprogramm aufgenommen werden. Das Anklicken der Schaltfläche nach Erhalt der einschlägigen Informationen stellt eine ausdrückliche Einwilligung ohne jeden Zweifel dar, da das Anklicken der Schaltfläche deutlich genug ist und keine Zweifel daran lässt, dass die jeweilige Person tatsächlich in das Programm aufgenommen werden möchte.

Eine ausdrückliche Einwilligung kann auch mündlich durch Erklärungen gegeben werden, die die Einwilligung zum Ausdruck bringen sollen. In der folgenden Situation würde eine ausdrückliche mündliche Einwilligung erteilt werden.

[28] Europäischer Garantiefonds für die Landwirtschaft (EGFL) und Europäischer Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER).

[29] Schlussanträge der Generalanwältin Sharpston vom 17. Juni 2010, Volker und Markus Schecke GbR, verbundene Rechtssachen C-92/09 und C-93/09. Es sollte angemerkt werden, dass der Gerichthof in seinem Urteil vom 9. November 2010 entschied, dass sich die Datenverarbeitung nicht auf eine Einwilligung stützte: *„63. Die fraglichen Unionsrechtsvorschriften, die lediglich vorsehen, dass die Mittelempfänger vorab über die Veröffentlichung ihrer Daten unterrichtet werden, stützen demnach die mit ihnen eingeführte Verarbeitung personenbezogener Daten nicht auf die Einwilligung der betroffenen Empfänger."*

Beispiel: mündliche Einwilligung in den Erhalt von Werbeinformationen
Beim Zahlen am Checkout-Schalter eines Hotels fragt der Hotelangestellt die Gäste, ob sie ihre Adresse angeben möchten, so dass Ihnen das Hotel Angebote zuschicken kann. Die Gäste, die ihre Adresse angeben, nachdem sie von dem Hotelangestellten gefragt wurden und die einschlägigen Informationen erhalten haben, haben ihre ausdrückliche Einwilligung erteilt. Das Angeben der Adresse kann ein unmissverständlicher Hinweis auf den Wunsch der Person sein. Der für die Datenverarbeitung Verantwortliche wird sich aber möglicherweise für andere Mechanismen entscheiden, mit denen die Einwilligung zuverlässiger nachgewiesen werden kann.

Unter manchen Umständen kann eine Einwilligung ohne jeden Zweifel aus bestimmten Handlungen *geschlossen* werden. Dies ist insbesondere dann der Fall, wenn die Handlungen zu der unmissverständlichen Schlussfolgerung führen, dass eine Einwilligung erteilt wurde. Dazu müssen jedoch die einschlägigen Informationen über die Datenverarbeitung gegeben worden sein, so dass die betroffene Person wirklich eine Entscheidung treffen kann (wer ist der für die Datenverarbeitung Verantwortliche, was sind die Zwecke der Verarbeitung usw.).

Beispiel: Einwilligung, fotografiert zu werden
Beim Einchecken in einem Hotel informiert ein Hotelangestellter die Gäste darüber, dass am Nachmittag in einer der Cafeteria des Hotels ein Fototermin stattfinden wird. Ausgewählte Bilder sollen für Werbezwecke genutzt werden, insbesondere für die Hotelbroschüren in Papierform. Hotelgäste, die sich fotografieren lassen wollen, sind dazu eingeladen, zu der entsprechenden Zeit in die Cafeteria zu kommen. Eine andere Cafeteria steht denjenigen Hotelgästen zur Verfügung, die nicht fotografiert werden wollen.

Bei Hotelgästen, die sich nach Erhalt der Informationen dazu entscheiden, während des Fototermins in die Cafeteria zu gehen, kann man davon ausgehen, dass sie ihre Einwilligung erteilt haben, fotografiert zu werden. Ihre Einwilligung wird daraus geschlossen, dass sie zu der Zeit in die Cafeteria gehen, in der der Fototermin stattfindet. Das Aufsuchen der Cafeteria ist ein Hinweis auf den Wunsch der Person. Dies kann im Prinzip als ohne jeden Zweifel angesehen werden, da nur ein geringer Zweifel daran besteht, dass die in die Cafeteria gehende Person fotografiert werden möchte. Das Hotel könnte es jedoch als weise ansehen, anhand eines Schriftstückes nachweisen zu können, dass die Einwilligung eingeholt wurde, falls die Gültigkeit einer solchen Einwilligung in absehbarer Zukunft angefochten werden sollte.

Wie bereits gesagt, gelten sowohl in der Offline- als auch in der Online-Welt dieselben Anforderungen, einschließlich der Einwilligung ohne jeden Zweifel. Die Datenschutzgruppe merkt jedoch an, dass das Risiko einer missverständlichen Einwilligung in der Online-Welt größer ist. Darauf muss besonders geachtet werden. Das folgende Beispiel zeigt einen Fall, in dem die aus einer bestimmten Handlung (Teilnahme an einem Online-Spiel) geschlossene Einwilligung die Anforderungen an eine gültige Einwilligung nicht erfüllt.

Beispiel: Online-Spiel
Der Anbieter eines Online-Spiels fordert die Spieler zum Zweck der Teilnahme an dem Online-Spiel zur Angabe von Alter, Name und Adresse auf (Aufteilung der Spieler nach Alter und Adressen). Auf der Website befindet sich ein über einen Link zugänglicher Hinweis (es ist nicht notwendig, den Hinweis zu lesen, um an dem Spiel teilzunehmen), dass die Spieler durch die Nutzung der Website (und das damit verbundene Bereitstellen der Informationen) einwilligen, dass ihre Daten durch den Anbieter des Spiels und durch Dritte verarbeitet werden, um den Spielern Werbung zu senden.

Der Zugang zu und die Teilnahme an dem Spiel ist nicht gleichbedeutend mit einer Einwilligung ohne jeden Zweifel in die zukünftige Verarbeitung der personenbezogenen Daten für andere Zwecke als die Teilnahme an dem Spiel. Die Teilnahme an dem Spiel impliziert nicht die Absicht des Spielers, in eine Verarbeitung einzuwilligen, die nicht für das Spiel erforderlich ist. Diese Art Verhalten stellt keine zweifelsfreie Angabe des Wunsches der Person dar, dass ihre Daten für Werbezwecke verwendet werden.

Beispiel: Privatsphäre-Voreinstellungen
Die Voreinstellungen in privaten Netzwerken, auf die Nutzer nicht unbedingt Zugriff nehmen müssen, um das Netzwerk zu nutzen, ermöglichen die gesamte „Friend of a Friend" Kategorie, bei der die personenbezogenen Daten jedes Nutzers allen „Friends of a Friend" sichtbar gemacht werden. Nutzer, die nicht möchten, dass ihre personenbezogenen Daten von „Friends of a Friend" gesehen werden, müssen eine Schaltfläche anklicken. Wenn sie passiv bleiben oder die Schaltfläche nicht anklicken, geht der für die Datenverarbeitung Verantwortliche davon aus, dass sie eingewilligt haben, dass ihre Daten sichtbar sind. Es ist jedoch sehr fraglich, ob das Nicht-Anklicken einer Schaltfläche bedeutet, dass die Nutzer im Allgemeinen einwilligen, ihre Informationen allen „Friends of a Friend" sichtbar zu machen. Aufgrund der Unsicherheit, ob das Ausbleiben einer Handlung wirklich als Einwilligung gemeint ist, kann das Nicht-Anklicken nicht als Einwilligung ohne Zweifel gelten.

Das vorgenannte Beispiel zeigt einen Fall, in dem die Person passiv bleibt (d.h. Ausbleiben einer Handlung oder „Schweigen"). Eine Einwilligung ohne jeden Zweifel passt nicht gut zu einem Verfahren, in dem die Einwilligung aufgrund von Inaktivität oder Schweigen der Personen eingeholt wird: Das Schweigen einer Partei oder das Ausbleiben einer Handlung ist an sich mehrdeutig (die betroffene Person könnte die Zustimmung gemeint haben oder möglicherweise wollte sie nur die Handlung nicht ausführen). Das folgende Beispiel führt das weiter aus.

