ARTIKEL-29-DATENSCHUTZGRUPPE

01269/07/DE
WP 137

Bericht 1/2007 über die erste gemeinsame Durchsetzungsmaßnahme: Bewertung und zukünftige Schritte

Angenommen am 20. Juni

Die Datenschutzgruppe ist gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt worden. Sie ist ein unabhängiges europäisches Beratungsgremium in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG festgelegt.

Die Sekretariatsgeschäfte werden wahrgenommen von: Europäische Kommission, GD Justiz, Freiheit und Sicherheit, Direktion C (Ziviljustiz, Grundrechte und Unionsbürgerschaft), B-1049 Brüssel, Belgien, Büro Nr. LX-46 01/43.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm

DIE GRUPPE FÜR DEN SCHUTZ NATÜRLICHER PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN –

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

gestützt auf Artikel 29 sowie auf Artikel 30 Absatz 1 Buchstabe a und Absatz 3 dieser Richtlinie, ferner auf Artikel 15 Absatz 3 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002,

gestützt auf Artikel 255 EG-Vertrag und auf Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission,

gestützt auf ihre Geschäftsordnung –

HAT FOLGENDEN BERICHT ANGENOMMEN:

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

ERSTE GEMEINSAME DURCHSETZUNGSMASSNAHME
PRIVATE KRANKENVERSICHERUNGSUNTERNEHMEN

BERICHT

Erster Teil:

Erste gemeinsame Durchsetzungsmaßnahme: Bewertung und zukünftige Schritte

I. Hintergrund – Durchsetzung

In ihrem ersten Bericht über die Durchführung der Datenschutzrichtlinie (KOM(2003) 265 endgültig) forderte die Europäische Kommission die Artikel-29-Datenschutzgruppe (WP29) auf, *"die Frage der besseren Durchsetzung insgesamt periodisch zu erörtern … und zu erwägen, sektorale Untersuchungen auf EU-Ebene durchzuführen und die diesbezüglichen Normen anzugleichen"*. Das Ziel dieser Aktivitäten besteht darin, Informationen über den Grad der Durchführung zu sammeln und die Sektoren dabei zu unterstützen, mit möglichst geringem Aufwand eine bessere Rechtsbefolgung zu erzielen.

Dementsprechend beauftragte die Gruppe die Taskforce *Rechtsdurchsetzung* (Enforcement Task Force – ETF) im Juni 2004 damit, Überlegungen zu einer EU-Strategie und zu Durchsetzungskriterien anzustellen. Im November 2004 verpflichtete sich die WP29 in ihrer Entschließung zum Thema Rechtsdurchsetzung (WP101), *"proaktive Strategien zur Rechtsdurchsetzung zu entwickeln [und] Durchsetzungsmaßnahmen voranzutreiben"* und legte sechs Kriterien zur Ermittlung eines für gemeinsame Durchsetzungsmaßnahmen geeigneten Sektors fest.

Die in WP101 definierte Kombination von Kriterien legte die Wahl eines Sektors mit hochgradig harmonisierten Aktivitäten und großem Einfluss in Bezug auf den Schutz personenbezogener Daten nahe. Aus diesem Grund beschloss die WP29, sich bei ihrer ersten

gegenseitig abgestimmten Intervention auf private Krankenversicherungen und insbesondere auf die Erbringung von Krankenversicherungsleistungen zu konzentrieren.

Kürzlich bekannte sich die Kommission erneut zur Harmonisierung der Datenschutzpraxis sowie zur Verringerung der länderspezifischen Unterschiede in der Gesetzgebung. Sie rief die WP29 auf, sich weiter für diese Ziele einzusetzen und appellierte an die nationalen Datenschutzbehörden *"ihre Praxis im eigenen Land der gemeinsamen Linie anzupassen, auf die sie sich in der Datenschutzgruppe geeinigt haben"* (Mitteilung über den Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie (95/46/EG), KOM(2007) 87 endgültig, angenommen am 7. März 2007). Die Kommission hielt darüber hinaus fest, dass Abweichungen *"aufgrund des Ermessensspielraums, den die Richtlinie den Mitgliedstaaten zubilligt"* nicht generell Probleme für den Binnenmarkt schaffen. Ein höheres Maß an Konvergenz wäre jedoch nach wie vor wünschenswert, um Vereinfachungen und Initiativen zur Selbstregulierung zu fördern, die den Durchsetzungsaufwand der Datenschutzbehörden potenziell verringern und die sektorweite Rechtsbefolgung (z. B. durch die Nutzung verbindlicher unternehmensinterner Vorschriften) verbessern.

In der genannten Mitteilung führt die Kommission diese gemeinsame Untersuchung, die sich zum damaligen Zeitpunkt gerade im Durchführungsstadium befand, ausdrücklich als Argument gegen die Änderung der Richtlinie an. Ob diese Durchsetzungsmaßnahme jedoch die Ziele des im Ersten Bericht der Kommission über die Durchführung der Datenschutzrichtlinie (KOM(2003) 265 endgültig) festgelegten Arbeitsprogramms wirklich erfüllt, ist von ihren Ergebnissen abhängig. Doch selbst wenn die Ergebnisse nicht für sich sprechen – sie können nicht den einzigen Maßstab für den Erfolg dieser gemeinsamen Durchsetzungsmaßnahme bilden oder die sofortige Durchführung einer weiteren, ähnlichen Maßnahme rechtfertigen. Zur Erhöhung der Wirksamkeit künftiger Aktivitäten der Artikel-29-Datenschutzgruppe auf diesem Gebiet müssen nicht nur die Ergebnisse, sondern auch verschiedene andere Aspekte dieser ersten Erfahrung in Bezug auf gemeinsame Durchsetzungsmaßnahmen kritisch geprüft werden.

