RAe Dr. Jürgen W. Goebel und Jürgen Scheller

Frankfurt am Main

Datenschutzrechtliche Probleme bei der Einrichtung und dem Betrieb von X.500-Directories im Rahmen des Deutschen Forschungsnetzes

Frankfurt am Main

Februar 1993

Februar 1993

RAe Dr. Goebel und Scheller
Frankfurt am Main

Datenschutzrechtliche Probleme bei der Einrichtung und dem Betrieb von X.500-Directories im Rahmen des Deutschen Forschungsnetzes

Übersicht | Seite

1. Einführung

Weltweite Kommunikationssysteme sind heute zu einem wichtigen Instrument geworden, um Daten, Nachrichten und Meinungen effektiv und ohne Zeitverlust zwischen den beteiligten Stellen auszutauschen. Das gilt für den wirtschaftlichen und administrativen Bereich ebenso wie für die weltweite Kommunikation zwischen Wissenschaftlern der verschiedensten Fachgebiete. Erst durch diese Möglichkeit des leichten Austauschs von Daten, Ideen und Meinungen wird die vielbeschworene scientific community realisiert, die erforderlich ist, um die komplexen wissenschaftlichen Herausforderungen der heutigen Zeit zu meistern. Damit jeder Teilnehmer in einem solchen Kommunikationssystem erreicht werden kann, bedarf es eines zentralen oder vieler dezentraler Verzeichnisse (=Directory-Dienst), die man sich wie ein erweitertes weltweites elektronisches Telefonbuch vorzustellen hat und in denen nach einzelnen Teilnehmern nach verschiedenen Kriterien recherchiert werden kann. Grundlage für einen solchen Directory-Dienst bilden Datensammlungen bei den einzelnen Directory-Betreibern, die nach dem weltweiten Standard X.500 aufgebaut und organisiert sind. Auch die Mitglieder des Deutschen Forschungsnetzes e.V. betreiben solche X.500-Directories selbst oder lassen die Daten ihrer Mitarbeiter und Kommunikationsteilnehmer in solchen Verzeichnissen bei entsprechenden Service-Anbietern speichern und verarbeiten.

Soweit die Einträge in den Directories sich dabei auf die Angaben zu den Institutionen (Universitäten, Forschungsinstitute, Unternehmen etc.) beschränken, die über das Kommunikationssystem erreicht werden können, ist die Verarbeitung der Teilnehmerdaten in den Directories rechtlich relativ unproblematisch. Sobald jedoch in die Directories auch Einzelangaben über natürliche Personen aufgenommen werden, zwischen denen ja letztlich die gewünschte Kommunikation stattfinden soll, ist durch die Speicherung und Weiterverarbeitung ihrer personenbezogenen Daten deren Recht auf informationelle Selbstbestimmung (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 Grundgesetz = GG) tangiert. Für den konkreten Verarbeitungsvorgang im Hinblick auf die Teilnehmerdaten, von der Speicherung bis hin zur Übermittlung ins Ausland, ergibt sich damit die Notwendigkeit, das dafür einschlägige Datenschutzrecht zu beachten. Wie dies mit vertretbarem Aufwand realisiert werden kann, ist Gegenstand dieser Expertise.

2. Problemstellung und Auftrag

Selbstverständlich war und ist den Betreibern von X.500-Directories in der Bundesrepublik Deutschland bewußt, daß es sich bei den zu verarbeitenden Teilnehmerangaben im wesentlichen um personenbezogene Daten im Sinne des geltenden Datenschutzrechts handelt. Man war daher von Anfang an bemüht, die einschlägigen datenschutzrechtlichen Vorschriften zu beachten.

Dabei ergeben sich jedoch zwei grundsätzliche Probleme. Zum einen ist wegen der Vielgestaltigkeit der Directory-Betreiber nicht immer klar, welche Vorschriften im einzelnen auf die jeweiligen Verarbeitungsvorgänge anzuwenden sind. Speichert etwa eine Hochschule diese Daten, erscheint das jeweilige Landesdatenschutzgesetz einschlägig. Wird das Directory von einem privaten Unternehmen betrieben, dürfte demgegenüber der dritte Abschnitt des Bundesdatenschutzgesetzes (BDSG) anzuwenden sein. Wird das Directory von der betreffenden Stelle technisch nicht selbst, sondern etwa von einem Service-Betrieb unterhalten, liegt möglicherweise eine Auftragsdatenverarbeitung vor.

Zum anderen wurde zwar von den Directory-Betreibern von Beginn ihrer Tätigkeit an versucht, dem Buchstaben des Datenschutzrechts auch hinsichtlich seiner strengsten Anforderungen gerecht zu werden. So versuchte man etwa, den einzelnen Teilnehmer, dessen personenbezogene Daten im Directory gespeichert werden sollten, möglichst umfassend über die möglichen Verarbeitungsmodalitäten für die Daten und die dafür geltenden Datenschutzbestimmungen aufzuklären. Außerdem war man bemüht, entsprechend einer Empfehlung aus dem sogenannten VERDI-Projekt, auf die weiter unten noch näher einzugehen sein wird, jeden Teilnehmer vor der Verarbeitung seiner personenbezogenen Daten eine Einwilligungserklärung unterschreiben zu lassen. Gerade letzteres erforderte jedoch einen recht hohen Verwaltungsaufwand und führte dennoch nur zu einer geringen Rücklaufquote bei den Einwilligungserklärungen (nach Auskunft des Auftraggebers unter 10 %). Auch das Problem der Aktualisierung der Teilnehmerdaten konnte bisher nicht zufriedenstellend gelöst werden.

Dies veranlaßte den DFN-Verein als Koordinator der deutschen Directory-Betreiber im DFN-Netz dazu, die vorliegende Expertise in Auftrag zu geben. Mit Wirkung vom 26. Oktober/09. November 1992 wurden die Verfasser beauftragt, eine Expertise zu datenschutzrechtlichen Problemen bei der Einrichtung und dem Betrieb von X.500-Directories im Rahmen des Deutschen Forschungsnetzes zu erstellen. Dabei sollen insbesondere folgende Themen behandelt werden:

(1) Darstellung der datenschutzrechtlichen Fragen im Zusammen- hang mit X.500-Directories im Überblick;

(2) Auswertung der Datenschutzgesetze der Bundesländer und des Bundes im Hinblick auf die zu beachtenden Regelungen;

(3) Herstellung eines Meinungsbildes zu der zu erwartenden Kontrollpraxis der Aufsichtsorgane durch Befragung ausge- wählter Stellen;

(4) Behandlung des Sonderproblems: Übermittlung personenbezo- gener Daten ins (europäische) Ausland unter Berücksichti- gung der geplanten EG-Richtlinie zum Datenschutz;

(5) Erarbeitung von Vorschlägen für die datenschutzgemäße Spe- icherungs- und Verarbeitungspraxis mit möglichst ge- ringem administrativem Aufwand.

Als Ausgangspunkt für die zu erstellende Expertise wurden den Verfassern verschiedene Materialien zur Verfügung gestellt, auf die noch näher einzugehen sein wird.

3. Vorarbeiten und Gespräche

Wie schon erwähnt, wurden vom Auftraggeber dieser Expertise bereits im Vorfeld der Einrichtung von X.500-Directories datenschutzrechtliche Überlegungen angestellt. Diese schlugen sich im wesentlichen in zwei Arbeitspapieren nieder, die auch den Verfassern zur Verfügung standen. Es handelte sich dabei zum einen um die Studienarbeit von Ursula Meyer zu Natrup, Aspekte des Datenschutzes im X.500-Verzeichnisdienst, März 1991. Darauf basierend wurde dann von Ursula Meyer zu Natrup und Sven Krause im Rahmen des VERDI/III-Projekts ein Papier mit dem Titel "DFN-Directory-Datenschutzhandbuch für den Pilotbetrieb", Juni 1991, erstellt, das der weiteren Praxis als Grundlage diente. In diesem Papier ist insbesondere das Informationsblatt und das Einwilligungsformular enthalten, das den DFN-Teilnehmern vor der Einspeicherung ihrer Daten in das X.500-Directory übergeben wurde und von diesen unterschrieben an den Directory-Betreiber zurückgegeben werden sollte. Auf diesen wertvollen Vorarbeiten konnten die Verfasser bei der Erstellung ihrer Expertise aufbauen.

Neben dem Studium der einschlägigen Gesetzestexte, Kommentare und Gerichtsentscheidungen oblag es den Verfassern aber auch, im direkten Kontakt mit Directory-Betreibern und den für den Bereich des Datenschutzrechts zuständigen Kontrollinstitutionen einerseits die praktischen Probleme bei der Anwendung der datenschutzrechtlichen Grundsätze zu ermitteln und andererseits die Meinung der Kontrollorgane zu eruieren. Dem erstgenannten Zweck dienten ein ausführliches Gespräch mit Mitarbeitern des DFN-Vereins in Berlin sowie die Teilnahme an der Vortragsveranstaltung am Vorabend der 24. Mitgliederversammlung des DFN-Vereins am 07. Dezember 1992 in Bonn. Kontakte und Gespräche bestanden bzw. wurden ferner zur Realisierung der zweiten Zweckbestimmung geführt mit dem Landesdatenschutzbeauftragten von Berlin, dem Landesdatenschutzbeauftragten von Bayern und dem Bundesdatenschutzbeauftragten.

Zum Teil legten die angesprochenen Stellen ihre Rechtsauffassung auch schriftlich nieder. Auf diese wird im einzelnen noch einzugehen sein. Die wichtigsten Dokumente dieser Art wurden auch in den Anhang der Expertise aufgenommen.

4. Anzuwendende Vorschriften

Abgesehen von den einzelnen Problemfeldern, die im nächsten Abschnitt noch ausführlich zu behandeln sein werden, ist in einer ersten Näherung zu dem hier interessierenden Problemkomplex zu klären, welche datenschutzrechtlichen Vorschriften für die weitere Prüfung überhaupt in Erwägung zu ziehen sind.

Dabei beantwortet sich diese Frage zunächst einmal durch die Rechtsnatur, d.h. die Rechtsform, in der das X.500-Directory jeweils betrieben wird. Anhand der rechtlichen Konstitution des Trägers des Directory und damit der "speichernden Stelle" im Sinne des Datenschutzrechts (vergleiche dazu weiter unten in Abschnitt 5.1) läßt sich eine Vorauswahl für die anzuwendenden Rechtsvorschriften treffen. Handelt es sich dabei um eine öffentliche Stelle des Bundes (etwa eine Bundesbehörde, ein Bundesinstitut oder eine Körperschaft des öffentlichen Rechts wie etwa eine Bundeswehrhochschule), so wäre der zweite Abschnitt des Bundesdatenschutzgesetzes vom 20. Dezember 1990 (= §§ 12 ff. BDSG) auf die Verarbeitung der personenbezogenen Daten im Directory anzuwenden.

