

Tätigkeitsbericht  
des Datenschutzbeauftragten  
der Evangelischen Landeskirche Württemberg

Dr. Axel Gutenkunst

6. März 2006

---

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>7</b>
1.1	Kirchlicher Datenschutz, warum? . . . . .	7
1.2	Datenschutz als Wahrnehmung eines kirchlichen Auftrags . . .	9
<b>2</b>	<b>Organisation des landeskirchlichen Datenschutzes</b>	<b>11</b>
2.1	Der landeskirchliche Datenschutzbeauftragte . . . . .	11
2.1.1	Kontrollen . . . . .	12
2.1.2	Reaktionen auf Beschwerden und Anfragen . . . . .	12
2.1.3	Betriebsbeauftragte für den Datenschutz . . . . .	13
2.1.4	Prävention . . . . .	13
2.2	Kirchenbezirkliche Datenschutzbeauftragte . . . . .	14
2.2.1	Aufgabenprofil . . . . .	16
2.2.2	Erforderliche Kenntnisse . . . . .	17
2.2.3	Noch offen – Flächendeckende Kontrolle . . . . .	18
2.3	Datenschutz im Bereich der Diakonie . . . . .	18
<b>3</b>	<b>Beschwerden, Anfragen, Anmerkungen</b>	<b>23</b>
3.1	Vorbemerkung . . . . .	23
3.2	Eine Prüfstelle will ständigen Einblick in Personal. . . . .	24
3.3	Offenlegung Telefonrechnungen von Pfarrern . . . . .	25
3.4	Fundraising und Datenschutz . . . . .	25
3.5	Weitergabe von Einzelheiten über Mitarbeiter . . . . .	27
3.6	Unzulässige Datenübermittlungen an den Betriebsarzt . . . . .	28
3.7	Fürsorgliche Personalverwaltung . . . . .	29
3.8	Auskunftfreudige MAV . . . . .	29
3.9	Keine Auskunft über Goldene Konfirmation . . . . .	31
3.10	Ahnenforschung . . . . .	31
3.11	Eingestellte Personalbefragung im Bereich der Diakonie . . . . .	32
3.12	Pflegedienstplanung auf Privat-PC . . . . .	33
3.13	Unzulässige Erhebung von Listen kirchlicher Mitarbeiter. . . . .	33
3.14	Datenschutzbeschwerde wegen einer Werbeaktion. . . . .	34
3.15	Datenschutz und Wählerlisten . . . . .	34
3.16	Verwendung von Stellenplänen bei Bezirkssynode. . . . .	35

3.17	Veröffentlichung von Jubiläen . . . . .	36
3.18	Einhalten von Zusagen . . . . .	37
3.19	Fehlzeiten am schwarzen Brett . . . . .	37
3.20	Veröffentlichung von Mitarbeiterdaten auf der Homepage . . . . .	38
3.21	Verweigerung von Auskünften . . . . .	39
3.22	Krankenhausseelsorge . . . . .	40
3.23	Mut zur Pflicht . . . . .	40
3.24	Kassenprüfung bei Psychologischen Beratungsstellen . . . . .	41
3.25	Auslagerung der Buchhaltung einer Diakonischen Bezirksstelle . . . . .	42
3.26	Datenschutz bei psychologischen Beratungsstellen . . . . .	43
3.27	Kindergärten erheben Bruttoeinkommen . . . . .	44
3.28	Arbeitszeiterfassung bei Kindergärten . . . . .	45
3.29	Herausgabe von Namen von Einschulungskindern . . . . .	46
3.30	Beobachtungsbögen in Kindergärten . . . . .	46
3.31	Zeiterfassungssysteme . . . . .	47
3.32	Elektronisches Banking . . . . .	48
3.33	Pishing-Mails . . . . .	48
3.34	Zentralrechnergestütztes Meldewesen . . . . .	50
3.35	EDV-Dienstvereinbarungen . . . . .	51
3.36	Unzulässige Speicherung von Personaldaten . . . . .	53
3.37	Nutzung eines kostenlosen E-Mail-Anbieters . . . . .	55
3.38	Programmfreigaben . . . . .	56
<b>4</b>	<b>Technisches</b>	<b>59</b>
4.1	Vorbemerkung . . . . .	59
4.2	Datenschutzweb . . . . .	60
4.3	Lernprogramm Datenschutz . . . . .	60
4.4	Erhebungsprogramm Orgdia . . . . .	61
4.5	Sichere Nutzung des Internets . . . . .	63
4.6	IT-Grundschutzhandbuch . . . . .	66
4.7	Verschlüsselung des E-Mail-Verkehrs . . . . .	68
4.8	Sicherheitsgefahr durch eigene Mitarbeiter . . . . .	69
4.9	Kennwörter . . . . .	70
<b>5</b>	<b>Sonstiges</b>	<b>73</b>
5.1	Künftige Entwicklungen . . . . .	73
5.1.1	Arbeitnehmerdatenschutzgesetz: . . . . .	73
5.1.2	Informationszugangsgesetz . . . . .	74
<b>6</b>	<b>Anlage: Kirchlicher Datenschutz - Warum?</b>	<b>77</b>
6.1	Vorbemerkung . . . . .	77
6.2	Das Bundesverfassungsgericht - die Kernsätze . . . . .	78
6.2.1	Ergänzende Anmerkungen . . . . .	80
6.3	Beweggründe des kirchlichen Datenschutzes . . . . .	81

6.4 Überlegungen zur Eigenständigkeit des kirchlichen Datenschut-	
zes . . . . .	88
<b>Linkliste</b>	<b>94</b>

*INHALTSVERZEICHNIS*

---

# Kapitel 1

## Einleitung

### 1.1 Kirchlicher Datenschutz, warum?

„... Ein Kirchengesetz über den Datenschutz, muss das denn sein?, mag der eine oder andere von Ihnen fragen. Dem, der weiß, was Datenschutz heißt, kann die Antwort nicht schwer fallen. Datenschutz ist Persönlichkeitsschutz. Unser Personsein macht aus, was wir denken, meinen fühlen, tun, unterlassen, erfahren und erinnern. Von all dem teilen wir anderen immer nur soviel mit, wie uns in der jeweiligen Situation zweckmäßig und sinnvoll erscheint, einmal mehr, einmal weniger, je nachdem, worum es geht und welches Maß an Vertrauen wir unserem Gegenüber entgegenbringen. Beim Datenschutz geht es also nicht, wie leider immer noch viele glauben, um Nicht-Wissen-Dürfen oder gar Geheimniskrämerei, sondern um die Freiheit des einzelnen, in eigener Verantwortung zu entscheiden, wer wann was bei welcher Gelegenheit über ihn wissen darf, also um die Möglichkeit, unsere Kommunikationsbeziehungen zur Umwelt selbst zu gestalten und dadurch vorzusorgen, dass uns niemand mit seinem Wissen über uns bedrängen, manipulieren oder gar ausgrenzen darf.

Diesen Freiraum brauchen wir. Ohne ihn könnten wir uns als Christen weder in unserer Kirche noch in der Welt engagieren. Gerade aber das wollen wir und sollten wir auch tun, ist doch lebendige Kirche ohne engagierte Christen genauso wenig denkbar wie lebendige Demokratie ohne Staatsbürger.

Wohin es führt, wenn das Grundrecht auf Datenschutz mit Füßen getreten wird, haben unsere Schwestern und Brüder aus den östlichen Gliedkirchen jahrzehntelang leidvoll erfahren; die Stasi-Akten sind beredtes Zeugnis dessen. Doch auch unter den ganz anderen Bedingungen des demokratischen Rechtsstaats wäre unser Recht auf Datenschutz ohne wirksame Datenschutzgesetze, nicht zuletzt durch die moderne Informationstechnik, ernsthaft gefährdet. Dessen sind sich viele freilich noch nicht recht bewusst. Wir erfahren in aller Regel Datenschutz nicht so unmittelbar und existenziell im Leben

wie anderes. Was es heißt, arbeitslos oder auf Sozialhilfe angewiesen zu sein, kann auch der ermesen, der sein täglich Brot gut selbst verdient. Beim Datenschutz dagegen stellt sich persönliche Betroffenheit meist nur und erst dann ein, wenn jemand offenbar völlig unkorrekt mit unseren Daten umging, wenn also das Kind bereits in den Brunnen gefallen ist. Bis dahin halten es viele lieber mit dem Motto: Was sind schon ein paar Daten? Mehr Datenschutzbewusstsein brauchen wir deshalb auch noch in der Kirche.

Natürlich hat der Datenschutz Grenzen. Weil wir in der Gemeinschaft leben und Erwartungen an sie haben, müssen wir auch unserer Kirche zugestehen, dass sie eine Reihe von Informationen über ihre Kirchenmitglieder ohne deren Zutun und Wissen erhält. Der vorliegende Gesetzentwurf versucht, das Spannungsfeld zwischen kirchlichem Informationsbedarf und informationeller Selbstbestimmung auszutarieren. Ob das, was hier geschrieben steht, in allem befriedigt, mag der Rechtsausschuss noch einmal kurz bedenken. Dabei und sonst überhaupt sollten wir aber nicht aus dem Auge verlieren: Das Datenschutzgesetz gibt der Kirche und ihren Einrichtungen einen Grundbestand an Informationen über ihre Mitglieder. Darüber hinaus - das wissen auch viele nicht - darf die Kirche selbstverständlich alles erfahren, was ihr das Kirchenmitglied aus eigenem Antrieb sagt, und das wird umso mehr sein, je vertrauensvoller Pfarrer, Gemeinde und kirchliche Einrichtungen zusammenarbeiten. Auf solches Vertrauen ist die Arbeit unserer Kirche ohnehin angelegt, nicht nur wegen des Datenschutzes. . . .“

*(Bericht über die 4. Tagung der 8. Synode der EKD, hg. V. Kirchenamt der EKD, Hannover 1994, S. 324 f.)*

Was ist heute, 12 Jahre danach, dazu zu sagen?

*Die Herausforderungen für den Datenschutz haben im vergangenen Jahr erneut zugenommen. Selbst wenn in Deutschland niemand ausdrücklich nach dem allwissenden Staat ruft, wie er beispielsweise in den USA unter dem an George Orwell erinnernden Stichwort „Total Information Awareness“ (Totales Informationsbewusstsein) vorangetrieben werden soll, besteht auch hier zu Lande für den Datenschutzbeauftragten kein Grund zur Sorglosigkeit.*

So der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg in seinem Tätigkeitsbericht 2002, dem Jahr der 25jährigen Geltung des Bundesdatenschutzgesetzes. Die Betonung liegt wohl auf *ausdrücklich*. Kann man auch heute, nur zwei Jahre später, angesichts der Begehrlichkeiten bei der Nutzung der Informationen der DNA, der massiven Offenlegung privater Lebensverhältnisse bei der Zahlung von Arbeitslosen- und Sozialhilfe, dem Wegfall des Bankgeheimnisses, der Gesundheitskarte, der Speicherung der Verbindungsdaten aller Internet-Nutzer, der nur vom Bundesverfassungsgericht gestoppten Ausweitung des Großen Lauschangriffs, einer zentralen landesweiten Schülerindividualdatei, um nur die bekannteren Beispiele zu nennen, die Zuversicht haben, dass es in Deutschland nicht doch zum allwissenden Staat kommt? Zum allwissenden Staat gesellte sich dann

nicht weniger bedrohlich eine Wirtschaft, die Menschen mit immer filigraneren Scoring-Methoden in genehme und weniger genehme selektiert. Die Zweifel wachsen, in den Medien finden sich zunehmend wieder Beiträge, die sich diesen Fragen zuwenden. Was verhindert eine Entwicklung in Richtung Überwachungsstaat? Das, worauf der Datenschutz als potentielle Möglichkeit ständig hingewiesen hat, steht nun als faktische Möglichkeit vor der Tür und wartet auf die Realisierung. *Stete Wachsamkeit ist der Preis für die Freiheit* gilt auch und gerade im Informationszeitalter und ist deshalb auch das Motto der Startseite des Datenschutzwebs

<http://okrweb.elk-wue.de/datenschutz/index.htm>.

## 1.2 Datenschutz als Wahrnehmung eines kirchlichen Auftrags

... Der Wesensverschiedenheit der Rechtsnormen entspricht eine unterschiedliche Gestaltung staatlicher Exekutive und kirchlicher Leitung. So kommt dem Datenschutz gegenüber pastoralen Leitungsstrukturen und kirchlichen Ordnungsprinzipien nicht die Abwehrfunktion gegen hoheitliche Eingriffsverwaltung zu. Denn die Rechtsbeziehungen zu Betroffenen beruhen nicht auf der Unterwerfung unter die Staatsgewalt, sondern auf freier Entscheidung.

...

(*Auszug aus der Gesetzesvorlage des Rates zur Begründung zum Kirchengesetz über den Datenschutz, siehe Herbert Claessen, Datenschutz in der Evangelischen Kirche, S. 157 ff*).

Eben deshalb ist der kirchliche Datenschutz grundlegender als der staatliche. Beim Staat kann der Gesetzgeber das „Recht auf informationelle Selbstbestimmung“ im Interesse der Allgemeinheit, soweit noch verfassungsgemäß, wieder einschränken. Bei der Kirche würde jede Einschränkung der freien Entscheidung die Gemeindeglieder vor die Alternative, dies zu akzeptieren oder auszutreten, eine Einschränkung der *informationellen Selbstbestimmung* kann bei ihr immer nur eine *ultima ratio*, ein letztes Mittel sein, das sich überzeugend damit rechtfertigen muss, dass andernfalls die Wahrnehmung des kirchlichen Auftrags gefährdet ist.

Ganz praktische gesehen und auf den Alltag bezogen ist kirchliche und diakonische Arbeit ohne die freiwillige Bereitschaft vieler, Einblicke in ihre näheren Lebensumstände zu gewähren, schlichtweg unmöglich, betrachtet man nur etwa den ehrenamtlichen Bereich. Entsprechendes gilt hinsichtlich der in zunehmendem Umfang stattfindenden Datenübermittlungen aus Bund und Ländern. So übermittelt das Land Baden-Württemberg gemäß seiner Rechtsbestimmungen die Meldedaten nur dann an die Landeskirche, wenn vergleichbare Datenschutzregelungen gelten, entsprechendes gilt für Datenweitergaben des Justizministeriums an die Landeskirche. Im Bereich

der Diakonie nehmen viele Werke und Einrichtungen Aufgaben im Rahmen der staatlichen Daseinsvorsorge wahr, mit entsprechenden Datenflüssen. Eine solche Delegation staatlicher Aufgaben in den kirchlichen Bereich ist nur möglich, wenn die Wahrung des Sozialheimnisses gewährleistet ist. Es wäre eine fahrlässige Gefährdung ihres Auftrags, würden die Kirchen die bestehende Vertrauensbasis durch Beschneidung der Freiwilligkeit oder durch schlampigen Umgang mit anvertrauten Daten in Gefahr bringen. Ganz grundsätzlich dürfte die gesellschaftliche Erwartungshaltung an die Kirchen nicht die sein, dass auch sie Informations- und Kommunikationstechnologie in enormem Umfang einsetzen, sondern dass sie mit ihrer Sicht der Welt und aus Sorge um den Stand des Menschen in der Informationsgesellschaft auch darüber nachdenken, was getan werden muss, dass diese Entwicklung dem Menschen nicht zum Nachteil gerät<sup>1</sup> und entsprechende Vorbilder setzen.

---

<sup>1</sup>Martin Luthers tiefe Erkenntnis war, dass der „freie“ Wille des Menschen zwar zwischen Butter- und Käsebrot wählen kann, aber nicht, ob er das Gute tun will oder das Böse. Ein evangelischer Christ kann eigentlich nicht anders, als in jedem neuen technischen Mittel immer auch die Möglichkeit zu erkennen, dass es für böse Zwecke verwendet wird. Dies gilt auch für die Informationstechnik. Daraus resultiert dann eine besondere Verantwortung evangelischer Christen, wenn sie selbst solche Mittel in erheblichem Umfang einsetzen.

## Kapitel 2

# Organisation des landeskirchlichen Datenschutzes

### 2.1 Der landeskirchliche Datenschutzbeauftragte

... Datenschutz ist ein Rechtsbereich, in dem, insbesondere in der Wirtschaft, ein gewaltiges Vollzugsdefizit besteht. Nicht nur formelle Regelungen (Meldepflichten, Durchführung von Vorabkontrollen, Benachrichtigungen), sondern auch materielle Datenschutznormen werden in großem Umfang - teilweise mangels Kenntnis, oft aber sehenden Auges und gewollt - ignoriert. Dem stehen staatliche Aufsichtsbehörden gegenüber, die - personell unterbesetzt und technisch ungenügend ausgestattet, - allenfalls Stichprobenkontrollen durchführen und der Gesamtentwicklung weitgehend machtlos ausgesetzt sind. ... *(Recht der Datenverarbeitung 1/2005, Dr. Thilo Weichert, Regulierte Selbstregulierung - Plädoyer für eine etwas andere Datenschutzaufsicht).*

Diese Analyse der Situation lässt sich auch auf den kirchlichen Bereich übertragen. Dabei kann das Bundesdatenschutzgesetz immerhin noch mit einem Bußgeldkatalog mit 17 Tatbeständen und Bußgeldern von 25.000 bzw. 250.000 Euro und Strafbestimmungen mit bis zu 2 Jahren Freiheitsentzug aufwarten, die Kirche hingegen kann weder strafen noch Bußgelder verhängen.

Ich übe mein Amt des landeskirchlichen Datenschutzbeauftragten im Rahmen einer halben Stelle aus und bin zuständig

- für die Landeskirche Württemberg
- das Diakonische Werk Württemberg
- den Oberkirchenrat als Stelle

Im Wesentlichen wird mit folgenden Maßnahmen auf die Einhaltung der Datenschutzbestimmungen hingewirkt:

- Kontrollen durch den landeskirchlichen Datenschutzbeauftragten
- Reaktionen auf Beschwerden und Anfragen
- Präventionsmaßnahmen
- Aktivitäten der kirchenbezirklichen Datenschutzbeauftragten
- Aktivitäten der Betriebsbeauftragten für den Datenschutz (Diakonie)

### 2.1.1 Kontrollen

Die Kontrollen wurden in den letzten Jahren zugunsten der anderen Ebenen zurückgefahren. Vorkommnisse der letzten Zeit zeigen aber, dass schwerpunktmäßige Kontrollbesuche vor Ort dringend erforderlich sind, sie werden deshalb wieder vermehrt durchgeführt. Eine Kontrolle zieht ein Schreiben nach sich, wo die festgestellten Mängel genau benannt und Vorschläge zur Abhilfe gemacht werden. Eine Nachkontrolle, ob dies auch umgesetzt wurde, wurde bislang nicht durchgeführt. Es zeigt sich aber, dass ohne Nachkontrollen eine nachhaltige Besserung nur bedingt zu erreichen ist. Andererseits sind solche Kontrollen sehr zeitintensiv, haben kaum Wirkung über die kontrollierten Stellen hinaus und es werden immer nur relativ wenige Stellen sein, die einer direkten Kontrolle unterzogen werden können.

### 2.1.2 Reaktionen auf Beschwerden und Anfragen

Dieser Bereich hat in den letzten Jahren beständig zugenommen. Das nachfolgende Kapitel enthält einige in bestimmter Hinsicht *typische* Beispiele. Was immer mehr Zeit beansprucht ist der Bereich *Sozialdatenschutz*. Hier nehmen viele Stellen der Landeskirche und Diakonie staatliche Aufgaben wahr, gleichzeitig muss der Staat sicherstellen, dass das Sozialgeheimnis gewahrt bleibt. Das besondere Problem liegt in der Vielschichtigkeit der Lebenshilfe, die seitens des Datenschutzes ein sehr differenziertes Agieren erfordert, bis dahin, Lebensbereiche vorzufinden, wo Sinn und Zweck des Durchsetzens der *informationellen Selbstbestimmung* hinter dringenderen Bedürfnissen und Problemen zurückstehen muss. Gelegentlich wenden sich von einer kirchlichen Datenverarbeitung betroffene Personen auch zuerst an den Landesdatenschutzbeauftragten, der die Anfrage dann weiterleitet. Umgekehrt beziehen sich Beschwerden und Anfragen auf staatliche Stellen, wo dann kirchlicherseits der Landesdatenschutzbeauftragte einbezogen werden muss. Diese Zusammenarbeit funktioniert dankenswerterweise ganz hervorragend.

### **2.1.3 Betriebsbeauftragte für den Datenschutz**

Die meisten Kirchenbezirke haben mittlerweile für ihren Bereich kirchenbezirkliche Datenschutzbeauftragte bestellt und diese Bestellung vom Kirchenbezirksausschuss bestätigen lassen. Dies ist ein erfreulicher und anerkennenswerter Umstand. Stellenanteile und Zeitkontingente sind dafür in aller Regel nicht reserviert, Richtlinie ist der übliche Aufwand für die Wahrnehmung einer bezirksdienlichen Aufgabe. Auch die meisten der größeren Werke und Einrichtungen der Diakonie Württemberg haben bestellte Datenschutzbeauftragte. Die meisten haben eine entsprechende Ausbildung, nur die wenigsten konkret ausgewiesene Stellenanteile. In der Regel einmal jährlich wird eine Tagung sowohl für die Gruppe der Datenschutzbeauftragten der Kirchenbezirke als auch für die der größeren Werk und Einrichtungen der Diakonie veranstaltet. Zu überlegen ist, ob man nicht beide Gruppen zusammen fasst und häufigere Veranstaltungen durchführt. Auf die besondere Problematik der betrieblichen und kirchenbezirklichen Datenschutzbeauftragten wird im nachfolgenden Kapitel eingegangen.

### **2.1.4 Prävention**

Datenschutz ist an sich Prävention im Sinne eines vorgezogenen Grundrechtsschutzes. Bereits der Umstand, dass es einen Datenschutzbeauftragten gibt, der vorstellig werden könnte, hat eine nicht zu unterschätzende Wirkung. Ein weiteres präventives Mittel sind Vorträge zum Datenschutz bei Stellen der Landeskirche und Diakonie, die immer mehr angefragt werden. Auch die künftige regelmäßige Veröffentlichung eines Tätigkeitsberichts, wenngleich unter Verzicht auf die Nennung der Stellen, bei denen ein Datenschutzverstoß festgestellt werden musste, dürfte eine vorbeugende Wirkung haben. Bei den Bundesländern ist es üblich, dass der Landtag die Kenntnisnahme des Tätigkeitsberichts des Landesdatenschutzbeauftragten, eventuell ergänzt durch Stellungnahmen und Anmerkungen von Abgeordneten oder Fraktionen beschließt, teilweise wurde auch eine zustimmende Kenntnisnahme beantragt. Im Bereich der Landeskirche sollte ebenfalls eine Kenntnisnahme durch das Kollegium des Oberkirchenrats, verbunden mit einer angemessenen Aussprache, institutionell verankert werden. Es ist vorgesehen, jedes Jahr bei einer bestimmte Art kirchlicher Stellen, im Jahr 2006 die Schuldekane, schwerpunktmäßig zu untersuchen, welche datenschutzrechtlichen Besonderheiten zu beachten sind und wie die entsprechenden Regelungen eingehalten werden. Schließlich finden, im Hinblick auf die Datenschutzsituation in der Diakonie erste Kontakte mit einer Hochschule statt mit dem Ziel zu prüfen, ob nicht auf der Basis einer stichprobenartig nachgeprüften Selbsterklärung so etwas wie ein Datenschutz-Gütesiegel etabliert werden kann, hinter dem die Einhaltung einer im Internet veröffentlichen Checkliste mit Datenschutzanforderungen steht. Der Bedarf, mit dem Einhalten von Datenschutzbestim-

mungen auch werben zu können, wird im Bereich der Diakonie immer wieder artikuliert.