II. Schlussfolgerungen aus der Durchsetzungsmaßnahme

A. Überlegungen zur aktuellen Durchsetzungsmaßnahme

1. Die Untersuchung wurde von den Datenschutzbehörden der folgenden Mitgliedstaaten durchgeführt: *Belgien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Schweden, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Vereinigtes Königreich, Zypern.*

Die Maßnahme wurde im März 2006 durch ein Auskunftsverlangen der Datenschutzbehörden an die für die Datenverarbeitung Verantwortlichen in den einzelnen Ländern eingeleitet. Sie dauerte 13 Monate und endete mit der Vorstellung der Untersuchungsergebnisse, die diesem Bericht beiliegen. Die Vorgangsweise bestand in einer gemeinsamen Analyse von Antworten auf einen zuvor vereinbarten Fragenkatalog, der von allen teilnehmenden Datenschutzbehörden an ausgewählte für die Datenverarbeitung Verantwortliche in ihrem Land verteilt wurde. Diese Methode wurde gewählt, um Unterschiede hinsichtlich Untersuchungsqualität und -tiefe innerhalb der verschiedenen europäischen Datenschutzbehörden zu vermeiden, die über unterschiedliche Zuständigkeitsbereiche und Durchsetzungsmöglichkeiten verfügen.

Der beschriebene Ansatz beschränkte die Ausübung der Überwachungsfunktion durch die Datenschutzbehörden in Bezug auf die Überprüfung von Fakten und Unterlagen vor Ort von Anfang an erheblich. So war ein direkter, sofortiger Zugang zu den gewünschten Antworten und das Führen unmittelbarer Gespräche mit den für die Datenverarbeitung Verantwortlichen von vornherein ausgeschlossen, obwohl dies wesentliche Bestandteile jeder Überprüfungs- oder Auditmaßnahme sind.

Bedingt durch diese Einschränkung konnten einige nicht zufrieden stellende Antworten nicht näher untersucht werden. In anderen Fällen ergaben sich Situationen, die auf nationaler Ebene weiter verfolgt werden könnten. Eine genaue Untersuchung ist auf gemeinsamer europäischer Ebene aber nicht möglich, weil dazu, wie oben erwähnt, zum Abklären von Informationen (z. B. welche Arten von genetischen Informationen gesammelt werden, wozu, auf welcher rechtlichen Grundlage) ein direkter Kontakt mit den für die Datenverarbeitung Verantwortlichen erforderlich wäre.

2. Ein weiterer verbesserungswürdiger methodischer Aspekt der Maßnahme ist ihr zentrales Befragungsinstrument: der Fragenkatalog, der von allen beteiligten Datenschutzbehörden gemeinsam ausgearbeitet wurde. Die Erarbeitung des Fragenkatalogs bildete einen

wesentlichen Bestandteil der Arbeit der Taskforce *Durchsetzung* (von Januar 2005 bis März 2006), da der Aufwand zur Zusammenstellung aller für die unterschiedlichen Anforderungen der nationalen Datenschutzgesetze erforderlichen Fragen erheblich war. Infolgedessen waren bestimmte Fragen für die Verantwortlichen für die Datenverarbeitung in Mitgliedstaaten mit andersartigen Datenschutzsystemen und -strukturen unverständlich oder irrelevant.

Ein weniger erschöpfender und ausführlicher Fragenkatalog hätte sich in diesem Fall – gemeinsam mit der Möglichkeit der unmittelbaren, praktischen Ausweitung der Prüfung (z. B. in Form von Audits oder Inspektionen) – als effektiver erweisen können. Aus diesem Grund ist es unbedingt erforderlich, dass alle Datenschutzbehörden in die Lage versetzt werden, derartige Direktmaßnahmen zu treffen und auch mit den dafür notwendigen Mitteln ausgestattet werden.

Ein besonders positiver Aspekt der ersten gegenseitig abgestimmten Durchsetzungsmaßnahme ist die dadurch hervorgerufene Tendenz der beteiligten Datenschutzbehörden zur Durchführung gemeinsamer Aktivitäten in diesem Bereich. Die durch die gemeinsame Maßnahme erzielten Vorteile und Ergebnisse haben gezeigt, dass koordinierte Durchsetzungsaktivitäten eine neue, wirksame Überwachungsstrategie sein können.

Ein weiterer ebenso wichtiger wie positiver Faktor ist die Zusammenarbeit mit Vertretungsorganisationen des Versicherungssektors auf nationaler und europäischer Ebene. Der von der Europäischen Kommission initiierte Kontakt mit dem Dachverband der nationalen Verbände der Versicherungsunternehmen (Comité Européen des Assurances – CEA) machte diese Zusammenarbeit möglich und produktiv. Der CEA kommunizierte seinen Mitgliedern die mit der Teilnahme an der Untersuchung verbundenen Vorteile und das Potenzial der Ergebnisse, zur Verbesserung der Verfahren zur Datenverwaltung beizutragen. Gleichzeitig sorgte dieser unmittelbare Kontakt mit Vertretern des Sektors für ein besseres Verständnis der Bedürfnisse und Praktiken dieser Branche und ihres Einflusses auf die Verarbeitung der Daten der Begünstigten.

Hinsichtlich der Aufbereitung der Ergebnisse stellte sich die Frage, ob die Schlussfolgerungen nach Ländern oder nach Unternehmen untergliedert werden sollten. Sollten sich die Prozentangaben für jede Frage auf die Praxis in den einzelnen Mitgliedstaaten oder auf jene

der Unternehmen auf europäischer Ebene beziehen? Bei dieser ersten Untersuchung haben wir uns aus rein praktischen Gründen für Ersteres entschieden, da die nationalen Berichte keine einzelnen Unternehmen benannten, sondern nach Mitgliedstaaten aufgeschlüsselte Ergebnisse zur gängigen Praxis enthielten. Die andere genannte Variante wäre auch deshalb schwierig umzusetzen, da die Ergebnisse in den einzelnen Mitgliedstaaten keine vergleichbaren Marktanteile bzw. Unternehmen vergleichbarer Größe abdecken (möglicherweise gibt es viele Unternehmen, die die Richtlinie nicht einhalten, aber sie gehören einer kleinen Anzahl von Ländern an). Für künftige Maßnahmen muss diese Frage im Voraus entschieden werden, um die jeweiligen Kriterien festzulegen und die Fragenkataloge entsprechend anzupassen.