Ist Träger des Directory und damit die speichernde Stelle eine private (oder wie das Datenschutzrecht formuliert: eine nicht-öffentliche) Stelle, so greift in diesem Falle der dritte Abschnitt des BDSG (= §§ 27 ff. BDSG) ein.

Unübersichtlicher wird jedoch die datenschutzrechtliche Lage, wenn der verantwortliche Träger des X.500-Directory eine öffentliche Stelle des Landes ist. In diesem Fall muß auf die jeweiligen Länderdatenschutzgesetze rekurriert werden. Die Verfasser hatten sich daher im Rahmen ihrer Untersuchung mit folgenden Landesdatenschutzgesetzen zu befassen:

(1) Baden-Württembergisches Gesetz zum Schutz personenbezogener Daten vom 27. Mai 1991 (bawü. LDSG).
(2) Bayerisches Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung vom 28. April 1978 (BayDSG).
(3) Gesetz über den Datenschutz in der Berliner Verwaltung vom 12. Juli 1978 (BlnDSG).
(4) Gesetz zum Schutz personenbezogener Daten im Land Brandenburg vom 20. Januar 1992 (BbgDSG).
(5) Bremisches Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung vom 19. Dezember 1977 (BrDSG).
(6) Hamburgisches Datenschutzgesetz vom 05. Juli 1990 (HmbDSG).
(7) Hessisches Datenschutzgesetz vom 11. November 1986 (HDSG).
(8) Niedersächsisches Datenschutzgesetz vom 26. Mai 1978 (NDSG).
(9) Gesetz zum Schutz personenbezogener Daten NordrheinWestfalen vom 15. März 1988 (DSG NW).
(10) Landesgesetz zum Schutz des Bürgers bei der Verarbeitung personenbezogener Daten Rheinland-Pfalz vom 21. Dezember 1978 (LDatG RhPf.).

(11) Saarländisches Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung vom 17. Mai 1978 (SDSG).
(12) Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen vom 11. Dezember 1991 (SächsDSG).
(13) Gesetz zum Schutz personenbezogener Daten der Bürger Sachsen-Anhalt vom 12. März 1992 (DSG-LSA).
(14) Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Information (LDSG Schl.-H.).
(15) Thüringer Datenschutzgesetz vom 29. Oktober 1991 (ThürDSG).
(16) Gesetz zum Schutz des Bürgers beim Umgang mit seinen Daten Mecklenburg-Vorpommern vom 24. Juli 1992 (DSGMV).

Selbstverständlich waren diese Landesdatenschutzgesetze jeweils in ihrer aktuellen Version in die Untersuchung einzubeziehen.

Ergänzend zu den "allgemeinen" Vorschriften des Bundes- und der Länderdatenschutzgesetze waren aber noch weitere Spezialregelungen zu beachten, die sich entweder aus supranationalen Regelungen oder Kodifizierungen für den grenzüberschreitenden Verkehr mit personenbezogenen Daten ergeben oder in Gesetzen enthalten sind, die spezifische Bestimmungen für eine ganz bestimmte Art von Daten enthalten. Wie in Abschnitt 5.3 noch näher darzulegen sein wird, sind das insbesondere Spezialbestimmungen aus dem Personaldaten- oder Arbeitsrecht, Regelungen, die sich auf die Verarbeitung von personenbezogenen Daten zu Forschungszwecken beziehen, oder die Datenübernahme aus allgemein zugänglichen oder bereits publizierten Quellen regeln. Diese Sonderregelungen können im Hinblick auf die Verarbeitung personenbezogener Daten liberalere aber auch restriktivere Regelungen enthalten als die allgemein gültigen Bestimmungen des Bundes- und der Länderdatenschutzgesetze. Inwieweit erstere hier überhaupt zum Zuge kommen, wird noch zu erörtern sein.

5. Einzelne Problemfelder

5.1 Begriffliche Vorklärungen

Der Beurteilung der datenschutzrechtlichen Zulässigkeit des vorgesehenen Betriebs von X.500-Directories muß zunächst die Verdeutlichung von Schlüsselbegriffen des Datenschutzrechts vorausgehen. Dies ist schon deswegen erforderlich, weil von der Erfüllung dieser Begriffe zum einen die grundsätzliche Anwendbarkeit datenschutzrechtlicher Regelungen abhängen kann, zum anderen aber auch entschieden wird, ob Bundes- oder Landesrecht zum Tragen kommt.
Hierzu soll aber nicht das Datenschutzrecht in seinen gesamten Grundzügen dargestellt (zu diesem Zweck gibt es bereits unübersehbare Literatur), sondern nur die für den in Rede stehenden Fall für besonders wichtig erachteten Begriffe erläutert werden. Soweit sich Regelungsunterschiede zwischen dem Bundesdatenschutzgesetz und Datenschutzgesetzen einzelner Länder ergeben, die Beachtung verdienen, wird auf diese jeweils eingegangen.

(1) Personenbezogene Daten
Gemäß der Definition des § 3 Abs. 1 BDSG sind personenbezogene Daten "Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)". Die Definitionen des Begriffs weichen in den landesrechtlichen Regelungen inhaltlich von § 3 Abs. 1 BDSG nicht ab. Was hierunter im einzelnen zu verstehen ist, soll im folgenden durch einige Beispiele kurz erläutert werden.

Einzelangaben über persönliche oder sachliche Verhältnisse sind bereits etwa Name, Vorname, Geburtsdatum, Adresse, aber auch Familienstand, Personalnummer, Vergütungsgruppe, Blutgruppe, Beurteilungen (Zeugnisse etc.). Der Gesetzgeber wollte nämlich auch elementare Angaben zu einer Person keineswegs aus dem Schutz des BDSG ausklammern[1]. Die Aufzählung verdeutlicht zudem, daß es für die Qualifikation als "personenbezogen" nicht darauf ankommt, wie sensibel die einzelne Angabe ist (so ist die schlichte Namensnennung sicher weniger geheimhaltungsbedürftig als ein Zeugnis). Entscheidend ist vielmehr, ob eine Angabe von demjenigen, der die Daten verarbeitet, eindeutig einer bestimmten Person zugeordnet werden kann.

Bestimmte Person ist jede natürliche Person, die aus den Daten unmittelbar erkennbar ist, während die bestimmbare Person erst durch Abfragen weiterer Daten ermittelt werden muß. Natürliche Person ist beispielsweise ein Arbeitnehmer, ein Kunde, ein Lieferant etc.; die Definition des § 3 Abs. 1 BDSG stellt hiermit nur klar, daß die Daten juristischer Personen wie etwa einer Aktiengesellschaft, einer GmbH etc. nicht unter den Schutz des BDSG fallen. Keine personenbezogenen Daten sind somit statistische Daten, anonymisierte Daten und Firmendaten.

---

1. Hierzu näher Simitis/Dammann/Geiger/Mallmann/Walz, Kommentar zum Bundesdatenschutzgesetz, 4. Auflage, Baden-Baden 1992, Rn. 8 zu § 3.

Damit ist klar, daß es sich bei den für die X.500-Directories vorgesehenen Angaben, auch bei dem "Minimalset" aus Namen, Telefonnummer und E-Mail-Adresse, jedenfalls um "personenbezogene Daten" handelt.

(2) Speichernde Stelle

§ 3 BDSG trifft auch für diesen Begriff eine Definition: "Speichernde Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst verarbeitet oder durch andere im Auftrag verarbeiten läßt" (Abs. 8). Kennzeichnendes Merkmal ist also die eigene Datenverarbeitung beziehungsweise die Verarbeitung im Auftrag. Wenn auch der Gesetzeswortlaut ausdrücklich von "speichern" ausgeht, so ist doch selbstverständlich vorausgesetzt, daß auch sonstige Verarbeitungsvorgänge stattfinden können[2]. Dies wird in den Landesdatenschutzgesetzen, die durchweg inhaltlich gleiche Kriterien anlegen wie das BDSG, zuweilen auch im Wortlaut schon deutlich, wo von "datenverarbeitender Stelle" die Rede ist[3]. Trotz des inhaltlich gleichen Maßstabs eigener Verarbeitung oder der Verabeitung personenbezogener Daten im Auftrag besteht zwischen dem BDSG und den Datenschutzgesetzen der Länder jedoch ein grundlegender systematischer Unterschied: Während die Datenschutzgesetze der Länder nur auf Behörden oder sonstige öffentliche Stellen, die als "speichernde Stelle" anzusehen sind, Anwendung finden, gilt das BDSG nicht nur für öffentliche Stellen des Bundes, sondern auch für nicht-öffentliche (=private) Stellen.

Damit wird klar, daß der Beantwortung der Frage, wer im Rahmen der Erstellung und des Betriebs der X.500-Directories als "speichernde Stelle" anzusehen ist, eine regelrechte Schlüsselrolle zukommt. Käme man etwa zu dem Ergebnis, nur eine nicht-öffentliche Institution sei "speichernde Stelle ", so fände lediglich das BDSG Anwendung, nicht aber landesrechtliche Regelungen. Daneben knüpfen die vom Gesetz festgelegten Rechte und Pflichten an den Begriff an. Letztlich ist aber auch eine Übermittlungsfeststellung nicht denkbar, wenn nicht zuvor geklärt ist, wer "speichernde Stelle" ist[4]. Im folgenden soll daher auf einige denkbare Varianten eingegangen werden, wer als speichernde Stelle der Directories in Frage kommen könnte.

Denkbar ist zunächst, jede Institution, die sich im Rahmen des Deutschen Forschungsnetzes engagiert und deshalb die Daten ihrer Mitarbeiter in das Directory aufnimmt, als die speichernde Stelle anzusehen. Dies liegt nahe, weil der rein technische Speicherungsvorgang[5] häufig bei diesen Institutionen selbst bewerkstelligt werden wird.

2. Vergleiche Simitis et al., aaO., Rn. 221 zu § 3.

3. So etwa in § 3 Abs. 3 des Sächsischen Landesdatenschutzgesetzes.

4. So auch Simitis et al., aaO., Rn. 219 zu § 3.

5. Dieser ist nicht identisch mit der Festlegung der "speichernden Stelle", wie bereits die Einbeziehung der Verarbeitung im Auftrag in diesen Begriff zeigt.