Die Situation ist mehrdeutig, wenn man davon ausgeht, dass Personen ihre Einwilligung dadurch gegeben haben, dass sie auf einen Brief nicht geantwortet haben, in dem sie darüber informiert werden, dass das Ausbleiben einer Antwort ihre Einwilligung bedeutet. In einer solchen Situation weckt das Verhalten der betroffenen Person (oder das Ausbleiben der Handlung) ernsthafte Zweifel daran, ob sie Zustimmung zum Ausdruck bringen wollte. Aus der Tatsache, dass sie keine positive Handlung ausgeführt hat, darf nicht geschlossen werden, dass sie ihre Einwilligung gegeben hat. So wird die

Anforderung einer Einwilligung ohne jeden Zweifel nicht erfüllt. Außerdem ist es für den für die Datenverarbeitung Verantwortlichen wie nachstehend gezeigt wird, auch sehr schwer, einen Nachweis über die erfolgte Einwilligung zu erbringen.

Die Datenschutzgruppe hat festgestellt, dass eine Einwilligung, die auf dem Schweigen der Person im Zusammenhang mit dem Versenden von Direktwerbung per E-Mail beruht, nicht angemessen ist*: "Eine implizite Einwilligung zur Zusendung solcher Nachrichten ist nicht mit der Definition der Einwilligung in der Richtlinie 95/46/EG vereinbar ... Analog sind auch bereits angekreuzte Kästchen, beispielsweise auf Websites, nicht mit der Definition der Richtlinie vereinbar."*[30] Diese Ansicht wird durch das folgende Beispiel bestätigt:

Beispiel: ungültige Einwilligung in die weitere Nutzung von Kundendaten
Ein Online-Buchhändler sendet seinen an einem Treueprogramm teilnehmenden Kunden eine E-Mail und informiert sie darüber, dass ihre Daten an ein Werbeunternehmen übermittelt werden, das diese zu Werbezwecken nutzen möchte. Die Nutzer haben zwei Wochen Zeit, auf die E-Mail zu antworten. Sie werden darüber informiert, dass das Ausbleiben einer Antwort als Einwilligung in die Datenübermittlung angesehen wird. Diese Art Mechanismus, bei dem eine Einwilligung aus der ausbleibenden Reaktion von betroffenen Personen geschlossen wird, stellt keine gültige Einwilligung ohne jeden Zweifel dar. Es ist nicht möglich, anhand der ausgebliebenen Reaktion zweifelsfrei festzustellen, ob die Personen wirklich in die Datenübermittlung eingewilligt haben.

Aus Vorstehendem ergibt sich, dass die für die Datenverarbeitung Verantwortlichen als Folge der Forderung nach einer Einwilligung *ohne jeden Zweifel*, *de facto* dazu angehalten werden, Verfahren und Mechanismen anzuwenden, die keinen Zweifel daran lassen, dass die Einwilligung erteilt wurde. Dies kann entweder eine ausdrückliche Handlung der Person sein oder eine Handlung der Person, aus der die Einwilligung eindeutig geschlossen werden kann.

Wie oben dargelegt, sollte die Verwendung einschlägiger Verfahren und Maßnahmen eine bewährte Praktik für die für die Datenverarbeitung Verantwortlichen sein, mit der gezeigt werden kann, dass die Einwilligung erteilt wurde. Je komplizierter das Umfeld ist, in dem sie handeln, desto mehr Maßnahmen sind erforderlich, um sicherzustellen, dass die Einwilligung nachprüfbar ist. Die Einwilligung sollte der Datenschutzbehörde auf Anfrage vorgelegt werden.

III.A.3. Artikel 8Absatz 2 Buchstabe a

Artikel 8 der Richtlinie sieht einen besonderen Schutz für *„besondere Kategorien personenbezogener Daten"* vor, die aufgrund ihrer Art als sehr sensible eingeschätzt werden. Die Verarbeitung solcher Daten ist verboten, sofern nicht mindestens eine von mehreren genau festgelegten Ausnahmen Anwendung findet. Artikel 8Absatz 2 Buchstabe a sieht vor, dass das Verbot keine Anwendung findet,

[30] Stellungnahme 5/2004 zu unerbetenen Werbenachrichten im Sinne von Artikel 13 der Richtlinie 2002/58/EG, angenommen am 27. February 2004 (WP90).

wenn die betroffene Person *ausdrücklich* in die Verarbeitung der genannten Daten *eingewilligt* hat.

Juristisch gesehen umfasst eine „ausdrückliche Einwilligung" alle Situationen, in denen Personen ein Vorschlag gemacht wird und sie einer bestimmten Verwendung oder der Offenlegung ihrer personenbezogenen Daten entweder zustimmen oder diese ablehnen können und sie aktiv entweder schriftlich oder mündlich auf die Frage antworten. Normalerweise wird die ausdrückliche Einwilligung in Schriftform erteilt und handschriftlich unterzeichnet. Wenn eine betroffene Person beispielsweise ein Einwilligungsformular unterzeichnet, in dem eindeutig dargelegt wird, warum der für die Datenverarbeitung Verantwortliche personenbezogene Daten erheben und weiter verarbeiten möchte, liegt eine ausdrückliche Einwilligung vor.

Auch wenn eine ausdrückliche Einwilligung üblicherweise in Schriftform, entweder auf dem Papier oder elektronisch, erteilt wird, ist die Schriftform gemäß Kapitel III.A.2 nicht erforderlich und die Einwilligung kann auch mündlich erteilt werden. Das wird durch die Tatsache bestätigt, dass die ursprüngliche Anforderung aus Artikel 8, dass die Einwilligung in Schriftform erfolgen muss, in der Endfassung der Richtlinie gestrichen wurde. Wie in dem vorgenannten Kapitel dargelegt wird, ist es aber möglicherweise schwierig, eine mündliche Einwilligung nachzuweisen. Deshalb wird es den für die Datenverarbeitung Verantwortlichen aus Gründen der Nachweisbarkeit empfohlen, schriftliche Einwilligungen einzuholen.

Die Anforderung, dass die Einwilligung ausdrücklich zu sein hat, bedeutet, dass eine implizite Einwilligung normalerweise nicht die Anforderungen von Artikel 8Absatz 2 Buchstabe a erfüllt. In diesem Zusammenhang ist es sinnvoll, sich die Stellungnahme der Artikel-29-Datenschutzgruppe zu elektronischen Patientenakten[31] ins Gedächtnis zu rufen. Dort steht: *„Bei sensiblen personenbezogenen Daten und damit auch bei für die elektronische Patientenakte bestimmten Daten muss die Einwilligung im Gegensatz zu den Bestimmungen in Artikel 7 der Richtlinie* ***ausdrücklich*** *erfolgen. Opt-out-Lösungen … genügen nicht dem Erfordernis der „ausdrücklichen" Einwilligung."*

Beispiel: medizinische Daten für Forschungszwecke
Wenn ein Patient von einem Krankenhaus darüber informiert wird, dass seine Krankenakte an einen Forscher übermittelt wird, sofern er nicht widerspricht (indem er unter einer bestimmten Nummer anruft) wird das Erfordernis der ausdrücklichen Einwilligung nicht erfüllt.

Wie oben in Kapitel II.A.2 dargelegt wurde, können Personen ihre ausdrückliche Einwilligung sowohl schriftlich als auch mündlich erteilen, indem sie ihren Wunsch, in eine Form der Datenverarbeitung einzuwilligen, durch eine positiv bejahende Handlung zum Ausdruck bringen. In der Online-Umgebung kann eine ausdrückliche Einwilligung durch die Verwendung elektronischer oder digitaler Signaturen gegeben werden. Sie kann abhängig vom Zusammenhang aber auch durch anklickbare Schaltflächen, das

[31] WP131 – Arbeitspapier Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA).