Es ist darauf hinzuweisen, dass diese Durchsetzungsmaßnahme in Bezug auf die Veröffentlichung der Ergebnisse absolute Vertraulichkeit gewährleistete. Die Angabe der Ergebnisse erfolgt anteilsmäßig und lässt keinerlei Rückschlüsse auf die untersuchten für die Datenverarbeitung Verantwortlichen zu. Die Wahrung der Vertraulichkeit und die gewählte Methode des gemeinsam erarbeiteten Fragenkatalogs sollte für die Durchsetzung kein Hindernis darstellen. Wenn erforderlich, werden die nationalen Datenschutzbehörden mit der Überwachung fortfahren und gegebenenfalls Korrekturmaßnahmen ergreifen.

B. Bewertung der Untersuchung

1. Was die zahlenmäßigen Ergebnisse der Umfrage anbelangt, verlief die Untersuchung positiv. In jeder Fragengruppe erwies sich die Lage in der Mehrzahl der Mitgliedstaaten als den Kriterien laut Fragenkatalog – welche die allgemeinen Grundsätze der Richtlinie reflektieren – entsprechend. Somit kann davon ausgegangen werden, dass die Grundsätze und Bestimmungen der Datenschutzrichtlinie 95/46/EG bei der Verarbeitung personenbezogener Daten durch private Krankenversicherungen generell eingehalten werden.

Trotzdem müsste größeres Augenmerk auf zwei wichtige Punkte gelegt werden:
- Selbst wenn die Ergebnisse mehrheitlich positiv sind, zeigen die ermittelten Zahlen, dass die Rechtsbefolgung in Bezug auf spezifische Fragen in einigen Mitgliedstaaten niedriger ist und

dass selbst in den Mitgliedstaaten mit hohen Befolgungsraten verschiedene Probleme im Zusammenhang mit der Praxis bestimmter Unternehmen bestehen.
- Die Ergebnisse dieser Untersuchung bestehen in einer Zusammenstellung der Antworten verschiedener Unternehmen auf einen Fragenkatalog, der unter Berücksichtigung der von der WP29 festgelegten Kriterien eigens zusammengestellt wurde. Diese Untersuchung sollte letztlich nicht nur zu einer Bewertung der richtlinienkonformen Verarbeitung von personenbezogenen Daten in den Mitgliedstaaten führen, sondern auch zu einer Überprüfung der entsprechenden Mittel.

2. Auf der Grundlage der Schlussfolgerungen ist auf einige Problemkreise und spezifische Elemente hinzuweisen, die von der WP29 und den Datenschutzbehörden bei künftigen Maßnahmen zu berücksichtigen sind:
- Aufnahme einer Frage zur Länge des Zeitraums, in dem von den untersuchten für die Datenverarbeitung Verantwortlichen personenbezogene Daten gesammelt und verarbeitet werden.
- In Bezug auf die Arten der verarbeiteten Daten erwies es sich als notwendig, weitere Informationen über alle möglichen Anwendungen zu sammeln, damit eine spezifischere Bewertung der Notwendigkeit oder rechtlichen Zulässigkeit der Verarbeitung bestimmter Datentypen vorgenommen werden kann.
- Hinsichtlich spezifischer Sicherheitsmaßnahmen, die von den für die Datenverarbeitung Verantwortlichen angewendet werden, sollten künftige Fragenkataloge einen stärker präskriptiven Charakter haben. Was die verschiedenen Positionen der Mitarbeiter angeht, die sich mit den unterschiedlichen Datentypen beschäftigen oder Zugang zu verschiedenen Anwendungen haben und dementsprechend verschiedene Arten von Informationen benötigen, wären detailliertere Angaben wünschenswert.

3. Selbst unter Berücksichtigung der operativen und methodischen Beschränkungen dieser Durchsetzungsmethode wurde im Rahmen dieser Maßnahme eine Reihe von – teilweise erheblichen – Problemen bei der Verarbeitung von Daten durch verschiedene für die Datenverarbeitung Verantwortliche ermittelt. Auf diese Probleme wird im zweiten Teil dieses Berichts eingegangen. Sie müssen – sei es im Rahmen einer separaten Initiative oder durch geeignete Maßnahmen von Seiten der entsprechenden Datenschutzbehörden – behoben werden. Darin besteht der Hauptzweck jeder Durchsetzungsmaßnahme. Das primäre Ziel wurde erreicht, doch darüber hinaus kann die Maßnahme auch einen vorauswirkenden,

beispielhaften Effekt auslösen, der sich auch auf für die Datenverarbeitung Verantwortliche ausdehnt, die von der Untersuchung nicht unmittelbar betroffen waren. Sie erhalten die Möglichkeit, ihre Praxis unter Berücksichtigung von Empfehlungen zu verbessern, die aus den Erfahrungen anderer für die Datenverarbeitung Verantwortlicher in vergleichbaren Situationen abgeleitet sind.

III. Eine Strategie für die Zukunft: gemeinsame Durchsetzungsmaßnahmen zur Harmonisierung der Vorschriften und Verbesserung der Rechtsbefolgung weltweit

Das Resultat der ersten gemeinsamen Durchsetzungsmaßnahme der WP29 war generell positiv. Die Vorteile gegenseitig abgestimmter Audits anhand identischer Kriterien, des Vergleichs von Ergebnissen und der Verbreitung vorbildlicher Verfahren in einem bestimmten Sektor stehen außer Frage. Genau diese Funktion zählt gemäß Artikel 28 und 29 der Richtlinie 95/46/EG zu den zentralen Fähigkeiten der europäischen Datenschutzbehörden.

Derartige gemeinsame Durchsetzungsmaßnahmen können und sollen verbessert werden und sich in die Richtung echter Auditaktivitäten entwickeln, die die Möglichkeit der unmittelbaren Überprüfbarkeit der Richtigkeit der Antworten erfordern. Darüber hinaus ist die Durchführung stichprobenartiger Prüfungen bei den ausgewählten für die Datenverarbeitung Verantwortlichen als integrierter Bestandteil solcher Untersuchungen nötig.