Nimmt man diesen Fall einmal als gegeben an, so hat diese Einordnung zur Folge, daß die hieraus resultierende Gesetzeslage außerordentlich unüberschaubar wird. Man hat dann nämlich etwa auf eine öffentliche Stelle des Bundes sowie auf nicht-öffentliche Stellen das BDSG anzuwenden, auf öffentliche Stellen eines Landes aber das jeweilige Landes-datenschutzgesetz. Dies aber ist sicher kein Grund, ein solches Ergebnis abzulehnen; vielmehr käme es sogar einer (unzulässigen) Zweckargumentation zumindest nahe, dies mit der Begründung der Kompliziertheit zu tun. Jedoch läßt die Betrachtungsweise "Jeder für sich" außer acht, daß die Datenverarbeitungsvorgänge nicht im Rahmen der ureigenen Aufgaben der jeweiligen Einzelinstitution, sondern vielmehr im Zusammenwirken innerhalb einer umspannenden Einrichtung stattfinden, die von einem gemeinsamen Interesse getragen wird.

Dies gibt Anlaß, die weitere Variante zu betrachten, ob etwa der DFN-Verein generell als "speichernde Stelle" anzusehen sein könnte. Dies hat seinen Grund darin, daß dem Kriterium der Datenverarbeitung letztlich ein gewisses finales Element zu eigen ist, das es nicht erlaubt, von der bloß faktisch-technischen Abwicklung auszugehen; sondern es ist in die Beurteilung mit einzubeziehen, wem letztlich die Verarbeitung der personenbezogenen Daten dient. Richtig ist gewiß, daß etwa eine Universität die fraglichen Daten bereitstellen wird, um in der wissenschaftlichen Kommunikation nicht hintanzustehen; jedoch erfolgt die konkrete Art und Weise, wie sie dies im Rahmen des Deutschen Forschungsnetzes durch vorgegebene Anforderungen der fraglichen Directories tut, nicht innerhalb ihres universitären Aufgabenbereichs, sondern in Erfüllung ihrer Mitwirkungspflichten, die ihr als Mitglied des DFN-Vereins obliegen. Das finale Element der Datenvararbeitung weist also eher auf den DFN-Verein in seiner Gesamtheit als auf die einzelne in ihm tätige Institution. Es erscheint vor diesem Hintergrund daher plausibler, den DFN-Verein selbst als "speichernde Stelle" anzusehen[6], wovon im folgenden ausgegangen wird. Dies zieht als positiven Effekt nach sich, daß Datenschutzgesetze der Länder nicht zur Anwendung gelangen. Auf die hier in Rede stehenden Vorgänge beim DFN-Verein, ein eingetragener privatrechtlicher Verein, als einer Einrichtung außerhalb des öffentlichen Bereichs finden vielmehr nur die Vorschriften des dritten Abschnitts des BDSG Anwendung.

(3) Abrufverfahren

Im BDSG sowie in einigen Landesdatenschutzgesetzen[7] sind Sonderregelungen für die Fälle getroffen worden, in denen ein Abrufen gespeicherter personenbezogener Daten über automatisierte Verfahren ermöglicht wird. Diese Regelungen befassen sich zum Teil sowohl mit der Frage, wem die datenschutzrechtliche

---

6. Hiervon geht im übrigen auch der Berliner Datenschutzbeauftragte aus, allerdings ohne ersichtliche Begründung.

7. Sonderregelungen der hier besprochenen Art finden sich keineswegs in allen Landesdatenschutzgesetzen. Vielmehr trifft ein gutes Drittel hierzu keine explizite Regelung, was bedeutet, daß in diesen Ländern auch auf automatisierte Abrufverfahren lediglich die allgemeinen Vorschriften anzuwenden sind.

Verantwortung im Falle solcher Abrufe zukommt, als auch oftmals mit Ausnahmetatbeständen.

Gemäß § 10 Abs. 1 BDSG ist die Einrichtung automatisierter Abrufverfahren zur Übermittlung personenbezogener Daten nur dann zulässig, wenn sie nach Abwägung der Interessen der Betroffenen gegenüber den Geschäftszwecken und den Aufgaben der beteiligten Stellen "angemessen" ist. Daß damit noch nichts über die Zulässigkeit des einzelnen tatsächlich stattfindenden Abrufs ausgesagt ist, stellt § 10 Abs. 1 Satz 2 BDSG klar, indem er festlegt, daß "die Vorschriften über die Zulässigkeit des einzelnen Abrufs" unberührt bleiben. Allerdings ist die Verantwortung für die Zulässigkeit des einzelnen Abrufs gemäß § 10 Abs. 4 BDSG grundsätzlich dem Empfänger desselben übertragen, wohingegen die speichernde Stelle nur bei bestehendem Anlaß die Zulässigkeit zu überprüfen hat. Indes hat sie ein Stichprobenverfahren zur Kontrolle des einzelnen Abrufs einzurichten.

Weiter schreibt § 10 Abs. 2 BDSG Pflichten fest, die alle beteiligten Stellen, also auch die speichernde Stelle, zu beachten haben. Hierbei handelt es sich um Maßnahmen, die eine Kontrolle der Zulässigkeit des Abrufverfahrens ermöglichen sollen, wobei im einzelnen der Anlaß und der Zweck des Abrufverfahrens, die Datenempfänger, die Art der übermittelten Daten und bestimmte technische und organisatorische Maßnahmen (zum Beispiel Datensicherungsmaßnahmen) schriftlich festzulegen sind.

Indes enthält § 10 Abs. 5 BDSG eine sehr wichtige Ausnahmeregelung: Abrufe "aus Datenbeständen, die jedermann, sei es ohne oder nach besonderer Zulassung, zur Benutzung offenstehen", sollen nicht in den Anwendungsbereich des § 10 fallen. Gemeint sind hiermit quasi öffentlich zugängliche Datenbanken. Um solche handelt es sich bei den X.500-Directories deshalb nicht, weil schlicht nicht "jedermann" Mitglied im DFN-Verein werden kann. Voraussetzung für eine Mitgliedschaft ist nämlich gemäß § 10 der Satzung des DFN-Vereins, daß es sich um juristische Personen des öffentlichen oder privaten Rechts handelt.

Die Ausnahmeregelung des § 10 Abs. 5 BDSG greift für den DFN-Verein als speichernde Stelle daher nicht ein. Damit haben also nach dem bisherigen Kenntnisstand der DFN-Verein und die am Abrufverfahren beteiligten Stellen auf die Einhaltung der obengenannten Pflichten zu achten.

Jedoch ist in diesem Zusammenhang deutlich darauf hinzuweisen, daß § 10 BDSG ohnehin nur dann zur Anwendung kommt, wenn die Online-Anbindung dem Abruf von einem Dritten dient, also eine echte Übermittlung im Sinne des § 3 Abs. 5 S. 2 Nr. 3 b BDSG vorliegt. Dies bedeutet umgekehrt, daß bei einem Online-Abruf in einem Datenverarbeitungsauftragsverhältnis, also zwischen Auftraggeber und -nehmer (und umgekehrt) lediglich § 11 BDSG, nicht aber die Spezialvorschrift des § 10 in Betracht kommt[8]. Hierauf wird unter Abschnitt 5.4 (2) noch einzugehen sein.

5.2 Allgemeine Verarbeitungsvoraussetzungen

Entsprechend der hier vertretenen Auffassung, wonach wegen der Eigenschaft des DFN-Vereins als "speichernde Stelle" Landesdatenschutzgesetze nicht zur Anwendung kommen, soll im folgenden nur dargestellt werden, unter welchen Voraussetzungen die Verarbeitung personenbezogener Daten nach dem BDSG zulässig ist.

(1) Gesetzliche Regelungen
Gemäß § 4 Abs. 1 BDSG ist die Verarbeitung und Nutzung personenbezogener Daten nicht nur bei Vorliegen einer Einwilligung des Betroffenen, Erlaubnis oder Anordnung durch das BDSG, sondern auch bei Erlaubnis oder Anordnung durch "eine andere Rechtsvorschrift" zulässig. Hierdurch stellt das BDSG selbst auf vorrangige Spezialregelungen, beispielsweise in Regelungeszusammenhängen des Personal- oder Fiskalrechts ab.
Derartige vorrangige spezielle Regelungen sind im vorliegenden Fall zunächst einmal nicht ersichtlich, weswegen im folgenden geprüft werden soll, ob das BDSG die im Rahmen des Deutschen Forschungsnetzes vorgesehenen Verarbeitungen in X.500-Directories zuläßt (zu einigen Sonderbereichen siehe aber noch unten Abschnitt 5.3).

(2) Erforderlichkeit für die Vertragsabwicklung
Wenn auch hier wegen der Eigenschaft des DFN-Vereins als nicht-öffentliche Stelle nur auf die Regelungen des dritten Abschnitts des BDSG näher eingegangen werden soll, so sei doch vorab der Hinweis nicht versäumt, daß auch die Vorschriften über die Verarbeitung peronenbezogener Daten öffentlicher Stellen Regelungen enthalten, die die Zulässigkeit der Verarbeitung davon abhängig machen, ob sie zur Erfüllung der Aufgaben der Stelle "erforderlich" ist[9]. Für den Bereich nicht-öffentlicher Stellen sei aber das Erforderlichkeitskriterium nun im einzelnen dargestellt:

Gemäß § 27 Abs. 1 Nr. 1 BDSG findet der dritte Abschnitt des BDSG auf nicht-öffentliche Stellen Anwendung, "soweit (diese) personenbezogene Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke" verarbeiten oder nutzen. Durch diese Formulierung hat der Gesetzgeber lediglich deutlich gemacht, daß dateimäßig geführte personenbezogene Daten im rein privaten

---

8. Vgl. Simitis, aaO, Rn 16 zu § 11. Sobald aber ein Datentransfer ins Ausland vorliegt, so gilt wiederum § 11 BDSG nicht; in diesen Fällen liegt stets eine Übermittlung vor, weil § 3 Abs. 9 BDSG jedweden Auftragnehmer im Ausland als "Dritten" definiert!

9. Vgl. §§ 13 ff BDSG. Die Datenschutzgesetze der Länder (die ja nur für öffentliche Stellen gelten) treffen hier durchweg fast identische Regelungen, gehen also auch von einer "Erforderlichkeit" für die Aufgabenerfüllung aus. Darüberhinaus trifft aber der überwiegende Teil der Landesgesetze zusätzlich die Festlegung, daß die Datenverarbeitung grundsätzlich nur zu dem ursprünglich festgelgten Zweck erfolgen darf (siehe etwa § 12 Abs. 1 Nr. 2 des LDSG Baden-Württemberg).

Bereich (beispielsweise eine auf PC geführte Adreßdatei eines Privathaushalts oder eine Mitgliederliste eines Sportvereins) nicht dem BDSG unterfallen sollen[10].