## 2.2 Kirchenbezirkliche Datenschutzbeauftragte

Das Amt des Datenschutzbeauftragten ist nicht einfach: Eben dadurch, dass diese Person *dazugehören* soll, ist sie einerseits Mitarbeiterin oder Mitarbeiter bzw. Kollege oder Kollegin und wird von der betreffenden Stelle oder Institution bezahlt, andererseits verursacht sie im Namen des Allgemeininteresses Kosten und Umstände, übt Kritik und soll dies tun.

Dass Datenschutzbeauftragter ein Beruf ist, wurde gerichtlich festgestellt. Nicht ohne Grund wurde als Voraussetzung zur Wahrnehmung des Berufs Konfliktfähigkeit verlangt. Dabei ist der Konflikt nicht nur zwischen betrieblichen bzw. kirchenbezirklichen Datenschutzbeauftragten und Stellenleitungen, sondern auch in ihnen selbst. Wird die Tätigkeit als Datenschutzbeauftragter beispielsweise nur zu 10% ausgeübt, stehen diesen 90% gegenüber, wo diese Person vielleicht selbst ein Interesse an möglichst umstandsloser Datenverwendung hat. Diesen Konflikt zwischen dem Allgemeininteresse und dem Interesse seiner Stelle muss ein betrieblicher oder behördlicher Datenschutzbeauftragter in sich selbst austragen, wird die Beauftragung ernst genommen. Dies kann und soll nicht allein bewältigt werden, die landeskirchliche Datenschutzverordnung erwähnt deshalb in § 7 Abs. 2 ausdrücklich die Pflicht der Datenschutzbeauftragten zur Zusammenarbeit (entsprechend auch § 19 Abs. 9 DSGVO-EKD).

Hat eine Stelle einen Datenschutzbeauftragten oder eine Datenschutzbeauftragte, findet sich oft die Meinung, dieser oder diese seien nun auch verantwortlich, wenn es trotzdem zu einem Datenschutzverstoß kommt. Das kann schon deshalb nicht sein, weil Datenschutzbeauftragte keine Anweisungsbefugnis haben (es gab bei der Novellierung des Bundesdatenschutzgesetzes wohl Überlegungen, betriebliche Datenschutzbeauftragte mit der Befugnis auszustatten, den EDV-Betrieb stillzulegen, wenn sie gravierende Mängel feststellen, allerdings hat dies keinen Niederschlag im novellierten Bundesdatenschutzgesetz gefunden. Es wäre auch fraglich gewesen, ob man dies so in den kirchlichen Bereich übernommen hätte. So wichtig die technische Seite ist, darf man nicht vergessen, dass die meisten Verstöße auf der inhaltlichen Seite passieren z.B. unzulässige oder unzulässig lange Speicherungen oder Übermittlungen). Datenschutz ist *Chefsache*, weil erforderliche Maßnahmen nur von der Stellenleitung umgesetzt werden können. Diese bleibt verantwortlich, auch und insbesondere gegenüber den Betroffenen. Die betrieblichen Datenschutzbeauftragten beobachten die Datenverwendung bei ihrer Stelle und weisen auf Mängel hin. Damit sie dies effektiv tun können, sind sie hinsichtlich ihrer Tätigkeit direkt der Stellenleitung zu unterstellen; diese kann damit nie behaupten, die Informationen seien in der Hierarchie *stecken*

## 2.2. KIRCHENBEZIRKLICHE DATENSCHUTZBEAUFTRAGTE

---

*geblieben*. Damit endet dann aber auch die Verantwortung des Datenschutzbeauftragten einer Stelle, die Beseitigung der Mängel ist dann Aufgabe der Stellenleitung.

Kommt die Stellenleitung dem nicht nach, wird es kritisch. Der Datenschutzbeauftragte einer größeren kirchlichen Stelle hat aus diesem Grund sein Amt aufgegeben. Nach dem Datenschutzgesetz können sich betriebliche und kirchenbezirkliche Datenschutzbeauftragte auch direkt an mich wenden, wenn sie Zweifel haben, dass die Stellenleitung den Pflichten nach dem Datenschutzgesetz nicht hinreichend nachkommt. Damit ein solches Verhalten den Beauftragten nicht zum Nachteil gerät, sieht das Datenschutzgesetz entsprechende Schutzbestimmungen vor. Das mag bei betrieblichen Datenschutzbeauftragten mit einem Stellenanteil von 50% und mehr die gewünschte Wirkung haben. Wenn der Stellenumfang für diese Tätigkeit aber nur wenige Prozent ausmacht, und dies ist für den Bereich der Landeskirche und Diakonie der Normalfall, darf man nicht erwarten, dass jemand das persönliche Risiko auf sich nimmt und sich in Sachen Datenschutz mit der Stellenleitung anlegt, insbesondere bei der heutigen Situation auf dem Arbeitsmarkt. Meist wird der Umstand noch dadurch verschärft, dass die Stellenleitung selbst mit Kostenproblemen kämpft, letztlich sogar im Interesse des betrieblichen Datenschutzbeauftragten am Erhalt der restlichen 90% seiner Stelle. Diese bedauerliche Sachlage dürfte bei realistischer Betrachtung die Grenzen dessen definieren, was von betrieblichen oder kirchenbezirklichen Datenschutzbeauftragten erwartet werden darf. Diese haben ihre Pflicht erfüllt, wenn sie Mängel erkennen und, möglichst nachweislich, darauf hinweisen. Die Beseitigung zu betreiben, kann nicht ihre Aufgabe sein.

Nach der Datenschutzverordnung nehmen kirchenbezirkliche Datenschutzbeauftragter für den Kirchenbezirk und die kirchlichen Stellen mit Sitz im Kirchenbezirk die Aufgaben wahr, die ein betrieblicher Datenschutzbeauftragter nach § 22 DSG-EKD dieser Stellen wahrnehmen müsste, d.h. sie stellen die Ausführung der Bestimmungen zum Datenschutz sicher. Insbesondere überwachen sie die ordnungsgemäße Anwendung von Datenverarbeitungsprogrammen und machen bei der Datenverarbeitung beschäftigte Personen mit den Bestimmungen des Datenschutzes vertraut (sogar bezogen auf die besonderen Verhältnisse des jeweiligen Arbeitsplatzes). Eine solche Aufgabenzuweisung erweist sich in der Praxis zunehmend als schwierig. Der Sinn eines betrieblichen Datenschutzbeauftragten liegt darin, dass dieser bei der betreffenden Stelle beschäftigt ist und die internen Abläufe mitbekommt. Das ist beim kirchenbezirklichen Datenschutzbeauftragten für fast alle Stellen seines Zuständigkeitsbereichs gerade nicht der Fall. Es ist auch schwer vorstellbar, dass ein Pfarrer das Pfarramt eines Kollegen in seinem Bezirk daraufhin inspiziert, ob bei der EDV-Nutzung hinreichend die Datenschutzbestimmungen beachtet werden. Das Anliegen, eine Reihe an sich kleinerer Stellen, etwa Kirchengemeinden, davon zu entlasten werden, einen Datenschutzbeauftragten bestellen zu müssen, ist richtig, allerdings sollte dann

auch geregelt werden, welche Aufgaben kirchenbezirkliche Datenschutzbeauftragte wahrnehmen sollen. Eine Kontrolle einzelner Stellen im Sinne einer Begehung sollte besser nicht dazugehören.

### 2.2.1 Aufgabenprofil

**Information anderer:** Unabdingbar scheint mir, dass die kirchenbezirklichen Datenschutzbeauftragten bei passenden Gelegenheiten, etwa Dienstbesprechungen, mit einer gewissen Regelmäßigkeit über aktuelle oder sonstige (rechtliche, technische) Aspekte des Datenschutzes informieren. Datenschutz umzusetzen ist, insbesondere wenn es in konkrete Details geht, nicht immer einfach, nur eine regelmäßige Arbeit an überschaubaren Details führt weiter. Als erste Anlaufstelle für Informationen bietet sich das Datenschutzweb

<http://okrweb.elk-wue.de/datenschutz> an.

**Fortbildung:** Wichtig ist ferner eine regelmäßige Teilnahme an den regelmäßigen von mir organisierten Treffen, bei denen ein Referent zu einem Thema vorträgt und Raum für einen gegenseitigen Austausch bleibt.

**Datenschutz auf der eigenen Stelle:** Eine dritte Aufgabe für kirchenbezirkliche Datenschutzbeauftragte wäre, auf der eigenen Stelle die Datenschutzbestimmungen konkret und umfassend umzusetzen und Kollegen und mich darüber zu informieren, welche Probleme sich zeigen und wie sie ggf. gelöst werden. Diese Personengruppe hat Kraft ihres Amtes die Zeit und Aufgabe, sich in einem bestimmten Umfang solchen Aspekten zuzuwenden und entsprechende Wahrnehmungen zu dokumentieren. Es ist deshalb wünschenswert, wenn bei den kirchenbezirklichen Datenschutzbeauftragten eine möglichst breite Palette von Tätigkeitsfeldern vertreten ist, also nicht nur Pfarrer und Pfarrerrinnen, sondern beispielsweise auch Verwaltungsstellenmitarbeiter, Sekretärinnen, Bezirksrechner. Dekaninnen und Dekane sollten versuchen, in diese Richtung Einfluss zu nehmen.

**Übersicht der Datenverarbeitungen:** Eine vierte Aufgabe für kirchenbezirkliche Datenschutzbeauftragte wäre, sich eine Übersicht über die Datenverarbeitungen in ihrem Kirchenbezirk zu verschaffen. Damit ist nicht ein Anhäufen von Formularen oder Daten gemeint, sondern die Herstellung des Zustandes, dass es eine Person im Kirchenbezirk gibt, die einen relativ guten Überblick im Kopf hat, was wo an Datenverarbeitung stattfindet. Um die praktische Durchführung zu erleichtern, wurde ein Erhebungsprogramm entwickelt und verteilt (für geringfügige Datenverwendung steht auch ein Formular bereit, für noch geringere reicht auch ein Anruf). Damit lassen sich etwa dienstliche Nutzungen privater PC oder die Speicherung sensibler Datenarten feststellen bzw.

getroffene Schutzmaßnahmen erfragen und Anhaltspunkte gewinnen, wo es sich für den Datenschutzbeauftragten lohnt, sich genauer kundig zu machen.

**Einweisungen:** Eine fünfte Aufgabe, die sich an die gesetzlichen Bestimmungen anlehnt, ist das vertraut machen der Bestimmungen zum Datenschutz der Personen, die mit personenbezogenen Daten umgehen. Dazu wurde ein Lernprogramm Datenschutz entwickelt, das innerhalb der Landeskirche und Diakonie Württemberg (und Baden) lizenzfrei verteilt werden kann. Es sollte eigentlich auf jedem PC, der in der Landeskirche eingesetzt wird, installiert sein. Die kirchenbezirklichen Datenschutzbeauftragten können sich dann beispielsweise bestätigen lassen, dass dieses Lernprogramm durchgearbeitet wurde, etwa bei neu angestellten Mitarbeiterinnen und Mitarbeitern oder von Ehrenamtlichen, und würden damit in allgemeiner Form der Pflicht betrieblicher Datenschutzbeauftragten nachkommen, über die Bestimmungen des Datenschutzes zu informieren.

**Verpflichtungserklärungen:** Eine sechste Aufgabe liegt darin, dafür zu sorgen, dass die Verpflichtungserklärungen zum Datenschutz, auch die Version für Ehrenamtliche, immer eingeholt werden. Da diese auch Erläuterungen enthalten, werden die jeweiligen Personen auch dadurch mit den Bestimmungen zum Datenschutz vertraut gemacht.

Insgesamt ergibt sich so ein recht konkretes Profil für die Tätigkeit eines kirchenbezirklichen Datenschutzbeauftragten, das mit vertretbarem Aufwand auch leistbar ist und das nach einiger Zeit auch einiges an Fachkunde mit sich bringen kann (*im staatlichen Bereich muss eine Schulung zum betrieblichen Datenschutzbeauftragten nach einem entsprechenden Gerichtsurteil mindestens 5 Tage umfassen*).

### 2.2.2 Erforderliche Kenntnisse

Die oft anzutreffende Meinung, dass dafür nur Personen mit besonderen EDV-Kenntnissen in Frage kommen, ist nur bedingt richtig. Jemand, der dafür sorgt, dass eine Stelle einen ordentlichen Briefkasten bekommt, der nicht ständig überquillt und in den auch DIN-A4-formatiges hineinpasst, tut nicht weniger für den Datenschutz als jemand, der auf einem PC das Installieren eines Virenschutzprogrammes bewirkt (so erfreulich es ist, wenn es in einigen Kirchenbezirken Datenschutzbeauftragte gibt, die im edv-technischen Bereich weitergehende Kenntnisse haben und damit ihren Kolleginnen und Kollegen weiterhelfen). Es ist durchaus praktikabel, das Amt auch ohne größere PC-Kenntnisse wahrzunehmen und bei dazu auftauchenden Fragen die Zusammenarbeit mit einer kundigen Person zu suchen. Wenn in bestimmten

Fällen das benötigte edv-technische Fachwissen nicht vorhanden ist, kann man sich gerne von mir Hinweise und Ratschläge einholen.

### **2.2.3 Noch offen – Flächendeckende Kontrolle**

Geregelt werden muss die Frage einer flächendeckenden Kontrolle, dass wenigstens die grundlegenden Anforderungen an Datenschutz und Datensicherheit eingehalten werden. Hier wäre vielleicht denkbar, dass die Stellen im Rahmen von Visitationen und Prüfungen des Rechnungsprüfamt eine von der Stellenleitung unterzeichnete Erklärung vorlegen müssen, und damit im Sinne einer Selbsterklärung die Einhaltung der dort aufgeführten Anforderungen bestätigen. In meiner Eigenschaft als landeskirchlicher Datenschutzbeauftragter könnte ich dann stichprobenartig solche Erklärungen nachprüfen. Das Ergebnis könnte eine veröffentlichte Feststellung sein, dass die Datenschutzbestimmungen im Bereich der Evangelischen Landeskirche im Rahmen des genannten Kontrollverfahrens als eingehalten betrachtet werden können. Dieses Modell kann auch auf den Bereich der Diakonie übertragen werden. Die von diesen Stellen abgegebene Selbsterklärung muss allerdings in besonderer Weise berücksichtigen, dass hier in den meisten Fällen Gesundheits- und Sozialdaten verarbeitet werden.

## **2.3 Datenschutz im Bereich der Diakonie**

Zu meinem Zuständigkeitsbereich gehört auch das Diakonische Werk Württemberg.

Im Bereich der Diakonie ist der Datenschutz bei den größeren Werken und Einrichtungen einigermaßen geregelt. Diese haben in vielen Fällen betriebliche Datenschutzbeauftragte, die nach dem „Ulmer Modell“ ausgebildet wurden. Diese Ausbildung an der technischen Akademie Ulm (nunmehr unter dem Namen Udis eigenständig) sah 3 Schulungen in Blöcken zu je einer Woche und eine Abschlussprüfung vor. Diese Datenschutzbeauftragten lade ich einmal jährlich zu einer Tagung mit einem Referenten (abwechselnd eher technisch oder eher rechtlich) mit anschließendem internem Austausch ein. Erfreulicherweise nimmt auch der Vorsitzende der Konferenz der katholischen Datenschutzbeauftragten regelmäßig mit teil.

Weniger erfreulich ist, dass eine zunehmende Zögerlichkeit festzustellen ist, ausgeschiedene betriebliche Datenschutzbeauftragte adäquat zu ersetzen bzw. dass es Stellen gibt, die aufgrund ihrer Größe auch einen solchen Datenschutzbeauftragten haben müssten aber nicht haben. Des Weiteren wird erkennbar, dass die Interessenskonflikte in den Personen schwieriger werden. Bislang wurde es akzeptiert, wenn die Leiter der EDV-Abteilung als betriebliche Datenschutzbeauftragte bestellt wurden. Das Datenschutzgesetz hat da zwar aus gutem Grund Vorbehalte, aber solche Personen bringen von Hause aus die bei großen Stellen unabdingbaren profunden EDV-Kenntnisse

mit und können, wenn sie ihre Ausbildung zum Datenschutzbeauftragten absolviert haben und sich dann auch dafür engagieren recht viel erreichen. Mittlerweile scheint der Effizienz- und Rationalisierungsdruck aber so groß zu sein, dass es sich diese Personen nur noch mit Mühe leisten können, Zeit und Energie für den Datenschutz zu erübrigen. So wie die Stimmung teilweise ist, ist es ohne weiteres nachvollziehbar, wenn es sich solche Leute fünfmal überlegen, ob sie in Sachen Datenschutz „aufmucksen“. Diese Entwicklung ist auch insofern bedauerlich, als gerade der im Datenschutz ausgebildete und sich dafür engagierende EDV-Leiter für eine ganze Reihe von Werken und Einrichtungen der Diakonie eigentlich eine effiziente Art und Weise ist, dem Datenschutz genüge zu tun. Dass dies zunehmend in Frage gestellt werden muss ist wohl nur ein weiteres Beispiel dafür, wie kurzfristige (Pseudo-)Rationalisierung mittelfristige Ineffizienz bewirkt.

Angesichts dieser Entwicklung werde ich künftig nur noch dann von einer Beanstandung absehen, wenn bei der Bestellung von Personen mit Leitungsaufgaben im IT-Bereich zum Datenschutzbeauftragten ein konkreter Stellenanteil für diese Aufgabe mit ausgewiesen wird. Ob dies auf Dauer hilft, bleibt abzuwarten. Ein Anhaltspunkt für den Umfang eines solchen Stellenanteils könnte sein, dass der Landesdatenschutzbeauftragte in seinem Tätigkeitsbericht 2004 eine 70%-Stelle für drei Krankenhäuser akzeptiert. Eine Bestellung eines Datenschutzbeauftragten für ein kirchliches Krankenhaus oder einer kirchlichen Einrichtung vergleichbarer Größenordnung mit einem Stellenanteil von weniger als 20% wäre damit zunächst einmal fragwürdig.

Der Datenschutz bei den mittleren und kleineren Stellen in der Diakonie ist weit weniger geregelt, was Anlass zu zunehmender Besorgnis gibt. Viele dieser Stellen erheben, verarbeiten und nutzen Daten nach § 2 DSGVO, also besondere Arten personenbezogener Daten. Diese sind auch besonders zu schützen. Diese Hervorhebung besonderer Datenarten wurde aus dem Bundesdatenschutzgesetz mit übernommen, gilt also auch in Staat und Wirtschaft, die Kirche kann hier keinen Sonderweg gehen. Schon um den Verdacht, die Diakonie wolle sich einen Wettbewerbsvorteil verschaffen, indem sie es sich erspart, den daraus resultierenden Anforderungen zu entsprechen, gar nicht erst aufkommen zu lassen, muss dringend ein überzeugendes und präsentables Konzept gefunden werden.

Immer wieder wird angefragt, ob denn die Bestellung externer Datenschutzbeauftragter zulässig wäre. Die entsprechende Bestimmung im Datenschutzgesetz (§ 22 DSGVO) schließt dies zumindest nicht aus; die in diesem Paragraphen enthaltene Regelung, dass sich die Bestellung auch auf mehrere Werk und Einrichtungen bzw. kirchliche Körperschaften erstrecken kann, legt die Zulässigkeit sogar nahe. Allerdings liegt der eigentliche Sinn eines betrieblichen Datenschutzbeauftragten darin, dass dieser zur Mitarbeiterschaft der Stelle zählt und so sehen kann, ob in den alltäglichen normalen Abläufen die Datenschutzbestimmungen eingehalten werden. Ein externe Person müsste sich diesen Kenntnisstand durch Befragungen und Erhebungen erst

verschaffen, was zum einen bezahlt werden muss und zum anderen weitere Kosten dadurch verursacht, dass dabei die Mitarbeiter und Mitarbeiterinnen von der Arbeit abgehalten werden. Auf diese Schwierigkeit ist wohl auch die Beobachtung zurückzuführen, dass mit externen Beauftragungen häufig die Tendenz einhergeht, den Datenschutz auf (oft nicht billige) EDV-technische Maßnahmen herunterzurechnen. Die wirklich „dicken Hunde“ beim Umgang mit Daten bleiben dabei meist unentdeckt. In aller Regel dürfte es sinnvoller sein, mit einem vergleichbaren Aufwand an Zeit und Kosten eine interne Person zu schulen, die auf der betreffenden Stelle eine längerfristige Perspektive hat, und ihr ein ausreichendes Zeitkontingent für die Umsetzung der Datenschutzerfordernungen zuzubilligen.

Für einen externen Datenschutzbeauftragten könnte es allerdings sprechen, wenn dieser für eine bestimmte Anzahl von Stellen gleichen Typs zuständig wäre, etwa für alle Diakonie- und Sozialstationen in einem bestimmten Bereich. In einer solchen Konzeption liegt für die Diakonie vielleicht ein Weg, mit tragbarem Aufwand den gesetzlichen Anforderungen glaubwürdig und vorzeigbar Genüge zu tun. Dies ist unabdingbar. Die Einordnung der Diakonie unter den kirchlichen Datenschutz hat nur dann eine Chance auf Dauer, wenn damit nicht eine Nivellierung des Datenschutzes nach unten verbunden ist, etwa aufgrund der fehlenden Sanktionsmöglichkeiten, wie sie im Bundesdatenschutzgesetz vorhanden wären. Es muss deutlich werden, dass im Bereich der Diakonie den Datenschutzerfordernungen nicht weniger nachgekommen wird als bei vergleichbaren privatwirtschaftlichen oder staatlichen Stellen.

Die oft gestellte Frage, welchen Umfang das Zeitbudget eines betrieblichen Datenschutzbeauftragten haben muss, kann nicht in der Form beantwortet werden, dass in eine Formel bestimmte Kenngrößen wie Anzahl der Mitarbeiter und Anzahl der PC eingegeben werden und dann eine bestimmte Stundenzahl ausgewiesen wird. Eine solche Formel gibt es nicht und macht auch keinen Sinn. Weiterführend ist die Vorstellung, dass es gilt, kurzfristig einen Berg abzarbeiten, und dann mittel- und langfristig deutlich weniger Aufwand benötigt wird. Für den Abbau der dringendsten Anforderungen kann dann eine verkraftbare Stundenzahl pro Woche festgesetzt werden und im Zuge der Durchführung dieser Aktion werden sich genügend Anhaltspunkte dafür ergeben, wie groß der Aufwand im normalen Alltag der Stelle dann noch sein muss.

Gelegentlich wurde im Bereich der Diakonie auch danach gefragt, ob es so etwas wie ein Gütesiegel gäbe, mit der ein Mitglied etwa auf seinen Briefbögen werbewirksam kundtun könne, dass es die Datenschutzbestimmungen einhält. Ein solches Gütesiegel gibt es im kirchlichen Bereich nicht. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet ein IT-Grundschutz-Zertifikat an, wo für einen IT-Verbund bestätigt wird, dass die Standardsicherheitsmaßnahmen nach dem IT-Grundschutzhandbuch umgesetzt wurden. Der Aufwand zur Erlangung eines solchen Zertifikates ist nicht

unerheblich und dürfte zunächst außerhalb der Reichweite des größten Teils der Mitglieder des Diakonischen Werkes liegen. Hier wäre es viel nahe liegender, selbst ein Konzept für eine Selbsterklärung zu entwickeln, in der die Einhaltung einer im Internet veröffentlichten Checkliste mit grundlegenden Datenschutzmaßnahmen behauptet wird. Unabdingbar für die Akzeptanz eines solchen Siegels dürfte jedoch sein, dass einer vertrauenswürdigen übergeordneten Instanz, etwa dem landeskirchlichen Datenschutzbeauftragten, eine solche Selbsterklärung gemeldet werden muss und diese mit hinreichender Häufigkeit nachprüft wird. Damit wäre sowohl eine Werbewirksamkeit erreicht als auch ein Signal Richtung Bund und Ländern, dass im Bereich der Diakonie Datenschutzerfordernungen beachtet werden. Dabei sollte die oben genannte Checkliste auch auf den Umgang mit Sozialdaten umfassen, da Stellen im Bereich der Diakonie sehr häufig mit staatlichen Aufgaben betraut sind und die betrauende Stelle sicherstellen muss, dass der Datenschutz beim Umgang mit Sozialdaten gewahrt ist.