Die Auswahl neuer Sektoren oder konkreter Praktiken für derartige Audits sollte auf einer Risikobewertung bestimmter Sektoren oder Tätigkeitsfelder in Bezug auf die Wahrung der Rechte der Personen, deren Daten verarbeitet werden, basieren. Dabei sollten die Vorteile koordinierter Interventionen auf europäischer Ebene im Vergleich zu Einzelaktionen berücksichtigt werden. Diese Auswahl und Bewertung schafft ein neues Aufgabengebiet für die WP29. Gleichzeitig bietet sie eine Herausforderung für die europäischen Datenschutzbehörden, ihre Methoden, Effizienz und Fähigkeiten zur Zusammenarbeit zu verbessern.

Dementsprechend sollten wir auch die Möglichkeit einer künftigen Zusammenarbeit zwischen der WP29 und anderen internationalen Einrichtungen oder Organisationen mit der Fähigkeit zur Durchsetzung des Datenschutzes und internationalen Zusammenarbeit (Kartellbehörde,

OECD, APEC etc.) prüfen, um so zu einer weltweiten Verbesserung des Datenschutzes beizutragen. Derartige Kooperationen beruhen nicht auf rein hypothetischen Überlegungen. Mit der OECD-Arbeitsgruppe über Informationssicherheit und Datenschutz (Working Party on Information Security and Privacy – WPISP) wird bereits die Annahme von Empfehlungen für eine grenzüberschreitende Zusammenarbeit bei der Durchsetzung von Datenschutzgesetzen erörtert.

Die WPISP-Empfehlungen orientieren sich stark an dem von der WP29 genutzten Rahmen für die Zusammenarbeit und den bei dieser ersten gemeinsamen Durchsetzungsmaßnahme gewonnenen Erkenntnissen. Sie sehen die Anpassung der nationalen Systeme und die Ermächtigung der nationalen Behörden zur Förderung der Zusammenarbeit und zur Entwicklung internationaler Kooperationsmechanismen ähnlich jener der WP29 vor. Die WPISP empfiehlt auch die Umsetzung eines zuverlässigen Systems zur gegenseitigen Unterstützung, das Parallelen zur durch Artikel 28 der Richtlinie 95/46/EG festgelegten Zusammenarbeitsverpflichtung der europäischen Datenschutzbehörden aufweist. Schließlich enthalten die WPISP-Empfehlungen auch eine Aufforderung zum offenen Dialog mit den Interessengruppen, wie beispielsweise den entsprechenden Branchenverbänden, die sich bei dieser Durchsetzungsmaßnahme als ausgesprochen hilfsbereit erwiesen haben.

Die WP29 verfügt über das institutionelle Wissen, die Erfahrung, Infrastruktur und das Mandat zur weiteren Gewährleistung gemeinsamer Durchsetzungsmaßnahmen nicht nur auf europäischer und regionaler, sondern auch auf globaler Ebene. Zur Beteiligung an derartigen internationalen Maßnahmen und zur Gewährleistung, dass gemeinsame Durchsetzungsmaßnahmen weiter verfeinert und durch die kritische Bewertung von Methoden und Strategien verbessert werden, befinden wir uns daher in einer einzigartigen Position. Detaillierte Analysen von Maßnahmen wie dieser können wichtige Erkenntnisse für gemeinsame Durchsetzungsaktivitäten in einem internationalen Rahmen liefern, das Erzielen eines angemessenen Status' durch Drittländer beschleunigen und für Fortschritte in Bezug auf globale Datenschutzstandards und den ungehinderten grenzüberschreitenden Informationsfluss sorgen.

Zweiter Teil:

Schlussfolgerungen aus der Untersuchung

Dieser Teil des Berichts enthält die Schlussfolgerungen, die in den jeweiligen nationalen Berichten aus der Untersuchung der privaten Krankenversicherungen gezogen wurden. Wir haben uns entschlossen, die Rechtsbefolgung in Bezug auf die Mitgliedstaaten, nicht auf die Anzahl der Unternehmen auszulegen. Diese Entscheidung beruhte auf praktischen Überlegungen, da Marktdurchdringung und Unternehmensgrößen von Mitgliedstaat zu Mitgliedstaat unterschiedlich sind. Dementsprechend beziehen sich die Zahlen auf Mitgliedstaaten und die Prozentangaben auf den Anteil der Unternehmen in einem Mitgliedstaat, der die Richtlinie laut nationalem Bericht befolgt.

Die Ergebnisse aus der Beantwortung des Fragenkatalogs lassen sich in fünf Kategorien unterteilen: Art und Kooperativität der Unternehmen, Datenverarbeitung, Information der Personen, deren Daten verarbeitet werden, Weitergabe von Daten an Dritte, Sicherheitsmaßnahmen.

A. Unternehmen

1. Art des Unternehmens

Der Fragenkatalog richtete sich an drei Arten von Unternehmen: Unternehmen, zu deren Zielgruppen (i) Einzelpersonen, (ii) Personengruppen (z. B. Mitarbeiter eines Unternehmens) oder (iii) Familien zählen. Die Art der Zielgruppe ist ein wichtiges Element, da davon das Produktangebot und die gesammelten Daten abhängen.

In 10 Mitgliedstaaten wurden bei der Untersuchung Unternehmen berücksichtigt, die alle Arten von Versicherungen anbieten.

In 5 Mitgliedstaaten wurden bei der Untersuchung Unternehmen berücksichtigt, die Versicherungen für Einzelpersonen und Personengruppen anbieten.

In 4 Mitgliedstaaten wurden bei der Untersuchung Unternehmen berücksichtigt, die nur Versicherungen für Einzelpersonen anbieten.

In 2 Mitgliedstaaten wurden bei der Untersuchung Unternehmen berücksichtigt, die Versicherungen für Einzelpersonen und Familien anbieten.

Da bei der Untersuchung nur in 4 Mitgliedstaaten Unternehmen berücksichtigt wurden, die nur Versicherungen für Einzelpersonen anbieten, ist davon auszugehen, dass eine recht repräsentative Abdeckung erzielt wurde.