Bereits unter Abschnitt 5.1 (1) wurde festgestellt, daß die im Rahmen der X.500-Directories aufgenommenen Daten "personenbezogene Daten" sind. Diese werden in der hier in Rede stehenden Konstellation auch als "Datei" verarbeitet, denn hierunter versteht das Gesetz "eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (auotmatisierte Datei)", § 3 Abs. 2 Nr. 1 BDSG, sowie "jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht-automatisierte Datei)", § 3 Abs. 2 Nr. 2 BDSG. Ausgeschlossen sind lediglich "klassische" Akten und Aktensammlungen. Bei der Verarbeitung der für die X.500-Directories vorgesehenen Daten ist somit von einer automatisierten Datei auszugehen.

Maßgebliche Norm des dritten Abschnitts des BDSG für das Vorhaben des DFN-Vereins ist § 28, der die Datenspeicherung ,
-übermittlung und -nutzung für eigene Zwecke regelt. Die Vorschrift enthält verschiedene Fallvarianten, unter denen die Zulässigkeit von Datenverarbeitungsvorgängen festgeschrieben wird.

§ 28 Abs. 1 Nr. 1 BDSG erklärt die Verarbeitung personenbezogener Daten für die Erfüllung eigener Geschäftszwecke für zulässig, soweit diese "im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen" stattfindet. Hierzu ist zu sagen, daß die Betroffenen, deren Daten hier gespeichert werden sollen, zwar in der Regel Verträge oder vertragsähnliche Beziehungen zu den Institutionen haben werden, die sich dem Deutschen Forschungsnetz angeschlossen haben, jedoch stehen sie selbst zum DFN-Verein als der verarbeitenden Stelle nicht in einer solchen Beziehung. Nach Dafürhalten der Bearbeiter bietet sich eine Anwendung des § 28 Abs. 1 Nr. 1 BDSG daher nicht an. Vielmehr sehen die Autoren den Lösungsweg über die Regelung des § 28 Abs. 1 Nr. 2 BDSG, wonach es für die Zulässigkeit der Datenverarbeitung ausreicht, daß sie "zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verarbeitung oder Nutzung überwiegt".

Zielsetzung des DFN-Vereins ist es, die Kommunikation innerhalb wissenschaftlicher Kreise und Institutionen durch die Möglichkeit eines gezielten Ansprechens einzelner wissenschaftlich tätiger Personen zu verbessern. Hierzu gehört die namentliche Nennung dieser Personen ebenso unerläßlich wie die Angabe der E-

---

10. Das Fehlen einer derartigen Formulierung und das Festmachen der Anwendbarkeit des Bundesdatenschutzgesetzes maßgeblich am Begriff der "Datei" im alten BDSG von 1977 hat in dieser Frage zu wiederholten Auslegungsstreitigkeiten geführt.

Mail-Adresse dieser Personen in eben diesem Medium, in dem sich ihre Namensangabe findet, da ansonsten zwar eine im Interesse eines wissenschaftlichen Diskurses anzusprechende Person hierüber gefunden, jedoch im Anschluß nur auf dem "klassischen" Postwege angesprochen werden könnte. Letzterer hat sich indes gerade als hinderlich in der wissenschaftlichen Zusammenarbeit erwiesen, da er das Risiko verspäteter oder gar unzutreffender Zustellung in sich trägt. Gerade dieses Risiko soll mit einem derartigen Forschungsnetz ausgeschaltet oder wenigstens minimiert werden. Zur Erfüllung des Geschäftszwecks des DFN-Vereins ist die Verarbeitung jedenfalls der Daten, die als "Minimalset" bezeichnet werden, daher unbedingt erforderlich.

Zu prüfen ist nun jedoch, ob diesem legitimen Vereinsinteresse gegenläufige schutzwürdige Interessen der Betroffenen entgegenstehen, die dieses möglicherweise überwiegen. Die genannte Vorschrift des BDSG spricht hier von "kein Grund zu der Annahme besteht, das das schutzwürdige Interesse ... überwiegt". Dies bedeutet, daß der Gesetzgeber hier nicht eine Interessenabwägung im konkreten Einzelfall für notwendig erachtet hat, sondern es ausreichen lassen wollte, eine solche Interessenabwägung pauschal vorab vorzunehmen.

Sicher ist generell von einem schutzwürdigen Interesse der Betroffenen dahingehend auszugehen, daß mit ihren personenbezogenen Daten nicht jedermann nach Belieben verfahren darf; dies resultiert schon aus dem allgemeinen Datenschutzgedanken. Jedoch wird man im vorliegenden Fall nicht sagen können, daß dieses schutzwürdige Recht auf informationelle Selbstbestimmung die hier in Rede stehenden Geschäftsinteressen des DFN-Vereins überwiegt. Es darf nämlich nicht außer acht gelassen werden, daß jeder Betroffene, dessen Angaben sich in den Directories finden, nicht nur selbst Zugriff auf diese Angaben im Sinne eines Leserechts, sondern hinsichtlich der Angaben zu seiner eigenen Person auch ein Schreiberecht erhalten soll, das es ihm beispielsweise ermöglicht zu bestimmen, ob seine Daten allgemein zugänglich sein sollen oder nicht. Der einzelne Betroffene hat es damit selbst in der Hand, eine Abwägung vorzunehmen zwischen der Gefährdung seiner informationellen Integrität und den Interessen eines speditiveren wissenschaftlichen Dialogs. Somit besteht nach Auffassung der Autoren für den DFN-Verein im Sinne des § 28 Abs. 1 Nr. 2 kein Grund zur Annahme eines überwiegenden Interesses der Betroffenen, das der Datenverarbeitung entgegenstünde.

Zusammenfassend zu diesem Abschnitt läßt sich daher festhalten, daß die Verarbeitung des "Minimalsets" gemäß § 28 Abs. 1 Nr. 2 BDSG für zulässig erachtet werden kann.

(3) Einwilligung oder Widerspruchslösung

Das Ergebnis des Unterabschnitts (2) beantwortet zugleich die Frage, die im Rahmen des DFN-Vorhabens bislang immer wieder gestellt wurde: Ist man genötigt, bei der bisherigen Praxis zu bleiben und die Betroffenen um ihre schriftliche Einwilligung zur Einspeicherung wenigstens des "Minimalsets" zu bitten, oder reicht eine "Widerspruchslösung" aus, die den Betroffenen angeboten wird? Die Anwort lautet: Eine Einwilligung ist nicht erforderlich.

Folgendes sei aber um der Verdeutlichung willen ergänzt: Klar ist, daß eine Einwilligung der Betroffenen die datenverarbeitende Stelle von der wohl oftmals schwer vorzunehmenden Interessenabwägung befreit; liegt also eine Einwilligung vor, so kann die Stelle jedenfalls ein "ruhiges Gewissen" haben, weil sie die Einwilligung im Zweifel auch den Aufsichtsbehörden vorweisen kann, während sie bei der hier vertretenen Lösung darauf vertrauen muß, daß sich diese dem hier erzielten Ergebnis der Interessenabwägung anschließen werden[11].

Jedoch besteht hinsichtlich der Einordnung der "Widerspruchslösung" nach Dafürhalten der Verfasser Anlaß zu betonen, daß das Gesetz lediglich im Falle der Weitergabe personenbezogener Daten für Zwecke der Werbung oder der Markt- und Meinungsforschung eine echte Widerspruchslösung kennt (§ 28 Abs. 3 BDSG), die - bei Ausübung des Widerspruchsrechts - zur Unzulässigkeit der Nutzung oder Übermittlung führt. Im hier in Rede stehenden Umfeld kann die "Widerspruchslösung" nur in dem unter 5.2. (2) entwickelten Sinne verstanden werden, wonach der Betroffene durch Äußerung seines der Verarbeitung entgegenstehenden Willens die Gefährdung seiner schutzwürdigen Interessen ausschließt. Es handelt sich also nicht um eine echte Alternative zur Einwilligung, die die Zulässigkeit der Datenverarbeitung selbständig begründen würde, sondern um eine mögliche Willensäußerung des Betroffenen, die die Interessenabwägung im Rahmen der Prüfung allgemeiner Zulässigkeitsvoraussetzungen beeinflußt.

5.3 Sonderregelungen

Als speziellere Regelung im Hinblick auf die Verarbeitung personenbezogener Daten in den X.500-Directories gegenüber den allgemein gültigen Bestimmungen des Bundesdatenschutzgesetzes und der Länderdatenschutzgesetze soll nun eingegangen werden auf Vorschriften, die sich auf die Verarbeitung von Personalaktendaten, die Verarbeitung von personenbezogenen Daten zu Forschungszwecken sowie auf die Übernahme solcher Daten aus Publikationen beziehen.

(1) Personalaktendatenrecht

Soweit die Kommunikationsteilnehmer, deren Nutzerdaten in X.500-Directories gespeichert werden sollen, in einem Arbeitsverhältnis (etwa zur Universität, zu einem privaten Forschungsinstitut etc.) stehen, bietet es sich an, die für den Directory-Eintrag erforderlichen Daten aus den Personalunterlagen des jeweiligen

---

11. Die Chancen hierfür stehen, vorbehaltlich der technischen Realisierung der Verfügungsrechte der Betroffenen über ihre eigenen Daten, angesichts der Stellungnahmen des bayerischen und des Berliner Datenschutzbeauftragten so schlecht allerdings nicht.

Nutzers zu entnehmen und in das Verzeichnis aufzunehmen. Eine solche Übernahme erscheint aber deswegen problematisch, weil für die einschlägigen Daten möglicherweise der strengere Schutz von Vorschriften des Personalaktendatenrechts gilt, die in diesem Fall für dem öffentlichen Dienstrecht unterliegende Arbeitsverhältnisse eine ausdrückliche Einwilligung des Betroffenen voraussetzen.

Für den Bereich von Bundesbehörden ist dabei die am 01. Januar 1993 in Kraft getretene Vorschrift des § 90g des Bundesbeamtengesetzes (BBG) einschlägig, nach der Personaldaten in Dateien nur für Zwecke der Personalverwaltung oder der Personalwirtschaft verarbeitet und genutzt werden dürfen. Ein automatischer Abruf dieser Daten ist unzulässig, soweit durch eine besondere Rechtsvorschrift nichts anderes bestimmt ist (§ 90g Abs. 1 S. 3 BBG). Danach wäre der automatische Abruf von Nutzerdaten eines Kommunikationssystems, die gleichzeitig Personalaktendaten sind, nur zulässig, wenn es dafür eine spezielle gesetzliche Vorschrift gäbe, die aber zur Zeit nicht ersichtlich ist.
Eine derart restriktive Regelung der Nutzung von Personalaktendaten durch entsprechende Ländergesetze ist derzeit noch nicht ersichtlich. Jedoch planen einige Länder vergleichbare Regelungen für die ihrer Hoheit unterfallenden Personalaktendaten (Beispiel: Bayern).