Versenden einer bestätigenden E-Mail, das Anklicken von Icons usw. erteilt werden[32]. Die Billigung von Verfahren, die eine positiv bejahende Handlung einer natürlichen Person zur Folge haben, werden in Erwägungsgrund 17 der Datenschutzrichtlinie für elektronische Kommunikation ausdrücklich anerkannt: *„Die Einwilligung kann in jeder geeigneten Weise gegeben werden, wodurch der Wunsch des Nutzers in einer spezifischen Angabe zum Ausdruck kommt, die sachkundig und in freier Entscheidung erfolgt; hierzu zählt auch das Markieren eines Feldes auf einer Internet-Website."*

Eine Einwilligung muss nicht aufzeichenbar sein, um gültig zu sein. Es liegt jedoch im Interesse des für die Datenverarbeitung Verantwortlichen, einen Nachweis aufzubewahren. Es ist offensichtlich, dass die Beweiskraft der einzelnen, spezifischen Mechanismen unterschiedlich ist und sie die Einwilligung in größerem oder kleinerem Maße nachweisen. Eine Einwilligung, die durch das Anklicken einer Schaltfläche erhalten wurde und bei der die Identität der betroffenen Person durch eine E-Mail-Adresse unterstützt wird, hat eine deutliche geringere Beweiskraft als ein ähnlicher Prozess, der beispielsweise durch aufzeichenbare Einwilligungsmechanismen[33] gestützt wird. Die Notwendigkeit hoher Beweiskraft hängt auch von der Art der erhobenen Daten und dem verfolgten Zweck ab: für die Einwilligung in den Erhalt von Werbeangeboten ist keine elektronische Signatur erforderlich. Sie kann jedoch für die Einwilligung in die Online-Verarbeitung bestimmter Finanzdaten erforderlich sein. Eine ausdrückliche Einwilligung, die in einer Online-Umgebung gegeben wurde, muss aufzeichenbar sein, sodass sie für eine spätere Bezugnahme zugänglich ist.[34]

Angesichts oben Stehenden wird davon ausgegangen, dass Online-Registrierungsformulare, in denen natürliche Personen ihre Identifikationsinformationen angeben und ihre Zustimmung zur Datenverarbeitung erteilen müssen, die Anforderungen für eine ausdrückliche Einwilligung erfüllen, sofern alle anderen Anforderungen erfüllt sind. Zum Anlegen einer personalisierten, elektronischen Krankenakte können die Patienten beispielsweise ihre Einwilligung geben, indem sie ihre Kontaktdaten angeben und auf eine bestimmte Schaltfläche klicken, um ihre Einwilligung zu zeigen. Die Verwendung stärkerer Authentifizierungsmethoden – zum Beispiel die Verwendung digitaler Signaturen - führt selbstverständlich zum gleichen Ergebnis, hat aber höhere Beweiskraft.[35]

In bestimmten Fällen können die Mitgliedstaaten entscheiden, dass eine bestimmte Datenverarbeitung durch eine Einwilligung legitimiert werden muss und die Art der Einwilligung festlegen. Beispielsweise können die Mitgliedstaaten entscheiden, dass

---

[32] Diese Auslegung steht im Einklang mit der EU-Gesetzgebung, hauptsächlich zum elektronischen Geschäftsverkehr und der breiten Nutzung digitaler Signaturen. Sie forderte von den Mitgliedstaaten eine Änderung ihrer Gesetze, die die formalen Anforderungen an Dokumente hatten, dass sie „in Schriftform" oder „handschriftlich" sein mussten. Denn ihre elektronischen Gegenstücke sind gleichermaßen anzuerkennen, sofern bestimmte Voraussetzungen erfüllt sind.

[33] Siehe diesbezüglich beispielsweise das griechische und deutsche Recht in Bezug auf die Anforderungen an eine Einwilligung auf elektronischem Weg. Die Einwilligung muss auf eine sichere Weise aufgezeichnet sein und von dem Teilnehmer oder Nutzer jederzeit abgerufen und jederzeit widerrufen werden können (Artikel 5 Absatz 3 des griechischen Gesetzes 3471/2006 zum Schutz personenbezogener Daten im elektronischen Kommunikationssektor; Artikel 13 Absatz 2 des Teledienstegesetzes, Artikel 94 des Telekommunikationsgesetzes und Artikel 28 Absatz 3 Buchstabe a des Bundesdatenschutzgesetzes).

[34] Es liegt nicht innerhalb des Anwendungsbereichs dieser Stellungnahme, die technischen Voraussetzungen zu untersuchen, die von elektronischen Dokumenten und digitalen Signaturen erfüllt werden müssen, damit sie die gleiche Beweiskraft wie ihre handschriftlichen Gegenstücke erhalten. Das ist eine Frage, die über die Datenschutzgesetzgebung hinausgeht und die auf EU-Ebene reguliert wurde.

[35] Das ist der Fall, da von bestimmten Arten der digitalen Signaturen (fortgeschrittene elektronische Signaturen, die auf einem qualifizierten Zertifikat basieren und mit einer sicheren Signaturerstellungseinheit erstellt wurden) automatisch angenommen wird, dass sie dieselbe rechtliche Beweiskraft wie handschriftliche haben.

Personen, die Online einen Antrag auf eine Gesundheitskarte mit Zugang zur Krankengeschichte stellen, mit einer bestimmten digitalen Signatur unterzeichnen müssen. So wird sichergestellt, dass die Einwilligung ausdrücklich ist und der für die Datenverarbeitung Verantwortliche ist sicherer, dass er die Einwilligung nachweisen kann.

III.A.4. Artikel 26 Absatz 1

Artikel 26 Absatz 1 Buchstabe a sieht die Einwilligung der betroffenen Person ohne jeden Zweifel als Ausnahme zu dem Verbot vor, personenbezogene Daten an ein Drittland zu übermitteln, das kein angemessenes Schutzniveau gewährleistet. Die vorstehenden Überlegungen zu Artikel 7 Buchstabe a finden hier ebenfalls Anwendung. Das heißt, dass die Einwilligung zusätzlich zu den Anforderungen für eine gültige Einwilligung gemäß Artikel 2 Buchstabe h auch noch ohne jeden Zweifel erfolgen muss.

Die Artikel-29-Datenschutzgruppe hat viele Anstrengungen unternommen, um Anleitungen zur Anwendung der Artikel 25 und 26 der Richtlinie zu geben, einschließlich der Ausnahme zur Einwilligung. In diesem Zusammenhang sollte an das Dokument WP12[36] der Datenschutzgruppe zur Bedeutung der Einwilligung ohne Zweifel erinnert werden: *„Da die Einwilligung ohne jeden Zweifel erfolgen muss, führt jeglicher Zweifel daran, ob die Einwilligung tatsächlich gegeben worden ist, ebenfalls dazu, dass die Ausnahmeregelung nicht gilt. Damit würde auch in einer Vielzahl von Fällen, in denen die Einwilligung unterstellt wird (weil die betreffende Person beispielsweise auf die Übermittlung aufmerksam gemacht wurde und keinen Einwand dagegen erhoben hat), die Ausnahmeregelung nicht greifen."*

Angesichts oben Stehenden wird eine Einwilligung ohne jeden Zweifel eher erteilt, wenn die betroffenen Personen eine positiv bejahende Handlung durchführen, um ihre Einwilligung in die Übermittlung zu signalisieren, beispielsweise, indem sie ein Einwilligungsformular unterzeichnen oder eine andere Handlung durchführen, die die Schlussfolgerung unmissverständlich stützt, dass sie ihre Einwilligung erteilt haben.

In WP 114[37] zur Verwendung der Einwilligung für die Übermittlung von Daten hat die Datenschutzgruppe festgestellt, dass *„die Einwilligung in Fällen der wiederholten oder gar routinemäßigen Übermittlung von Daten zu deren Verarbeitung wahrscheinlich langfristig keinen angemessenen Rechtsrahmen für die Verantwortlichen für die Verarbeitung bietet. Besonders, wenn die Übermittlung von Daten für die Verarbeitung unabdingbar ist (z.B. Zentralisierung einer internationalen Humanressourcen-Datenbank, die kontinuierlich und systematisch mit Daten gespeist werden muss, die aus den einzelnen Ländern übermittelt werden müssen), könnte es die für die Verarbeitung Verantwortlichen vor unlösbare Probleme stellen, wenn auch nur ein Betroffener im Nachhinein beschließt, seine Einwilligung zurückzuziehen. Streng genommen dürfen die Daten dieser Person nach Widerruf der Einwilligung nicht übermittelt werden. Andernfalls würden Daten teilweise auf der Grundlage der Einwilligung des*

[36] WP12 - Arbeitsunterlage: Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU, angenommen am 24. Juli 1998.

[37] Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995, angenommen am 25.11.2005.

Betroffenen weiterhin übermittelt werden, doch müsste für Daten von einer Person, die ihre Einwilligung zurückzieht, eine Alternativlösung (Vertrag, verbindliche Unternehmensregelung usw.) gefunden werden. Das Erfordernis der Einwilligung kann also als vermeintlich gute Lösung erscheinen, die auf den ersten Blick einfach, in der Praxis jedoch komplex und schwerfällig ist."

III.A.5. Einwilligung von Personen mit eingeschränkter Rechts- und Geschäftsfähigkeit

Richtlinie 95/46/EG sieht keine besonderen Regeln vor, die bei dem Einholen der Einwilligung von Personen mit eingeschränkter Rechts- und Geschäftsfähigkeit, einschließlich Kindern, einzuhalten sind. Es ist wichtig, dass dies bei der Überprüfung der Datenschutzrichtlinie berücksichtigt wird. Zusätzlich zu den oben angesprochenen Fragestellungen, sind mit der Einwilligung von Personen dieses Personenkreises eigene, besondere Probleme verbunden.