Der hinter einem solchen Konzept stehende Aufwand wäre kirchlichen Dimensionen weit eher angepasst als die hohe Hürde eines IT-Grundschutz-Zertifikates, letzteres ist allenfalls für sehr große kirchliche Stellen denkbar. Das BSI sieht die Institution eines lizenzierten IT-Grundschutz-Auditors vor, damit könnte die Qualität des kirchlichen Gütesiegels weiter gesteigert werden. In der Organisation eines Gütesiegels für Mitglieder des Diakonischen Werkes könnte auch eine Aufgabe der Geschäftsstelle des Diakonischen Werkes gesehen werden.

Zusammenfassend lässt sich sagen, dass es auch im Hinblick auf die angespannte wirtschaftliche Situation für den diakonischen Bereich unabdingbar ist, Datenschutzerfordernungen nachzukommen. Effizienterweise sollte man dies so gestalten, dass damit eine Werbemöglichkeit verbunden ist.



## Kapitel 3

# Beschwerden, Anfragen, Anmerkungen

### 3.1 Vorbemerkung

Es ist bewährte Tradition der Tätigkeitsberichte von Bundes- und Landesdatenschutzbeauftragten, signifikante Praxisbeispiele aufzuführen.

Damit werden mehrere Zwecke verfolgt. Zum einen wird recht anschaulich, um was es beim Datenschutz geht. Zum anderen werden Datenschutzverstöße nicht unbedingt zur Freude der jeweiligen Stellen öffentlich bekannt gemacht. Schließlich können über die Auswahl der Beispiele aktuelle Schwerpunkte und Tendenzen verdeutlicht werden.

Von einer konkreten Nennung der jeweiligen kirchlichen Stellen, die in die geschilderten Fälle involviert sind, wird in diesem Tätigkeitsbericht jedoch abgesehen. Dahinter steht die Überlegung, dass ein „Anprangern“ sich im kirchlichen Rahmen als kontraproduktiv erweisen dürfte. In aller Regel gaben die Stellen, mit denen Fragen des Datenschutzes zu klären waren, bereitwillig Auskunft, auch wenn dabei Versäumnisse und Mängel offenbar wurden. Diese Bereitschaft ist eine nicht unerhebliche Arbeitserleichterung, die nicht ohne triftigen Grund in Frage gestellt werden sollte.

Dieser Gesichtspunkt war auch ursächlich dafür, dass bislang überhaupt vom Erstellen eines Tätigkeitsberichts abstand genommen wurde. Schon das Aufzeigen von Beispielen, von denen man weiß, dass dies bei irgend einer kirchlichen Stelle so gelaufen ist, kann durchaus seine Wirkung entfalten, wenn Verantwortliche oder Mitarbeiter einer anderen Stelle feststellen, dass dies bei ihnen genauso oder ähnlich abläuft und beispielsweise eine Mitarbeitervertretung sich aufgerufen fühlt, Interessen der von ihr vertretenen Personen zu wahren.

Auch so macht der Tätigkeitsbericht deutlich, dass es auch im Bereich der Kirche nicht wenige und auch gravierende Verstöße gegen Datenschutzbestimmungen gibt.

Dies ist vermutlich der erste Tätigkeitsbericht im Bereich der evangelischen (und möglicherweise auch katholischen) Kirche in Deutschland. Betrachtet man den zunehmenden Umfang, in dem im Bereich der Kirchen Informations- und Kommunikationstechnik eingesetzt wird, erscheint es an der Zeit, dass auch dort, wie von den Datenschutzbeauftragten der Länder und des Bundes schon lange praktiziert, eine Erstellung von Tätigkeitsberichten zum Standard wird.

### 3.2 Eine Prüfstelle will ständigen Einblick in Personalinformationssystem

Kaum war bei einer kirchlichen Stelle das Personalinformationssystem etabliert, wuchsen auch schon die Begehrlichkeiten. So verlangte eine Buchprüfungsstelle, dass ihren Mitarbeitern Zugriff auf die damit geführten Personalfälle gewährt wird, genauer gesagt, dieser Zugriff war faktisch schon eingerichtet.

Dem standen nach meiner Meinung die Datenschutzbestimmungen entgegen. Dass der Umfang der erteilten Berechtigungen die Erforderlichkeit übersteigt, war beispielsweise schon daran erkennbar, dass auch ein rechtlicher Berater der Prüfstelle Zugriff auf das Personalinformationssystem bekommen sollte. Des Weiteren war in der Dokumentation dieses Zugriffs die dienstliche Erfordernis, obwohl im Formular vorgesehen, überhaupt nicht begründet.

Eine Rechtsgrundlage für solch umfassende Berechtigungen ist auch nicht erkennbar. Für den landeskirchlichen Bereich ist in § 3 des Gesetzes über das Rechnungsprüfamt lediglich geregelt, dass diesem auf Verlangen Auskünfte zu erteilen und Unterlagen vorzulegen sind, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. Eine Erforderlichkeit kann sich allenfalls hinsichtlich aktuell laufender oder vorbereiteter Prüfungen ergeben, ein ständiger Zugriff auf alle Personaldaten ist dazu nicht erforderlich. Auf „Verlangen Auskunft erteilen“ bedeutet gerade nicht, einen ständigen Zugriff gewähren. Diese Regelungen entsprechen denen in den einschlägigen Regelwerken über die Rechnungslegung der Vereine, gGmbHs etc.

Nach der II. Arbeitsrechtlichen Regelung zum Schutz personenbezogener Daten kirchlicher Mitarbeiter und Mitarbeiterinnen bei der Anwendung von Personalerfassungs- und Informationssystemen (Beschluss der Arbeitsrechtlichen Kommission vom 2. Dezember 1999) ist in § 2 Abs. 1 ferner festgelegt, dass die Daten ausschließlich für Zwecke der Personalabrechnung, der Personalverwaltung sowie der Wirtschaftsplanung und betriebswirtschaftlichen Auswertung verwendet wird. Keiner dieser Zwecke tangiert die Aufgabenstellung einer Buchprüfungsstelle.

Zwar kann nach § 5 Abs. 3 Datenschutzgesetz zum Zwecke der Rechnungs- oder Buchprüfung bei einer konkreten Prüfung ohne Datenschutzverstoß auf die dazu erforderlichen Daten zugegriffen werden. Ein genereller Zugriff auf

alle Daten ist aber als Datenübermittlung anzusehen. Eine solche Datenübermittlung ist unzulässig. Der Zugriff wurde deshalb beanstandet.

### 3.3 Offenlegung Telefonrechnungen von Pfarrern

Ein Pfarrer beschwerte sich darüber, dass er aufgefordert wurde, künftig nicht nur die Summenblätter dem Zahlungsverzeichnis als begründende Unterlage beizulegen, sondern die ganze Rechnung.

Ich habe die Rechtmäßigkeit dieses Vorgehens angezweifelt. Man wird die Frage zu stellen haben, wozu eine solche Erhebung dient. Soll der nächste Schritt eine Überprüfung der angerufenen Nummern mit dem Ziel sein, Hinweise zu finden, dass dies keine dienstlichen Gespräche waren?

Hier tritt in anderer Variante der öfters feststellbare Konflikt zwischen dem Anspruch auf eine lückenlosen Kontrolle und anderen Rechtsgütern, hier das Seelsorgegeheimnis, auf. Ähnlich der Schweigeverpflichtung nach § 203 Strafgesetzbuch ist auch beim Seelsorgegeheimnis bereits der Umstand, eine solche in Anspruch genommen zu haben, ein schützenswertes Geheimnis. Davon, dass dem so ist, gehen Gemeindeglieder in aller Regel aus. Jemand, der in einer seelischen Notlage oder aus sonstigen Gründen fünfmal am Tag bei der Pfarrerin oder dem Pfarrer anruft (und/oder von diesem zurückgerufen wird), muss sich darauf verlassen können, dass davon nicht immer auch andere kirchliche Mitarbeiter erfahren. Wird das anders gesehen, muss die Landeskirche eine gegenüber dem Beichtgeheimnis vorrangige Rechtsvorschrift erlassen und die Gemeindeglieder regelmäßig darüber informieren, dass ihre naive Einschätzung, dass sie mit solchen Dingen unter sich bleiben, nicht den Tatsachen entspricht.

### 3.4 Fundraising und Datenschutz

Den „neues handeln news“ der „neues handeln gmbh“ für April 2005 ist folgende Feststellung zu entnehmen: *In der Praxis lautet so die entscheidende Frage: Wie lernen wir unsere SpenderInnen, ihre Wünsche und Bedürfnisse kennen? Neben dem neuen notwendigen Selbstverständnis der Organisation schlägt hier auch die Stunde der Bewährung für die Datenbank. Denn sie macht die Bewertung der SpenderInnen und deren Zusammenfassung in differenzierten Segmenten möglich. Dazu werden unterschiedliche Methoden angewandt, die entweder allein auf den bei der Organisation vorliegenden Daten beruhen (z.B. Pareto- oder RFM-Analyse) oder bei denen weitere Informationen von kommerziellen Anbietern herangezogen werden (z.B. Datenanreicherung, Marktforschung).* Dementsprechend bestehen in einer evangelischen Landeskirche konkrete Überlegungen, die normalen Meldedaten um Angaben wie Familienoberhaupt bzw. Haushaltsvorstand bzw. Spendenentscheider oder um mikrogeographische Angaben wie Wohngebiet, Gebäude-

typ bzw. Garten bzw. Garage, Wohnstil, Besitzverhältnisse zu erweitern. Dies geht dann weiter mit Angaben zu Einkommen, Vermögen, Sprachkenntnisse, Konsumgewohnheiten, Autotyp, Bildungsstand/soziale Schicht, Familiensammensetzung/Beziehungen, Hobby/Interessen und so weiter.

Konsequenterweise soll auf EKD-Ebene eine Fundraising-Verordnung geltendes Recht werden. Die anhand des bislang vorgelegten Entwurfs erkennbaren Tendenzen sind unter Datenschutzgesichtspunkten bedenklich, so sollen Kirchengemeinden verpflichtet sind, für einen Spendenaufruf einer Stelle der Evangelischen Kirche oder Diakonie die Meldedaten ihrer Gemeindeglieder zu übermitteln. Auch wenn nur ein Erlaubnistatbestand geschaffen werden soll, stellen sich folgende Fragen:

1. Wie will man verhindern, dass die Gemeindeglieder mit Spendenaufrufen zugehäuft werden? Soll dafür eine zentrale Koordinationsstelle auf EKD-Ebene geschaffen werden? Oder will man gar eine zentrale deutschlandweite evangelische Spenderdatei im Sinne der oben genannten „Bewährungsstunde der Datenbank“ schaffen? In der im Sinne einer umfassenden Pflege der „Spender-Relationship“ genau notiert wird, wann wieviel gespendet wurde, ergänzt um Angaben zu den jeweiligen Bedürfnissen? Dann abgeglichen mit kommerziellen Datenbanken, etwa um anhand der Betuchteit der Wohnlage eines Spenders ein Scoring-Wert für künftige Spendenerwartungen zu errechnen?
2. Wie will man Widersprüche von Gemeindegliedern gegen eine Weitergabe ihrer Daten für Spendenzwecke berücksichtigen? Will man eine zentrale deutschlandweite Datei spendeunwilliger Gemeindeglieder schaffen? Es gibt nicht wenige Menschen, die das, was sie Spenden können, für einen bestimmten Zweck spenden und dann, mit gutem Recht, in Ruhe gelassen werden wollen.
3. Die Kirchengemeinden überschauen am besten, was in ihrem Bereich bereits an Spendenaufrufen läuft und ab wann es zu viel wird. Wäre es nicht sinnvoller, anstatt zentraler Koordinierungsstelle, Datenbank und Verordnung praktikable Standards festzulegen, die es teilnahme-willigen Kirchengemeinden schnell und effizient erlauben, ihre Daten für eine bestimmte Spendenaktion zu koordinieren und diese Aktion damit durchzuführen, auch über Landeskirchen hinweg? In Gemeinde-briefen könnten die Aktionen angekündigt und (ggf. dauerhafte) Wi-dersprüche ermöglicht werden. Damit wäre man immer dicht bei den Menschen, ohne diese in einem Datenregister zu führen.
4. Aktuelle Studien zeigen, dass die Menschen immer sensibler werden, was fragen wie „Identitätsdiebstahl“ usw. anbelangt. Wenn sich die Leute nicht darauf verlassen können, dass ihre Spenderdaten geschützt sind, sind erhebliche Glaubwürdigkeitsprobleme vorprogrammiert. Ein

### 3.5. WEITERGABE VON EINZELHEITEN ÜBER MITARBEITER

publik gewordener Datenschutzvorfall würde genügen, um auf Dauer tiefes Misstrauen gegenüber einem kirchlichen Umgang mit Spenderdaten hervorzurufen.

Nicht wenige Gemeindeglieder sind mit Misstrauen und Unmut davon überzeugt, dass die Kirchen alles Mögliche an Daten über sie speichern; dem konnte ich bislang dadurch entgegenreten, dass ich ihnen erläuterte, welche Daten tatsächlich gespeichert sind und das dies nicht nach Belieben geschieht, sondern in kirchlichen Gesetzen wie der Kirchenregisterverordnung genau geregelt ist. Gibt man diese Selbstbeschränkung auf, und wird dies auch noch öffentlich bekannt, kann ganz schnell eine Abwehrhaltung gegen den kirchlichen Umgang mit Daten entstehen. Die für das Ehrenamt unabdingbare Bereitschaft, Einblicke in persönliche Lebensverhältnisse zu gewähren, sollte nicht um einer ungewissen Hoffnung auf mehr Geld willen verspielt werden.

Sinnvoller wären wohl kleine praktische Schritte. Schon vor längerer Zeit hatte ich mich an die zuständige zentrale Institution der Kreditwirtschaft gewandt und vorgeschlagen, in Überweisungsformularen (auch beim Online-Banking) die Möglichkeit vorzusehen, einem Eintrag der eigenen Adressdaten in den Kontoauszug des Empfängers zuzustimmen. Mit weiteren Angaben in den Zweckfeldern („nur Spendenquittung“, „keine Aufnahme in Spenderliste“) könnten die Spender dann schon mit dem Überweisungsformular signalisieren, welchen Umgang sie mit ihren Spenderdaten wollen. Eine solche Option dürfte für eine ganze Reihe gesellschaftlicher Bereiche interessant sein und könnte auch dem Spendenbereich neue Möglichkeiten eröffnen.

Unabhängig von solchen eher praktischen Überlegungen muss eine Fundraising-Verordnung auf alle Fälle eine zufrieden stellende Antwort auf die oben genannten Fragen (und weitere, die sich erst bei genauerer Betrachtung stellen) geben.

### **3.5 Weitergabe von Einzelheiten über Mitarbeiter**

Eine Mitarbeiterin einer größeren kirchlichen Stelle nutzte regelmäßig die Möglichkeit, dort private Kopien erstellen zu lassen. Das übliche Verfahren war, dass für einen solchen privaten Druckauftrag eine Genehmigung eingeholt wird, dann erfolgt die Rechnungsstellung.

Da es in der Welt nicht immer friedlich zugeht, hatte diese Person privat mit einem juristischen Streitfall zu tun, und die Gegenseite, die irgendwie Wind von der Möglichkeit privater Druckaufträge bekommen hatte, war frech genug, bei der Buchhaltung dieser Stelle anzurufen und nachzufragen, ob die Mitarbeiterin denn auch immer alle Rechnungen bezahlt hätte.

Eine ganz besonders zuvorkommende Mitarbeiterin sucht dann, es war schließlich ein Anwalt, also eine „Rechtsperson“, prompt alle Rechnungen heraus und kontrollierte nach und teilte das Ergebnis dann auch brav mit.

Wie das Leben so spielt, stellte sich tatsächlich heraus, dass vor Jahren eine Rechnung nicht bezahlt wurde. Es erfolgte aber auch nie eine Zahlungserinnerung, wie man eigentlich hätte erwarten können, anscheinend war die Buchhaltung durch eine EDV-Umstellung nicht mehr so ganz im Bilde. Diese Informationen wurden im privaten juristischen Streitfall von der Gegenseite genüsslich dazu verwendet, die betroffene Mitarbeiterin in ein schlechtes Licht zu rücken.

Noch erstaunlicher war schließlich der Umstand, dass die etwas zuvorkommende Mitarbeiterin, obwohl konkret auf ihr Verhalten angesprochen, nicht das mindeste Empfinden hatte, sich nicht ganz richtig verhalten zu haben.

Das Hauptverschulden ist aber bei der Leitung der betreffenden kirchlichen Stelle zu suchen. Das Datenschutzgesetz verlangt unmissverständlich, dass mit dem Umgang mit Daten betraute Personen auf das Datengeheimnis zu verpflichten sind und dass es diesen Personen untersagt ist, personenbezogene Daten unbefugt zu erheben, verarbeiten (dazu zählt auch übermitteln) oder zu nutzen. Des Weiteren ist mit der Verpflichtung eine Belehrung über den Datenschutz zu verbinden, damit sich die Mitarbeiter und Mitarbeiterinnen hinreichend im Klaren darüber sind, was von ihnen verlangt wird.

### **3.6 Unzulässige Datenübermittlungen an den Betriebsarzt**

Eine Mitarbeiterin einer Diakonie-Sozialstation beschwerte sich über ihrer Ansicht nach viel zu weitgehende Übermittlungen von Angaben zu ihrer Person an den zuständigen Betriebsarzt.

Dazu ist zunächst festzustellen, dass die Einsatzleitung einer Diakoniestation im Rahmen von betriebswirtschaftlichen Überlegungen, wo es darum geht, festzustellen in wieweit eine bestimmte Person aufgrund ihrer gesundheitlichen Situation für bestimmte Tätigkeiten einsetzbar ist oder nicht, sich beim Betriebsarzt entsprechende Auskünfte durchaus einholen kann.

Dies muss jedoch zweckgerichtet geschehen. Das ist dann nicht mehr der Fall, wenn an den Betriebsarzt keine konkreten Anfragen gestellt werden, sondern diesem umfassende, schriftlich niedergelegte personelle Vorüberlegungen zur künftigen Tätigkeit dieser Mitarbeiterin zugestellt werden. Dies war im vorliegenden Fall zu weitgehend. Die Einsatzleitung hätte ihre Vorüberlegungen zu konkreten Fragestellungen hinsichtlich der Zumutbarkeit bestimmter Tätigkeiten weiterführen müssen. Dazu hätte sie dann eine Stellungnahme des Betriebsarzt einholen können.

Da es künftig möglicherweise in vermehrtem Umfang Anfragen an Betriebsärzte geben wird, sei darauf hingewiesen, dass diese zum einen der Schweigepflicht nach § 203 Strafgesetzbuch unterliegen, zum anderen gesundheitliche Angaben zu den besonderen Datenarten nach § 2 Abs. 11 Daten-

schutzgesetz der Evangelischen Kirche gehören, bei deren Erhebung, Verarbeitung und Nutzung besondere Vorsicht geboten ist. Hätte sich die Stellenleitung an diese Vorschrift gehalten, wäre es wohl nicht zu diesem Vorfall gekommen. Auf das im hinteren Teil dieses Tätigkeitsberichts vorgestellte „Lernprogramm Datenschutz“ (siehe auch unter <http://okrweb.elk-wue.de/datenschutz/download.htm#t2>) sei schon hier hingewiesen.

## 3.7 Fürsorgliche Personalverwaltung

Es war sicherlich gut gemeint. Eine Person war längere Zeit krankgeschrieben, wurde erfreulicherweise wieder gesund und erhielt von der zuständigen Personalverwaltung ein Schreiben, wo dieses seine Anteilnahme am positiven Verlauf des Ganzen zum Ausdruck brachte.

Etwas irritiert war die betroffene Person allerdings dann darüber, dass in diesem Schreiben eine Fülle an Details zur Krankheit und deren Verlauf angesprochen wurden. Ganz so hatte sich die betroffene Person eine gute und effiziente Personalverwaltung nicht vorgestellt. Dass Personalverantwortliche von der Krankheit, dem dadurch bedingten Ausfall der Amtsgeschäfte sowie von der Genesung wissen müssen, ist klar, was aber genauere Details anbelangt, hätte man dann doch erwartet, dass diese im Rahmen der Kostenabwicklung dann möglichst auf Sachbearbeiterebene verbleiben.

So löste das das gut gemeinte Schreiben nur bedingt das Gefühl aus, von einer Personalverwaltung gut betreut zu werden, sondern weckte die Befürchtung, künftig nunmehr ständig als mit dem Etikett „durchgemachte X-Krankheit“ versehen wahrgenommen zu werden.

Es hat seinen guten Sinn, dass gesundheitliche Daten von allen Datenschutzgesetzen als besonders schutzwürdig eingestuft werden, dazu gehört auch, dass innerhalb einer Stelle organisatorisch gewährleistet wird, dass jede Person nur das weiß, was sie zur Aufgabenwahrnehmung wissen muss. Dazu gehört auch, dass Leitungspersonen in die Details der Sachbearbeitung grundsätzlich nur insoweit Einblick nehmen, wie dies zur Wahrnehmung ihrer Leitungsfunktion erforderlich ist. Der gelegentlich geäußerte Anspruch dieser Personen, nach eigenem Gutdünken ständig in alles Einblick nehmen zu dürfen wird dem Persönlichkeitsrecht der Betroffenen nicht gerecht (im Datenschutzjargon nennt sich dies die „vertikale Gewaltenteilung“).