Dies muß nun allerdings im Ergebnis nicht dazu führen, daß die Übernahme von Personalaktendaten in die Verzeichnis-Datei des E-Mail-Systems mangels gesetzlicher Regelung grundsätzlich unzulässig ist oder nur nach ausdrücklicher Einwilligung des Betroffenen vorgenommen werden darf. Jedenfalls ergibt sich das aus der Stellungnahme des Bayerischen Landesbeauftragten für den Datenschutz vom 11. Januar 1993[12]. Diese Stellungnahme geht davon aus, daß es selbst nach dem Inkrafttreten eines Personalaktendatenrechts (jedenfalls in Bayern) zulässig wäre, Personalaktendaten, wie sie für das Mail-Directorys-System einer Universität verwendet werden sollen, aus den Personalakten bzw. -dateien "für Zwecke der Personalwirtschaft" zu entnehmen und an das für den Dienstbetrieb der betreffenden Behörde zuständige Sachgebiet weiterzuleiten. Bei diesem Sachgebiet, das dann das Directory betreibt, wären die Daten nicht mehr dem strengen Personalaktendatenrecht unterworfen. Einschlägig wären dann wiederum die Vorschriften des "allgemeinen" Datenschutzrechts, also etwa des (bayerischen) Landesdatenschutzgesetzes. Dies gilt dann sowohl für die Verarbeitung im Directory als auch für die Zulässigkeit der online-Datenübermittlung aus dem Directory an Dritte.

Werden nach dieser vom Landesbeauftragten geäußerten Ansicht personenbezogene Daten in das Directory eingespeichert, die über die betreffenden Mitarbeiter bereits im Personalverzeichnis etwa der Universität veröffentlicht wurden, so soll dann für die Einspeicherung und Weiterverarbeitung nach den Vorschriften des allgemeinen Datenschutzrechts das Erfordernis der vorherigen Einwilligung des

12. Siehe den vollen Wortlaut dieser Stellungnahme im Anhang zu dieser Expertise.

Betroffenen wegfallen und lediglich ein Widerspruchsrecht für den Betroffenen Platz greifen (Stellungnahme vom 11. Januar 1993, Seite 2 unten). In keinem Fall darf nach dieser Ansicht allerdings das X.500-Directory Bestandteil der zentralen Personaldatei der jeweiligen Behörde sein. Diese Bewertung wird in der erwähnten Stellungnahme des Landesbeauftragten analog auch für die Einrichtung eines E-Mail-Systems für die Kommunikation von Wissenschaftlern vorgenommen. Ob diese Analogie auch für die weltweite Kommunikation und Verfügbarkeit der Teilnehmerdaten gelten sollen, wird allerdings nicht ausdrücklich ausgeführt (vergl. dazu noch unten Abschnitt 5.5).

Bemerkenswert an dieser Argumentation erscheint den Verfassern zweierlei zu sein. Zum einen wird zunächst der Bezug der hier interessierenden Teilnehmerdaten zum Bereich des geplanten Personalaktendatenrechts deutlich, nach dem die Verarbeitung dieser Daten nur unter erschwerten Bedingungen zulässig wären (auf der Grundlage einer spezialgesetzlichen Regelung oder nach ausdrücklicher Einwilligung des Betroffenen). Zum anderen wird aber auch ein Lösungsweg für diese Problematik aufgezeigt, indem vorgeschlagen wird, die betreffenden Personaldaten von der Personalabteilung an die Abteilung "Allgemeiner Dienstbetrieb" weiterzuleiten, bei dem dann das Directory angesiedelt ist. Dort finden dann nur noch die allgemeinen Datenschutzvorschriften Anwendung, die hier sogar Raum für das Widerspruchsmodell lassen, sofern die entsprechenden Daten sich mit den Einträgen über die jeweiligen Personen aus dem publizierten Personalverzeichnis decken. Dieser Lösungsweg für die Einwilligungsproblematik ist sowohl gangbar, wenn die Abteilung "Allgemeiner Dienstbetrieb" das Directory selbst verantwortlich betreibt, als auch für den Fall, daß die entsprechende organisatorische Untereinheit (etwa einer Universität) die Verarbeitung im Auftrag des DFN-Vereins durchführt.

Sicherlich kann diese Argumentation nicht ohne weiteres auf die übrigen Bundesländer und den Bund übertragen werden, da es dort zumeist noch an den entsprechenden Vorschriften zum Personalaktendatenschutz fehlt. Wenn diese Argumentation aber bereits für den Anwendungsbereich des (geplanten) strengen Personalaktendatenrechts gilt, so kann bei Beachtung der übrigen Rahmenbedingungen das Widerspruchsmodell jedenfalls für den universitären Bereich generell als datenschutzrechtlich zulässig propagiert werden.

Bejaht man also (insbesondere für die Zukunft) die Anwendbarkeit des Personalaktendatenrechts (das zum Teil erst noch geschaffen werden wird), so kann bei der Einspeicherung von personenbezogenen Nutzerdaten aus Gründen der Praktikabilität das Widerspruchsmodell mit einiger Aussicht auf rechtlichen Bestand Anwendung finden.

(2) Forschungsprivileg

Sowohl im Bundesdatenschutzgesetz (§ 40 BDSG) als auch in verschiedenen Länderdatenschutzgesetzen (etwa § 28 Bbg DSG, § 33 HDSG, § 27 DSG-LSA) sind Sondervorschriften für die Verarbeitung personenbezogener Daten im Forschungsbereich oder für wissenschaftliche Zwecke enthalten. Da auch die hier in den Directories zu speichernden personenbezogenen Daten sich im wesentlichen auf Mitarbeiter aus dem Forschungsbereich beziehen, ist die Einschlägigkeit dieser Regelung zu prüfen.

Schon der Wortlaut der genannten Bestimmungen, der Formulierungen wie etwa "Verarbeitung personenbezogener Daten für wissenschaftliche Zwecke" oder "für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten" enthält, macht jedoch deutlich, daß diese Vorschriften für unser Problem nicht einschlägig sind. Denn diese finden nur dann Anwendung, wenn sich die personenbezogenen Daten auf die wissenschaftlichen Inhalte beziehen oder selbst Gegenstand der wissenschaftlichen Forschung sind. Das trifft etwa zu auf Krankendaten in medizinischen Forschungsvorhaben oder Angaben über natürliche Personen im Rahmen eines sozialwissenschaftlichen Projekts. In keinem Fall sind damit jedoch die personenbezogenen Daten der Forscher selbst gemeint, jedenfalls soweit diese nicht selbst Gegenstand des wissenschaftlichen Vorhabens sind.

Für die in das X.500-Directory einzutragenden Teilnehmerdaten gelten somit die Spezialvorschriften über die Verarbeitung personenbezogener Daten für wissenschaftliche Zwecke nicht.

(3) Datenübernahme aus Publikationen

Ein weiterer Sonderfall der Verarbeitung personenbezogener Daten sei hier noch kurz erwähnt, die Übernahme von Angaben aus Publikationen oder anderen öffentlich zugänglichen Quellen. Geregelt ist dies etwa in § 14 Abs. 2 Nr. 5 und § 28 Abs. 1 Nr. 3 BDSG sowie in ähnlichen Vorschriften der Länderdatenschutzgesetze (Beispiel: § 13 Abs. 2 Buchstabe f. Bbg DSG). Allerdings dürften diese Vorschriften nur dann Bedeutung erlangen, wenn die für das Directory zu speichernden Daten auch wirklich vollständig aus allgemein zugänglichen Quellen entnommen werden können. Existiert eine solche Quelle, wie dies bei dem in Unterabschnitt 5.3 (1) erwähnten Personalverzeichnis der Universitäten meistens der Fall ist, so ist die Übernahme der darin enthaltenen Nutzerangaben in das Directory unproblematisch. Größere Probleme bereitet jedoch die Frage, wie die in der allgemein zugänglichen Quelle enthaltenen Daten dorthin gelangt sind und wie dabei den einschlägigen Datenschutzregelungen Genüge getan werden kann. Dazu sei auf die obigen Ausführungen zum Personalaktendatenrecht verwiesen, die dafür einen vertretbaren Weg aufzeigen.

5. 4 Rechte des Betroffenen

Auch bei festgestellter Zulässigkeit der Verarbeitung personenbezogener Daten in den Directories hat der Betroffene bestimmte unabdingbare Rechte. Welche dies im einzelnen sind und (vor allem) wem gegenüber der Betroffene sie ausüben kann, soll im folgenden aufgezeigt werden.

(1) Auskunft/Berichtigung/Sperrung/Löschung
Die Rechte des Betroffenen auf Auskunft, Berichtigung, Sperrung oder Löschung sind im einzelnen zwar - für nicht-öffentliche Stellen - ebenfalls im dritten Abschnitt des BDSG geregelt, jedoch stellt bereits § 6 Abs. 1 BDSG klar, daß diese Rechte des Betroffenen "nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden" können. Dahingehende Vereinbarungen vertraglicher Art sind somit nichtig. Desweiteren enthält § 6 Abs. 2 BDSG eine zur Durchsetzung dieser Rechte des Betroffenen ganz entscheidende Regelung. Diese stellt nämlich fest, daß sich der Betroffene in Fällen, in denen mehrere Stellen speicherungsberechtigt sind, zur Durchsetzung seiner Rechte an jede dieser Stellen wenden kann; diese ist dann jeweils verpflichtet, "das Vorbringen des Betroffenen an die speichernde Stelle weiterzuleiten" (§ 6 Abs. 2 S. 2 BDSG) und den Betroffenen "über die Weiterleitung und die speichernde Stelle zu unterrichten" (§ 6 Abs. 2 S. 3 BDSG). Es soll eben nicht zu Lasten des Betroffenen gehen, wenn er selbst nicht feststellen kann, wer nun konkret "Herr seiner Daten" ist.