In Bezug auf Kinder variieren die Bedingungen für eine gültige Einwilligung von Mitgliedstaat zu Mitgliedstaat. Die Artikel-29-Datenschutzgruppe hat das Thema der Einwilligung von Kindern bei mehreren Gelegenheiten überdacht und die nationalen Verfahrensweisen untersucht[38].

Wie bisherige Arbeiten zeigen, kann in Bezug auf die Einwilligung von Kindern die rechtliche Verpflichtung bestehen, die Einwilligung des Kindes und seines Vertreters einzuholen oder nur des Kindes, wenn es bereits mündig ist. Das Alter, in dem die eine oder die andere Regel gilt, ist unterschiedlich. Es gibt keine harmonisierten Vorgehensweisen zur Überprüfung des Alters des Kindes.

Der Mangel an diesbezüglichen Regeln führt zu einem fragmentierten Ansatz. Dadurch wird nicht anerkannt, dass Kinder aufgrund ihrer Verletzlichkeit unter bestimmten Umständen eines besonderen Schutzes bedürfen und dass dieser fragmentierte Ansatz zu Rechtsunsicherheit führt, insbesondere in Bezug auf die Weise, in der die Einwilligung des Kindes eingeholt wird.

Die Datenschutzgruppe ist der Ansicht, dass die fehlende Harmonisierung Folgen für die Rechtssicherheit hat. Eine Harmonisierung der Voraussetzungen, unter denen Personen mit eingeschränkter Rechts- und Geschäftsfähigkeit ihre Rechte auf EU-Ebene insbesondere in Bezug auf die Altersgrenze ausüben können, würde sicher zusätzliche Garantien mit sich bringen. Der Datenschutzgruppe ist es jedoch bewusst, dass dies möglicherweise über den Geltungsbereich des Datenschutzes hinausgeht, da eher zivilrechtliche Fragen betroffen sind. Die Datenschutzgruppe lenkt die Aufmerksamkeit der Kommission auf die Herausforderungen in diesem Bereich.

Außerdem ist die Artikel-29-Datenschutzgruppe der Ansicht, dass die Interessen von Kindern und von anderen Personen mit eingeschränkter Rechts- und Geschäftsfähigkeit besser geschützt wären, wenn die Richtlinie zusätzliche Bestimmungen enthalten würde,

[38] WP147 - Arbeitspapier 1/2008 zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen); WP160 Stellungnahme 2/2009 zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen).

die sich besonders auf die Erhebung und weitere Verarbeitung ihrer personenbezogenen Daten beziehen. Diese Bestimmungen könnten die Umstände nennen, unter denen die Einwilligung des Vertreters entweder zusammen mit der Einwilligung der Person mit eingeschränkter Rechts- und Geschäftsfähigkeit erforderlich ist oder an deren Stelle. Sie könnte auch die Umstände nennen, unter denen es nicht möglich ist, die Einwilligung als Grundlage für die Legitimierung der Verarbeitung personenbezogener Daten zu nutzen. Es sollte auch eine Anforderung für die Verwendung von Online-Mechanismen zur Überprüfung des Alters vorgesehen werden. Es gibt verschiedene Mechanismen und verschiedene Grenzwerte. Die Altersüberprüfung könnte beispielsweise statt Gegenstand einer einzelnen Bestimmung zu sein, auf dem Ansatz einer gleitenden Skala beruhen, bei der die zu verwendenden Mechanismen von den Umständen, wie der Art der Verarbeitung (Zwecke), dem Vorliegen eines besonderen Risikos, der Art der erhobenen Daten, der Verwendung der Daten (für die Offenlegung bestimmt oder nicht) usw. abhängen könnten.

III.B. Richtlinie 2002/58/EG

Die kürzlich geänderte Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG)[39] ist ein *lex specialis* im Hinblick auf die Richtlinie 95/46/EG, das sie eine sektorspezifische Regelung in Bezug auf die Privatsphäre und die elektronische Kommunikation bietet. Die meisten ihrer Bestimmungen finden nur auf die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste Anwendung (z.B. Anbieter von Telefon- oder Internetdiensten usw.).

Einige der Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation setzen auf die Einwilligung als Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste[40]. Das ist beispielsweise der Fall bei der Verwendung von Verkehrs- oder Standortdaten.

Die Artikel-29-Datenschutzgruppe hält es für sinnvoll, ausgewählte Aspekte von besonderem Interesse in Hinblick auf die Verwendung der Einwilligung im Sinne der Datenschutzrichtlinie für elektronische Kommunikation zu kommentieren. Diesbezüglich werden die folgenden fünf Fragen erörtert:

a) Die Beziehung zwischen der Definition und der allgemeinen Bedeutung der Einwilligung in Bezug auf die Richtlinie 95/46/EG und die Datenschutzrichtlinie für elektronische Kommunikation, basierend auf Artikel 2 Absatz 2 Buchstabe f der Datenschutzrichtlinie für elektronische Kommunikation.

b) Die Frage ob für eine Verletzung der Vertraulichkeit der Kommunikation (beispielsweise zur Überwachung oder zum Abfangen einer Telefonnachricht) die

---

39 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, 18.12.2009.

40 „Verkehrsdaten“ sind Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden. Dazu zählen auch Daten über Leitwege, Dauer und Zeitpunkt einer Nachricht.

Einwilligung eines oder beider Kommunikationspartner erforderlich ist. Dies wird in Artikel 6 Absatz 3 und in Artikel 5 Absatz 1 geregelt.

c) Die Frage bezüglich des Zeitpunkts, zu dem die Einwilligung erhalten werden muss. Diese Frage wird in verschiedenen Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation geregelt, einschließlich Artikel 5 Absatz 3, Artikel 6 und 13.

d) Den Anwendungsbereich des Rechts auf Ablehnung der Verarbeitung und die Unterscheidung zwischen dem Recht auf Ablehnung und der Einwilligung. Diese Unterscheidung kann in Artikel 13 der Datenschutzrichtlinie für elektronische Kommunikation analysiert werden.

e) Die Möglichkeit, die Einwilligung zurückzuziehen, wie es ausdrücklich in Artikel 6 Absatz 3 und in Artikel 9 Absätze 3 und 4 der Datenschutzrichtlinie für elektronische Kommunikation vorgesehen ist.

III.B.1. Artikel 2 Buchstabe f – Einwilligung und Bezug zu Richtlinie 95/46/EG

„Einwilligung eines Nutzers oder Teilnehmers“

Artikel 2 der Datenschutzrichtlinie für elektronische Kommunikation legt ausdrücklich fest, dass die Begriffsbestimmungen der Richtlinie 95/46/EG auch für die Richtlinie 2002/58/EG gelten. In Artikel 2 Buchstabe f steht: *„Einwilligung eines Nutzers oder Teilnehmers* (bezeichnet) *die Einwilligung der betroffenen Person im Sinne von Richtlinie 95/46/EG.“*

Das heißt, immer wenn gemäß der Datenschutzrichtlinie für elektronische Kommunikation eine Einwilligung erforderlich ist, gelten für die Gültigkeit der Einwilligung die in Richtlinie 95/45/EG festgelegten Kriterien, also die Definition in Artikel 2 Buchstabe h und die spezielle Bestimmung aus Artikel 7 Buchstabe a. Die Ansicht, dass die Einwilligung in der Datenschutzrichtlinie für elektronische Kommunikation unter Bezugnahme auf Artikel 2 Buchstabe h und Artikel 7 Buchstabe a zu verstehen ist, wird in Erwägungsgrund 17[41] bestätigt.

III.B.2. Artikel 5 Absatz 1 – Zur Frage, ob die Einwilligung von einer oder zwei Parteien erforderlich ist

“*…Einwilligung der betroffenen Nutzer …*”

Artikel 5 Absatz 1 der Datenschutzrichtlinie für elektronische Kommunikation schützt die Vertraulichkeit von Nachrichten, indem er jede Art des Abfangens oder Überwachens von Nachrichten ohne Einwilligung der betroffenen Nutzer verbietet.

[41] Dort steht zu lesen: *„Für die Zwecke dieser Richtlinie sollte die Einwilligung (...) dieselbe Bedeutung haben wie der in der Richtlinie 95/46/EG (...)“*.

In diesem Fall fordert Artikel 5 Absatz 1 die Einwilligung *„aller betroffenen Nutzer“*, mit anderen Worten beider Kommunikationspartner. Die Einwilligung nur einer der beiden Parteien reicht nicht aus.