## 3.8 Auskunftsfreudige MAV

Das Verhältnis zwischen Mitarbeitern und der Dienststellenleitung kann sich manchmal schwierig gestalten. Damit dann die Rechte der Mitarbeiter gewahrt werden, gibt es die Mitarbeitervertretung (MAV). Jemand, der sich dann an eine solche MAV wendet, geht mit einem gewissen Grundvertrauen

davon aus, dass diese dann, wie schon der Name ausdrückt, seine Sache vertritt. Zur Art und Weise, wie die MAV die Sache ihrer Mitarbeiter vertritt gehört auch, mit Sorgfalt darauf zu achten, dass die Inhalte dazu ergehender Schreiben an die Dienststelle oder andere Stellen nicht dazu verwendet werden können, die Stellung der vertretenen Person unnötigerweise noch mehr zu verschlechtern. Dass dies nicht völlig selbstverständlich ist zeigte ein Beschwerdefall hinsichtlich einer Mitarbeitervertretung eines Kirchenbezirks. Von einem damit befassten Amt um eine Stellungnahme zu einer außerordentlichen Kündigung gebeten, erging sich diese in aller Breite in einer Darlegung über die in diesem Zusammenhang stattgefundenen Gespräche mit der betreffenden Person und befeiligte sich sogar dahingehend, auch eine Chronologie der Gespräche und ihrer Themen aufzuführen. Dabei wäre ein einziger schlichter Satz, etwa dahingehend, dass sich diese MAV mit der Sache auseinander gesetzt hat, dass Gespräche geführt wurden und dass nach einer Beratung der Beschluss gefasst wurde, der Kündigung zuzustimmen (oder auch nicht), ausreichend gewesen. Damit jedoch nicht genug, schickte diese MAV eine Kopie des Schreibens an das Amt auch gleich noch an die Dienststellenleitung, um die Stellungnahme dieser gegenüber gleich mit zu erledigen. Das war für selbige sehr erfreulich, konnte sie so vor dem Arbeitsgericht hervorragend darlegen, dass das Arbeitsverhältnis zerrüttet war, was dann auch ein entsprechendes Urteil nach sich zog. Auch gegenüber der Dienststellenleitung wäre ein Schreiben mit einem lapidaren Satz wie dem oben genannten (dann hätte man sogar dieses einfach kopieren können) ausreichend gewesen. Dass diese MAV aber sehr wohl imstande war, kurz und knapp zu antworten, zeigte sie, als die betroffene Person Auskunft darüber begehrte, was denn dem oben genannten Amt mitgeteilt wurde. Hier auf einmal schwang man sich zur Feststellung auf, dass man keine Veranlassung sehe, das Schreiben an eine andere Stelle abzugeben als an die, die es angefordert hat. Dabei trug das in Frage stehende Schreiben an das Amt sogar den ausdrücklichen Vermerk, dass eine Kopie an die Dienststellenleitung geht, was aber diese MAV nicht weiters irritierte. Das Gebaren dieser MAV wurde beanstandet. Dass hier unter Datenschutzgesichtspunkten gegen Vorschriften zur Übermittlung von Daten verstoßen und das Recht von Betroffenen auf Auskunft verletzt wurde, ist. Hier kommt jedoch die besondere Vertrauensstellung einer Mitarbeitervertretung hinzu. Diese muss, und jeder, der sich an eine solche wendet, sollte sich darauf verlassen können, dass dem so ist, nicht nur prüfen, ob eine Übermittlung von Angaben überhaupt zulässig ist, sondern, wenn dies gegeben ist, zusätzlich, ob dies der betreffenden Person schaden könnte. Wer verunsichert ist, ob seine Kontaktaufnahmen mit der Mitarbeitervertretung Rechtsnachteile für ihn bewirkt, wird auf die Inanspruchnahme solcher Dienste verzichten.

In aller Regel richten sich MAV'en auch danach. Aufgrund des hier geschilderten Vorfalles ist die landeskirchliche Mitarbeitervertretung jedoch gut beraten, wenn diese in ihren Schulungen für gewählte Mitarbeitervertreter

künftig auch etwas Zeit für die Erläuterung der wichtigsten Datenschutzbestimmungen vorsieht.

### 3.9 Keine Auskunft über Goldene Konfirmation

Ein Gemeindeglied wollte zur Organisation eines Treffens zur Goldenen Konfirmation von einer größeren kirchlichen Stelle Angaben zu noch wenigen fehlenden Personen eines bestimmten Jahrgangs haben. Es erhielt dann die lapidare Auskunft, dass es „der Datenschutz“ nicht zuließe, solche Informationen weiterzugeben.

Richtig ist daran zunächst, dass die betreffende speichernde Stelle Daten nur weitergeben darf, wenn es dafür eine Rechtsvorschrift gibt oder wenn die betreffenden Personen eingewilligt haben. Beides lag tatsächlich nicht vor. Richtig ist auch, dass wenn die betreffende Stelle die Daten einfach weitergegeben hätte, es durchaus hätte sein können, dass dies der betreffenden Person gegen den Strich gegangen wäre und diese Datenschutzbeschwerde eingelegt hätte. Dieser hätte man dann wohl Recht geben müssen.

Andererseits ist das Anliegen nun durchaus verständlich, und es ist bestimmt nicht im Sinne des Datenschutzes, das Knüpfen oder Wiederaufleben sozialer Kontakte zu vereiteln. Das einfachste ist doch, dass die speichernde Stelle, wenn sie brauchbare Adressangaben hat, der betreffenden Person eine kurze Mitteilung schickt und dort die Kontaktadresse nennt. Dann kann diese selbst entscheiden, wie sie sich verhalten will.

In aller Regel steht der dafür erforderliche Aufwand in keinem Verhältnis zu den Kosten für die Zeiten, die dann zur Abwicklung von Beschwerdebriefen und Unmutsbekundungen benötigt werden. Ich meine, es sollte den betreffenden kirchlichen Stelle wert sein, hier ein gewisses entgegenkommen zu zeigen. Schaden tut's bestimmt nicht.

### 3.10 Ahnenforschung

Die Frage nach dem Datenschutz bei der Ahnenforschung ist eigentlich einfach zu beantworten: Datenschutz gilt nur für noch lebende Personen. Eine Grauzone entsteht dann, wenn Angaben zu Verstorbenen für die noch lebenden Nachkommen zu einer Belastung werden könnten. So muss z.B. nicht jeder in Erfahrung bringen können, dass der Vater von Frau X anscheinend Alkoholprobleme hatte. Manche Datenschutzbeauftragte sehen deshalb auch eine „Abklingzeit“ des Datenschutzes bei Verstorbenen, innerhalb derer eine mutmaßliche „Selbstbestimmung“ zu beachten wäre.

Gelegentlich fragen Pfarrämter an, ob sie einem Ahnenforscher Einblick in ihre Kirchenbücher gewähren müssen bzw. Ahnforscher beschweren sich, wenn Pfarrämter eine solche Einblicknahme ablehnen.

In diesem Zusammenhang weise ich immer auch darauf hin, dass im Landeskirchlichen Archiv nahezu vollständig Mikrofilm-Ablichtungen aller Kirchenbücher der Landeskirche Württemberg verfügbar sind. Dort wird auch eine ganze Anzahl von Lesegeräten bereitgehalten. Damit ist auch der Zweck verbunden, Anfragen an Pfarrämter oder andere kirchliche Stelle zu bündeln und zu kanalisieren, also z.B. zu verhindern, dass eine Person mehrere Ämter mit derselben Sache vorstellig wird. Eine Archivordnung regelt die Einblicknahme in die Unterlagen.

Auch wenn eine Einblicknahme durch einen Ahnenforscher rechtlich zulässig wäre, heißt dies noch lange nicht, dass die Pfarrämter diese auch gewähren müssen. Unbeaufsichtigt kann eine solche Einblicknahme nicht gestattet werden, da sichergestellt werden muss, dass Einblicke in die Daten noch lebender Personen tabu bleiben. Es sind durchaus schon Fälle bekannt geworden, wo das Interesse an Ahnenforschung nur vorgeschoben war und es tatsächlich darum ging, Anhaltspunkte für erbrechtliche Ansprüche zu finden. Ein Pfarramt braucht die Umstände, die das Gewähren von Einblicken in Kirchenbücher mit sich bringen, nicht auf sich nehmen und kann auf das landeskirchliche Archiv verweisen. Dies müssen die Ahnenforscher akzeptieren.

### **3.11 Eingestellte Personalbefragung im Bereich der Diakonie**

An sich war die ganze Sache begrüßenswert. Für Mitarbeitende im Bereich der ambulanten Pflege sollte im Rahmen eines Forschungsprojektes erhoben werden, wie man das Fortbildungsangebot optimieren könne. Handlungsspielräume und Mitgestaltungsmöglichkeiten sollten erweitert werden, Kompetenzen gefördert und Ergebnisse aus der Stressforschung als „Burn-Out“-Prophylaxe nutzbar gemacht werden. Schließlich sollten die Ergebnisse auch Einfluss auf eine entsprechende Personalplanung nehmen. Dazu sollte eine Ist-Analyse durchgeführt werden.

Weniger begrüßenswert war, dass die Mitarbeiterinnen und Mitarbeiter auf namentlich gekennzeichneten Fragebögen Auskünfte darüber geben sollten, wo sie bei sich Defizite sahen oder besondere Probleme hatten, ihre Aufgaben zu bewältigen. Weniger glücklich war auch eine Vermischung der Erhebung von Daten im Rahmen des Forschungsprojektes und der Erhebung von Daten zur Personalplanung. Dass die Mitarbeitervertretung dagegen Sturm laufen würde und sich an mich wenden würde, war vorhersehbar.

Dieser zeigte dann Wege auf, wie man die Befragung so durchführen kann, dass die Anonymität gewahrt bleibt, sich aber dennoch die gewünschten statistischen Daten für die Stellenleitung ergaben; allerdings war die Zeit für eine vernünftige Einigung wohl bereits vorbei.

Eigentlich schade, auch im Interesse der Mitarbeiterinnen und Mitar-

beiter. Nur: Solche elementaren Fehler, wie sie sich die Stellenleitung hier geleistet hat, darf man sich heutzutage nicht mehr erlauben.

### 3.12 Pflegedienstplanung auf Privat-PC

Angaben zu gesundheitlichen Verhältnissen gehören zu den besonderen Arten personenbezogener Daten nach § 2 Abs. 11 DSGVO.

Das Erstellen einer Pflegeplanung im Privatbereich oder auf privaten PCs wäre allenfalls im Rahmen einer Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag nach § 11 DSGVO denkbar. Danach ist beauftragte Stelle oder Person unter besonderer Berücksichtigung der Eignung der von ihr getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Bei der Tätigkeit bei einer Diakonie-/Sozialstation muss die besondere Schutzwürdigkeit von Angaben zu gesundheitlichen Verhältnissen beachtet werden.

Obwohl das persönliche Engagement, das in der Bereitschaft, den eigenen PC für dienstliche Zwecke zur Verfügung zu stellen, zum Ausdruck kommt, durchaus zu begrüßen ist, wurde die betreffende Anfrage abschlägig beschieden. Zwar ließen sich die Pflegedaten durch eine Verschlüsselung recht gut vor einer unbefugten Einblicknahme schützen und es wäre wohl auch möglich gewesen, dass die verschlüsselten Daten auf einem separaten Datenträger gehalten werden, allerdings stellen diese Maßnahmen noch nicht hinreichend sicher, dass es während der Arbeit mit solchen Daten nicht doch zu ungewollten und unbemerkten Datenspuren auf dem PC kommt, etwa dadurch, dass die verwendeten Programme in bestimmten Zeitabständen temporäre Zwischenabspeicherungen vornehmen. Entsprechende EDV-Kompetenz vorausgesetzt, ließe sich auch dies abschalten, aber bei Daten, die letztlich der Schweigepflicht nach § 203 Strafgesetzbuch unterliegen, können solche Ungewissheiten nicht akzeptiert werden. Hier bedarf es schon eines dienstlichen PC in dienstlichen Räumen oder eines dienstlichen Notebooks mit kompletter Festplattenverschlüsselung. Niederschwelligere Lösungen können nicht akzeptiert werden.

### 3.13 Unzulässige Erhebung von Listen kirchlicher Mitarbeiter durch Kommunen

Eine Pfarrerin einer Kirchengemeinde wurde von der Kommune aufgefordert, dieser eine Adressliste der jugendlichen Mitarbeiter zum Zwecke der Rechnungsprüfung als Vorbedingung der Gewährung von Zuschüssen zu übermitteln.

Da eine Kommune beteiligt war, wurde der Landesdatenschutzbeauftragte um Stellungnahme gebeten. Diese ergab, was zu erwarten war: Danach wäre eine solche Übermittlung nur dann erforderlich und damit daten-

schutzrechtlich zulässig, wenn konkrete Anhaltspunkte dafür vorliegen, dass hinsichtlich der Zahl der jugendlichen Mitglieder falsche Angaben gemacht werden. Dafür gab es seitens der Kirchengemeinde aber keinerlei Anhaltspunkte. Somit haben Kommunen im allgemeinen keine rechtliche Grundlage für die Anforderung von Adresslisten kirchlicher Mitarbeiter. Da die Kirchengemeinden das Persönlichkeitsrecht achten müssen, steht es auch nicht in deren belieben, „freiwillig“ dennoch zu übermitteln, vielmehr müssen sie entsprechende Anforderungen von Kommunen unter Hinweis auf die Datenschutzbestimmungen ablehnen. Beim mir kann eine Kopie der Stellungnahme des Landesdatenschutzbeauftragten angefordert werden, falls es Nachfragen geben sollte.

### **3.14 Datenschutzbeschwerde wegen einer Werbeaktion für das Evangelische Gemeindeblatt**

Solche Beschwerden gibt es immer wieder. Dabei ist die Rechtslage hier eindeutig: Die Kirchengemeinden sind Herr der Daten und können im Rahmen ihres kirchlichen Auftrags auch eine Werbemaßnahme für das Evangelische Gemeindeblatt machen. In der Praxis zeigt der Vertriebsbereich des Gemeindeblattes Interesse an einer Werbeaktion und bitte die Kirchengemeinde um Zustimmung.

Was dann aber immer wieder unterlassen wird ist, die Gemeindeglieder kurz über die beabsichtigte Werbeaktion zu unterrichten, etwa im Gemeindebrief und im Schaukasten, und ihnen dabei eine Möglichkeit anzubieten, einer Übermittlung ihrer Adressdaten zu diesem Zweck zu widersprechen, etwa durch Angabe einer Telefonnummer des Pfarramtes. Der damit verbundene Aufwand dürfte wesentlich geringer sein, als der, der entsteht, wenn sich verärgerte Gemeindeglieder an mich wenden und ich eine Stellungnahme einfordere.

Die Werbemaßnahme beschränkt sich nicht nur auf die Zustellung eines Werbeexemplars, sondern im nach hinein wird auch ein Werber oder eine Werberin nach Ankündigung persönlich vorgestellt, was nicht unwesentlich zum Erfolg der Sache beiträgt. Gerade wegen dieser mit der Aktion verbundenen Nachdrücklichkeit muss aber Gemeindegliedern, denen das Zuviel des Guten wird, die Möglichkeit eröffnet werden, einer Verwendung ihrer Daten zu diesem Zweck zu widersprechen.

### **3.15 Datenschutz und Wählerlisten**

Um künftigen Anfragen rechtzeitig vorzubeugen, sei hier auch die Frage aufgeworfen, wie denn das öffentliche Auslegen der Wählerliste mit dem Datenschutz zu vereinbaren sei. Nun ist dafür in § 10 Wahlordnung eine vorrangige Rechtsgrundlage gegeben, aber dies ist keine überzeugende Antwort.

Hinter der Auslegung stehen offensichtlich folgende Überlegungen: a) Jemand, der sich nicht eingetragen vorfindet, kann Einspruch erheben, also Gewährleistung der Vollständigkeit. Zwingend ist diese Begründung aber nicht, denn da jedem Eingetragenen auch die Wahlunterlagen zugestellt werden, wäre dies von der betroffenen Person daran erkennbar, dass sie nichts erhält. Macht man also rechtzeitig, etwa im Gemeindebrief, darauf aufmerksam, dass nun die Zustellung der Wahlunterlagen erfolgt und eröffnet parallel die Möglichkeit, dass jemand, der aufgrund irgendwelcher Umstände Zweifel hat, ob er eingetragen ist, beim Pfarramt rückfragen kann, ist dies eigentlich kein Grund für eine öffentliche Auslegung. b) Jemand könnte bezweifeln, dass eine andere Person korrekt eingetragen ist, etwa weil ihm Umstände bekannt sind, die der die Wählerliste erstellenden kirchlichen Stelle nicht bekannt sind. Also eine gegenseitige Kontrolle der Wahlberechtigung über das Medium Wählerliste. Da dürfte der eigentliche Knackpunkt mit dem Datenschutz liegen: Muss der Betroffene diesen Kontrollmechanismus als Vorrangig gegenüber seinem Persönlichkeitsrecht hinnehmen, also akzeptieren, dass sich seine Daten in einer öffentlich ausgelegten Liste vorfinden. Und da sagt eben die Landeskirche durch die vorrangige Rechtsvorschrift in der Wahlordnung, dass er dies hinnehmen muss.

Hier habe ich vorgeschlagen, dass die Kirchenleitung diese Bestimmung überdenken soll, zumal sich das Interesse an einer Einblicknahme in diese Listen wohl in engen Grenzen hält. Es ist tatsächlich nicht leicht, die Auslegung der Wählerliste und Datenschutz überzeugend zur Deckung zu bringen, umso mehr ist der anstehende Gesetzentwurf des Oberkirchenrats zur Änderung der Wahlordnung zu begrüßen, der einen Schritt in die richtige Richtung darstellt.

### **3.16 Verwendung von Stellenplänen bei Bezirkssynode und Bezirksausschuss?**

In einem Kirchenbezirk wurde in Frage gestellt, ob die Bezirkssynode und der Bezirksausschuss Einblick in die Stellenpläne des Bezirks nehmen darf bzw. ob diese Stellenpläne zur Verfügung gestellt werden müssen.

Zur Beurteilung dieser Anfrage wurden § 7 und § 17 des „Kirchlichen Gesetzes über die evangelischen Kirchenbezirke“ (Kirchenbezirksordnung - KBO) zu Rate gezogen.

Keine der dort genannten Aufgaben lies die Erfordernis erkennen, dass Bezirkssynode und Bezirksausschuss regelmäßig und pauschal eine Übersicht darüber erhalten müssen, mit welcher Person welche Stelle des Kirchenbezirks besetzt ist. Dies gilt auch hinsichtlich der Feststellung des Haushaltsplans. Dieser kann in bestimmten Verwendungszusammenhängen sehr wohl die einzelnen Stellen des Kirchenbezirks und deren Besetzung aufführen, allerdings war eine Erfordernis, eine solche Übersicht immer auch an die Be-

zirkssynode oder den Bezirksausschuss zu übermitteln, unter Umständen sogar mit Geburtsdatum, nicht erkennbar.

In diesem Sinne wurde Stellung genommen.

Für den Fall, dass es in bestimmten begründeten Einzelfällen dennoch zur Übermittlung der Stellenplandaten an die Bezirkssynode kommt, wäre zu beachten, dass nach § 15 a DSG-EKD die betroffenen Personen über regelmäßige Übermittlungen von Daten sowie die Empfänger zu unterrichten sind, soweit sie nicht mit solchen Übermittlungen rechnen müssen. Dies wäre etwa bei der Übermittlung von Haushaltsplänen mit personenbezogenen Stellenplänen von Kirchengemeinden an den Bezirksausschuss oder die Bezirkssynode zu beachten, da nicht davon ausgegangen werden kann, dass alle Mitarbeiterinnen und Mitarbeiter darüber im Bilde sind.

### 3.17 Veröffentlichung von Jubiläen

Immer wieder beschwerten sich bei mir Personen dahingehend, dass sie gegen ihren Willen in ihren Gemeindebriefen mit runden hohen Geburtstagen oder anderen Jubiläen veröffentlicht wurden. Meist hat das seine durchaus nachvollziehbaren Gründe, etwa weil durch die Veröffentlichung ausgelöste Besuche als Belastung empfunden werden oder ähnliches.

Die Kirchenregisterverordnung führt in § 35 Absatz 3 dazu aus: *Die Kirchengemeinden dürfen Alters- und Ehejubiläen von Gemeindegliedern in Gemeindebriefen und anderen örtlichen kirchlichen Publikationsorganen mit Namen, Anschrift sowie Tag und Ort des Ereignisses veröffentlichen. Die Betroffenen können verlangen, dass die Veröffentlichung unterbleibt. Auf dieses Recht sind die Betroffenen rechtzeitig vor Veröffentlichung hinzuweisen. Bei regelmäßigen Veröffentlichungen ist auf das Recht jährlich hinzuweisen. Die Bekanntmachung an derselben Stelle wie die Veröffentlichung genügt, wenn angenommen werden kann, dass sie den betroffenen Personenkreis erreicht.* Ich empfehle, am Jahresanfang und in der Jahresmitte darauf hinzuweisen, dass verlangt werden kann, dass die Veröffentlichung unterbleibt, und eine entsprechende Telefonnummer und Adresse anzugeben. Ähnlich verfahren auch die Kommunen in ihren Amtsblättern.

Teilweise wird von den sich beschwerenden Personen die Forderung erhoben, dass vor jeder Veröffentlichung das Einverständnis der Betroffenen eingeholt werden soll. Dies ist sicherlich zu weit gehend. Bei dem dadurch verursachten Aufwand müssten dann in vielen Fällen solche Veröffentlichungen ganz eingestellt werden. Dem steht aber entgegen, dass sich die allermeisten darüber durchaus freuen. Wird konsequent wie oben dargelegt verfahren, ist dem Datenschutz genüge getan.

### 3.18 Einhalten von Zusagen

Ein Gemeindeglied beschwerte sich bei mir darüber, dass es mit dem Pfarrer vereinbart hatte, für ein bestimmtes Projekt regelmäßig zu spenden, dabei aber die Zusage verlangt hatte, dass es nicht als Spender genannt werde. Dass es diesem Gemeindeglied durchaus ernst war, war auch daran erkennbar, dass es sich genau erkundigte, welche Rechtsmittel ihm denn offen stehen. Nachdem sich die ganze Sache dann für alle Beteiligten nicht ganz so erfreulich entwickelt hatte, wie wohl gehofft, teilte der Pfarrer dem Kirchengemeinderat dann doch mit, wer die spendende Person war. Dabei interpretierte er eine bestimmte Wendung in einer Mitteilung des Gemeindeglieds, in dem wohl einiger Unmut zutage trat, als Entbindung von seiner Zusage.

Die genaue datenschutzrechtliche Einschätzung, auch inwieweit hier das eventuell das Amtsgeheimnis tangiert war, war etwas schwieriger und soll hier nicht weiter erläutert werden.

Allerdings wäre es für alle Beteiligten wohl besser gewesen, der Pfarrer hätte nochmals konkret nachgefragt, ob das Gemeindeglied mit einer Bekanntgabe seines Namens im Kirchengemeinderat einverstanden sei oder nicht. Wenn nein, hätte man dies respektieren und nach anderen Handlungsalternativen suchen müssen. Jemand, der von einem Pfarrer eine Zusage erhalten hat, nicht genannt zu werden, sollte sich darauf verlassen können, auch in schwierigen Situationen. Bei der „Interpretation“ von schriftlichen, mündlichen oder elektronischen Dokumenten ist äußerste Zurückhaltung angesagt.

### 3.19 Fehlzeiten am schwarzen Brett

Transparenz ist eine gute Sache, scheint man sich in der Abteilung eines Krankenhauses gedacht zu haben. Insoweit fand man dann auch nichts dabei, in einer Jahresstatistik die Krankheitsausfälle der Mitarbeiterinnen und Mitarbeiter namentlich aufzuführen und in der Abteilung auszulegen.

Dies erschien der Mitarbeitervertretung dann doch suspekt, und sie hat Recht.

Zwar sind die Adressaten des Datenschutzgesetzes der Evangelischen Kirchen in Deutschland (DSG-EKD) die kirchlichen Stellen, doch hört der Schutz des Persönlichkeitsrechts nicht an der Pforte auf. Im Rahmen eines Beschäftigungsverhältnisses ist es nicht erforderlich, eine namentliche Übersicht der Krankheitsausfälle abteilungsweit auszulegen, damit ist auch keine Rechtsgrundlage dafür gegeben. Hinzu kommt, dass Angaben über die Gesundheit, dazu gehört auch, an welchen Tagen man krank war, zu den besonderen Arten personenbezogener Daten nach § 2 Abs. 11 DSG-EKD gehören, bei deren Verarbeitung sind besonders strenge Maßstäbe anzuwenden sind. Nun gelten die Datenschutzbestimmungen nicht nur beim Umgang

mit Patientendaten, sondern auch für die Daten von Mitarbeiterinnen und Mitarbeitern. Dies hätte man rechtzeitig bedenken sollen.