Da dieser Fall im Rahmen der Organisation der X.500-Directories im Deutschen Forschungsnetz durchaus auftreten kann, weil hier rein technisch letztlich eine Verbunddatei geführt wird, deren Einzelbestandteile auf verschiedenen Rechnern verarbeitet werden können, sollte der DFN-Verein folgendes vorab sicherstellen:

Mit den angeschlossenen Teilnehmern (Mitglieder des DFN-Vereins) sollten Absprachen getroffen werden, in welcher Weise die Weiterleitung des Vorbringens eines Betroffenen an die (technisch) speichernde Stelle erfolgen soll; die Information an den Betroffenen anhand eines festgelegten Standards, der die Inhalte dieser Information festlegt, müßte diesen Vorgang abrunden. Denkbar wäre aber auch, jedem angeschlossenen Teilnehmer die Verpflichtung aufzuerlegen, als Mitglied des DFN-Vereins (der ja letztlich speichernde Stelle ist) dessen Pflichten direkt wahrzunehmen und das Vorbringen des Betroffenen selbst zu behandeln, sofern hierzu technisch die Möglichkeit besteht[13].

Vor diesem Hintergrund sollten die nachfolgend behandelten einzelnen Rechte des Betroffenen gesehen werden.
Das Recht auf Auskunft regelt § 34 BDSG. Dessen Absatz 1[14] legt fest, daß der Betroffene Auskunft "über die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen" verlangen kann, daneben aber auch über den Speicherungszweck und (bei automatisierter Verarbeitung) über Personen und Stellen, an die eine regelmäßige Übermittlung seiner Daten erfolgt. Daß die Auskunft über Herkunft und Empfänger der Daten nur erteilt werden muß, wenn auch diese Angaben mitgespeichert sind, ergibt sich aus der Systematik der

---

13. Die technische Frage wird etwa bei einem Sperrungs- oder Löschungsbegehren eines ausgeschiedenen Mitarbeiters relevant, der ja selbst mangels Zugang nicht mehr über Schreib- und Leserechte verfügt.

14. § 34 Abs. 2 BDSG kommt nicht zur Anwendung, weil er sich auf Auskunfteien bezieht.

genannten Formulierung. Soweit der DFN-Verein einzelne Abrufvorgänge also nicht protokolliert, beschränkt sich die Auskunft auf die personenbezogenen Daten des Betroffenen. Die Auskunft ist grundsätzlich schriftlich zu erteilen (§ 34 Abs. 3 BDSG) und in der Regel unentgeltlich (§ 34 Abs. 5 BDSG). Gemäß § 34 Abs. 4 BDSG entfällt die Auskunftspflicht in solchen Fällen, in denen gemäß § 33 Abs. 2 Nr. 2 bis 6 der Betroffene nicht zu benachrichtigen ist. Diese Fälle sind hier indes nicht einschlägig[15], so daß es bei der Auskunftspflicht des DFN-Vereins bleibt.
Das Recht auf Berichtigung, Löschung und Sperrung von Daten regelt § 35 BDSG. Dabei sind gemäß § 35 Abs. 1 BDSG unrichtige personenbezogene Daten stets zu berichtigen. Diese Funktion dient schon dem Eigeninteresse des Betreibers der Directories; er wird einem Begehren dieser Art daher sicher gerne und bereits von sich aus nachkommen. Im übrigen ist daran zu denken, die Betroffenen selbst zu einer Mitwirkung an der Aktualisierung ihrer eigenen Daten anzuhalten.

Bezüglich Löschung und Sperrung geht das Gesetz davon aus, daß grundsätzlich die Löschung vorgehen sollte und die Sperrung personenbezogener Daten nur in Ausnahmefällen vorgenommen wird. Deshalb stellt § 35 Abs. 2 fest, daß nicht mehr benötigte personenbezogene Daten zu löschen sind (§ 35 Abs. 2 Nr. 3 und 4 BDSG), daneben aber auch solche, die unzulässigerweise gespeichert werden (Nr. 1 der genannten Vorschrift) und solche sensibler Art[16], deren Richtigkeit von der speichernden Stelle nicht bewiesen werden kann. Darüberhinaus kann jederzeit eine Löschung erfolgen, soweit nicht Fälle des § 35 Abs. 3 Nr. und 2 BDSG vorliegen.

Es sind dies Fälle, in denen eine Löschung gegen gesetzliche oder anderweitige Aufbewahrungspflichten verstoßen würde oder in denen eine Löschung möglicherweise die schutzwürdigen Interessen des Betroffenen selbst beeinträchtigen könnte, weswegen für diese Fallvarianten an die Stelle der Löschung eine Sperrung der Daten tritt. Ergänzt wird diese Auflistung der Sperrungsfälle durch eine Art "Erleichterungsnorm" für die speichernde Stelle in § 35 Abs. 3 Nr. 3 BDSG. Der speichernden Stelle wird hierdurch erlaubt, statt der Löschung eine Sperrung vorzunehmen, wenn durch die Art der Speicherung eine Löschung nur mit unverhältnismäßig großem Aufwand möglich wäre. Dies wird mit zunehmender Datenspeicherung auf irreversiblen optischen Datenträgern wie CD-ROM wachsende Bedeutung gewinnen[17].
Für die Verarbeitungsvorgänge beim DFN-Verein dürfte aber unproblematisch der Schluß zulässig sein, daß etwa Daten von ausgeschiedenen Mitarbeitern generell

---

15. Um die Ausarbeitung nicht unnötig aufzublähen, wird daher an dieser Stelle auf den Wortlaut der genannten Vorschrift verwiesen. Ergänzt sei allerdings, daß auch einem mißbräuchlichen Auskunftsbegehren, z. B. einem täglich neu gestellten, nicht Folge geleistet werden muß.

16. Vgl. die Aufzählung in § 35 Abs. 2 Nr. 2 BDSG.

17. Der ferner in § 35 Abs. 4 BDSG geregelte Sperrungsfall der bestrittenen und unbewiesenen Richtigkeit der gespeicherten Daten dürfte angesichts der Datenart und der Organisation von Zugriffsrechten der Betroffenen irrelevant sein.

aus den Directories zu löschen sind.

Nachzutragen bleibt, daß neben den bereits in der Überschrift dieses Abschnitts genannten Rechten auch die Benachrichtigungspflicht zum Tragen kommen kann, die im bereits in anderem Zusammenhang kurz erwähnten § 33 BDSG geregelt ist. Dessen Absatz 1 Satz 1 ist für den DFN-Verein grundsätzlich von Bedeutung, denn bei der erstmaligen Speicherung personenbezogener Daten für eigene Zwecke ist hiernach der Betroffene von der Speicherung und der Art der Daten zu unterrichten. Zu beachten ist indes auch § 33 Abs. 2 Nr. 1 BDSG, wonach diese Benachrichtigungspflicht nicht besteht, "wenn der Betroffene auf andere Weise von der Speicherung ... Kenntnis erlangt hat". Diese Ausnahmeregelung sollte nicht in der Art überdehnt werden, daß man sich seitens des DFN-Vereins auf den Standpunkt stellt, wer Wissenschaftler sei, wisse auch, daß seine Daten in den fraglichen Directories gespeichert würden. Vielmehr sollte die Benachrichtigungspflicht Anlaß bieten, die Betroffenen, etwa in Merkblättern, die bei der Einstellung von den beteiligten Institutionen verwendet werden könnten, auf den Umstand der Speicherung ebenso hinzuweisen wie auf die bestehenden Schreibrechte der Betroffenen in den Verzeichnissen. Schon vor dem Hintergrund der oben unter 5.2 (2) behandelten Interessenabwägung ist diese den Betroffenen positv verschaffte Kenntnis wichtig.

(2) Behandlung weitergegebener Daten
Weiter ist die Frage zu beantworten, welche Vorschriften zu beachten sind, wenn Daten innerhalb des Forschungsnetzes und der darin geführten Verzeichnisse abgerufen (und dabei eventuell sogar dupliziert), also an Nutzer weitergegeben werden.

Hier könnte zunächst daran gedacht werden, die Vorschriften über die Datenübermittlung einer näheren Betrachtung zu unterziehen. Schließt man sich indes der hier vertretenen Auffassung an, daß die Verarbeitungsvorgänge nicht der einzelnen Institution, sondern dem DFN-Verein zu dienen bestimmt sind, so muß man zu dem Ergebnis kommen, daß es sich bei den Abrufen nicht um Übermittlungen an "Dritte", sondern vielmehr um Datenbewegungen innerhalb ein und derselben Organisation handelt, für die deren angeschlossene Mitglieder quasi nur helfend tätig werden.

Es erscheint daher angebrachter, im Verhältnis zwischen dem DFN-Verein und dessen Mitgliedern die Vorschriften über die Datenverarbeitung im Auftrag, § 11 BDSG, heranzuziehen.
Dieser stellt in Absatz 1 zunächst fest, daß in Auftragsverhältnissen der Auftraggeber der Hauptverantwortliche für die Einhaltung datenschutzrechtlicher Vorschriften ist. Der Betroffene hat seine Rechte diesem Auftraggeber gegenüber geltend zu machen.

Weiter bestimmt § 11 Abs. 2 BDSG, daß der Auftragnehmer vom Auftraggeber sorgfältig auszuwählen ist. Die Auftragserteilung hat schriftlich zu erfolgen, wobei

die Datenverarbeitung und
-nutzung und technische und organisatorische Maßnahmen ebenso in diesem Vertrag festzuhalten sind wie etwa bestehende Unterauftragsverhältnisse. Der DFN-Verein sollte daher eine Art "Mustervereinbarung" mit seinen Mitgliedern tr-effen, in der die genannten Kriterien enthalten sind. Dabei ist darauf zu achten, daß auch ein gewisses Weisungsrecht des DFN-Vereins hinsichtlich der stattfind-enden Verarbeitung der personenbezogenen Daten in den Verzeichnissen in dies-er Mustervereinbarung deutlich zum Ausdruck kommt; diese Notwendigkeit resultiert aus den Erfordernissen des § 11 Abs. 3 BDSG.

Wenn auch oben gesagt wurde, daß der DFN-Verein der Hauptverantwortliche in diesem Auftragverhältnis ist, so bedeutet dies doch nicht, daß die übrigen an dem Vorgang beteiligten Stellen keine datenschutzrechtlichen Pflichten haben. Gemäß § 11 Abs. 4 BDSG haben diese Stellen nämlich ihre Mitarbeiter auf das Datengeheimnis zu verpflichten (§ 5 BDSG), technische und organisatorische Maßnahmen zu treffen, um den Datenschutz zu gewährleisten (§ 9 BDSG), ihrer Meldepflicht gegenüber der zuständigen Aufsichtsbehörde nachzukommen (§ 32 BDSG)[18] und ab fünf regelmäßig mit der Datenverarbeitung befaßten Mitarbeitern einen Datenschutzbeauftragten zu bestellen (§ 36 BDSG). Die Aufsichtsbehörde überwacht auch beim Auftragnehmer die Einhaltung datenschutzrechtlicher Vorschriften (§ 38 BDSG).