Bei der Ausarbeitung ihrer Stellungnahme 2/2006[42] hat die Artikel-29-Datenschutzgruppe Dienste untersucht, die das Filtern des Inhalts von E-Mails und in einigen Fällen das Öffnen von E-Mails beinhalten. Die Datenschutzgruppe hat Bedenken geäußert, dass eine der beiden Kommunikationspartner nicht informiert wurde. Damit diese Dienste die Bestimmungen von Artikel 5 Absatz 1 erfüllen, ist die Einwilligung beider Parteien erforderlich.

III.B.3 Artikel 5 Absätze 3, Artikel 9 und 13 und Artikel 5 Absatz 3 – Zeitpunkt, wann die Einwilligung erforderlich ist

„... klare und umfassende Informationen erhalten hat ...“

Mehrere Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation bringen entweder explizit oder implizit zum Ausdruck, dass die Einwilligung vor der Verarbeitung eingeholt werden muss. Dies entspricht der Richtlinie 95/46/EG.

Artikel 6 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation bezieht sich ausdrücklich auf die vorherige Einwilligung des betroffenen Teilnehmers oder Nutzers und legt die Pflicht fest, dass vor der Verarbeitung personenbezogener Daten für die Zwecke der Vermarktung elektronischer Kommunikationsdienste oder von Diensten mit Zusatznutzen, Informationen erteilt und die Einwilligung eingeholt werden muss. Für manche Arten von Diensten kann die Einwilligung des Teilnehmers zum Zeitpunkt der Subskription des Dienstes eingeholt werden. In anderen Fällen ist es vielleicht möglich, die Einwilligung direkt vom Nutzer zu erhalten. Artikel 9 zur Verarbeitung anderer Standortdaten als Verkehrsdaten verfolgt einen ähnlichen Ansatz. Der Diensteanbieter muss die Nutzer oder Teilnehmer über die Art der anderen Standortdaten als Verkehrsdaten informieren, die verarbeiten *werden, bevor er ihre Einwilligung erhält*. Artikel 13 legt fest, dass die Verwendung von automatischen Anrufsystemen ohne menschlichen Eingriff, Faxgeräten oder elektronischer Post für die Zwecke der Direktwerbung nur bei vorheriger Einwilligung der Teilnehmer gestattet werden darf.

Artikel 5 Absatz 3 enthält eine spezielle Bestimmung bezüglich der Speicherung von Informationen oder des Zugriffs auf Informationen, die im Endgerät eines Nutzers gespeichert sind. Darunter fällt auch der Zweck der Verfolgung der Online-Aktivitäten des Nutzers. Auch wenn Artikel 5 Absatz 3 das Wort „vorherig“ nicht nutzt, ist dies eine klare und eindeutige Schlussfolgerung aus dem Wortlaut der Bestimmung.

Es ist sinnvoll, die Einwilligung zu erhalten, bevor die Datenverarbeitung beginnt. Andernfalls wäre die Verarbeitung in dem Zeitraum zwischen dem Einsetzen der Datenverarbeitung und dem Erhalt der Einwilligung wegen des Fehlens der Rechtsgrundlage rechtswidrig. Wenn sich die betroffene Person in einem solchen Fall

[42] Stellungnahme 2/2006 zu Datenschutzfragen bei Filterdiensten für elektronische Post, angenommen am 21.2.2006 (WP118).

gegen die Einwilligung entscheiden würde, wäre die Datenverarbeitung, die bereits stattgefunden hat, auch noch aus diesem Grund rechtswidrig.

Aus oben Stehendem ergibt sich, dass eine *erforderliche* Einwilligung stets vor dem Beginn der Datenverarbeitung vorliegen muss. Die Möglichkeit, mit der Verarbeitung zu beginnen, bevor die Einwilligung vorliegt, ist nur dann rechtmäßig, wenn die Datenschutzrichtlinie oder die Datenschutzrichtlinie für elektronische Kommunikation nicht die Einwilligung fordert, sondern stattdessen eine andere Rechtsgrundlage bietet und auf das Recht der betroffenen Person verweist, zu widersprechen oder die Verarbeitung abzulehnen. Diese Mechanismen unterscheiden sich deutlich von der Einwilligung. In diesen Fällen kann die Verarbeitung bereits begonnen haben und die betroffene Person hat das Recht zu widersprechen oder sie abzulehnen.

Ein Beispiel befindet sich in Artikel 5 Absatz 3 der ehemaligen Datenschutzrichtlinie für elektronische Kommunikation. Hier steht, dass (eigene Hervorhebung*): „die Benutzung elektronischer Kommunikationsnetze für die Speicherung von Informationen oder den Zugriff auf Informationen, die im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur unter der Bedingung gestattet ist, dass der betreffende Teilnehmer oder Nutzer gemäß der Richtlinie 95/46/EG klare und umfassende Informationen insbesondere über die Zwecke der Verarbeitung erhält und durch den für diese Verarbeitung Verantwortlichen auf das Recht hingewiesen wird, diese Verarbeitung zu verweigern.“* Das sollte mit dem neuen Wortlaut von Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation in der durch die Richtlinie 2009/136/EG[43] geänderten Fassung verglichen werden. Diese legt fest, dass *„die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer (...) seine Einwilligung gegeben hat.“* Die Folgen dieser Änderung des Wortlauts von Artikel 5 Absatz 3 wurden in der Stellungnahme 2/2010 der Artikel-29-Datengruppe zur Werbung auf Basis von Behavioural Targeting[44] erklärt. Der Unterschied zwischen Widerspruch und Einwilligung wird im nächsten Kapitel weiter ausgeführt

In vielen Fällen, in denen die Datenschutzrichtlinie für elektronische Kommunikation oder die Datenschutzrichtlinie die Möglichkeit bieten, die Verarbeitung der personenbezogenen Daten abzulehnen, ist der Grund, dass die Rechtsgrundlage für die ursprüngliche Datenverarbeitung eine *andere* als die Einwilligung ist, wie beispielsweise ein bestehender Vertrag. Das wird im nächsten Abschnitt weiter dargelegt, der Artikel 13 der Datenschutzrichtlinie für elektronische Kommunikation kommentiert.

---

43 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, Text von Bedeutung für den EWR, ABl. L 337 vom 18.12.2009, S. 0011-0036.

44 Stellungnahme vom 22. Juni 2010, WP 171: die Frage, ob eine Einwilligung über die „entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung” [Erwägungsgrund 66 der Richtlinie 2009/136/EG] erfolgen kann, wird ausdrücklich in Punkt 4.1.1 von WP 171 behandelt.

III.B.4. Artikel 13 Absätze 2-3 – Recht auf Widerspruch und Abgrenzung zur Einwilligung

„…die Kunden klar und deutlich die Möglichkeit erhalten, (...) abzulehnen"

Artikel 13 der Datenschutzrichtlinie für elektronische Kommunikation sieht vor, dass das Versenden von elektronischen Nachrichten für die Direktwerbung durch den Erhalt der Einwilligung rechtmäßig ist. Sie stützt sich dabei auf ein Standardprinzip und auf eine spezielle Bestimmung.

Die Verwendung von automatischen Anrufmaschinen, Faxgeräten oder elektronischer Post bedarf der vorherigen Einwilligung der betroffenen Person.

Wenn der Empfänger einer Werbenachricht ein bestehender Kunde ist und der Anbieter mit der Nachricht Werbung für eigene ähnliche Produkte oder Dienstleistungen machen möchte, bedarf es nicht der Einwilligung, sondern es muss gemäß Artikel 13 Absatz 2 sichergestellt werden, dass der Kunde *„die Möglichkeit erhalten hat, abzulehnen"*. Erwägungsgrund 41 erklärt, warum der Gesetzgeber in diesem Fall keine Einwilligung verlangt hat: *„Im Rahmen einer bestehenden Kundenbeziehung ist es vertretbar, die Nutzung elektronischer Kontaktinformationen zuzulassen, damit ähnliche Produkte oder Dienstleistungen angeboten werden"*. Folglich ist im Prinzip die Kundenbeziehung zwischen der betroffenen Person und dem Diensteanbieter die Rechtsgrundlage, die den ersten Kontakt über E-Mail erlaubt. Die betroffenen Personen sollten jedoch die Möglichkeit haben, weitere Kontaktaufnahmen abzulehnen. Das hat die Datenschutzgruppe bereits angegeben: *„Diese Möglichkeit sollte ferner mit jeder weiteren als Direktwerbung gesendeten Nachricht gebührenfrei angeboten werden, wobei Kosten für die Übermittlung der Ablehnung nicht unter die Gebührenfreiheit fallen."*[45]

Das Erfordernis der Einwilligung sollte von dem Recht auf Widerspruch unterschieden werden. Wie in dem vorstehenden Kapitel III.A.2 dargelegt wurde, erfüllt eine Einwilligung, die auf der ausbleibenden Handlung der betroffenen Person beruht, beispielsweise durch vorher angekreuzte Kästchen, nicht die Anforderung einer gültigen Einwilligung im Sinne der Richtlinie 95/46/EG. Dieselbe Schlussfolgerung gilt für Browser-Einstellungen, die standardmäßig das Targeting der Nutzer zulassen (durch die Verwendung von Cookies). Das wird in dem oben in Kapitel III.B.3 zitierten neuen Wortlaut von Artikel 5 Absatz 3 deutlich gemacht. Diese beiden Beispiele erfüllen insbesondere die Forderung nach einer Willensbekundung ohne jeden Zweifel nicht. Es ist unerlässlich, dass die betroffene Person die Möglichkeit erhält, eine Entscheidung in Hinblick auf den Zweck der Datenverarbeitung zu treffen und diese zum Ausdruck zu bringen, beispielsweise, indem sie das Feld selbst markiert.