### 3.20 Veröffentlichung von Mitarbeiterdaten auf der Homepage

Die Präsentation kirchlicher Stellen, Werke und Einrichtungen im Internet wird zunehmend für erforderlich gehalten. Dabei stellt sich regelmäßig die Frage, inwieweit es dabei auch zu einer Veröffentlichung von Angaben bestimmter Beschäftigter kommen darf.

Die Veröffentlichung des eigenen Namens im Internet kann eine Belästigung durch so genannte Spam auch im privaten Bereich oder, durch Abgleich mit anderen Verzeichnissen, eine Erzeugung eines wahrscheinlichsbeiziferten Persönlichkeitsprofils zur Folge haben. Ein solches Persönlichkeitsprofil birgt immer die Gefahr, dass es verdeckt in den unterschiedlichsten Zusammenhängen mit zur Entscheidungsfindung herangezogen wird.

Bei Internet-Präsentationen wird meist ein einheitliches Erscheinungsbild angestrebt, d.h. es genügt nicht, dass auf einer Webseite bei einigen Funktionsbereichen auch der Name steht, bei anderen nicht. Damit ist in der Regel ein Druck auf die davon betroffenen Beschäftigten gegeben, da auch geschlossen mitzumachen.

Damit stellt sich die Frage, inwieweit Mitarbeiterdaten ohne Einwilligung auf einer Internetseite veröffentlicht werden dürfen bzw. inwieweit der Arbeitsvertrag dafür eine Erlaubnisnorm darstellt. Der Stand der Literatur, der Rechtssprechung und der Meinungsbildung der Datenschützer dazu ist mit großer Einigkeit etwa wie folgt:

Es muss zwischen Funktionsträgern und Nichtfunktionsträgern unterschieden werden. Funktionsträger in diesem Zusammenhang ist, wer Außenkontakt hat, ein gewisses Maß an Entscheidungsbefugnis besitzt und/oder eine Repräsentationsfunktion wahrnimmt. Angaben zu solchen Personen dürfen ohne vorherige Einwilligung veröffentlicht werden, die Daten von Nichtfunktionsträgern nur mit vorheriger Einwilligung. Was den Umfang der veröffentlichten Daten bei Funktionsträgern anbelangt, ist zwischen Basiskommunikationsdaten, funktionsrelevanten Zusatzdaten und Privatdaten zu unterscheiden. Basisdaten und funktionsrelevante Zusatzdaten dürfen ohne Einwilligung veröffentlicht werden. Zu den Basiskommunikationsdaten gehören der Name, die dienstliche postalische Anschrift, Telefon- und Telefaxnummer und die eMail-Adresse. Funktionsrelevante Zusatzdaten sind Angaben, die in engem Zusammenhang zur konkreten Funktion und zum tatsächlichen Aufgabengebiet eines Mitarbeiters stehen, etwa berufliche Qualifikationen. Beispielsweise kann eine Anwaltskanzlei Fortbildungen und Spezialisierungen von angestellten Anwälten auf der Homepage veröffentlichen.

Einigkeit sowohl in der Literatur als auch bei den Landesdatenschutzbe-

auftragten besteht weiterhin darüber, dass Fotos von Mitarbeiterinnen und Mitarbeitern sowohl bei Funktionsträgern als auch bei Nichtfunktionsträgern nur mit deren vorherigen Einwilligung auf einer Homepage veröffentlicht werden dürfen. Maßgebend dafür ist allerdings nicht das Datenschutzrecht, sondern das Recht am eigenen Bild gemäß § 22 Satz 1 KUG, wonach Bildnisse grundsätzlich nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden dürfen.

Eine andere Frage ist, inwieweit Daten von Mitarbeiterinnen und Mitarbeitern in kennwortgeschützten Webseiten veröffentlicht werden dürfen. Seitens der Stellenleitungen gibt es da teilweise zu weitgehende Vorstellungen von der Darlegung der Ausbildung bis zur Auflistung der Nebentätigkeiten. Datenschutzrechtlich handelt es sich bei einem kennwortgeschützten Webzugang um eine Übermittlung (in der Form eines Bereithaltens zum Abruf). Die gelegentlich anzutreffende Meinung, dass mit der Einwilligung der Betroffenen alles zulässig sei, ist falsch. Vielmehr muss auch dann die Übermittlung für die Aufgabenerfüllung der übermittelnden oder empfangenden kirchlichen Stelle erforderlich sein.

### **3.21 Verweigerung von Auskünften**

Eine Person beschwerte sich dahingehend, dass sich eine größere kirchliche Einrichtung weigerte, Auskunft darüber zu geben, welche Daten sie von ihr gespeichert hat. Besonders irritierend war dabei, dass diese Verweigerung der Auskunft mit dem Datenschutz begründet wurde.

Ganz so einfach kann es sich eine kirchliche Stelle jedoch nicht machen. Nach § 15 DSGVO besteht ein grundsätzlicher Rechtsanspruch eines Betroffenen auf Auskunftserteilung zu den zu seiner Person gespeicherten Daten, auch was die Herkunft oder die empfangenden Stellen dieser Daten anbelangt. Von dieser Auskunft sind auch die Empfänger sowie ggf. die Kategorien von Empfängern umfasst, ferner muss der Zweck der Speicherung benannt werden.

Eine Auskunftserteilung kann allenfalls dann verweigert werden, wenn die Daten oder die Tatsache ihrer Speicherung aufgrund einer speziellen Rechtsvorschrift oder wegen überwiegender berechtigter Interessen Dritter geheim gehalten werden müssen und das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss oder wenn durch die Auskunft die Wahrnehmung des Auftrags der Kirche gefährdet wird.

Eine Gefährdung der Wahrnehmung des Auftrags der Kirche wird man selten antreffen, und Geheimhaltungsvorschriften waren hier nicht tangiert. Relevant waren aber die berechtigten (Datenschutz-)Interessen Dritter. Allerdings darf dies nicht zum Anlass genommen werden, keine Auskunft zu erteilen, sondern diese muss dann eben so gegeben werden, dass deren Belange gewahrt werden. Das kann dann manchmal durchaus Umstände ver-

ursachen, die aber hinzunehmen sind. Dies ist ein Grund mehr, sparsam mit Daten umzugehen.

### 3.22 Krankenhausseelsorge

Dazu fand sich im aktuellen Tätigkeitsbericht des Landesdatenschutzbeauftragten eine Anmerkung, die von den Krankenhäusern im kirchlichen Bereich und von den Krankenhausseelsorgern zur Kenntnis genommen werden sollte (Ziffer 3.1.3 TB 2004). Moniert wurde zum einen, dass bei der Aufnahme auch Religionszugehörigkeiten erfasst werden, für die keine Krankenhausseelsorger ausgewiesen waren. Hier ist allerdings anzumerken, dass bei evangelischen Gemeindegliedern in solchen Fällen der Gemeindepfarrer zuständig ist und es möglich sein muss, dass im Bedarfsfall dessen Unterrichtung ermöglicht wird. Moniert wurde zum zweiten, dass den Krankenhausseelsorgern und -seelsorgerinnen die kompletten Wohnadressen, das Geburtsdatum und das Geschlecht übermittelt wurden. Hier wäre sicherlich zu prüfen, ob diese Angaben nicht zu dem Zweck erforderlich sein könnten, um ggf. den jeweiligen Gemeindepfarrer informieren zu können. Zum dritten wurde festgestellt, dass solche Daten auch von Patienten angezeigt wurden, die längst entlassen waren. Diese Kritikpunkte sollten von den kirchlichen Krankenhäusern umgesetzt und von den dort ihren Dienst versiehenden Seelsorgern und Seelsorgerinnen akzeptiert werden. Im Datenschutzweb findet sich unter <http://okrweb.elk-wue.de/datenschutz/praxkran.htm> auch eine Seite zur Krankenhausseelsorge, dort werden auch Formulierungen vorgeschlagen, wie die Information des Heimatpfarrers gleich bei der Patientenaufnahme geregelt werden könnte. Gerade bei den immer kürzeren Verweildauern im Krankenhaus selbst, denen dann meist längere Genesungszeiten Zuhause folgen, könnte eine solche Information immer bedeutungsvoller werden.

### 3.23 Mut zur Pflicht

Im Rahmen einer kleineren Straftat wurde auch eine Scheckkarte verwendet. Bei einer kirchlichen Einrichtung, die schwierige Jugendliche betreut, erschien dann ein Kriminalbeamter und wollte die genaue Anschrift der auf der Scheckkarte mit Namen gespeicherten Person. Ein Mitarbeiter der Einrichtung wollte nicht einfach einer Person, die von sich behauptete, ein Kriminalbeamter zu sein, Auskunft erteilen und verlangte den Ausweis. Mehr als eine Dienstmarke vermochte diese Person jedoch nicht beizubringen, so dass der Mitarbeiter unter Hinweis, dass sich die Kriminalpolizei sicher auch bei der Meldebehörde erkundigen könne, die Auskunft ablehnte. Das Verhalten des Mitarbeiters war korrekt. Es ist im Gegenteil etwas arg verwunderlich, dass sich Mitarbeiter einer Behörde, die das Recht hat, die Identität anderer Bürger zu überprüfen, sich selbst nicht mit einem Personalausweis zu

identifizieren vermögen.

Im Ernstfall ist jedoch immer wieder eine Verunsicherung festzustellen, insofern sei darauf hingewiesen, dass Sozialarbeiterinnen und Sozialarbeiter im Zusammenhang mit Strafverfahren gegenüber Gericht und Staatsanwaltschaft (nicht Polizei!) kein Zeugnisverweigerungsrecht haben, sie müssen wahrheitsgemäße Angaben machen und dürfen nichts verschweigen (ausgenommen sind nur Sozialarbeitern/innen, die in anerkannten Beratungsstellen nach §3 des Gesetzes über Aufklärung, Verhütung, Familienplanung und -beratung und der Drogenberatung tätig sind; vgl. §53 Abs. 1, Ziff. 3a und 3b sowie §53 Abs. 1, Ziff. 3 in Verbindung mit §53a StPO).

Das Bundesverfassungsgericht hat 1972 in einer umstrittenen Entscheidung festgestellt, dass eine Gleichstellung mit den in §53 StPO genannten Berufsgruppen nicht geboten sei, weil für Sozialarbeiter/innen die Begründung höchst persönlicher Vertrauensverhältnisse nicht kennzeichnend sei. Der Klient/die Klientin, so meinte das Bundesverfassungsgericht damals, erwarte auch gar nicht, dass Sozialarbeiter/innen die offenbaren Tatsachen aus der Privatsphäre verschweigen.

Das mag man heute vielleicht anders sehen, aber zurzeit müssen Sozialarbeiterinnen und Sozialarbeiter, auch wenn sie es manchmal nicht wahrhaben wollen, damit zurechtkommen. Davon unbenommen ist, dass sie zu den schweigepflichtigen Personen nach § 203 Strafgesetzbuch gehören. Als Konsequenz daraus müssen, soweit die Verschwiegenheitspflicht nach § 203 Strafgesetzbuch reicht, im Bereich der Zivilgerichte, der Arbeitsgerichte, der Verwaltungs-, Finanz- und Sozialgerichte Geheimnisse der Klientel nicht offenbart werden.

### **3.24 Kassenprüfung bei Psychologischen Beratungsstellen**

In vielen Fällen kann Menschen geholfen werden, wenn sie Gelegenheit bekommen, ihre Anliegen mit erfahrenen und geschulten Personen zu besprechen. Dazu gibt es in vielen Kirchenbezirken Psychologische Beratungsstellen. Völlig umsonst ist eine solche Beratung freilich nicht, so werden Ratsuchende etwa aufgefordert, einen bestimmten kleinen Prozentsatz ihres Nettoeinkommens als Entgelt an die Beratungsstelle zu entrichten. Diese Beträge werden aufaddiert und an die Bezirkskasse weitergereicht, natürlich ohne die Klienten zu nennen, die diese Beträge bezahlt haben. Dies wäre denn auch strafbar, da die Psychologen wie etwa Ärzte und Sozialarbeiter der Schweigepflicht nach § 203 Strafgesetzbuch unterliegen. Diese Schweigepflicht umfasst bereits den Umstand, eine Beratungsstelle aufgesucht zu haben. Logisch korrekt fragt sich dann natürlich die Bezirkskasse, wie sie denn überprüfen solle, dass die ihr genannten Beträge richtig und vollständig sind; ob es denn nicht möglich sei, eine namentliche Liste der Klienten zu bekommen.

Wenn überhaupt, ginge das nur mit Einwilligung der Klienten, dabei ist „Einwilligung“ im datenschutzrechtlichen Sinne zu verstehen. So muss man nachfragenden Klienten auch offen legen können, welche Folgen es hat, wenn sie die Einwilligung nicht geben, und es muss ihnen konkret genannt werden, welche Daten an welche Stelle, hier die Bezirkskasse, gehen. Die betroffene Person kann dann selbst entscheiden, ob es ihr nichts ausmacht, wenn andere kirchliche Mitarbeiter ihre Inanspruchnahme einer psychologischen Beratungsstelle mitbekommen, oder eben doch. Zieht man in Betracht, dass sich Personen in aller Regel in der Hoffnung auf irgendeine Art von Hilfe an psychologische Beratungsstellen wenden, kann man erhebliche Zweifel an der „Freiwilligkeit“ einer solchen Einwilligung haben.

### 3.25 Auslagerung der Buchhaltung einer Diakonischen Bezirksstelle

In einem Kirchenbezirk wurde erwogen, die Buchhaltung der Diakonischen Bezirksstelle zur Kirchenpflege auszulagern. Solche Zentralisierungen unter betriebswirtschaftlichen Gesichtspunkten werden im Bereich der Landeskirche in den unterschiedlichsten Zusammenhängen noch öfters erwogen werden.

Gegen geltendes Recht sollte dabei aber nicht verstoßen werden. So sollte bedacht werden, dass auf der Diakonischen Bezirksstelle Sozialarbeiterinnen und -arbeiter tätig sind, die der Schweigepflicht nach § 203 Strafgesetzbuch unterliegen. Davon umfasst ist auch der Umstand, dass jemand eine Beratung in Anspruch genommen hat. Es dürfte auch schwer möglich sein, die Mitarbeiterinnen und Mitarbeiter der Kirchenpflege als Gehilfen der Sozialarbeiterinnen und Sozialarbeiter der Diakonischen Bezirksstelle zu betrachten.

Vielleicht sollte neben der rechtlichen Beurteilung auch die praktische Auswirkung in das Blickfeld genommen werden. Jemand, der in einer bestimmten Lebenssituation, sehr oft wohl krisenhaft, die Hilfe der Diakonischen Bezirksstelle in Anspruch nimmt, geht in aller Regel davon aus, dass dies dem Sozialarbeiter oder der Sozialarbeiterin, die sie dort antrifft, bekannt wird und darüber hinaus allenfalls noch einer weiteren Person dieser Stelle, die mit der Terminplanung und weiteren Verwaltungsaufgaben betraut ist. Alles Weitere wäre für eine Rat suchende Person überraschend. Diese müsste auf alle Fälle darauf aufmerksam gemacht werden, dass der Umstand, dass sie die Diakonische Bezirksstelle aufgesucht hat, immer auch der Kirchenpflege bekannt wird. Da dort dann Rechnungsunterlagen entstehen, müsste diese Person auch darauf hingewiesen werden, dass ihre Inanspruchnahme der Diakonischen Bezirksstelle auch dem Rechnungsprüfer bekannt wird, unter Umständen zieht die Sache noch weitere Kreise. Es mag sicher Personen geben, für die dies keine Rolle spielt, aber es wird andere

Personen geben, die damit nicht gerechnet haben und die dies auch nicht wollen. Insbesondere mit der Kirche verbundene Personen werden vielleicht nicht wollen, dass weitere kirchliche Stellen von ihrer Inanspruchnahme der Diakonischen Bezirksstelle erfahren.

Es wurde dann angeregt, zu prüfen, ob nicht wie folgt verfahren werden kann:

Die Diakonische Bezirksstelle bietet ihren Ratsuchenden eine Barzahlung an (mit Aushang der Sätze). Die eingehenden Zahlungen werden auf der Diakonischen Bezirksstelle nicht mit Namen, sondern mit Aktenzeichen vermerkt. Die einzelnen Berater melden die Zahl ihrer Beratungsfälle, so dass eine gewisse Kontrolle der Barzahlungen möglich ist. Sofern eine Ratsuchende Person statt der Barzahlung überweisen möchte, verweist man diese auf die Kirchenpflege; diese Person wäre dann über die Alternativen im Bilde und auch über den Umstand, dass bei einer Überweisung zwangsläufig weitere Personen Kenntnis von der Beratung erlangen. Im Falle eines Überweisungswunsches nennt die Beraterin oder der Berater das Aktenzeichen, das auf dem Überweisungsformular als Zweck eingetragen werden kann. Die Kirchenpflege verbucht dann den eingegangenen Betrag anhand dieses Aktenzeichens und nicht namentlich.

Bei einem solchen Verfahrensablauf wären den Bedenken hinsichtlich der Wahrung der Vertraulichkeit Rechnung getragen.

### **3.26 Datenschutz bei psychologischen Beratungsstellen**

Seitens der Landesstelle der psychologischen Beratungsstelle wurde ich um Stellungnahme hinsichtlich der Rechtmäßigkeit der sog. *Integrierten Berichterstattung im örtlichen Raum (IBÖ)* im Rahmen der Jugendhilfeplanung gebeten.

Dabei ging es um Bedenken gegen eine gemeindebezogene (bzw. stadtteilbezogene) Erhebung von Daten von Klienten. Es sollten von den Beratungsstellen für statistische Zwecke an die zuständige Stelle des Landes die Angaben Herkunftsort (also Gemeinde bzw. Stadtteil), Alter, Geschlecht und Deutsch/Nicht-Deutsch ihrer Klientinnen oder Klienten übermittelt werden, um dort nach verschiedenen Auswertungsperspektiven akkumuliert zu werden.

Bedenklich erschien dabei der Umstand, dass es dabei zu einer Identifizierung von Personen kommen könnte, die eine Beratung in Anspruch nehmen; dies wäre nicht mit der Schweigepflicht zu vereinbaren.

Diese Bedenken waren ernst zu nehmen. So veröffentlichen beispielsweise Gemeinden in Amtsblättern oder ähnlichen Medien geschlechtsspezifische Altersstatistiken, auch getrennt nach deutschen Staatsbürgern und ausländischen Bürgern. Dabei kann es leicht zur Identifikation einzelner kommen.

Sicherlich ist nicht zu erwarten, dass eine solche Konstellation häufig auftritt, aber Betroffene können bei dieser Sachlage verunsichert werden, ob nicht unter bestimmten Bedingungen ihre Identifizierung möglich sein könnte. Man wird hier bedenken müssen, dass das Aufsuchen einer psychologischen Beratungsstelle gerade bei ausländischen Jugendlichen ein Schritt sein kann, der eines besonderen Vertrauens in die Schweigepflicht und den Datenschutz bedarf.

In dieser Sache wurde dann Kontakt mit dem Landesdatenschutzbeauftragten aufgenommen und es konnte eine Lösung gefunden werden, bei der eine Identifizierung weitestgehend ausgeschlossen war.

### 3.27 Kindergärten erheben Bruttoeinkommen

Ein Kirchengemeinderat hatte für seinen Kindergarten beschlossen, nun auch schon 2-jährige aufzunehmen, allerdings nur in bestimmter Anzahl. Das war mit der den Abmangel übernehmenden Kommune auch schon abgesprochen. Diese hatte allerdings weitergedacht und sich überlegt, wie das denn sei, wenn sich mehr Interessenten melden als Plätze zur Verfügung stehen. Man beschloss dann, dies so zu handhaben, dass Eltern oder Alleinerziehende mit geringerem Einkommen Vorrang haben sollen, die Kirchengemeinde als Träger des Kindergartens wurde aufgefordert, dies so zu handhaben.

Dort erschien diese Regelung durchaus einleuchtend und man entwarf schon ein Formular, in dem neben den üblichen Daten auch das Bruttoeinkommen der Interessenten an einem dieser Kindergartenplätze für 2-jährige abgefragt wurde, denn dann, so überlegt man sehr logisch, könne man eine Rangliste der Einkommen erstellen und danach die Plätze vergeben.

Bei diesem Stand der Sache kamen dann allerdings einem Mitarbeiter/einer Mitarbeiterin dann doch Bedenken, ob dies mit dem Datenschutz zu vereinbaren sei und fragte bei mir nach. Eine Erörterung der Sachlage ergab dann zunächst einmal, dass es wohl eher so sei, dass es weniger Interessenten als Plätze geben würde. Dies angenommen, hätte man also völlig überflüssig von den Interessenten verlangt, ihr Einkommen offen zu legen. Eine Datenerhebung auf Vorrat, das heißt nur aufgrund einer Vermutung, man könnte diese einmal benötigen, stellt jedoch einen gravierenden Datenschutzverstoß dar.

Aber auch wenn die Situation eintritt, dass mehr Interessenten als Plätze da sind, besteht zunächst keine Erfordernis, die Bruttoeinkommen abzufragen. Hier wäre wohl zunächst zu prüfen, ob nicht durch Anwendung anderer Auswahlkriterien, die dem Kindergarten bereits bekannt sind, etwa ob bereits Geschwister im Kindergarten sind, ein Auswahl vorgenommen werden kann.

Erst für den Fall, dass auch dies nicht hinreichend ist, kann erwogen werden, wie bei den einkommensgestaffelten Kindergartenbeiträgen zu verfahren und von den Interessenten zu verlangen, eine Zuordnung zu einem von

vielleicht 5 Einkommensbereichen anzugeben. Allerdings wäre auch hier darauf zu achten, dass diese Angaben den Erzieherinnen nicht bekannt werden, also beispielsweise in der Kirchenpflege verbleiben, natürlich unter strikter Wahrung des Datenschutzes.

### 3.28 Arbeitszeitenerfassung bei Kindergärten

Arbeitszeiten, Öffnungszeiten, Urlaube, AZV-Tage, Jahresplanungen, wohl auch Krankheitszeiten oder sonstige Abwesenheitsgründe, all dies muss auch für die Mitarbeiterinnen in Kindergärten erfasst und verarbeitet werden. Dazu benutzt man zweckmäßigerweise Formulare. Damit nun nicht jeder Kindergarten das Rad noch einmal neu erfindet und seine eigenen Formulare entwickelt, werden diese zentral zur Verfügung gestellt, in Form von Excel-Tabellen.

Dagegen wäre dann nichts einzuwenden, wenn diese Formulare vor Ort ausgedruckt und in Papierform verwendet werden würden. Sollen hingegen solche Formulare an einem PC ausgefüllt und abgespeichert werden, hat dies unter Umständen zur Folge, dass jede Mitarbeiterin die Daten aller anderen einsehen kann, es sei denn, es werden entsprechende Schutzmaßnahmen getroffen. Solche Schutzmaßnahmen müssen aber auch greifen, wenn der PC beispielsweise gestohlen oder entsorgt wurde, ohne dass daran gedacht worden ist, die Festplatte effektiv zu löschen.

Es böte sich an, zu diesem Zweck mit einem so genannten Datensafe zu arbeiten. Das ist ein Programm in Verbindung mit einer oder mehreren Dateien mit der Eigenschaft, dass die Dateien verschlüsselt sind und erst nach einer Anmeldung an dem Programm in Gestalt eines simulierten Laufwerks zur Verfügung stehen. Ein solcher Datensafe ist damit eine einfach zu handhabende und preiswerte Möglichkeit, Daten verschlüsselt zu speichern.