5.5 Datentransfer ins Ausland

Die Nutzer des DFN- und anderer Forschungsnetze wollen natürlich nicht nur landesweit sondern möglichst global miteinander kommunizieren. Dabei ist es erforderlich, daß die jeweiligen Daten des Kommunikationspartners, der erreicht werden soll, aber unter Umständen auch größere Teile des jeweils betroffenen inländischen Directory ins Ausland verbracht werden. In diesem Fall liegt eine "Übermittlung" im Sinne des Datenschutzrechts vor. Nach § 3 Abs. 5 Nr. 3 BDSG versteht das Gesetz unter "Übermitteln" das Bekanntgeben der personenbezogenen Daten an einen Empfänger in der Weise, daß die Daten durch die speichernde Stelle an den Empfänger weitergegeben werden (hier wird die speichernde Stelle aktiv), oder der Empfänger von der speichernden Stelle zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft (hier wird der Daten-Empfänger aktiv). Für diese Vorgänge ist zu prüfen, unter welchen Voraussetzungen eine solche Übermittlung zulässig ist, insbesondere ob sie vom Gesetz auch ohne Einwilligung des Betroffenen für zulässig erachtet wird.

Ausgeklammert aus der Betrachtung bleibt an dieser Stelle die Frage, ob eine Auftragsdatenverarbeitung (etwa im Sinne des § 11 BDSG) über Grenzen hinweg

18. Dies gilt aber in Auftragsverhältnissen nur bei geschäftsmäßiger Verarbeitung als Dienstleistungsunternehmen.

zulässig ist. Diese Frage stellt sich, wenn man den DFN-Verein als "speichernde Stelle" betrachtet und die Mitglieder des Vereins die personenbezogenen Daten der Nutzer in den von ihnen betriebenen Directories lediglich im Auftrag des Vereins verarbeiten. Geschähe dies durch ein Directory im Ausland, so läge nach den oben in Abschnitt 5.1 (2) genannten Gründen keine nach dem Gesetz erlaubte Auftragsdatenverarbeitung sondern eine Übermittlung vor.

(1) Beeinträchtigung schutzwürdiger Belange

Dreh- und Angelpunkt der Diskussion um die Zulässigkeit der Übermittlung personenbezogener Daten ins Ausland ist die Frage, ob durch diese "schutzwürdige Belange" des Betroffenen beeinträchtigt werden. Die einschlägigen Rechtsvorschriften für die datenschutzrechtliche Beurteilung dieser Frage ergeben sich aus dem dritten Abschnitt des BDSG, da die speichernde Stelle nach unseren obigen Ausführungen [Abschnitt 5.1 (2)] der DFN-Verein und damit eine nicht-öffentliche Stelle ist.

Es kann dabei dahingestellt bleiben, welche der dabei gesetzlich vorgesehenen Varianten der Übermittlung hier einschlägig ist (§ 28 Abs. 1, § 28 Abs. 2, § 29 BDSG). In jedem Fall (bis auf die Übermittlung im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses nach § 28 Abs. 1 Nr. 1 BDSG) dürfen die erwähnten schutzwürdigen Belange des Betroffenen durch die Übermittlung nicht beeinträchtigt werden.

Was nun im Einzelnen darunter zu verstehen ist, bedarf zwar prinzipiell einer eingehenden Konkretisierung. Dabei kann an den Schutz der "engeren persönlichen Lebenssphäre" ebenso gedacht werden wie an das, was das Bundesverfassungsgericht im sogenannten Volkszählungsurteil als das Recht des Einzelnen auf die Wahrung seines "informationellen Selbstbestimmungsrecht" bezeichnet hat[19]. Im hier einschlägigen Fall der Übermittlung personenbezogener Daten außerhalb eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Empfänger kommt es nach allgemeiner Ansicht allein darauf an, ob im Empfängerland die dorthin übermittelten Daten dem gleichen oder einem ähnlichen Rechtsschutz unterliegen, wie dies in der Bundesrepublik der Fall ist[20]. Sollen die Daten in ein Land übermittelt werden, das über keine eigene oder mit den hiesigen Standards vergleichbare Datenschutzgesetzgebung verfügt, läßt sich nicht ausschließen, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden. Eine datenschutzrechtlich korrekte Übermittlung in solche Länder ist nach dieser wohl als herrschend zu bezeichnenden Meinung dann nur zulässig, wenn der Betroffene zuvor (entweder schon bei der Einspeicherung seiner Daten ins Directory, spätestens jedoch vor der ersten Übermittlung) in die Weitergabe in derartige Länder einwilligt.

---

19. BVerfGE 65, 1.

20. Vergl. dazu Ordemann/Schomerus, Bundesdatenschutzgesetze, § 25 Anm. 5.

Zwar wurde zeitweilig die Meinung vertreten, daß es trotz fehlendem oder geringerem Schutz der personenbezogenen Daten im Empfängerland auch ohne Einwilligung des Betroffenen zulässig sei, dorthin zu übermitteln, wenn der Empfänger der Daten sich zuvor vertraglich verpflichtet, die Daten im Ausland ebenso zu schützen, wie dies im Inland der Fall wäre[21]. Diese Meinung wird jedoch insbesondere von den datenschutzrechtlichen Kontrollinstitutionen nicht geteilt und muß daher als überholt gelten (vergleiche auch die Stellungnahmen des Berliner Datenschutzbeauftragten vom 18. Juli 1990 und vom 21. Januar 1993, die im Anhang zu dieser Studie abgedruckt sind).

Es bleibt daher dabei, daß immer dann, wenn eine Datenübermittlung ins Ausland intendiert ist, im Einzelfall konkret geprüft werden muß, ob im Empfängerland für personenbezogene Daten ein dem deutschen Datenschutzrecht vergleichbarer Rechtsschutz besteht (eine für ein weltweit agierendes Kommunikationssystem kaum praktikable Anforderung). Ist das nicht zu bejahen, darf eine Übermittlung personenbezogener Daten (auch aus einem hier angesiedelten X.500-Directory) prinzipiell nur vorgenommen werden, wenn der Betroffene voher ausdrücklich in die Übermittlung eingewilligt hat.

(2) Übermittlungssperren

Als praktische Konsequenz aus den vorstehenden Ausführungen ist daher festzuhalten, daß eine weltweite Verfügbarkeit der Directory-Daten nur zulässig ist, wenn der Betroffene im Hinblick auf die grenzüberschreitende Übermittlung seine Einwilligung erteilt hat. Allerdings muß diese unseres Erachtens nicht von vornherein oder in schriftlicher Form erteilt werden. Es dürfte auch ausreichen, wenn, nach der Einspeicherung der Teilnehmerdaten in das Directory, diese für die Übermittlung ins Ausland zunächst gesperrt werden. Dem Teilnehmer kann dann aber die Möglichkeit gegeben werden, seine Daten im Hinblick auf die Übermittlung in einzelne oder alle ausländischen Länder zu entsperren. Dies kann er auch selbst technisch im Directory vornehmen. Zu Beweis-Zwecken sollte aber unseres Erachtens der Entsperrungsvorgang selbst und wer ihn veranlaßt hat (der Teilnehmer selbst oder der Daten-Administrator), protokolliert werden.

Die Verfasser halten es für eine übersteigerte Sicherheitsanforderung, wenn der Berliner Datenschutzbeauftragte in seiner Stellungnahme vom 18. Juli 1990 (zu Frage 4) verlangt, daß eine solche "elektronische" Einwilligung durch ein digitales Unterschriftsverfahren gesichert sein müsse. Die Systemsicherung durch eine Nutzerkennung und ein Passwort, wie sie heute praktiziert wird, dürfte vielmehr für die Abgabe einer solchen elektronischen Einwilligung in die Datenübermittlung völlig ausreichend sein.

(3) EG-Richtlinie zum Datenschutzrecht

Das vorstehend erörterte in praktischer Hinsicht nicht ganz einfach zu erfüllende

---

21. Ordemann/Schomerus, aaO., am Ende.

Ergebnis (Einwilligungserfordernis für die Datenübermittlung ins Ausland bei nichtadäquater Datenschutzsituation im Empfängerland) bedarf im Hinblick auf den Bereich der Länder der europäischen Gemeinschaft (EG) noch der Relativierung. Auch die Stellungnahme des Berliner Datenschutzbeauftragten vom 21. Januar 1993 (siehe Anhang) geht davon aus, daß die Regelungen des BDSG bereits jetzt vor dem Hintergrund des geänderten Vorschlags der EG-Kommission für eine Richtlinie des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 15. Oktober 1992 auszulegen sind[22]. Es ist damit zu rechnen, daß diese geplante Richtlinie im Laufe des Jahres 1993 verabschiedet und zu einer Modifikation des deutschen Datenschutzrechts bis zum Jahre 1994 führen wird. Schon heute kann daher der Entwurf dieser Richtlinie zur Auslegung des derzeit gültigen Datenschutzrechts herangezogen werden[23].

Der Richtlinienvorschlag sieht in seinem jetzigen Artikel 7 vor, daß die Datenverarbeitung (zu der auch die Übermittlung innerhalb der EG zählt) unter anderem zulässig ist, wenn entweder die betroffene Person dazu ihre Einwilligung gegeben hat oder die Verarbeitung erforderlich ist für die Erfüllung eines mit der betroffenen Person geschlossenen Vertrags oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen.

Die Übermittlung personenbezogener Daten in ein Drittland soll entsprechend dem deutschen Vorbild ohne Einwilligung des Betroffenen nur zulässig sein, wenn das Drittland ein angemessenes Schutzniveau gewährleistet (Art. 26 des EG-Entwurfs). Ist das nicht der Fall, kann nach Art. 26 und 27 des EG-Entwurfs die Übermittlung personenbezogener Daten ausnahmsweise genehmigt werden, wenn die datenverarbeitende Stelle ausreichende Nachweise erbringt, daß insbesondere die tatsächliche Wahrnehmung der Rechte des Betroffenen im Empfängerland gewährleistet ist. Solche Nachweise können etwa in der Vereinbarung entsprechender vertraglicher Regelungen zwischen speichernder Stelle (hier DFN-Verein) und Empfänger (hier ausländischer Directory-Betreiber) gesehen werden. Nach dieser Vorschrift des EG-Entwurfs reicht also in den Fällen der Übermittlung personenbezogener Daten in ein datenschutzloses Drittland nicht einmal die Einwilligung der betroffenen Person aus. Es muß die erwähnte Genehmigung des Datentransfers hinzukommen.