In ihrer Stellungnahme zur Werbung auf Basis von Behavioural Targeting steht folgende Schlussfolgerung der Datenschutzgruppe zu lesen: *„scheint es von größter Bedeutung zu sein, dass Browser standardmäßig über Datenschutz-Einstellungen verfügen. Anders ausgedrückt sollten sie die Einstellung „keine Annahme und keine Übermittlung von Third-Party-Cookies" haben. Zur Vervollständigung und für eine*

[45] Stellungnahme 5/2004 zu unerbetenen Werbenachrichten im Sinne von Artikel 13 der Richtlinie 2002/58/EG, angenommen am 27.02.2004.

größere Effizienz, sollten die Browser so eingestellt sein, dass Nutzer vor der Installation des Browser oder dem Herunterladen eines Updates von einem Assistenten durch ein Datenschutz-Programm geführt werden. Außerdem sollten Browser es den Nutzern ermöglichen, Wahlmöglichkeiten auf einfache Weise während der Nutzung des Browsers wahrzunehmen.“[46].

III.B.5. Artikel 6 Absatz 3, Artikel 9 Absätze 3-4. – Möglichkeit, die Einwilligung zurückzuziehen

„… Möglichkeit, die Einwilligung jederzeit zurückzuziehen …“

Die Möglichkeit, die Einwilligung zurückzuziehen, die in Richtlinie 95/46/EG implizit zum Ausdruck gebracht wird, wird in verschiedenen Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation aufgegriffen. Das wurde ausdrücklich in der Stellungnahme der Datenschutzgruppe zur Nutzung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen zum Ausdruck gebracht:[47]

„Gemäß Artikel 9 der Richtlinie 2002/58/EG können Personen, die ihre Einwilligung zur Verarbeitung anderer Standortdaten als Verkehrsdaten erteilt haben, diese Einwilligung jederzeit zurückziehen; ferner müssen sie die Möglichkeit haben, die Verarbeitung solcher Daten auf einfache Weise und gebührenfrei zeitweise zu untersagen. Die Gruppe misst diesen Rechten – die als Ausübung des Rechts auf Widerspruch gegen die Verarbeitung von Standortdaten ausgelegt werden können – größte Bedeutung bei, da es sich bei Standortdaten naturgemäß um sensible Daten handelt. Nach Überzeugung der Gruppe ist es eine Vorbedingung für die Ausübung dieser Rechte, dass die betroffenen Personen stets informiert werden, und zwar nicht nur, wenn sie sich für die Teilnahme an einem Dienst anmelden, sondern auch wenn sie den Dienst nutzen. Erfordert ein Dienst die kontinuierliche Verarbeitung von Standortdaten, so sollte der Diensteanbieter nach Auffassung der Gruppe die betroffene Person regelmäßig darauf hinweisen, dass der Standort ihres Endgeräts bestimmt wurde, bestimmt wird oder bestimmt werden kann. Somit ist die Person in der Lage, ihr Recht auf Widerruf der Einwilligung nach Artikel 9 der Richtlinie 2002/58/EG auszuüben, falls sie dies wünscht.“

Wie oben bereits dargelegt wurde, impliziert das, dass die Einwilligung für die Zukunft zurückgezogen wird und nicht für die Verarbeitung personenbezogener Daten, die bereits in der Vergangenheit stattgefunden hat, als die Daten rechtmäßig erhoben wurden. Entscheidungen oder Prozesse, die vorher auf der Grundlage dieser Informationen getroffen wurden, können folglich nicht einfach aufgehoben werden. Wenn es jedoch keine weitere Rechtsgrundlage gibt, die die weitere Speicherung der Daten rechtfertigt, sollten sie von dem für die Datenverarbeitung Verantwortlichen gelöscht werden.

---

[46] Stellungnahme vom 22.06.2010, WP 171, op.cit.

[47] Stellungnahme 5/2005 zur Nutzung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen, angenommen am 25.11.2005 (WP115).

IV. Schlussfolgerungen

Die vorliegende Stellungnahme befasst sich mit dem Rechtsrahmen für die Nutzung der Einwilligung im Sinne der Richtlinien 95/46/EG und 2002/58/EG. Damit werden zwei Ziele verfolgt: erstens sollen die bestehenden rechtlichen Erfordernisse geklärt werden. Es soll auch aufgezeigt werden, wie sie in der Praxis funktionieren. Gleichzeitig soll dabei zweitens überlegt werden, ob der bestehende Rechtsrahmen angesichts der vielen neuen Wege der Verarbeitung personenbezogener Daten nach wie vor geeignet ist oder ob Änderungen erforderlich sind.

IV.1. Klärung der Schlüsselaspekte des geltenden Rechtsrahmens

Artikel 2 Buchstabe h der Richtlinie 95/46/EC definiert Einwilligung als „jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden." Artikel 7 der Richtlinie legt die Rechtsgrundlage für die Verarbeitung personenbezogener Daten dar und nennt eine Einwilligung *ohne jeden Zweifel* als eine der Rechtsgrundlagen. Artikel 8 fordert eine ausdrückliche Einwilligung als Rechtsgrundlage für die Verarbeitung sensibler Daten. Artikel 26 Absatz 1 der Richtlinie 95/46/EG und verschiedene Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation verlangen die Einwilligung für bestimmte Datenverarbeitungen innerhalb ihres Anwendungsbereichs. Mit den in dieser Stellungnahme ausgearbeiteten Punkten sollen die verschiedenen Elemente dieses Rechtsrahmens geklärt werden, um so die Anwendung für die Beteiligten zu vereinfachen.

Elemente/Beobachtungen allgemeiner Natur

- Die Einwilligung ist eine der sechs Rechtsgrundlagen für die Verarbeitung personenbezogener Daten (eine von fünf für sensible Daten). Sie ist eine wichtige Rechtsgrundlage, da sie der betroffenen Person ein gewisses Maß an Kontrolle über die Verarbeitung ihrer Daten gibt. Die Bedeutung der Einwilligung als Voraussetzung für die Autonomie und Selbstbestimmung des Einzelnen stützt sich auf ihre Anwendung im richtigen Kontext und mit den notwendigen Elementen.

- Allgemein gesprochen findet der Rechtsrahmen der Richtlinie 95/46/EG immer Anwendung, wenn eine Einwilligung eingeholt werden soll, unabhängig davon, ob dies Offline oder Online geschieht. Wenn ein klassischer Einzelhändler beispielsweise nach Personen sucht, die sich auf einem Papiervordruck für ein Treuekartensystem registrieren lassen, gelten dieselben Regeln, wie wenn er sie über seinen Internetauftritt suchen würde. Außerdem legt die Datenschutzrichtlinie für elektronische Kommunikation bestimmte Datenverarbeitungen fest, die der Einwilligung bedürfen: sie beziehen sich meistens auf die Verarbeitung von Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste. Damit eine Einwilligung gültig ist, muss sie im Sinne der Richtlinien 2002/58/EG und 1995/46/EG dieselben Voraussetzungen erfüllen.