2. Marktdurchdringung

In 9 Mitgliedstaaten repräsentieren die untersuchten Unternehmen 90-100 % des Marktes. In 5 Mitgliedstaaten betrug der Grad der Marktdurchdringung 60-80 %, in 3 Mitgliedstaaten rund 50 %.

Da die Leitlinien der WP29 vorsahen, Kontakt zu Unternehmen aufzunehmen, die mindestens 50 % des Marktes repräsentieren, kann der Schluss gezogen werden, dass auch die Marktdurchdringung der befragten Unternehmen hoch ist und dass die Untersuchung von diesem Standpunkt aus betrachtet erfolgreich verlaufen ist.

3. Kooperativität

Laut Eigenbewertung durch die Datenschutzbehörden selbst wurde die Kooperativität in 15 Mitgliedstaaten als positiv oder sehr positiv eingeschätzt. Nur in 3 Mitgliedstaaten wurde die Kooperativität als negativ bzw. in einem Mitgliedstaat als mittelmäßig bezeichnet. Daraus können wir schließen, dass die Zusammenarbeit mit den beteiligten Unternehmen während der Untersuchung höchst positiv verlaufen ist.

Aus den meisten nationalen Berichten geht jedoch hervor, dass die Unternehmen die Fragen nicht immer in ausreichendem Maße verstanden haben. Im Großteil der Länder verfügen derartige Unternehmen aller Wahrscheinlichkeit nach über Teams von Juristen oder spezielle Datenschutzbeauftragte. Dementsprechend können zwar geringfügige Interpretationsschwierigkeiten auftreten, die meisten Unternehmen müssten die Rechtslage jedoch durchaus kennen. Probleme sind daher wohl nur teils auf die Fragestellung und teils auf die Ernsthaftigkeit der Bemühungen, komplette und ausführliche Antworten zu geben, zurückzuführen.

Der Fragenkatalog beinhaltete komplexe Fragestellungen. Die umfassende und aussagekräftige Beantwortung wäre mit einem erheblichen Zeit- und Arbeitsaufwand verbunden gewesen. Die Qualität der Antworten stand wohl eher im Zusammenhang mit dem für die Bearbeitung des Fragenkatalogs erforderlichen Aufwand als mit seiner Verständlichkeit.

Bei der Bewertung der Kooperativität der Unternehmen ist zu berücksichtigen, dass die Beteiligung an einer Untersuchung der Datenschutzbehörde in der überwiegenden Mehrheit der Mitgliedstaaten Bestandteil des in der nationalen Datenschutzgesetzgebung verankerten Überwachungssystems und damit verbindlich vorgeschrieben ist. Interessant wäre zu wissen, in welchen Mitgliedstaaten die Kooperativität nicht zufrieden stellend war, obwohl sie gesetzlich vorgesehen ist. Dies wäre ein lohnendes Thema für künftige Untersuchungen.

In mehreren Mitgliedstaaten wurde die Untersuchung durch den jeweiligen nationalen Verband der Versicherungsgesellschaften durchgeführt. Die Erfahrungen der Datenschutzbehörden, die mit den nationalen Verbänden Kontakt aufnahmen, waren sehr positiv. Hier zeigt sich die Wichtigkeit der Zusammenarbeit mit nationalen Verbänden bei derartigen Untersuchungen. Um einen umfassenderen Ansatz zu gewährleisten, empfiehlt es sich immer, auf nationaler Ebene mit Verbänden in Verbindung zu treten. Dies sollte bei künftigen Untersuchungen berücksichtigt werden.

B. Datenverarbeitung

1. Arten von Daten

Alle Unternehmen in allen 25 Mitgliedstaaten verarbeiten personenbezogene Informationen und Gesundheitsdaten. Dies scheint naheliegend. Doch wenn die Verarbeitung allgemeiner personenbezogener Informationen als normal betrachtet wird, müssen wir uns überlegen, in welchem Ausmaß Unternehmen Gesundheitsdaten erfassen dürfen. Gesundheitsdaten sind sensible Informationen, für die auf europäischer und nationaler Ebene strengere Schutzbestimmungen gelten und es ist nicht immer offensichtlich, dass zwischen diesen Informationen und dem Verarbeitungszweck (Verwaltung des Versicherungsvertrags) ein enger Zusammenhang besteht. Gesundheitsdaten sind eher parallelen Anwendungen wie der Risikoprüfung zuzuordnen. Das soll nicht heißen, dass diese Praxis gegen die nationale

Gesetzgebung einiger Mitgliedstaaten verstößt. Doch hier ist auf den Grundsatz der Verhältnismäßigkeit zu verweisen.

Finanzielle Daten werden in 23 Mitgliedstaaten verarbeitet. Der Zweck der Verarbeitung dieser Daten steht vor allem im Zusammenhang mit der Zahlung von Prämien und Entschädigungen.

Daten zum Versicherungsverlauf werden in 17 Mitgliedstaaten verarbeitet. Das ist ein recht hoher Anteil. Die Verarbeitung dieser Informationen erfolgt meist im Zusammenhang mit Risikoprüfungen. Das Unternehmen kann anhand dieser Daten abschätzen, ob ein Vertrag für das Unternehmen Gewinn abwirft, oder die Versicherungsprämien berechnen. Trotzdem ist es Versicherungsgesellschaften in einigen Mitgliedstaaten gesetzlich verboten, den Abschluss von Verträgen abzulehnen – vor allem aus Gründen der Gleichbehandlung beim Zugang zur Krankenversicherung. In solchen Fällen sollte die Verarbeitung von Daten zur Risikoprüfung auch dann nicht als gerechtfertigt gelten, wenn sie mit der Einwilligung der entsprechenden Person erfolgt.

In 17 Mitgliedstaaten findet eine Verarbeitung familiärer Daten statt. Dies ist nur gerechtfertigt, wenn die Familienmitglieder ebenfalls im Rahmen dieses Vertrags versichert sind. In diesem Zusammenhang sind zwei Punkte zu berücksichtigen:

(i) Einwilligung und Information der Familienmitglieder, insbesondere, wenn es sich nicht um Minderjährige handelt.