Zusammenfassend können die Konsequenzen aus der geplanten EG-Datenschutzrichtlinie wie folgt dargestellt werden:

---

22. Abgedruckt in RDV 1993, S. 37 ff.; vergl. dazu auch den ersten grundsätzlichen Entwurf für eine solche Datenschutzrichtlinie im ABl. EG C 277/3 vom 05. November 1990.

23. Zum Datenexport in Drittstaaten vergl. jetzt den Beitrag von R. Ellger, Datenexport in Drittstaaten, CR 1993, S. 2 ff.

- Die Übermittlung personenbezogener Daten in datenschutzlose Drittländer wird durch das Erfordernis der erwähnten Genehmigung durch das für die speichernde Stelle maßgebliche EG-Land noch verschärft. Tritt die Richtlinie in ihrer jetzigen Version in Kraft, ist dann wohl stets die Einwilligung des Betroffenen und die erwähnte Genehmigung notwendig.

- Innerhalb der EG dürfte, ebenso wie jetzt in der Bundesrepublik, das "Widerspruchsmodell" zur Anwendung kommen. Der Betroffene hat also die Möglichkeit, der Übermittlung seiner personenbezogenen Directory-Daten in ein anderes EG-Land zu widersprechen. Diese sind dann für die Übermittlung zu sperren. Einer ausdrücklichen vorherigen Einwilligung durch den Betroffenen in die Übermittlung bedarf es aber wohl nicht.

- Sofern sich die Datenübermittlung auf die Minimalangaben im Directory beschränkt (Name, Telefonnummer, Mail-Adresse), greift für diese in Nicht-EG-Länder mit adäquatem Datenschutzniveau (die es aber bis auf die USA und Kanada zur Zeit kaum geben dürfte) wohl ebenfalls das Widerspruchsmodell ein. Die Übermittlung weitergehender Directory-Daten über den Nutzer erfordern jedoch stets dessen vorherige Einwilligung.

5.6 Aufsicht

Abschließend sei noch kurz auf die Frage eingegangen, welche datenschutzrechtliche Aufsichtsinstitution für die ordnungsgemäße Verarbeitung der personenbezogenen Daten in den DFN-Directories zuständig ist und welche Meinung von dieser im Hinblick auf die hier einschlägige Problematik erwartet werden kann.

(1) Zuständige Organe
Da nach den vorstehenden Ausführungen "speichernde Stelle" im Sinne des Gesetzes der DFN-Verein und damit eine nicht-öffentliche Stelle ist, wird die datenschutzrechtliche Kontrolle durch die sogenannte Aufsichtsbehörde durchgeführt. Für das Land Berlin, in dem der DFN-Verein seinen Sitz hat, ist das gemäß § 33 des Berliner Datenschutzgesetzes die für den Datenschutz zuständige Senatsverwaltung für Inneres, nicht der Berliner Landesdatenschutzbeauftragte.

Die Stellen, die dann im Auftrag des DFN-Vereins die Verarbeitung der personenbezogenen Daten im jeweiligen Directory tatsächlich technisch vornehmen (also etwa die einzelnen Universitäten), haben dabei die Vorschriften der §§ 5 (Datengeheimnis), 9 (Technische und organisatorische Maßnahmen), 43 (Strafvorschriften) und 44 (Bußgeldvorschriften) zu beachten. Die Einhaltung dieser Vorschriften hat dann wiederum das für die jeweilige Stelle zuständige Aufsichtsorgan zu überwachen. Betreibt also eine Landesuniversität das Directory, hat der Landesdatenschutzbeauftragte die Einhaltung der genannten Vorschriften der §§ 5, 9, 43 und 44 BDSG zu überwachen; bei einer Bundeswehrhochschule wäre dies der Bundesdatenschutzbeauftragte; letzteres gilt auch für die GMD mbH, da sie eine nicht-öffentliche Stelle ist, bei der der öffentlichen Hand die Mehrheit der Anteile gehört.

In jedem Fall gilt aber für den Auftragnehmer im Auftragsverhältnis nicht das jeweilige Landesdatenschutzgesetz. Es ist lediglich durch die nach Landesrecht zuständige Instanz die Einhaltung der genannten Vorschriften des BDSG zu überprüfen.

(2) Meinungsstand

Obwohl nach den bisherigen Erörterungen primär die Regelungen des dritten Abschnitts des BDSG auf die Verarbeitung personenbezogener Daten in den X.500-Directories anwendbar sind und obwohl sich die Kontrolle insbesondere der Länderdatenschutzbeauftragten nach unserer Auffassung mehr oder weniger nur auf die Einhaltung der technisch-organisatorischen Vorgaben des BDSG beziehen kann, haben wir uns bemüht, auch bei der Diskussion der materiell-rechtlichen Fragen die Meinung der Datenschutzbeauftragten mit zu berücksichtigen. Diese hat sich insbesondere in den Stellungnahmen niedergeschlagen, die im Anhang zu der Expertise abgedruckt sind. Wir gehen daher davon aus, daß die hier niedergelegten und begründeten Standpunkte, jedenfalls im Grundsatz, auch von diesen Behörden akzeptiert werden. Da es jedoch für diesen Bereich keine langjährige einigermaßen gleichmäßige Kontrollpraxis gibt, wird man letztlich nicht völlig vor "überraschenden" Argumenten des einen oder anderen Datenschutzbeauftragten sicher sein können. Dazu ist die Meinungsbildung und Rechtsentwicklung gerade beim Datenschutz noch zu sehr im Fluß. Dennoch meinen wir, daß die von uns erarbeiteten Ergebnisse zumindest als vorläufige rechtliche Grundlage für die Speicherung personenbezogener Daten in X.500-Directories tragfähig sind.

6. Zusammenfassung

Die wesentlichen Ergebnisse der vorliegenden Expertise können somit wie folgt zusammengefaßt werden:

(1)
Die Einspeicherung und weitere Verarbeitung von Einzelangaben über natürliche Personen in X.500-Directories ist ein datenschutzrechtlich relevanter Vorgang.

(2)
Auch ein in diesem Zusammenhang verwendetes "Minimalset" an Daten, das aus dem Namen, der Telefonnummer und der E-Mail-Adresse des Betroffenen besteht, erfüllt das Kriterium der "personenbezogenen Daten".

(3)
Als "speichernde Stelle" im Sinne des § 3 Abs. 8 BDSG ist innerhalb des Deutschen Forschungsnetzes der DFN-Verein anzusehen. Daher finden nur die Vorschriften des BDSG, nicht aber die Datenschutzgesetze der Bundesländer Anwendung.

(4)
Die Sonderregelung des § 10 BDSG über automatisierte Abrufverfahren greift bezüglich der hier geplanten Datenverarbeitungsvorgänge deshalb nicht ein, weil zwischen den an den Directories beteiligten inländischen Stellen keine echte "Übermittlung" von Daten stattfindet, sondern vielmehr zwischen diesen eher ein Verhältnis besteht, auf das die Vorschriften über die Auftragsdatenverarbeitung anzuwenden sind. Dies gilt nicht für im Ausland gelegene Directories.

(5)
Die Verarbeitung der "Minimalsets" an Daten ist zur Erfüllung des Vereinszwecks des DFN-Vereins erforderlich. Ein überwiegendes entgegenstehendes Interesse der Betroffenen kann demgegenüber nicht angenommen werden. Eine Einwilligung der Betroffenen in die Verarbeitung der "Minimalsets" ist daher nicht erforderlich; vielmehr ist eine "Widerspruchslösung" zur angemessenen Berücksichtigung der Interessen der Betroffenen ausreichend.

(6)
Im Bereich der Personalaktendaten (zum Teil wird dieser Bereich erst in Zukunft gesetzlich geregelt) bestehende oder geplante Sonderregelungen lassen gleichfalls eine Lösung über die Widerspruchsmöglichkeit der Betroffenen zu. Allerdings kann die zu diesem Ergebnis führende Argumentation nicht als völlig gesichert gelten.

(7)
Das sogenannte Forschungsprivileg des § 40 BDSG greift im Falle des DFN-Vereins bzw. der Teilnehmerdaten in den Directories nicht ein.

(8)
Die Übernahme personenbezogener Daten aus Publikationen wie etwa einem Personalverzeichnis einer Universität ist nur dann ohne weiteres zulässig, wenn die einzuspeichernden Daten vollständig bereits in dieser Publikation enthalten sind. Dann können der Aufnahme dieser Angaben in das Directory kaum schutzwürdige Belange des Betroffenen entgegenstehen.

(9)
Den Betroffenen stehen die Rechte auf Auskunft über die zu ihrer Person gespeicherten Daten, auf Berichtigung unrichtiger Daten, auf Löschung nicht mehr benötigter oder unzulässig gespeicherter Daten und - wo letzteres nicht möglich ist - auf Datensperrung zu. Daneben ist der Betroffene über die Tatsache der erstmaligen Einspeicherung seiner Daten zu unterrichten. Der DFN-Verein als speichernde Stelle ist Adressat dieser Ansprüche der Betroffenen.

(10)
Die bei den einzelnen DFN-Mitgliedern vorgenommenen Datenspeicherungen in den X.500-Directories sowie die Abrufe hieraus dienen letztlich dem Vereinszweck des DFN-Vereins. Im Verhältnis zwischen dem DFN-Verein und seinen Mitgliedern stellt die Weitergabe personenbezogener Daten daher keine "Übermittlung" dar. Vielmehr sind die Vorschriften über die Auftragsdatenverarbeitung anzuwenden. Notwendig ist für dieses Verhältnis allerdings eine schriftliche Vereinbarung zwischen dem DFN-Verein und dem Directory-Betreiber, die die Datenverarbeitung und -nutzung festlegt und das hinsichtlich der Speicherung der fraglichen Daten in den X.500-Directories bestehende Weisungsrecht des DFN-Vereins gegenüber seinen Mitgliedern verdeutlicht.

(11)
Findet ein Datentransfer ins Ausland statt, so liegt stets eine Übermittlung im Sinne des BDSG vor. Ob diese zulässig ist, ist im Einzelfall zu prüfen. Kennt das betreffende Ausland keinen dem deutschen Datenschutzrecht vergleichbaren Rechtsschutz, so ist vor der Übermittlung prinzipiell die Einwilligung des Betroffenen einzuholen. Die Verfasser halten eine Einwilligung in elektronischer Form für ausreichend.

(12)
Im Bereich der EG kann aber wohl schon jetzt eine Übermittlung von Nutzerdaten als ohne Einwilligung für zulässig erachtet werden, wenn sich diese auf den Minimalset beschränkt. Eine weitergehende Übermittlung oder eine Übermittlung in Länder ohne adäquates Datenschutzrecht bedarf jedoch der ausdrücklichen Einwilligung des Betroffenen.