- Situationen, in denen für die Datenverarbeitung Verantwortliche die Einwilligung als Rechtsgrundlage für die Verarbeitung personenbezogener Daten nutzen, sollten nicht mit Situationen verwechselt werden, in denen der für die Datenverarbeitung Verantwortliche die Verarbeitung auf andere Rechtsgrundlagen stützt, die ein

individuelles Widerspruchsrecht beinhalten. Dies kann beispielsweise der Fall sein, wenn sich die Verarbeitung gemäß Artikel 7 Buchstabe f der Richtlinie 95/46/EG auf das „berechtigte Interesse“ des für die Datenverarbeitung Verantwortlichen bezieht, die betroffene Person jedoch im Sinne von Artikel 14 Buchstabe a der Richtlinie 95/46/EG ein Widerspruchsrecht hat. Ein weiteres Beispiel ist, wenn der für die Datenverarbeitung Verantwortliche E-Mail-Nachrichten an bestehende Kunden sendet, um seine eigenen oder ähnliche Produkte oder Dienstleistungen zu vertreiben, die betroffenen Personen aber gemäß Artikel 13 Absatz 2 der Richtlinie 2002/58/EG das Recht haben, abzulehnen. In beiden Fällen hat die betroffene Person das Recht auf Widerspruch. Das ist nicht das gleiche wie die Einwilligung.

- Die Berufung auf die Einwilligung zur Verarbeitung personenbezogener Daten enthebt den für die Datenverarbeitung Verantwortlichen nicht seiner Pflicht, die anderen Erfordernisse des Datenschutzrechtsrahmens zu erfüllen, beispielsweise das Prinzip der Verhältnismäßigkeit im Sinne von Artikel 6 Absatz 1 Buchstabe c, Sicherheit der Verarbeitung gemäß Artikel 17 usw.

- Eine gültige Einwilligung setzt die Fähigkeit der betroffenen Person zur Einwilligung voraus. Die Regeln bezüglich der Fähigkeit auf Einwilligung sind nicht harmonisiert und unterscheiden sich von Mitgliedstaat zu Mitgliedstaat.

- Personen, die eingewilligt haben, sollten die Möglichkeit haben, ihre Einwilligung zurückzuziehen und so eine weitere Verarbeitung ihrer personenbezogenen Daten zu verhindern. Das wird auch in der Datenschutzrichtlinie für elektronische Kommunikation für bestimmte Datenverarbeitungen bestätigt, die auf der Einwilligung basieren, wie beispielsweise die Verarbeitung von anderen Standortdaten als Verkehrsdaten.

- Die Einwilligung muss erteilt werden, bevor die Verarbeitung der personenbezogenen Daten beginnt. Sie kann jedoch im Fall eines neuen Zwecks auch während der Verarbeitung erforderlich sein. Dies wird in verschiedenen Bestimmungen der Richtlinie 2002/58/EG betont, entweder durch das Erfordernis „vorherig“ (z.B. Artikel 6 Absatz 4) oder durch den Wortlaut der Bestimmungen (z.B. Artikel 5 Absatz 3).

Spezielle Elemente des Rechtsrahmens, die sich auf die Einwilligung beziehen

- Damit eine Einwilligung gültig ist muss sie *ohne Zwang* erfolgen. Das heißt, dass kein Risiko der Täuschung, Einschüchterung oder deutlicher negative Folgen für die betroffene Person bestehen darf, wenn sie ihre Einwilligung nicht gibt. Bei der Datenverarbeitung im Beschäftigungsbereich, wo eine gewisse Abhängigkeit vorliegt und im öffentlichen Dienst, beispielsweise im Bereich der Gesundheit, muss möglicherweise genau bewertet werden, ob der Einzelne ohne Zwang einwilligen kann.

- Eine Einwilligung muss *für den konkreten Fall* erfolgen. Eine pauschale Einwilligung ohne genaue Festlegung des Zwecks ist nicht rechtmäßig. Diese Informationen sollten nicht in den allgemeinen Geschäftsbedingungen des Vertrags stehen, sondern es sollten stattdessen spezielle Einwilligungsklauseln gesondert von den allgemeinen Geschäftsbedingungen verwendet werden.

- Eine Einwilligung muss *in Kenntnis der Sachlage* erfolgen. Artikel 10 und 11 der Datenschutzrichtlinie listen die Informationen auf, die den betroffenen Personen unbedingt erteilt werden müssen. Sie müssen auf jeden Fall ausreichen, um den betroffenen Personen eine gut fundierte Entscheidung über die Verarbeitung ihrer personenbezogenen Daten zu ermöglichen. Die Notwendigkeit einer Entscheidung „in Kenntnis der Sachlage" wird in zwei zusätzliche Anforderungen umgesetzt. Erstens muss bei der Vermittlung der Information die Verwendung einer angemessenen Sprache sichergestellt werden, so dass die betroffenen Personen verstehen, in was und für welchen Zweck sie einwilligen. Das ist kontextabhängig. Die Verwendung eines überkomplizierten juristischen oder technischen Fachjargons erfüllt nicht die gesetzlichen Anforderungen. Zweitens müssen die dem Nutzer gegebenen Informationen klar und ausreichend auffällig sein, so dass die Nutzer sie nicht übersehen können. Die Informationen müssen den Betroffenen direkt gegeben werden. Es reicht nicht aus, dass sie irgendwo verfügbar sind.

- In Bezug auf die Art der Einwilligung fordert Artikel 8 Absatz 2 Buchstabe a eine *ausdrückliche* Einwilligung in die Verarbeitung sensibler Daten. Das bedeutet, dass eine aktive Antwort, entweder mündlich oder schriftlich erfolgen muss, durch die die betroffene Person ihren Wunsch zum Ausdruck bringt, dass ihre Daten für bestimmte Zwecke verarbeitet werden. Folglich kann eine ausdrückliche Einwilligung nicht durch ein vorher angekreuztes Kästchen eingeholt werden. Die betroffene Person muss eine positive Handlung durchführen, um ihre Einwilligung auszudrücken und sie muss die Möglichkeit haben, nicht einzuwilligen.

- Für die Verarbeitung von personenbezogenen Daten, die keine sensible Daten sind, fordert Artikel 7 Buchstabe a, dass die Einwilligung *ohne jeden Zweifel* gegeben werden muss. „Ohne jeden Zweifel" erfordert die Verwendung von Mechanismen zur Einholung der Einwilligung, die keinen Zweifel an der Einwilligungsabsicht der betroffenen Person lassen. Das heißt in der Praxis, dass die für die Datenverarbeitung Verantwortlichen verschiedenen Arten von Mechanismen nutzen können, um die Einwilligung einzuholen. Diese reichen von Erklärungen, mit denen die Zustimmung zum Ausdruck gebracht wird (ausdrückliche Einwilligung) bis zu Mechanismen, die auf Handlungen bauen, mit denen die Zustimmung zum Ausdruck gebracht werden soll.

- Eine Einwilligung, die auf der ausbleibenden Reaktion oder dem Schweigen der betroffenen Person basiert, ist normalerweise nicht gültig. Dies gilt insbesondere für das Online-Umfeld. Diese Frage stellt sich vor allem in Bezug auf die Verwendung von Standardeinstellungen, die die betroffene Person ändern muss, um die Verarbeitung abzulehnen. Das ist beispielsweise der Fall bei der Verwendung von vorher angekreuzten Kästchen oder bei Browser-Einstellungen, die standardmäßig auf das Erheben von Daten eingestellt sind.

IV.2 Bewertung des derzeitigen Rechtsrahmens und mögliche Notwendigkeit für Änderungen

Gesamtbeurteilung

Die Datenschutzgruppe ist der Ansicht, dass der derzeitige Rechtsrahmen eine Reihe gut durchdachter Regeln enthält, die die zu erfüllenden Voraussetzungen festlegen, damit

eine Einwilligung gültig ist und die Datenverarbeitung legitimiert wird. Diese Regeln gelten sowohl in der Offline- als auch der Online-Umgebung. Genauer gesagt:

Dem Rechtsrahmen gelingt die Balance zwischen einer Reihe von Bedenken. Einerseits stellt er sicher, dass nur eine echte Einwilligung in Kenntnis der Sachlage als Einwilligung angesehen wird. Diesbezüglich ist Artikel 2 Absatz h, der ausdrücklich fordert, dass die Einwilligung ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt, einschlägig und zufriedenstellend. Andererseits ist diese Anforderung keine Zwangsjacke, sondern ermöglicht eine ausreichende Flexibilität und vermeidet spezifische technologische Bestimmungen. Das illustriert der vorgenannte Artikel 2 Buchstabe h, der Einwilligung als Willensbekundung der betreffenden Person definiert. Das lässt für die Art der Willensbekundung ausreichend Gestaltungsspielraum. Artikel 7 und 8, die eine Einwilligung ohne jeden Zweifel beziehungsweise eine ausdrückliche Einwilligung fordern, erfassen gut die Notwendigkeit der Ausgeglichenheit zwischen den beiden Bedenken. Dadurch gewähren sie Flexibilität und vermeiden zu strikte Strukturen und garantieren gleichzeitig Schutz.