(ii) Art der familiären Daten. Aus den nationalen Berichten lässt sich nicht immer entnehmen, ob es sich bei den familiären Daten nur um allgemeine personenbezogene Informationen handelt, die zur Vertragsverwaltung erforderlich sind, oder ob darunter auch medizinische (oder sogar genetische) Informationen zu verstehen sind. In diesen Fällen vgl. die Bemerkungen zu diesen Themen.

In 6 Mitgliedstaaten werden genetische Daten gesammelt und verarbeitet. Dies ist ein hoher Prozentsatz. Die Verarbeitung genetischer Daten geschieht vor dem Hintergrund der Risikoprüfung, besitzt jedoch weit bemerkenswertere Implikationen hinsichtlich Datenschutz und Befolgung der Bestimmungen der anwendbaren Rechtsakte auf europäischer und nationaler Ebene. Laut *Arbeitspapier 91 der WP29 über genetische Daten, angenommen am 17. März 2004*, ist dies nur dann zulässig, wenn es im Gesetz vorgesehen ist. Auch die

entsprechende *Empfehlung des Europarats* aus dem Jahr 2002 ist hier anwendbar. In den meisten Mitgliedstaaten, in denen genetische Daten verarbeitet werden, wurde als wichtigste rechtliche Grundlage für diese Praxis die Einwilligung der betreffenden Person genannt. Doch diese Einwilligung kann nicht als einzige Rechtsgrundlage zur Verarbeitung genetischer Daten gelten. Dieses Thema sollte vor einem globaleren Hintergrund beleuchtet werden.

Generell lässt sich zu den verarbeiteten Daten sagen, dass ihre Art in unmittelbarem Zusammenhang mit dem Wesen des Produkts und dem Versicherungsrisiko steht. Der Fragenkatalog ging diesbezüglich nicht weiter ins Detail. Für künftige Maßnahmen wäre es sinnvoll, eine komplette Analyse aller Anwendungen und Formulare in den Fragenkatalog aufzunehmen, damit die Rechtsbefolgung besser eingeschätzt werden kann.

2. Zweck der Verarbeitung

In 22 Mitgliedstaaten bildet die Vertragsverwaltung den Hauptzweck der Datenverarbeitung. Dies ist zulässig. In einigen nationalen Berichten werden auch Identifikation und Kommunikation als Hauptzwecke für die Verarbeitung der personenbezogenen Daten genannt (in 15 bzw. 6 Mitgliedstaaten). Diese Antworten sind ebenfalls der Vertragsverwaltung zuzuordnen, da Identifikation und Kommunikation zu diesem Zweck erforderlich sind.

Risikoprüfung spielt in 20 Mitgliedstaaten eine große Rolle. Die Vereinbarkeit dieser Praxis mit dem gleichberechtigten Zugang zu privaten Krankenversicherungsleistungen sollte überdacht werden. Andererseits könnte das Verhindern von Risikoprüfungen in jenen Mitgliedstaaten, in denen diese nicht gesetzlich verboten sind, zu einer erheblichen Erhöhung der Versicherungsprämien führen. (Vgl. Bemerkungen zur Verarbeitung medizinischer und genetischer Daten oben.)

Darüber hinaus wurden als weitere wichtige Zwecke der Verarbeitung personenbezogener Daten angegeben: Direktmarketing (6 Mitgliedstaaten), Betrugsbekämpfung (4 Mitgliedstaaten), Statistik (1 Mitgliedstaat) und Beratung (1 Mitgliedstaat).

Generell muss die Verarbeitung personenbezogener Daten für sonstige Zwecke, insbesondere da diese nicht immer in engem Zusammenhang mit dem Hauptzweck stehen, in Bezug auf mehrere Faktoren bewertet werden: z. B. nationale Gesetzgebung, Befolgung der Richtlinie in

der nationalen Gesetzgebung, Einwilligung der Person, deren Daten verarbeitet werden, Qualität der Einwilligung der Person, deren Daten verarbeitet werden (freie und informierte Einwilligung) und Opt-in/Opt-out-Möglichkeiten für den Kunden. Letztere sind in einigen nationalen Gesetzen eine zulässige Praxis.

3. Rechtsgrundlagen

Die Einwilligung der Person, deren Daten verarbeitet werden, scheint die primäre Rechtsgrundlage für die Sammlung und weitere Verarbeitung personenbezogener Daten durch Versicherungsgesellschaften zu bilden. In 18 Mitgliedstaaten liegt die Einwilligungsrate bei 100 % und in weiteren 5 Mitgliedstaaten auf einem sehr hohen Niveau. Dieser Umstand kann als positives Ergebnis gewertet werden. Unklar ist jedoch, ob diese Einwilligung immer freiwillig und aufgrund ausführlicher Informationen erteilt wird. Freie und informierte Einwilligung sollte eines der Hauptkriterien für die Bewertung der Rechtsbefolgung der Unternehmen in diesem Bereich sein. In diese Richtung sollten Empfehlungen ausgesprochen werden.

Was Ausnahmeregelungen in Bezug auf die erforderliche Einwilligung anbelangt, wurde diese Frage in den nationalen Berichten nicht eindeutig behandelt, was die Bewertung erschwert. Nur in 3 Mitgliedstaaten bilden Ausnahmeregelungen hinsichtlich der benötigten Einwilligung die Rechtsgrundlage für die Sammlung und Verarbeitung personenbezogener Daten.

Dieselbe Problematik besteht im Zusammenhang mit dem Widerspruchsrecht. Die in den nationalen Berichten enthaltenen Informationen sind für eine gründliche Bewertung dieser Thematik nicht immer ausreichend oder eindeutig genug. Nur 4 Mitgliedstaaten haben diese Frage positiv beantwortet. Diese Unklarheit könnte mit der Formulierung "weitere Verarbeitung" zusammenhängen, der die betroffene Person widersprechen kann. Hier könnte eine nähere Definition dieser Verarbeitung (Direktmarketing etc.) durch die Datenschutz-behörden erforderlich sein.