Damit hätte man zwar der Anforderung einer verschlüsselten Speicherung von Daten gemäß der Verschlüsselungsverordnung genüge getan, aber wie lässt sich möglichst einfach erreichen, dass jede Mitarbeiterin nur ihre Daten einsehen kann und allenfalls die Stellenleitung sich einen Gesamtüberblick verschaffen kann? Hier böte sich ggf. die gute alte Diskette in der Form an, dass jede Mitarbeiterin die Excel-Tabelle mit ihren Angaben auf ihrer Diskette abspeichert und diese dann der Kindergartenleitung zum Kopieren in den Gesamtdatenbestand und weiteren Aufbewahrung übergibt.

Es wird deutlich, dass auch mit einfachen Mitteln und ohne großen Kostenaufwand und mit durchaus überschaubaren EDV-Kenntnissen dem Anliegen des Datenschutzes Genüge getan werden kann. Entscheidend ist, dass man überhaupt in entsprechende Überlegungen eintritt oder sich entsprechend beraten lässt. Unzulässig ist, solche Anforderungen einfach zu ignorieren; dann muss man so konsequent sein und ausschließlich die Papierform verwenden.

### 3.29 Herausgabe von Namen von Einschulungskindern

Ein Pfarrer fragte an, ob den von den Kindergärten die Namen der Kinder, die eingeschult werden, an ein an solchen Angaben interessiertes Kreditinstitut herausgegeben werden könnten. Dabei wies er darauf hin, dass eben dieses Kreditinstitut schon einiges für die Kindergärten getan hat, in Zeiten knapper Kassen sicherlich kein leichtgewichtiges Argument.

Die Rechtslage ist hier eindeutig, eine Rechtsgrundlage, die dies ermöglichen würde, gibt es nicht. Damit ist dies allenfalls mit Einwilligung der Eltern möglich. Nun ist diese Ablehnung wohl nicht ganz so schwerwiegend, wie man zunächst meinen möchte: Eltern die nicht einwilligen würden wohl auch nicht auf die mit der Adressenanfrage beabsichtigte Werbeaktion reagieren.

Das eigentliche Problem dürfte wohl eher darin liegen, wie denn der Kindergarten feststellen soll, welche Eltern mit einer Weitergabe ihrer Adressen einverstanden sind. Denkbar wäre vielleicht, dass die Kindergärten solche Stellen, von denen sie eine nennenswerte finanzielle oder materielle Förderung erfahren, dahingehend privilegieren, bei geeigneten Gelegenheiten, und solche wird es bei den Vorschulkindern sicherlich geben, die benötigten Einwilligungen unter der Elternschaft einzuholen. Eine andere Möglichkeit sehe ich nicht.

### 3.30 Beobachtungsbögen in Kindergärten

Sprachhilfe in Kindergärten ist sicherlich eine gute Sache, insbesondere für solche Kinder aus anderen Nationen. Es ist auch unmittelbar einsichtig, dass eine Sprachhelferin bei der Vielzahl der Kinder, die sie betreut, nicht zu jedem Kind dessen besondere Problematik und der erreichte Stand bei der Sprachhilfe im Gedächtnis bewahren kann.

Ob man dann allerdings umgehend zur Verwendung von Beobachtungsbögen greifen muss, erweckt dann doch einigen Zweifel, zumal in solchen Bögen dann nicht nur die vorhandenen oder nicht vorhandenen sprachlichen Fähigkeiten notiert werden sollten, sondern auch Verhaltensmerkmale wie „Störverhalten“, „Sucht Körperkontakt“ usw., und das Ganze dann auch noch in elektronisch gespeicherter Form.

Manchmal ist weniger mehr. Zunächst geht es doch einfach darum, der begrenzten menschlichen Merkfähigkeit durch Notizen auf die Sprünge zu verhelfen. Benutzt man dazu das Mittel der Pseudonymisierung, sieht die Sache schon wesentlich datenschutzfreundlicher aus. Konkret hieße das, dass die Sprachhelferinnen auf den Bögen nur die Angaben macht, die sie für ihre Aufgabe wirklich benötigt und statt Name, Geburtstag usw. lediglich eine fortlaufende Nummer notiert. Die zu dieser Nummer gehörenden per-

sonenidentifizierenden Daten vermerkt sie in ihrem persönlichen Notizbuch. Werden schließlich die Bögen nur solange aufbewahrt, wie die Sprachförderung stattfindet, gibt es seitens des Datenschutzes nichts mehr dagegen einzuwenden und vermeidet eine ganze Reihe sich sonst ergebender Datenschutzanforderungen wie etwa die nach einer Datenverschlüsselung. Ein weiteres Beispiel dafür, wie sinnvoll es unter Datenschutzgesichtspunkten ist, sich schlicht auf das zu beschränken, was man wirklich braucht.

### 3.31 Zeiterfassungssysteme

Wann Mitarbeiterinnen und Mitarbeiter ihren Dienst antreten und beenden, wird immer mehr elektronisch erfasst, auch bei kirchlichen Stellen. Es liegt auch völlig im Ermessen einer Stellenleitung, die Arbeitszeiten der Mitarbeiterschaft mittels Zeiterfassungssysteme zu überwachen. Man kann solche Systeme allerdings in einer datenschutzfreundlichen (und damit auch mitarbeiterfreundlichen) oder datenschutzunfreundlichen Art und Weise verwenden. Datenschutzunfreundlich ist es, wenn jeder Vorgesetzte Zugriff auf den Zeiterfassungsrechner bekommen und jederzeit Einblick nehmen kann, an welchem Tag welcher seiner Untergebenen von wann bis wann gearbeitet hat. Datenschutzfreundlich wäre es, wenn man den Umstand, dass die Zeitdaten in elektronischer Form vorliegen dahingehend nutzt, dass man auch die Arbeitszeitregelungen elektronisch hinterlegt und das System nur dann „Alarm“ schlagen lässt, wenn eine Mitarbeiterin oder ein Mitarbeiter gegen die Regelungen verstößt. So könnte das Zeiterfassungssystem prüfen, ob die Summe der Arbeitszeiten einer bestimmten Person im Lot ist, die Kernarbeitszeiten eingehalten wurden, nicht mehr als zulässig Überstunden auf den nächsten Monat übertragen wurden oder das Gesamtdefizit eine bestimmte Grenze nicht überschreitet. Nur wenn das Zeiterfassungssystem eine Regelverletzung feststellt, erhält der oder die zuständige Vorgesetzte eine Benachrichtigung, und kann die gespeicherten Daten genauer durchgehen. Da auch hinter Zeiterfassungssysteme letztlich einfach Computer stehen, sieht man einmal von der Elektronik zur Erfassung der Zeitdaten ab, und die Zeitdaten in ganz normalen Datenbanken abgespeichert werden, wäre dies technisch überhaupt kein Problem, und es wäre zudem mitarbeiterfreundlich.

Normalerweise wird EDV-Technik dazu eingesetzt, Personen von Tätigkeiten zu entlasten. Insbesondere gehören Vorgesetzte zu den besser bezahlten Leuten und es ist eigentlich nicht sehr effizient, wenn diese ihre Zeit damit verbringen, die Einhaltung von Arbeitszeitregelungen zu kontrollieren, wenn dies auch vom Zeiterfassungscomputer mit erledigt werden kann. Unter diesen Voraussetzungen könnten Zeiterfassungssysteme unter Datenschutzgesichtspunkten sogar ein Fortschritt darstellen, etwa gegenüber einer Erfassung auf papiernen Arbeitszeitlisten.

### 3.32 Elektronisches Banking

Dass es eine Vereinfachung für kirchliche Verwaltungsstellen und sonstige kirchlichen Stellen darstellen kann, wenn diese Geldüberweisungen mittels elektronischem Banking durchführen, ist unstrittig. Allerdings wurde vom mir gefordert, dass dafür Chipkarten und Chipkartenleser mindestens der Klasse 2 eingesetzt werden.

Dabei geht es primär nicht um die technische Sicherheit des zugrunde liegenden Verfahrens, sondern um den Schutz der betreffenden Mitarbeiter- und Mitarbeiterinnen. Eben weil das Verfahren einen hohen Sicherheitsstandard hat, gerät der Mitarbeiter oder die Mitarbeiterin in den Fällen, wo dann doch etwas Unregelmäßiges geschieht, in eine erhebliche Beweisnot, der oder die „Schuldige“ gewesen zu sein. Es ist sehr verführerisch, zu argumentieren, dass aufgrund der zugrunde liegenden Sicherheitstechnik nur die Inhaberin oder der Inhaber des von den beteiligten Rechnern registrierten privaten Schlüssels in der Lage hat sein können, die strittige Transaktion zu veranlassen, er es also auch gewesen sein muss. Dass dieser Schluss fragwürdig ist, wird auf der oben genannten Webseite anhand eines Szenarios, das die Schwachstelle „edv-unkundiger Mensch“ ausnutzt, nachgewiesen; man kann nur hoffen, dass im „Ernstfall“ alle Beteiligten das dort Gesagte zur Kenntnis nehmen und danach handeln. Es dürfte ein Fall reichen, wo weder Schuld noch Unschuld einer bestimmten Person festgestellt werden können, diese aber den aufgekommenen Verdacht ein Leben lang nicht mehr los wird, um eine Weigerung bei vielen hervorzurufen, sich auf dieses Verfahren einzulassen. Dann doch lieber die eigenhändige Unterschrift, diese hat man unter seiner vollen Kontrolle, zumindest wenn man will.

Auch die Forderung nach dem Einsatz einer Chipkarte und einem Leser der Klasse 2 bleibt ambivalent. Die klassische Trennung von Anordnung und Vollzug oder ein gleichwertiger organisatorischer Ersatz erübrigt sich beim elektronischen Banking nicht etwa, sondern ist noch notwendiger.

### 3.33 Pishing-Mails

Pishing-Mails sind eMails mit zwei Bestandteilen:

1. Es werden den Empfängern seriöse Absender, die im allgemeinen Bewusstsein als vertrauenswürdig gelten, vorgegaukelt und
2. es wird im Textteil der eMail versucht, die Empfänger auf eine Webseite zu locken, wo versucht wird, sie zur Eingabe vertraulicher Daten oder zum Download von ausführbaren Dateien zu verleiten.

Das so etwas kommen würde, war zu erwarten. In dem Maße, in dem zunehmend wirksame technische Schutzmaßnahmen ergriffen werden, wird als

Schwachstelle der edv-technisch unerfahrene Mensch zur Zielscheibe. Diese werden in die Situation gebracht, gerade dann, wenn sie spontan Vertrauen entgegenbringen, eigentlich besonders misstrauisch sein zu müssen. Erfahrungsgemäß wird die Echtheit von Systemmeldungen, Warnungen, amtliche Mitteilungen von Banken oder Behörden, Rechtsanwälten o.ä. nicht angezweifelt. Aber auch Überrumpelung durch Erschrecken ist ein bekanntes Mittel, etwa vorgeblich unbezahlte Rechnungen oder Schufa-Mitteilungen. Jedes Lehrbuch der Psychologie kann als „Kochbuch“ dafür missbraucht werden, hier auf weitere Ideen zu kommen.

Stark im kommen sind beispielsweise E-Mails, die von der Aufmachung aussehen wie solche seriöser Kredit-Institute und wo der Empfänger „aus Sicherheitsgründen“ aufgefordert wird, persönliche Daten, Pin-Nummer und Passwort zu aktualisieren. Natürlich muss man in den entsprechenden Eingabefeldern „als Legitimation“ zuerst die bestehenden Daten eingeben. Oder die E-Mail enthält einen Link auf eine gefälschte Webseite eines Online-Anbieters, auf der dann die Daten angegeben werden sollen. Anscheinend sind die Kreise, die solche Angriffe initiieren, gut organisiert, es wurden Pishing-Archive mit gefälschten Webseiten vieler großer Online-Anbieter entdeckt. Es ist mittlerweile erschreckend, wie häufig den Pishern auf den Leim gegangen wird. Es geht aber nicht nur ums Geldkonto, wesentlich kritischer kann es für eine datenverarbeitende Stelle sein, wenn es den Angreifern gelingt, auf dem Rechner ein „Hintertürchen“ einrichten, um jederzeit unbemerkt darauf zugreifen zu können.

Was kann man tun? Der ganze Missbrauch ist nur deshalb möglich, weil der Empfänger einer E-Mail keine einfache Möglichkeit hat, die Seriosität des Absenders zu prüfen. Dies ist ein weiterer Grund, wieso im Bereich der Landeskirche demnächst elektronische Ausweise, sog. „Zertifikate“, verteilt werden. Damit ist es nicht nur möglich, E-Mails verschlüsselt zu übertragen, sondern sie lassen sich auch digital unterschreiben, d.h. der Empfänger kann sich einigermaßen sicher sein, dass die E-Mail tatsächlich von der Stelle oder der Person stammt, die angegeben ist. Ein wirksamer Schutz gegen unseriöse E-Mails ergibt sich auf diese Weise zwar erst, wenn solche elektronischen Ausweise gesellschaftsweit eingesetzt werden<sup>1</sup>, aber es ist auch im kirchlichen Bereich ein Anfang gemacht. Eine aktuell wirksame Schutzmaßnahme ist die Beantragung einer elk-wue-Adresse. Bei der Umleitung der E-Mail über die Rechner des Oberkirchenrats werden diese automatisiert geprüft und der Betreff mit einer Warnung und einem Score-Wert ergänzt, wenn es Hinweise darauf gibt, dass es sich um Spam handelt.

---

<sup>1</sup>Der eigentliche Zweck ist zunächst, eine verschlüsselte und damit sichere Übertragung von E-Mails zu ermöglichen.

### 3.34 Zentralrechnergestütztes Meldewesen

Die Versorgung der Kirchengemeinden mit den Meldedaten ihrer Gemeindeglieder war bislang dezentral organisiert. Die Daten gingen vom Rechenzentrum zum Oberkirchenrat und wurden von dort an die einzelnen Kirchengemeinden auf der Basis des Programms „Datenverarbeitung im Pfarramt (Davip)“ verschlüsselt weiterverteilt.

Mittlerweile wurden auch zentralrechnergestützte Lösungen entwickelt und stehen vor dem Einsatz in den Landeskirchen. Danach sollen z.B. Pfarrämter sich über das Internet bei dem Zentralrechner anmelden können und bekommen dann Zugriff auf „ihre“ Gemeindegliederdaten und können diese unter verschiedenen Gesichtspunkten nutzen, etwa nach bestimmten Kriterien eine Liste von Gemeindegliedern zusammenstellen. Eine Verteilung dieser Daten auf die PC vor Ort findet dann, abgesehen von Ausdrucken und Bildschirmdarstellungen nicht mehr statt.

Diese Verfahren wurden von der vormaligen Datenschutzgruppe der Kigst GmbH überprüft und freigegeben bzw. stehen beim nachfolgenden Gutachterausschuss zur Freigabe an.

Dass ein zentrales Verfahren seine Vorteile hat, ist unstrittig. Es kann wohl auch davon ausgegangen werden, dass die Datensicherheit auf dem jeweiligen Zentralrechner und auch auf dem Übertragungsweg bis zum Pfarramt (oder der Stelle, die Zugriff auf die Daten haben soll) gewährleistet werden kann, wenngleich der letztere Punkt noch genauer zu spezifizieren wäre. Kritisch sind jedoch die jeweiligen kirchlichen Stellen, die Zugriff auf den Zentralrechner bekommen sollen:

1) Im Hinblick auf das mangelhafte Bewusstsein, was einen sorgsamsten Umgang mit Passwörtern angeht, wäre es bedenklich, wenn alleinig die Kenntnis eines Benutzernamens und eines Kennworts schon Tür und Tor zu den Daten auf dem Zentralrechner öffnen würden. Hier muss, etwa wie bei der Euro-Scheckkarte, das Prinzip *Wissen und Besitz* gelten, um einigermaßen sicher zu gewährleisten, dass nur befugte Personen auf diese Daten zugreifen. Bei den jeweiligen kirchlichen Stellen liefe dies auf den Einsatz eines Chipkartenlesers hinaus, ferner auf die Organisation der Erstellung und Verteilung dieser Karten an die befugten Personen.

2) Es gab Pfarrämter, auf deren PC neben Hintertürchen und sonstiger Schadenssoftware gleich vier Programme installiert waren, die teure Internetverbindungen hätten aufbauen können. Auf anderen waren Virenschutzprogramme zwar vorhanden, aber deaktiviert oder mit völlig veralteten Virenmustern versehen. Es kann nicht sein, dass von solchen PC aus auf einen Zentralrechner zugegriffen wird, auf dem die Meldedaten der Gemeindeglieder gespeichert sind. Sicherlich muss dieser Zentralrechner ein hohes Sicherheitsniveau aufweisen, aber kein noch so hoher Sicherheitsstandard kann alle Sicherheitsmängel bei den zugreifenden PC ausbügeln. Es muss gewährleistet sein, dass ein PC, von dem aus auf den Zentralrechner zugegriffen

wird, in Sachen Datensicherheit auf dem erforderlichen Stand ist. Um ein Mindestmaß an Sicherheit herzustellen, dass dem tatsächlich so ist, könnte beispielsweise so verfahren werden, dass die Zuständigen für diese PC einmal jährlich anhand einer Checkliste eine Selbsterklärung gegenüber den kirchenbezirklichen Datenschutzbeauftragten abgeben, dass die dort aufgeführten Maßnahmen umgesetzt werden (also etwa ein Virenschutzprogramm automatisch oder zumindest wöchentlich auf den aktuellen Stand gebracht wird). Diese Selbsterklärungen werden dann stichprobenartig überprüft, um die Funktionsfähigkeit dieses Verfahrens zu prüfen und zu dokumentieren.

3) Sofern auch bei diesem Verfahren Meldedaten auf den PC vor Ort gelangen, muss gewährleistet sein, dass sie automatisch in einem dafür angelegten verschlüsselten Bereich landen. Dies lässt sich heute mit vertretbarem Aufwand realisieren, etwa unter Nutzung sog. Datensafes.

4) Die Handhabung gesperrter Gemeindegliederdaten muss geklärt sein. Es ist technisch relativ einfach zu realisieren, dass solche Daten einfach nicht angezeigt werden. Man kann jedoch nicht ausschließen, dass gerade der Umstand, dass jemand nicht in einer Liste erscheint, obwohl er nach der Kenntnis weiterer Personen eigentlich erscheinen müsste, Aufmerksamkeiten weckt. Diese Punkt muss noch genauer geklärt werden.

5) Es muss geregelt sein, welche Stelle auch kirchengemeindenübergreifende Auswertungen machen kann. Es ist bei einer zentralen Datenhaltung nur der Umstand, ob in der Berechtigungsmaske an einer bestimmten Stelle ein Häkchen gesetzt ist oder nicht, der darüber entscheidet, ob jemand solche Auswertungen machen kann oder nicht. Hier muss die unter 2) aufgeführte Schutzmaßnahme, dass nur jemand zugreifen kann, der im Besitz einer Chipkarte ist und deren Kennwort weis, ergänzt werden um den Mechanismus, dass zentral protokolliert wird, wer welche Auswertungen vornimmt (zumindest wenn sie über den Kreis einer Kirchengemeinde hinausgeht) und dass in einem geeigneten organisatorischen Verfahren stichprobenartig das Protokoll in regelmäßigen Abständen eingesehen wird.

5) Der tatsächliche, praktische Einsatz vor Ort wird mit Sicherheit weitere Fragen aufwerfen, es muss geregelt werden, wie solche Erfahrungen Eingang in die Verbesserung der Datensicherheit finden. Denkbar wären etwa regelmäßige Besprechungen im Kreis der Datenschutzbeauftragten der Kirchenbezirke.

Unter den genannten Bedingungen wäre der Einsatz eines zentralen Verfahrens unter Datenschutzgesichtspunkten durchaus vertretbar.

### **3.35 EDV-Dienstvereinbarungen**

Immer wieder einmal werden mir insbesondere aus dem Bereich der Diakonie seitens der Mitarbeitervertretungen Dienstvereinbarungen mit der Bitte um Stellungnahme vorgelegt. Dabei geht es um Regelungen, mit denen

negative Auswirkungen neuer EDV-Verfahren auf die Mitarbeiterschaft verhindert werden sollen. Nun ist es nicht Aufgabe des landeskirchlichen Datenschutzbeauftragten, in das Verhältnis zwischen Stellenleitung und Mitarbeiterschaft einzugreifen. Theoretisch kann die Mitarbeiterschaft in entsprechenden Dienstvereinbarungen den Datenschutz sogar einschränken, weil diese Vorrang vor den Bestimmungen des Datenschutzgesetzes hat. Dies hat allerdings auch seine Grenzen, und es ist dann meine Aufgabe zu prüfen, ob diese gewahrt werden.

Dabei musste dann manches mal festgestellt werden, dass das halbe Bundesdatenschutzgesetz abgeschrieben oder aus dem Bereich der Wirtschaft im Internet gefundene Vereinbarungen mehr schlecht als recht angepasst wurden. Manches war sogar ausgesprochen kontraproduktiv, etwa wenn Begriffe verwendet wurden, die in den Datenschutzgesetzen überhaupt nicht vorkommen oder dort eine andere Bedeutung haben, als die Verfasser dieser Dienstvereinbarungen intendierten. Wer eine Dienstvereinbarung im EDV-Bereich verfasst sollte sich darüber im Klaren sein, dass die im Bundesdatenschutzgesetz verwendeten Begriffe ein aufeinander bezogenes Gefüge bilden, das durch Kommentierung und Rechtssprechung ein hohes Maß an Eindeutigkeit erreicht hat. Dieses Begriffsgefüge wurde auch in die kirchlichen Datenschutzbestimmungen übernommen. Auch Dienstvereinbarungen sollten nicht aus diesem Begriffssystem ausscheren. Auch macht es keinen Sinn, in Dienstvereinbarungen Dinge zu regeln, die bereits geregelt sind, etwa im Datenschutzgesetz. Im Datenschutzweb

<http://okrweb.elk-wue.de/datenschutz/>

wurden die wichtigsten Rechtsnormen zusammengestellt, damit man sich einen Überblick verschaffen kann, was bereits geregelt ist. In aller Regel kann es beim Einsatz neuer Software nur noch darum gehen, die breite Palette an Möglichkeiten und Funktionalitäten auf das vertretbare und sinnvolle zu begrenzen.

Zunehmend entstehen Zweifel darüber, ob es überhaupt noch angebracht ist, so zu verfahren, dass die Stellenleitung den Einsatz eines Verfahrens beschließt und die Mitarbeitervertretung dem dann zustimmt oder auch nicht. Das dafür erforderliche edv-Wissen ist bei der jeweiligen Mitarbeitervertretung oft nicht vorhanden und die Sachverhalte, die man wirklich regeln sollte, zeigen sich oft erst im praktischen Einsatz. Meiner Auffassung nach sollte, wenn irgend möglich, so vorgegangen werden, dass die Einführung einer Software als einen Vorgang betrachtet wird, der eine bestimmte Zeit dauert, und dass in dieser Zeit eine konstruktive Zusammenarbeit zwischen Stellenleitung und Mitarbeitervertretung etabliert wird, etwa in der Form regelmäßiger Treffen zum informellen Austausch zwischen Projektleitung und Mitarbeitervertretung. Dabei sollte der Mitarbeitervertretung das Recht zugestanden werden, dass ihr auf alle Fragen Auskunft gegeben wird. Auch strittige Einzelheiten werden dort geklärt und ausdiskutiert. Die endgültige Zustimmung der Mitarbeitervertretung erfolgt erst dann, wenn die

neue Software in den Produktivbetrieb geht. Das kann nur funktionieren, wenn ein entsprechendes Maß an gegenseitigem Vertrauen zwischen Stellenleitung und Mitarbeitervertretung vorhanden ist. Allerdings ist es doch wohl nur in seltenen Ausnahmen so, dass sich die Mitarbeiterschaft gegen neue Software sträubt; üblicherweise geht es um ausreichende Schulungen, Benutzerfreundlichkeit und die Begrenzung des jeder Software innewohnenden Überwachungspotentials. Hierüber sollte ein Einvernehmen herstellbar sein.