Das Ergebnis ist ein Rechtsrahmen, der bei der richtigen Anwendung und Umsetzung dazu in der Lage ist, mit der häufig aus technologischen Entwicklungen resultierenden großen Bandbreite an Datenverarbeitungen Schritt zu halten.

In der Praxis ist es jedoch aufgrund der fehlenden Einheitlichkeit zwischen den Mitgliedstaaten nicht immer einfach, zu entscheiden, wann eine Einwilligung erforderlich ist und insbesondere, welche Erfordernisse für eine gültige Einwilligung erfüllt sein müssen und wie sie konkret umzusetzen sind. Die Umsetzung auf nationaler Ebene hat zu unterschiedlichen Ansätzen geführt. Die nachfolgend beschriebenen, spezifischen Schwachstellen wurden in den Diskussionen mit der Artikel-29-Datenschutzgruppe herausgearbeitet und haben zu der vorliegenden Stellungnahme geführt.

Mögliche Änderungen

- Der Begriff der Einwilligung ohne jeden Zweifel ist hilfreich, um ein System zu erstellen, das nicht zu starr ist, aber dennoch einen großen Schutz bietet. Während die Einwilligung das Potential hat, zu einem vernünftigen System zu führen, wird ihre Bedeutung leider häufig missverstanden oder einfach ignoriert. Während die oben dargelegten Hinweise und Beispiele eigentlich zu einer Stärkung der Rechtssicherheit und des Schutzes der Rechte des Einzelnen beitragen sollten, wenn die Einwilligung als Rechtsgrundlage genutzt wird, verlangt die geschilderte Situation ein paar Änderungen.
- Genauer gesagt, ist die Artikel-29-Datenschutzgruppe der Ansicht, dass die Formulierung selbst („ohne jeden Zweifel“) von weiteren Klarstellungen als Teil einer Überprüfung des allgemeinen Datenschutzrechtrahmens profitieren würde. Mit der Klarstellung sollte betont werden, dass eine Einwilligung ohne jeden Zweifel die Nutzung von Mechanismen erforderlich macht, die keinen Zweifel an der Zustimmungsabsicht der betroffenen Person lassen. Gleichzeit sollte deutlich gemacht werden, dass die Verwendung von Standardeinstellungen (auf Schweigen basierende Einwilligung) nicht in sich eine Einwilligung ohne jeden Zweifel darstellt. Das gilt insbesondere in der Online-Umgebung.
- Zusätzlich zu der oben beschriebenen Klarstellung schlägt die Artikel-29-Datenschutzgruppe Folgendes vor:

i. *Erstens*, in die Definition von Einwilligung in Artikel 2 Absatz h sollte der Wortlaut „ohne jeden Zweifel“ (oder etwas Gleichwertiges) eingefügt werden, um die Ansicht zu stärken, dass nur eine Einwilligung, die auf Erklärungen oder Handlungen basiert, mit denen eine Zustimmung zum Ausdruck gebracht wird, auch eine gültige Einwilligung darstellt. Zusätzlich zu mehr Klarheit würde das das Konzept der Einwilligung im Sinne des Artikel 2 Buchstabe h an das Erfordernis einer gültigen Einwilligung im Sinne von Artikel 7 angleichen. Außerdem könnte die Bedeutung von „ohne jeden Zweifel“ in einem Erwägungsgrund des zukünftigen Rechtsrahmens näher erläutert werden.

ii. *Zweitens*, im Kontext einer allgemeinen Rechenschaftspflicht sollten die für die Datenverarbeitung Verantwortlichen nachweisen können, dass sie die Einwilligung eingeholt haben. Wenn die Beweislast verstärkt wird, so dass die für die Datenverarbeitung Verantwortlichen nachweisen müssen, dass sie die Einwilligung der betroffenen Person tatsächlich erhalten haben, sind sie dazu gezwungen, Standardpraktiken und –mechanismen einzuführen, um eine Einwilligung ohne jeden Zweifel einzuholen und sie auch nachweisen zu können. Die Art der Mechanismen ist kontextabhängig und sollte die Fakten und Umstände und insbesondere die Risiken der Verarbeitung berücksichtigen.

- Die Artikel-29-Datenschutzgruppe ist nicht überzeugt davon, dass der Rechtsrahmen grundsätzlich für jede Art der Verarbeitung, einschließlich der derzeit durch Artikel 7 der Richtlinie abgedeckten Verarbeitungen, eine ausdrückliche Einwilligung fordern sollte. Sie ist der Ansicht, dass eine Einwilligung ohne jeden Zweifel der geforderte Standard bleiben sollte. Sie umfasst sowohl eine ausdrückliche Einwilligung als auch eine Einwilligung aus *Handlungen*, die keinen Zweifel lassen. Diese Wahl gibt den für die Datenverarbeitung Verantwortlichen mehr Flexibilität beim Einholen der Einwilligung. Die Gesamtprozedur könnte so schneller und nutzerfreundlicher sein.

- Verschiedene, auf die Einwilligung Anwendung findende Aspekte des Rechtsrahmens werden aus dem Wortlaut oder der geschichtlichen Entwicklung geschlossen oder wurden durch Fallrecht oder die Stellungnahmen der Artikel-29-Datenschutzgruppe entwickelt. Die Rechtssicherheit wäre größer, wenn solche Aspekte ausdrücklich in den neuen Datenschutzrechtsrahmen integriert würden. Hierbei könnten die folgenden Punkte berücksichtigt werden:

  i. Das Einfügen einer ausdrücklichen Klausel, die den betroffenen Personen das Recht gibt, ihre Einwilligung zu widerrufen.

  ii. Die Betonung des Konzepts, dass die Einwilligung vor dem Beginn der Verarbeitung erteilt werden muss sowie vor der weiteren Nutzung der Daten für in der ursprünglichen Einwilligung nicht abgedeckte Zwecke, wenn kein anderer Rechtsgrund als die Einwilligung vorliegt.

  iii. Das Einfügen ausdrücklicher Erfordernisse bezüglich der Qualität (Pflicht, Informationen zur Datenverarbeitung in verständlicher Form und in einer klaren und einfachen Sprache zu geben) und der

Zugänglichkeit der Information (Pflicht, die Informationen auffällig, markant und direkt zugänglich zu platzieren). Dies ist von größter Bedeutung, um den betroffenen Personen eine Einwilligung in voller Kenntnis der Sachlage zu ermöglichen.

- Schließlich könnte in Bezug auf Personen, die nur eine eingeschränkte Rechts- und Geschäftsfähigkeit haben, ein verstärkter Schutz vorgesehen werden. Dies umfasst unter anderem:

    i. Klarstellung, unter welchen Umständen die Einwilligung von den Eltern oder Vertretern einer Person gegeben werden muss, die nur eingeschränkt rechts- und geschäftsfähig ist. Dazu gehört auch die Altersgrenze, bis zu der eine solche Einwilligung verpflichtend ist.

    ii. Festlegen der Pflicht, Mechanismen zur Überprüfung des Alters zu nutzen. Diese können - abhängig von den Umständen, wie dem Alter des Kindes, der Art der Verarbeitung, der Frage, ob diese besonders riskant ist und ob die Informationen bei dem für die Datenverarbeitung Verantwortlichen verbleiben oder Dritten zur Verfügung gestellt werden - variieren.

    iii. Pflicht, die Information kindgerecht zu gestalten. Denn Kinder könnten so einfacher verstehen, was eine Verarbeitung ihrer personenbezogenen Daten bedeutet und folglich einwilligen.

    iv. Besondere Sicherheiten zur Identifizierung von Datenverarbeitungen, bei denen eine Einwilligung keine mögliche Basis für die Legitimierung der Verarbeitung personenbezogener Daten sein dürfte. Ein Beispiel hierfür ist die verhaltensorientierte Internetwerbung.

Die Artikel-29-Datenschutzgruppe wird das Thema der Einwilligung wieder aufgreifen. Insbesondere entscheiden Datenschutzbehörden sowie die Datenschutzgruppe möglicherweise zu einem späteren Zeitpunkt, Leitlinien abzufassen, um diese Stellungnahme weiter zu entwickeln und dabei weitere praktische Beispiele für die Art der Einwilligung zu geben.

Brüssel, den 13. Juli 2011

Für die Datenschutzgruppe

Der Vorsitzende
Jacob KOHNSTAMM