Abschließend ist zu betonen, dass eine Bewertung der Rechtsgrundlagen für die Sammlung und Verarbeitung personenbezogener Daten nur in Bezug auf die entsprechenden nationalen Bestimmungen erfolgen sollte. In manchen Ländern kann die Sammlung spezifischer Daten

für den Hauptzweck bzw. sonstige Zwecke gesetzlich vorgeschrieben sein. Diesbezüglich besteht auch ein Zusammenhang mit der Zulässigkeit bzw. Unzulässigkeit von Risikoprüfungen in einigen Mitgliedstaaten. In diesen Fällen besitzt die Einwilligung der betreffenden Person möglicherweise kein großes Gewicht, da das Gesetz die primäre Rechtsgrundlage bildet.

C. Informationen

1. Informationen über Rechte

In den meisten Mitgliedstaaten ist die Rechtsbefolgung im Zusammenhang mit den Informationen, die der betroffenen Person zur Verfügung gestellt werden, gut. In 12 Mitgliedstaaten informieren 90-100 % der Unternehmen (100 % in 10 Mitgliedstaaten) die Personen, deren Daten verarbeitet werden, über ihre Rechte. In 5 Mitgliedstaaten tun dies 75-90 % bzw. in 3 Mitgliedstaaten 50-75 % der Unternehmen. Nur in 2 Mitgliedstaaten informieren weniger als 50 % der Unternehmen ihre Kunden ordnungsgemäß.

Die Information der betroffenen Person ist eine in Abschnitt IV der Richtlinie (Artikel 10 und 11) vorgesehene grundlegende Verpflichtung. Trotzdem ist dies nicht in allen Mitgliedstaaten immer der Fall. Die Information des Versicherungsnehmers, sonstiger versicherter Personen und Begünstigter des Versicherungsvertrags ist ein Bestandteil dieser grundlegenden Verpflichtung. Die Werte sind zwar hoch, es ist jedoch offen, weshalb diese Frage nicht zu 100 % positiv beantwortet wurde – zumindest in jenen Mitgliedstaaten, in denen Informationspflicht besteht.

2. Wer wird informiert?

In 23 Mitgliedstaaten wird der Versicherungsnehmer informiert. Doch nur in 5 Mitgliedstaaten werden die versicherte Person (sofern diese nicht mit dem Versicherungsnehmer identisch ist) oder sonstige Begünstigte informiert. Dieses Problem sollte unbedingt in Angriff genommen werden, da die Rolle der Person, deren Daten verarbeitet werden, innerhalb des rechtlichen Rahmens der Richtlinie keinen Einfluss auf die Informationspflicht hat. Jede Person, deren Daten verarbeitet werden, sollte einzig aufgrund dieses Kriteriums ordnungsgemäß informiert werden. Da es sich dabei um personenbezogene Daten jeder Art

handelt, ist das Unternehmen verpflichtet, den betreffenden Personen alle Informationen und entsprechenden Unterlagen zur Verfügung zu stellen.

3. Bereitgestellte Informationen

Drei Arten von Informationen für die Person, deren Daten verarbeitet werden, wurden berücksichtigt: (a) Informationen über die Empfänger der Daten, (b) Informationen über die Verarbeitung der Daten und (c) Informationen über die potenzielle internationale Weitergabe der Daten.

a) In 17 Mitgliedstaaten informieren 100 % der Unternehmen die Person, deren Daten verarbeitet werden, über die Empfänger der Daten. Das ist ein recht hoher Prozentsatz.

b) In 17 Mitgliedstaaten bieten 100 % der Unternehmen Informationen über die allgemeine Verarbeitung der Daten. Leider enthielten die nationalen Berichte keine ausreichenden Angaben zur Bewertung der Ausführlichkeit und der Qualität der Informationen in Bezug auf die automatisierte Datenverarbeitung.

c) Betreffend die internationale Weitergabe von Daten gaben die Unternehmen in 18 Mitgliedstaaten an, keine Daten weiterzugeben. In den übrigen Mitgliedstaaten informieren nur 30 % der Unternehmen oder weniger über die internationale Weitergabe von Daten.

D. Weitergabe von Daten

1. Weitergabe von Daten an Dritte

Aus den nationalen Berichten geht hervor, dass Versicherungsgesellschaften in sämtlichen Mitgliedstaaten personenbezogene Daten an Dritte weitergeben. In der überwiegenden Mehrheit der Fälle hängt dieser Umstand entweder unmittelbar mit der Datenverarbeitung zusammen oder ist unter Berücksichtigung der Empfänger der Daten in der nationalen Gesetzgebung verankert.

Nachstehend die wichtigsten Kategorien von Empfängern personenbezogener Daten laut der nationalen Berichte. Die Zahlen beziehen sich auf die Anzahl der Mitgliedstaaten:

Versicherungsbezogenes Umfeld / Rückversicherer	25
Medizinisches Umfeld	15
Einschlägige Dienstleister (Berater, Vermittler, Versand, Druck)	12
Banken	10
Sonstige Unternehmen (innerhalb / außerhalb des Konzerns)	7
Gerichtsverfahren (Rechtsanwälte, Notare, Gerichte)	6
Dienstleister verschiedenster Art	5
Behörden (Polizei, Aufsichtsorgane, sonstige)	5
Sozialversicherung	4
Versicherungsverbände	3
Parallele Zwecke (Kreditwürdigkeit, Direktmarketing)	2
Familie	2
Arbeitgeber	1
Sonstige	1

Die obige Aufstellung zeigt, dass in der überwiegenden Mehrheit der Mitgliedstaaten vor allem Empfänger aus dem Versicherungs- und medizinischen Umfeld (innerhalb oder außerhalb des Unternehmens), einschlägige Dienstleister und Banken personenbezogene Daten über die Versicherten erhalten.

Die Weitergabe von Daten an diese spezifischen Empfängerkategorien ist gerechtfertigt, da die Tätigkeit dieser Empfänger in mehr oder weniger engem Zusammenhang mit der Vertragsverwaltung und den daraus erwachsenden Verpflichtungen steht.