Ich war deshalb sehr froh, dass sich die Mitarbeitervertretung des Oberkirchenrats dazu entschloss, im Rahmen von POP (Prozessoptimierung im Pfarrdienst) der Dienststellenleitung die Einrichtung einer Begleitkommission vorzuschlagen und diese dem Verfahren zustimmte. Insbesondere die Einführung des Personalinformationssystems im Rahmen von POP wurde in dieser kleinen Gruppe Schritt für Schritt erläutert und durchgesprochen.

### 3.36 Unzulässige Speicherung von Personaldaten

Bei einer größeren kirchlichen Stelle im diakonischen Bereich kam es zu einer Umstrukturierung der EDV. Im Zusammenhang damit kam auch das Berechtigungs-system etwas durcheinander und Mitarbeitende hatten auf einmal Zugriff auf Bereiche, in denen frühere Vorgesetzte ihre Daten ablegten. Wie der Zufall so will, stießen Mitarbeiter auf einmal auf Worddokumente und andere Unterlagen zu ihrer Person, von deren Existenz sie bis dato überhaupt nichts wussten. Unangenehm für die Leitung der betreffenden Stelle war, dass einer dieser Mitarbeiter Mitglied der Mitarbeitervertretung war. Nicht ganz so erfreulich war auch, dass es sich unter anderem um Protokolle von Mitarbeitergesprächen handelte, die längst hätten gelöscht sein müssen.

Eine Überprüfung der ganzen Sache förderte eine ganze Reihe von Mängeln zu Tage. So gab es weder eine Übersicht über die eingesetzten Verfahren noch darüber, wo überall Daten und Dokumente zu Mitarbeitern abgelegt wurden. Es gab auch kein Konzept, wie mit den Dateien ausgeschiedener Mitarbeiter, auch Vorgesetzter, zu verfahren ist; eigentlich gab es überhaupt keine Regelungen hinsichtlich von Löschvorschriften. Unzulässig war auch, dass jeder EDV-Administrator einsehen konnte, welcher Vorgesetzte welche Word-Dokumente über bestimmte Mitarbeiter anlegte. Vor allem gilt aber der Grundsatz der Vollständigkeit der Personalakte: Eine Mitarbeiterin oder ein Mitarbeiter muss wissen können, wo was zu ihrer oder seiner Person gespeichert ist. Dies ist zunächst einmal die Personalakte. Diese kann von einem Personalinformationssystem als der elektronischen Variante ergänzt werden. Allerdings ist die Anlage irgendwelcher Verzeichnisse kein Personalinformationssystem, sondern hier muss es sich um eine Software handeln, die genau zu dem Zweck, Personaldaten zu speichern, entwickelt wurde. Nur von einer zu diesem Zweck entwickelten Software kann überhaupt angenommen werden, dass ein rechtmäßiges Speichern von Personaldaten möglich ist.

Bei der Einführung des Personalinformationssystems (POP) des Oberkirchenrats war ich von Anfang an begleitend dabei. Eine meiner Anforderungen war, dass *auf Knopfdruck* alle darin zu einer Person gespeicherten Daten zusammengestellt und, zusammen mit einer Erläuterung des Zwecks der jeweiligen Datenfelder, ausgedruckt oder als druckbare Datei bereit gestellt werden können. Jede Person, die es möchte, kann von ihrem Auskunftsrecht Gebrauch machen und umstandlos ihre Daten einsehen. Bereits dieses Wissen, dass man könnte, wenn man wollte, trägt dazu bei, dass diesem System das benötigte Vertrauen entgegengebracht wird. Mitarbeiterschulungen mit Echtdateien Bei einer größeren kirchlichen Stelle wurde eine Software entwickelt, die auch Personaldaten verarbeitete, und die zur Einführung anstand. Damit die Benutzer die Software auch anwenden können, wurden sie geschult. Nicht wenige waren erstaunt, als sie feststellten, dass sie es nicht mit Schulungsdaten zu tun hatten, sondern mit echten Daten ihrer Kolleginnen und Kollegen. Und da es bei den Schulungen noch keine ausdifferenzierten Benutzerberechtigungen gab, konnte, wer neugierig war, in persönliche und sachliche Verhältnisse von Mitarbeitern Einblick nehmen, die ihn schlichtweg überhaupt nichts angingen. Dies wurde umgehend abgestellt.

Ein solcher Vorfall macht dann doch nachdenklich. Dass, wenn es um Software geht, die personenbezogene Daten verarbeitet, Test und Schulung besonderer Überlegungen bedürfen, ist nun wirklich nicht neu. Hier hätte man von den Projekt- und EDV-Verantwortlichen erwarten können, dass sie mittlerweile vom Datenschutz wenigstens soviel mitbekommen haben, dass sie dafür keine Echtdateien verwenden. Ein solcher Vorfall weckt jedoch weitere Zweifel. Jede seriöse Softwarefirma, die Datenbankanwendungen entwickelt, wird im Rahmen der Qualitätssicherung und des Qualitätsmanagements ihres Produktes nicht umhin kommen, das zugrunde liegende Datenbankmodell mit einem gut durchdachten System von Testdatensätzen darauf hin zu prüfen, ob es sich genau wie gewünscht verhält. Dabei kommt es nicht darauf an, dass es viele Testdatensätze sind<sup>2</sup>, sondern dass diese so geschickt ausgewählt werden, dass erkennbar wird, ob sich das System im gesamten Bereich möglicher Datenwerte korrekt verhält. Dies gilt im Prinzip auch für die Schulungsdaten. Auch hier kommt es nicht auf Masse an, sondern darauf, anhand weniger, gut ausgewählter Datensätze demonstrieren zu können, wie man als Benutzer agieren muss, um eine bestimmte Aufgabe zu erledigen. Stellt man es geschickt an, kann man diese erfundenen Testdaten sogar im Echtbetrieb so im System belassen, dass die Benutzer jederzeit nachschlagen können.

An sich ist das, was Datenschutz effektiv an Mehraufwand auslöst, ziemlich bescheiden. Es ist oft nicht viel mehr als die Forderung nach Professio-

---

<sup>2</sup>Es gibt eine ironische Bemerkung von Ludwig Wittgenstein, wonach jemand, der eine Meldung in der Zeitung nicht glauben konnte, hinging, sich hundert Exemplare der Zeitung kaufte und die Meldung dann glaubte.

nalität, beginnend bei der Entwicklung von Software, weitergehend bei der Inbetriebnahme von Software und endend beim täglichen Umgang mit den Daten.

### 3.37 Nutzung eines kostenlosen E-Mail-Anbieters

Um die passende Werbung an die richtige Frau oder den Mann bringen zu können, braucht man weitere Informationen über die zu Beglückenden. Könnte man Mäuschen spielen und mitlesen, was in den E-Mails steht, die die Leute empfangen oder verschicken, käme einiges an Informationen zusammen. Nun mag wohl niemand den ganzen Tag E-Mails lesen, aber wozu gibt es Computerprogramme, die Texte automatisch nach bestimmten Wörtern oder Kombinationen von Wörtern absuchen und dann automatisch die dazu passende Werbung auswählen? Die damit erreichte Trefferquote ist auf alle Fälle wesentlich höher, als wenn man Werbung ins Blaue hinein verschickt. Nur, wie bringt man die Leute dazu, ihre E-Mails dafür zur Verfügung zu stellen? Auch wie das geht ist bekannt, man bietet einen kostenlosen Lockvogel.

So mögen die Manager der Internet-Suchmaschine Google gedacht haben, als sie ihren kostenlosen E-Mail-Dienst lancierten (Gmail, für Google-Mail). Damit nicht genug, von derselben Suchmaschine ist auch bekannt, dass sie die bei einer Suche gefundenen Internetadressen so ergänzt, dass beim Anklicken nicht die originalen Seiten angezeigt werden, sondern eine Umleitung auf andere ähnlich gelagerte bevorzugte Seiten erfolgt. Es ist zu befürchten, dass andere diesem Beispiel folgen werden, in der Spekulation, dass es hinreichende viele Leute gibt, denen dies alles egal ist. Des Weiteren ist geplant, dass die Suche nach Informationen auch auf die auf dem eigenen PC gespeicherten Daten ausgedehnt werden kann. Hoch bedenklich daran ist, dass dazu die entsprechenden Dokumente auf die Google-Rechner übertragen werden müssen. Zwar wird dabei sichergestellt, dass andere die eigenen Daten nicht einsehen können, dem Google-Personal stehen diese Daten jedoch offen. An solchen Entwicklungen wird deutlich, mit welcher Aggressivität teilweise versucht wird, mehr über möglichst viele in Erfahrung zu bringen.

Zumindest dann, wenn es um personenbezogene dienstliche Daten geht, sind die Stellen der Landeskirche und Diakonie verpflichtet, ihren E-Mail-Provider sorgfältig auszuwählen. Auf die Dienste von Providern, bei denen Zweifel aufkommen, ob sie dem Schutz des Persönlichkeitsrechts hinreichende Bedeutung beimessen, muss verzichtet werden. Eine weitere unverzichtbare Schutzmaßnahme bei E-Mails liegt darin, dass dienstliche Daten möglichst nur verschlüsselt übermittelt werden. Nur so kann sich der Absender wirklich sicher sein, dass nur der Empfänger Einblick nimmt. Auch deshalb ist der Einsatz sog. Zertifikate, die dies ermöglichen, für den Bereich der Landeskirche so wichtig.

### 3.38 Programmfreigaben

Nach den Richtlinien zum Einsatz der elektronischen Datenverarbeitung in der Evangelischen Landeskirche in Württemberg (EDV-Richtlinie) vom 25. März 1997 bedürfen EDV-Programme, mit denen personenbezogene Daten verarbeitet werden sollen und EDV-Programme, die im Bereich des Haushalts-, Kassen- und Rechnungswesens und des Meldewesens eingesetzt werden, der vorherigen Freigabe durch den Oberkirchenrat.

Dass bei einer Reduzierung des Stellenumfangs des landeskirchlichen Datenschutzbefragten von 100% auf 50% bestimmte Aufgaben nicht mehr wahrgenommen werden können, müsste einsehbar sein. So sollten meine Stellungnahmen, die maßgebliche Grundlage für die Erteilung von Programmfreigaben waren, entfallen. Leider wurde bis heute weder geklärt wurde, wer denn nun für die Beurteilung einer Freigabe oder Nichtfreigabe zuständig sein solle noch wurde die Vorschrift geändert, die eine solche Freigabe verlangt. Hinzukommt, dass auch das Datenschutzgesetz in bestimmten Fällen eine Vorabkontrolle verlangt. Im Bereich des Meldewesens muss gewährleistet bleiben, dass nur qualifizierte Software zu Einsatz kommt. Aber auch darüber hinaus wird immer wieder deutlich, dass das Instrument einer Freigabeberfordernis, sinnvoll angewandt, ein nützliches Steuer- und Schutzinstrument sein kann, etwa wenn es darum geht, Eigenprogrammierungen einzelner Personen auf Bereiche einzuschränken, wo es vertretbar ist. Da es sowohl für den Softwarehersteller als auch die Softwareanwender auf Dauer nicht zumutbar ist, gegen geltendes Recht agieren zu müssen, besteht weiterhin Bedarf an Stellungnahmen.

Abgesehen vom Bereich des Meldewesens und den Softwareprodukten, die einer Vorabkontrolle nach dem Datenschutzgesetz unterliegen, können Zweck und Adressat der Freigabevorschrift jedoch durchaus überdacht werden: So gibt es etwa die Meldepflichten und Verfahrensübersichten nach dem Datenschutzgesetz, die, würden sie auch konsequent umgesetzt, einen guten Überblick über die im Bereich der Landeskirche und Diakonie eingesetzten Verfahren ermöglichen würden. Man könnte überlegen, ob für bestimmte Anwendungsgebiete die Freigabeberfordernis entfallen kann, wenn organisatorisch sicherstellt ist, dass die Meldepflichten eingehalten werden. Dies auch unter dem Gesichtspunkt, dass ich jederzeit eine Beanstandung aussprechen kann, wenn eine eingesetzte Software datenschutzrechtlichen Anforderungen nicht genügt. Selbst wenn es zu einer Beanstandung kommt, stehen heute einige Möglichkeiten zur Verfügung, die festgestellten Mängel mittels weiterer Sicherheits-Software zu beheben. Mangelt es beispielsweise an einer Verschlüsselungsmöglichkeit, kann dies u.U. mittels einer entsprechenden Software, die auf Festplatten- oder Verzeichnisebene agiert, behoben werden. Zwar bringen solche Nachrüstungen weitere Kosten und Umstände mit sich, die vermeidbar wären, würde man schon vorher klären, ob die Software den Datenschutzbestimmungen genügt, aber der Einsatz der entsprechenden

Software muss nicht grundsätzlich untersagt werden. Zu einer nicht behebbaren Beanstandung kann es allerdings dann kommen, wenn mehrere Personen mit der Software arbeiten sollen und durch ein Berechtigungssystem gewährleistet sein muss, dass nur bestimmte Personen auf bestimmte Daten zugreifen können dürfen. In solchen Fällen ist eine Freigabeerfordernis nach wie vor sinnvoll, um rechtzeitig zu klären, ob mit der Software unter Beachtung der Bestimmungen des Datenschutzes gearbeitet werden kann.

Neben dem Datenschutz sind auch die Belange des Rechnungsprüfandes Gegenstand der Freigabevorschrift. Hier könnte von einer Freigabeerfordernis dann abgesehen werden, wenn ein Testat eines Wirtschaftsprüfungsinstituts vorliegt, also die Einhaltung der Grundsätze ordnungsgemäßer Buchführung (GOBS) überprüft wurde. Schwieriger wird es bei Software vom Typ „Verbandsverwaltung“ (z.B. Krankenpflegeverein), wo ebenfalls umfänglich gebucht wird, aber nicht im Rahmen kaufmännischer Buchführung, so dass es auch kein Testat geben kann. Handelt es sich allerdings um einigermaßen bekannte kommerzielle Software, wird man vermuten dürfen, dass sie korrekt arbeitet und könnte ebenfalls von einer Freigabeerfordernis absehen.

Problematisch sind selbst entwickelte Programme auf der Basis einer Tabellenkalkulation und der entsprechenden Makrosprache (z.B. Excel und Visual Basic), aber auch schon einfache Tabellen mit hinterlegten Formeln. Aber auch hier gibt es viele Anwendungsbereiche, wo sich in vertretbarer Weise Einnahmen und Ausgaben und wenige Berechnungen dazu ohne weiteres schnell und einfach mit einer Tabellenkalkulation buchen lassen, schließlich wurde letztere genau zu diesem Zweck entwickelt. Auf der Basis einer vollständigen und gut nachvollziehbaren Dokumentation, möglichst schon in der betreffenden Excel-Tabelle durch farbliche Hervorhebungen, Bemerkungen und Erläuterungen könnte ggf. auch hier auf eine Freigabeerfordernis verzichtet werden. Bedingung wäre, dass ein geschulter Blick mit vertretbarem Aufwand erkennen kann, ob die Tabelle genau das tut, was sie vorgibt und Grundlage der Rechnungslegung ausschließlich der Papierausdruck ist.

Es bleibt der Bereich selbst geschriebener komplexer Makroanwendungen. Hier ist das Durchsetzen einer Freigabe sinnvoll. Jeder, der im Bereich des Rechnungswesens etwas entwickelt muss sich darüber im klaren sein, dass die schnelle Erledigung bestimmter Dinge mit dem Computer nur die eine Seite ist, die andere besteht darin, dass Dritte mit vertretbarem Aufwand feststellen können müssen, ob das alles auch seine Richtigkeit hat. Sinnvoll wäre, dass das Rechnungsprüfamt entscheidet, ob es aufgrund der Komplexität einer nichtkommerziellen Anwendung im Bereich des Haushaltsrechts eine Freigabe für erforderlich hält oder nicht.

Innerhalb des hier skizzierten Rahmens hielte es auch der landeskirchliche Datenschutzbeauftragte für vertretbar, die bisherige Freigaberichtlinie neu zu überdenken.

*KAPITEL 3. BESCHWERDEN, ANFRAGEN, ANMERKUNGEN*

---

# Kapitel 4

## Technisches

### 4.1 Vorbemerkung

Datenschutz wird noch immer sehr schnell gleichgesetzt mit Schutz vor Computerviren, Absicherung des Internetzugangs, geschützten Datenübertragungen und so weiter, also Themen, die der Datensicherheit zuzurechnen sind. Datenschutz ist wesensmäßig jedoch vorgezogener Grundrechtsschutz. Geschützt werden nicht Bits und Bytes, sondern das Persönlichkeitsrecht der Menschen, die von einer Erhebung, Verarbeitung oder Nutzung ihrer Daten betroffen sind (es gilt deshalb auch nur für lebende Personen).

Nun hat Datenschutz natürlich auch die besonderen Gefährdungen durch die moderne Informations- und Kommunikationstechnologie im Auge und insofern sind in den Bestimmungen des Datenschutzgesetzes auch konkrete Anforderungen an die Art der Datenverarbeitung formuliert (früher die 10 Gebote der Datenverarbeitung genannt). Diese überschneiden sich zum Teil mit Gesichtspunkten der Datensicherheit. Dabei muss allerdings die Interessenslage genau gesehen werden: Datensicherheit betreiben die Stellen aus eigenem Interesse genau soweit, wie sie die Wahrnehmung ihrer Geschäfte gefährdet sehen, während die Sicherheitsanforderungen des Datenschutzes das Interesse der Betroffenen zur Geltung bringen. Die Berücksichtigung dieser Interessen kann für die Stellen weitere Umstände und Kosten nach sich ziehen, die sie in aller Regel nur auf Grund gesetzlicher Anforderungen und auf Nachdruck des zuständigen Datenschutzbeauftragten auf sich nehmen.

Trotz dieser Abgrenzung gehört zum Datenschutz auch eine technische Komponente. Um diesem Aufgabenbereich Rechnung zu tragen, wurden einige Werkzeuge geschaffen und bereitgestellt.

Als sinnvoll und hilfreich erwies sich der Betrieb eines Datenschutzwebs unter der Internetadresse

<http://okrweb.elk-wue.de/datenschutz>.

Gelohnt hat sich auch der Aufwand, mit Hilfe einer Softwarefirma ein für das Bundesdatenschutzgesetz entwickeltes Lernprogramm Datenschutz auf

kirchliche Verhältnisse umzuschreiben.

Als unabdingbar erwies es sich, ein Instrument zu schaffen, um die vom Datenschutzgesetz geforderte Verfahrensübersicht in elektronischer Form erstellen zu können. Wenig erfreuliche Erfahrungen an anderer Stelle zeigten, dass dabei Einfachheit und Benutzerfreundlichkeit das A und O ist. Ferner muss die einfache Anpassbarkeit auf die Verhältnisse größerer Werke und Einrichtungen der Diakonie geben sein. Unter dem Namen „Orgdia“ steht eine entsprechende Software bereit.

Immer wieder werden technische Anfragen zur „Sicheren Nutzung des Internets“ oder allgemeiner zur Datensicherheit gestellt. Antworten darauf finden sich im oben genannten Datenschutzweb, ergänzend fasst der entsprechende Abschnitt in diesem Kapitel das Wichtigste zusammen.

Als allgemeiner Standard, was die Sicherheit der IT-gestützten Geschäftsprozesse anbelangt, hat sich das sog. IT-Grundschutzhandbuch etabliert. Dazu enthält der letzte Abschnitt einige Anmerkungen.

## 4.2 Datenschutzweb

Der landeskirchliche Datenschutzbeauftragte betreibt als Kommunikationsinstrument ein Datenschutzweb. Die Adresse lautet:

<http://okrweb.elk-wue.de/datenschutz/>

Bei eher allgemeinen Fragen zum Datenschutz bietet es sich an, dort einen Blick hineinzuwerfen, es ist auch eine Suchmaschine enthalten, ergänzt um eine Seite mit Links auf Internetauftritte anderer Stellen und Organisationen, die als besonders hilfreich und zuverlässig in das Blickfeld getreten sind.

Des Weiteren ist dort ein Grossteil der kirchlichen (und auch staatlichen) Rechtsbestimmungen versammelt, die bei Datenschutzfragen mit berücksichtigt werden müssen. Das kirchliche Datenschutzgesetz ist wie alle anderen Datenschutzgesetze auch ein sog. Auffanggesetz, d.h. wenn ein Sachverhalt in einer anderen Bestimmung geregelt ist, geht diese vor.

Ergänzend geht ein Praxisteil auf Fragen oder Eingaben ein, die gehäuft gestellt werden.

Auch die dort enthaltenen Berichte über Begehungen bei Pfarrämtern, Diakoniestationen und Psychologischen Beratungsstellen haben, auch wenn sie länger zurückliegen, nur wenig von ihrer Relevanz eingebüßt.

Aktuell steht an, dass das Datenschutzweb auf eine modernere Basis gestellt wird (Content-Management-System, CMS), um besser als Kommunikationsschnittstelle zu meinem Amt nutzbar zu sein.

## 4.3 Lernprogramm Datenschutz

Zur Aufgabe betrieblicher oder kirchenbezirklicher Datenschutzbeauftragter gehört nach dem Datenschutzgesetz auch die Unterrichtung über die Bestim-

mungen des Datenschutzes. Man kann eine solche Unterrichtung gliedern in einen allgemeinen, grundsätzlichen Teil und einen Teil, der konkret darauf eingeht, was beim Arbeitsplatz zu beachten ist (z.B. bei Mitarbeiterin einer Diakoniestation).

Damit eine Konzentration auf die konkreten Arbeitsplatzumstände möglich ist, wurde für den allgemeinen Teil ein Lernprogramm Datenschutz entwickelt. Dieses kann vom Datenschutzweb heruntergeladen werden, die Lizenz umfasst die ganze Landeskirche und Diakonie Württemberg (sowie Landeskirche und Diakonie Baden). Mittlerweile haben auch andere Landeskirchen das Programm erworben und setzen es in ihrem Bereich ein.

Beispielsweise wird dieses Programm beim Oberkirchenrat in der Form eingesetzt, dass neue Mitarbeiterinnen und Mitarbeiter aufgefordert werden, innerhalb der ersten drei Monate nach dem Antreten der Stelle das Programm durchzuarbeiten und dies mir zu bestätigen. Dahinter stand die realistische Einschätzung, dass jemand, der eine Stelle antritt, alles andere im Kopf hat als den Datenschutz, also auch entsprechende Formulare in aller Regel mehr oder weniger unbesehen einfach unterzeichnet (allerdings zeigt beim Oberkirchenrat die Häufigkeit von in dieser Sache eingehender eMails, dass sich beim Durcharbeiten des Lernprogramms mittlerweile eine gewisse Nachlässigkeit eingeschlichen hat).

Es bietet sich für die anderen Stellen der Landeskirche und der Diakonie an, entsprechend zu verfahren. Das Datenschutzgesetz kennt auch Schadensersatzbestimmungen, und dies gilt für die Stelle unabhängig von einem Verschulden. Es dürfte dann im nachhinein stellenintern kaum Aussicht auf Erfolg haben, gegen einen grob fahrlässigen oder mutwilligen Mitarbeiter mit rechtlichen Schritten vorgehen zu wollen, wenn dessen Unterrichtung über die Datenschutzbestimmungen offensichtlich keine Bedeutung beigemessen wurde.

Eine Neuauflage, die neuen technischen Möglichkeiten und der Entwicklung in Recht und Praxis der letzten Jahre Rechnung trägt ist in Arbeit.