Die Informationen über das medizinische Umfeld sind nicht ausreichend, da nicht immer eindeutig ist, ob sich die Zahlen auf das medizinische Umfeld innerhalb des Unternehmens beziehen, ob ein spezifischer Vertrag besteht oder ob es sich um eigenständige medizinische

Einrichtungen handelt. In allen Fällen werden die entsprechenden nationalen Gesetze in Bezug auf Datenschutz und Medizinethik berücksichtigt.

Abgesehen davon wurde eine rege Weitergabe der Daten an verschiedenste Empfänger festgestellt, deren Tätigkeit parallel zum Hauptzweck, aber nicht unbedingt in engem Zusammenhang mit diesem verläuft (Direktmarketing, Handel mit Informationen, Kreditwürdigkeit, Strafverfolgung etc.). Die Zulässigkeit der Weitergabe von Daten für diese Zwecke sollte anhand der nationalen Gesetze und im Hinblick auf den Grundsatz der Zweckbindung überprüft werden.

2. Zweck der Weitergabe von Daten

In 20 Mitgliedstaaten besteht der Hauptzweck der Weitergabe von Daten an Dritte in der Erfüllung der Verpflichtungen des Unternehmens aus dem Versicherungsvertrag. In 10 Mitgliedstaaten werden auch Risikoprüfungen als Zweck der Weitergabe genannt. In 7 Mitgliedstaaten geben Unternehmen personenbezogene Daten für Direktmarketing-Zwecke weiter, in 5 Mitgliedstaaten zur Betrugsbekämpfung, in 3 Mitgliedstaaten für Gerichtsverfahren und in 2 Mitgliedstaaten zu Zwecken der Besteuerung. Sehr selten (je 1 Mitgliedstaat) erfolgt die Weitergabe von Daten bei Rechtsstreitigkeiten mit Verbrauchern, für Forschungszwecke, zur Verbrechensbekämpfung und im Rahmen des Handels mit personenbezogenen Daten.

3. Rechtliche Grundlagen für die Weitergabe von Daten

Laut der nationalen Berichte erfolgt die Weitergabe personenbezogener Daten an Dritte in 7 Mitgliedstaaten auf der Grundlage gesetzlicher Vorschriften, während in 6 Mitgliedstaaten die Einwilligung der betroffenen Person erforderlich ist.

Hinsichtlich der Weitergabe von Daten an Dritte ist auf drei Punkte hinzuweisen:
- Falls die Weitergabe nicht gesetzlich vorgesehen ist, sollte sie nur mit der Einwilligung der betroffenen Person erfolgen.
- Auch wenn eine Einwilligung vorliegt, sollte die Weitergabe unter dem Gesichtspunkt des Grundsatzes der Zweckbindung überprüft werden.

- Die Rechtsbefolgung bei der Weitergabe von Daten sollte (i) anhand des Grundsatzes der Verhältnismäßigkeit und/oder darauf hin überprüft werden, ob dabei (ii) die Interessen der betreffenden Person gewahrt werden.

E. Sicherheitsmaßnahmen

1. Sicherheitsmaßnahmen

In 17 Mitgliedstaaten wenden 100 % der untersuchten Unternehmen Sicherheitsmaßnahmen an. In 2 Mitgliedstaaten verfügen 70-90 % der Unternehmen über Sicherheitsmaßnahmen und in 1 Mitgliedstaat nur 60 %. Obwohl diese Prozentsätze recht hoch scheinen, sollten sich die Datenschutzbehörden einiger Ländern um eine Verbesserung der Situation bemühen, sodass auch dort 100 % erreicht werden. Dieses Ziel ist realistisch.

In Bezug auf die Anwendung von Sicherheitsmaßnahmen sollten die Fragen künftig präziser formuliert werden, um besser vergleichbare Antworten zu erhalten. Insbesondere sollte nicht nur ermittelt werden, ob Sicherheitsmaßnahmen getroffen werden, sondern auch, um welche Arten von Maßnahmen es sich dabei handelt und ob diese den anwendbaren Normen entsprechen.

2. Information der Mitarbeiter

In 18 Mitgliedstaaten informieren 100 % der Unternehmen ihr Personal über Sicherheitsthemen. Dieser Wert ist sehr hoch.

Auch hier sollten in künftigen Fragenkatalogen präzisere Fragen dazu gestellt werden, welche Arten von Mitarbeitern welche Informationen benötigen.

3. Arten von Sicherheitsmaßnahmen

Laut der nationalen Berichte bestehen in allen 25 Mitgliedstaaten in 100 % der Unternehmen Zugriffsbeschränkungen beim Zugang zu Daten. In 24 Mitgliedstaaten (davon in 22 Mitgliedstaaten in 100 % der Unternehmen) werden die Daten gesichert, in 20 Mitgliedstaaten täglich.

Sicherheitsmaßnahmen in Bezug auf den Fernzugriff auf Daten bestehen in 20 Mitgliedstaaten (in 12 Mitgliedstaaten in 100 % der Unternehmen).

In 19 Mitgliedstaaten kommen spezielle Sicherheitsmaßnahmen für die Verarbeitung sensibler Daten zum Einsatz (in 12 Mitgliedstaaten in 100 % der Unternehmen).

Die in allen Mitgliedstaaten am häufigsten verwendeten Sicherheitsmaßnahmen sind Zugriffsbeschränkungen und tägliche Datensicherung. Auch Sicherheitsmaßnahmen beim Fernzugriff auf Daten werden oft eingesetzt. Im Hinblick auf die allgemeine Datensicherheit ist dies ein sehr gutes Zeichen.

Obwohl in 19 Mitgliedstaaten für die Verarbeitung sensibler Daten Sicherheitsmaßnahmen gelten, werden nur in 9 dieser Mitgliedstaaten spezifische Sicherheitsmaßnahmen umfassend eingesetzt.

Im Namen der Arbeitsgruppe

Der Vorsitzende
Peter SCHAAR