## 4.4 Erhebungsprogramm Orgdia

Der Landesdatenschutzbeauftragte berichtete in seinem Tätigkeitsbericht 2004 über seine Erfahrungen, wie die Schulen des Landes der im Datenschutzgesetz verankerten Meldepflicht über eingesetzt EDV-Verfahren nachkommen. Zitat: ... Kämpferische Rektoren erklärten, dass sie das alles nicht einsehen wollten, sich sogar einfach nur untätig und trotzig auf den Hosensboden setzen wollten (obwohl stattdessen Nachsitzen angesagt wäre), und räumten ein, man könne in der Schule mit unserem Schreiben nichts anfangen und/oder unseren Forderungen wegen der notwendigen Aufrechterhaltung des Lehrbetriebs nicht nachkommen. ...

Weiteres Zitat: ... Kurios auch die Mitteilung einer Schule, wonach sie den

beigefügten Vordruck leider nicht erhalten habe . . . .

Dieser massive Widerstand, den gesetzlichen Meldepflichten nachzukommen, ist auch in der Kirche nicht ganz unbekannt. Vielleicht würde es helfen, wenn die Übersicht wirklich einfach und schnell erstellt werden könnte. Diesen Gedanken hatte man im *Ulmer Kreis* (Kreis der Datenschutzbeauftragten der Diakonie) schon länger und hat früh über eine Softwarelösung nachgedacht, mit der man die erforderlichen Angaben anhand der Auswahl aus vorgefertigten Textbausteinen *zusammenklicken* kann. Das, was eine durchaus namhafte Softwarefirma in dieser Hinsicht dann allerdings zustande brachte, genügte diesen Erwartungen nur unzureichend; eigentlich schade. Ein solches Produkt mochte ich dann doch nicht empfehlen und schon gar nicht zu dessen Verwendung aufzufordern, zumal es die einzelnen Stellen auch noch nicht wenig Geld kosten sollte (das Produkt wurde nicht mit landeskirchlichen Mitteln, auch nicht dem Datenschutzzetat, entwickelt).

Immerhin war dies ein bedenkenswerter Warnschuss dahingehend, dass die Sache anspruchsvoller war als zunächst angenommen. Ich programmierte dann selbst verschiedene Varianten, die eine solche Erhebung so einfach wie möglich machen sollten, das Ergebnis war ein Produkt namens „Orgdia“. Es ist schwer vorstellbar, wie man es den Anwendern noch einfacher machen kann. Es genügt nun, in einer strukturierten Art und Weise aus kontextbezogenen Auswahllisten die zutreffenden Textbausteine „zusammenzuklicken“. Soweit es eingesetzt wurde, hat es sich bislang durchaus als praxistauglich erwiesen. Weitere Erläuterungen zu diesem Programm finden sich im Datenschutzweb.

Im Kreis der kirchenbezirklichen Datenschutzbeauftragten, die sich damit den dringend notwendigen Überblick über die in ihrem Bereich eingesetzten Verfahren verschaffen sollen, wurde deshalb folgende Vorgehensweise verabredet.

1. Ganz kleine Stellen werden telefonisch oder sonst wie kontaktiert und der kirchenbezirkliche Datenschutzbeauftragte trägt die gemachten Angaben in seine elektronische Verfahrensübersicht (Orgdia) ein.
2. Ist erkennbar, dass die Dinge doch nicht so einfach liegen, aber relativ überschaubar sind, wird ein Formular (PC-Datenpass genannt) zugestellt. Die damit erhobenen Angaben werden vom zuständigen Datenschutzbeauftragten ebenfalls eigenhändig in seine elektronische Verfahrensübersicht eingetragen.
3. Bei Stellen mit komplexerer EDV, insbesondere wenn mehrere PC im Einsatz sind, wird auf Diskette das Orgdia zugestellt. Das Programm braucht nicht installiert zu werden, sondern kann direkt gestartet werden. Die erforderlichen Angaben werden auf dieser Stelle zusammengeklickt und die Diskette zurückgeschickt. Der kirchenbezirkliche Datenschutzbeauftragte kann diese Angaben dann auf Knopfdruck in seine elektronische Verfahrensübersicht integrieren.

Die Hoffnung ist, dass sich diese Methode als praxistauglich erweist und allgemeine Anwendung findet. Ergänzend sei darauf hingewiesen, dass nach den Datenschutzbestimmungen eine solche Verfahrensübersicht von jeder

Person eingesehen werden kann, die ein berechtigtes Interesse nachweist. Das dürfte regelmäßig dann gegeben sein, wenn diese Person von der Stelle datenmäßig erfasst ist. Vertrauen erfordert Transparenz; ein wirkliches Bild über eine Stelle kann sich der Einzelne aber nur dann verschaffen, wenn er sich nicht nur darüber informieren kann, welche Daten die Stelle über ihn gespeichert hat, sondern auch, welche Verfahren mit personenbezogenen Daten insgesamt zur Anwendung kommen.

Kirchliche Stellen werden künftig wohl damit rechnen müssen, dass sich Personen melden, die die Verfahrensübersicht einsehen wollen. Schon aus diesem Grunde, aber auch deshalb, weil sich fundierte Entscheidungen zur eingesetzten EDV nur treffen lassen, wenn als Entscheidungsgrundlage eine Verfahrensübersicht zur Verfügung steht.

## 4.5 Sichere Nutzung des Internets

Genauso wenig wie der Datenschutz die Daten schützt, sondern die Persönlichkeitsrechte der Betroffenen, schützt die IT-Sicherheit nicht die IT, sondern die IT-gestützten Geschäftsprozesse.

Immer wieder wird angefragt, wie man denn seinen PC, insbesondere den Internetzugang absichern solle. Ich helfe hier gerne mit Hinweisen und Ratschlägen, möchte aber auf folgendes aufmerksam machen:

1. Was oft nicht verstanden wird ist, dass die Sicherheit in der Informationstechnik prinzipiell so hergestellt wird, indem Schwachstellen umgehend öffentlich bekannt gegeben werden. Jeder kann sich entsprechende Newsletter abonnieren und sich täglich darüber unterrichten lassen, bei welcher Software- oder Hardwarekomponenten welche Schwachstelle entdeckt wurde. Neuerdings geht man noch weiter und benennt nicht nur die Schwachstelle, sondern demonstriert, wie unter welchen Bedingungen die Schwachstelle für einen Angriff ausgenutzt werden kann (Proof of Concept). Anders formuliert, serviert man potentiellen Hackern die Schwachstellen auf dem Servierteller. Dahinter steht natürlich die Überlegung, dass nur so ein hinreichender Druck auf die Hersteller der Produkte und die Anwender erzeugt wird, dass diese auch reagieren. Die Hersteller beheben umgehend die Schwachstelle oder geben bekannt, was man tun muss, um sie zu vermeiden, die Anwender updaten dann ihre Soft- oder Hardware so schnell wie möglich. Jeder, der sich auf die Nutzung von Informationstechnik einlässt, muss sich über diese „Spielregeln“ im Klaren sein. Für datenverarbeitende Stellen heißt dies, dass sie mit ihren Schutzmaßnahmen ständig aktuell sein müssen. Der dafür erforderliche zeitliche und finanzielle Aufwand ist als immanenter Kostenfaktor jeder EDV-Nutzung von vornherein in Rechnung zu stellen.

2. Es wurden in Sachen Datensicherheit drei Verordnungen erarbeitet, eine zu Computerviren, eine zur Datenverschlüsselung und eine zur Datensicherung. Es sind kurze und knappe Texte, die das regeln, was hier überhaupt

allgemein geregelt und verlangt werden kann. Zu jeder dieser Verordnungen wurden Umsetzungsvorschläge erarbeitet, alles ist im Datenschutzweb einsehbar. Der erste Schritt zur Absicherung des Internetzugangs muss darin bestehen, diese Verordnungen umzusetzen. Damit hat man dann schon eine ganze Menge getan. Am wichtigsten ist ein zuverlässiger Virenschutz. Es gibt Monate, an denen bis zu 3000 neue Viren, Trojaner, Pishing-Mails, Spams oder sonstiges Ungemach in Umlauf gesetzt wird. Angesichts dieser Realitäten verwundert es dann schon, wenn auf dienstlichen PC's der Landeskirche immer wieder festgestellt wird, dass die Benutzer den Virenschutz einfach abgeschaltet haben. In ihrer Bedeutung oft nicht richtig wahrgenommen wird die Datensicherungsverordnung. Eine Stelle, etwa ein Pfarramt, das nicht dafür sorgt, dass es an einem sicheren Ort eine Kopie der verwendeten Daten gibt, demonstriert damit recht deutlich, dass es diese Daten nicht wirklich benötigt. Damit liegt bereits ein Datenschutzverstoß vor. Der Einsatz von EDV stellt für die Betroffenen eine Gefährdung dar, die sich nur damit rechtfertigen lässt, dass eine Erforderlichkeit gegeben ist. Elektronische Speichermedien haben wie alle elektronischen Geräte eine gewisse Wahrscheinlichkeit zu versagen. Ist eine Stelle auf die Daten angewiesen, müssen Sicherungskopien gefertigt werden. Diese Kopien enthalten eine Fülle von Daten auf kleinem Raum, die sicher untergebracht werden müssen, womit eine weitere Anforderung gegeben ist. Es ist durchaus im Sinne des Datenschutzes, dass die so geschaffene Hürde zur Überlegung zwingt, ob eine edv-technische Datenspeicherung wirklich sinnvoll ist und der Nutzen den Aufwand überwiegt.

3. Darüber hinaus ist es unumgänglich, Korrekturen und Nachbesserungen (sog. Patches) des Betriebssystems (etwa Windows) oder von bestimmten Programmen (Internet-Explorer) möglichst zeitnah aufzuspielen und auf dem aktuellen Stand zu bleiben. Das gilt natürlich auch für die Aktualisierung der Virensuchprogramme, es ist schlicht nicht nachvollziehbar, dass man immer noch Anlass hat, darauf hinzuweisen.

4. Es ist auch unter Datenschutzgesichtspunkten durchaus angebracht, ein Upgrade auf eine aktuelle Betriebssystemversion vorzunehmen, da sich hier in der letzten Zeit doch einiges getan hat. Dies gilt auch für Software zur Bürokommunikation (z.B. Microsoft-Office). Hat man ein aktuelleres Betriebssystem, sollte man dessen Sicherheitsfunktionen, insbesondere die Firewall, dann aber auch einschalten.

Befolgt man dies, sind die grundlegenden Hausaufgaben gemacht. Weitergehendes lässt sich nur unter Ansehung eines konkreten EDV-Systems sagen. Hier allgemeine Strukturen zu abstrahieren, die sich zum Gegenstand einer kurzen und knappen „Internetzugangsverordnung“ machen ließen, ist mir bislang nicht gelungen und vermutlich grundsätzlich nicht möglich, ohne in ein umfassendes Kompendium auszuarten.

Für jemanden, der viel im Internet surft, kann als Selbstschutz ergänzend folgendes empfohlen werden:

5. Den Einsatz eines Programms, das auf im Hintergrund laufende Programme, kritische Registry-Einträge oder sonstige Bedenklichkeiten prüft (sog. Antispyware). Dieses muss dann ebenfalls regelmäßig aktualisiert werden. Solche Programme können, für den Privatgebrauch oft kostenlos, aus dem Internet heruntergeladen werden. Allerdings wird dieser Bereich immer mehr auch von Virenschutzprogrammen abgedeckt. Hier muss man sich dieses genauer ansehen, was aber für den hier angesprochenen Nutzerkreis kein Problem sein dürfte.

6. Den Einsatz eines Programms, das anzeigt, welche Programme und Hintergrundprogramme (sog. Prozesse) beim Hochfahren des Rechners gestartet werden. Auch solche Programme lassen sich aus dem Internet herunterladen, für Privatanwender ebenfalls oft kostenlos. Eine Schwierigkeit besteht hier darin, dass ein durchschnittlicher Anwender kaum anhand des Namens der gestarteten Systemdatei erkennen kann, ob dies seine Richtigkeit hat oder nicht. Hat man Zweifel, ob es mit einem der dann angezeigten Prozesse oder Programme seine Richtigkeit hat, genügt die Eingabe von dessen Namen auf einer Suchmaschine des Internets, um weitere Informationen zu bekommen. Meist wird dann sehr schnell klar, ob es einer der Prozesse ist, die üblicherweise im Hintergrund mitlaufen, oder ob es sich etwa um eine Trojaner oder einen Keylogger handelt. Gerade Keylogger sind nicht unproblematisch. Nach jüngsten Meldungen nimmt ihre Verbreitung stark zu. Verschafft sich jemand ein Protokoll der Tastaturanschläge, kann er in aller Regel Benutzername und Kennwort herauslesen, da diese immer am Anfang einer Computersitzung eingegeben werden. Er kann dann unter dem Benutzernamen der betroffenen Person agieren. Alles, was er dann „anstellt“, wird in den Systemprotokollen dieser Person zugerechnet. Diese kann nur hoffen, nachweisen zu können, dass sie das nicht gewesen sein kann.

7. Die regelmäßige Verwendung sog. Wiederherstellungspunkte bei Windows-Betriebssystemen. Der Aufwand, einen solchen Punkt zu erzeugen ist, gering, und er kann eine ganze Menge an Umständen und Ärger ersparen. Dies ist unter Datenschutzgesichtspunkten auch insofern relevant, als bei Schwierigkeiten oft weitere Personen hinzugezogen werden, die dabei Einblick in Daten anderer nehmen könnten, bis dahin, dass der ganze PC zur Wartung oder Reparatur irgendwohin verbracht wird.

8. Aktivieren oder installieren eines E-Mail bzw. Spam-Filters. Allerdings ist es nicht ganz einfach, automatisiert festzustellen, ob eine eingehende eMail als Spam zu bewerten ist. Die meiste Software zum Schutz vor Spam kann lediglich einen Wahrscheinlichkeitswert dafür errechnen (den sog. Score) und der Anwender muss dann den Wert festlegen, ab dem er eine eMail nicht mehr annimmt. Das wohl wichtigste Kriterium für den Scorewert sind bestimmte Kombinationen von Wörtern, die typischerweise in Spam-Mails anzutreffen sind. Der Anwender kann weitere Fangworte hinzufügen, allerdings mit Bedacht. Worte können in unterschiedlichen Zusammenhängen ganz unterschiedliche Bedeutung haben, hier ist ein Mitdenken der Anwender unab-

dingbar. Diese müssen Score und Fangworte auf ihre konkreten Verhältnisse abstimmen, um eine optimale Filterwirkung zu haben.

Für kirchliche Stellen, deren E-Mail über den Oberkirchenrat läuft, wurde ein besonderer Service eingerichtet. Der Betreff dieser E-Mails wird um den Score-Wert und eine Warnung ergänzt, wenn der Spam-Filter des Oberkirchenrats angeschlagen hat. Zu bedenken ist allerdings, dass der Oberkirchenrat aus rechtlichen Gründen E-Mails nur dann herausfiltern kann, wenn eindeutig feststeht, dass es sich um Spam handelt oder wenn ein Virus festgestellt wurde. Da aber auch den Vertreibern von Spam recht genau bekannt ist, welches die Kriterien sind, ist der vom Referat IT des Oberkirchenrats erreichbare Schutz vor Spam auf eine relativ grobe Vorfilterung beschränkt. So wird es auch künftig immer wieder vorkommen, dass etwa einzelne Pishing-Mails nicht schon vor der Weiterleitung herausgenommen werden. Die Feinfilterung kann nur bei den Empfängern selbst erfolgen. Eine Erfolg versprechende Entwicklung könnten selbstlernende Anti-Spam-Lösungen darstellen. Hier gibt der Anwender keine Regeln vor, sondern das Tool „beobachtet“ den Anwender, wie er mit welchen E-Mails umgeht, fragt bestimmte Informationen nach und leitet daraus das Regelwerk ab. Nach einiger Zeit hat es sich relativ genau auf die Benutzeranforderungen eingestellt.

Es ist erfreulich, wenn im Internet und Computerzeitschriften, zunehmend auch in Rundfunk und Fernsehen, über aktuelle Gefährdungen berichtet wird. Nicht ganz optimal ist allerdings, dass bei diesen Informationen häufig der Eindruck geweckt wird, von der aktuell genannten Gefährdung seien alle betroffen. Dem ist oft nicht so, vielfach ist aufgrund der Konfiguration der eigenen EDV-Anlage oder der verwendeten Programme oder Betriebssysteme die genannte Gefährdung gegenstandslos. Die richtige Reaktion auf solche Meldungen ist nicht Aufregung, sondern die nüchterne Prüfung, ob man davon überhaupt betroffen ist, etwa indem man beim vom Rechenzentrum der Universität Stuttgart betriebenen Cert-Dienst genauere Informationen einsieht (<http://cert.uni-stuttgart.de/ticker/>). Dort werden die Voraussetzungen, unter denen ein Risiko besteht, genauer aufgeführt. Sind diese allerdings gegeben, muss auch umgehend reagiert werden.

## 4.6 IT-Grundschutzhandbuch

Ich begrüße es sehr, dass, wenn auch nach beständigem Drängen, sich das IT-Referat entschlossen hat, die IT-Sicherheit durch Anwendung des IT-Grundschutzhandbuches des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) zu gewährleisten und dazu den Stand einer Selbsterklärung anstrebt.

Wie notwendig ein hinreichendes Niveau an IT-Sicherheit ist, zeigt folgende aktuelle Meldung:

Hacker knackt Mail-System der Uni Bochum Ein Hacker hat das Mail-System der Ruhr-Universität Bochum vorübergehend lahm gelegt. Der Unbekannte hatte am Sonntag eine Sicherheitslücke genutzt, um an die Mailboxen und Passwörter der 40.000 Studenten und Beschäftigten zu gelangen. Das teilte die Universität am Dienstag mit. Die Lücke sei inzwischen geschlossen worden. Studenten forderten nach dem Angriff, aus Datenschutzgründen auf die geplante Einrichtung eines neuen Systems zur elektronischen Verwaltung von Studien- und Prüfungsdaten zu verzichten. *Der Unbekannte hat einen elektronischen Drohbrief hinterlassen*, sagte Universitätssprecher Josef König. *Wenn die Studenten nicht umgehend aufgefordert würden, ihre Passwörter zu ändern, wolle er die Öffentlichkeit informieren*. Das Rechenzentrum veröffentlichte den Angriff daraufhin auf der Internet-Seite der Universität. Bei der Überarbeitung des Systems entdeckten Spezialisten noch ein Hintertürchen, über das der Hacker nach dem Neustart des Mail-Systems erneut Zugriff gehabt hätte. *Dieses Mauselloch ist jetzt auch geschlossen*, sagte König.

Es ist jedem selbst überlassen, welche Auswirkungen es hätte, würde ähnliches dem Netzwerk des Oberkirchenrats oder anderen großen Einrichtungen der Landeskirche und der Diakonie widerfahren.

Das BSI-Grundschutzhandbuch wirkt aufgrund seines Umfangs auf den ersten Blick etwas abschreckend. Dem liegt meist das Missverständnis zugrunde, dass immer das ganze Werk „durchgearbeitet“ werden müsste. Tatsächlich müssen nur die „Bausteine“ näher ins Auge gefasst werden, die bei der vorliegenden EDV überhaupt eine Rolle spielen. Ferner ist es viel zeitsparender, eine Checkliste abzuarbeiten, als selbst damit zu beginnen, systematisch zu überlegen, an welcher Stelle denn welche Sicherheitsaspekte zu beachten wären. Genau diese Arbeitserleichterung ist Sinn und Zweck des IT-Grundschutzhandbuchs und eben deshalb sollte es auch genutzt werden. Es kann im Internet unter <http://www.bsi.de/gshb/> eingesehen werden.

Die Fälle, in denen Zweifel aufkommen, ob ein Grundschutz ausreichend ist, dürften im Bereich der Landeskirche und Diakonie relativ überschaubar sein. Bevor man sich dann dilettierend an der Erstellung eines weiterführenden Sicherheitskonzeptes versucht, sollte man besser mit mir Rücksprache nehmen. Möglicherweise gibt es pragmatischere Lösungen, die mit wesentlich weniger Aufwand und Kosten verbunden sind, etwa, um wieder Bezug auf die obige Meldung zu nehmen, in dem eine entsprechend spezialisierte Firma mit Penetrationsversuchen gegen das eigene Netzwerk beauftragt wird, wenn Zweifel an dessen Sicherheit bestehen.

## 4.7 Verschlüsselung des E-Mail-Verkehrs

Hin und wieder, in der letzten Zeit immer häufiger, stellen Mitarbeiter beim Oberkirchenrat fest, dass sie, glaubt man den Systemmeldungen, angeblich eine E-Mail an einen bestimmten Empfänger geschickt haben. Des Rätsels Lösung ist könnte sein, dass jemandem, der einen offenen Mail-Server im Zugriff hat, deren E-Mail Adressen bekannt geworden sind, etwa weil sie auf einer Webseite veröffentlicht wurden, und diese Person nun ihr Unwesen damit treibt. Manchmal findet man sich auch damit konfrontiert, eine verschickte eMail ein paar Minuten später vorgeblich auch an eine andere eMail-Adresse verschickt zu haben, obwohl man genau weiß, das nicht getan zu haben. Dann könnte die Ursache sein, dass der Mail-Server des Empfängers fehlerhaft arbeitet. Vor einiger Zeit ging bei mir auch ein (echter!?) Spendenauftrag eines Pfarramtes für einen bestimmten Zweck ein. Das kann man aus bestimmten Anlässen heraus vielleicht tun, sollte aber bedenken, dass jemand, der einer solchen Aufforderung nachkommen will, schon gerne sicher sein möchte, dass diese eMail auch „echt“ ist, bevor er Geld auf ein dort angegebenes Konto überweist. Künftig ist auch mit Mitteilungen wie der folgenden zu rechnen: Dem Empfänger einer eMail wird mitgeteilt, dass unter seinem Benutzernamen massenhaft Spam verschickt wurde und dass seine Benutzerberechtigung umgehend gesperrt wird, wenn er nicht das im Anhang befindliche Formular ausfüllt. Öffnet dieser dann den Anhang, installiert sich ein Trojanisches Pferd, das den hinter der eMail stehenden Hackern eine Zugriffsmöglichkeit auf den betreffenden PC ermöglicht.

Die Liste ließe sich fortsetzen und macht deutlich, dass dringend ein Weg gefunden werden muss, der einem Empfänger einer eMail erlaubt festzustellen, ob diese „echt“ oder eher fragwürdig ist. Die oben genannten Beispiele zeigen auch, dass es eine Rücksichtslosigkeit gegenüber den Betroffenen ist, wenn man eMails mit Angaben zu deren Person bzw. zu deren persönlichen Verhältnissen einfach als eMail durch das Internet schickt.

Um die landeskirchliche Kommunikation trotzdem dauerhaft sicherzustellen, wurde im Referat Informationstechnologie unter meiner Mitwirkung und Einschaltung einer darauf spezialisierten Softwarefirma ein Open-Source-Verfahren entwickelt, das es erlaubt, an Stellen und Personen im Bereich der Landeskirche und Diakonie so genannte Zertifikate auszugeben. Damit können zum einen eMails verschlüsselt werden, zum anderen kann der Empfänger sich vergewissern, ob der Absender tatsächlich der ist, den er zu sein vorgibt. Den Stellen, die zuerst mit solchen Zertifikaten versorgt werden, werden in Kürze weitere Informationen zugestellt.

## 4.8 Sicherheitsgefahr durch eigene Mitarbeiter

Die Vorstellung, dass Sicherheitsrisiken und Datenklau hauptsächlich darauf zurückzuführen sind, dass Außen stehende in den eigenen PC oder das eigene Netzwerk eindringen, hält sich zwar zäh, ist aber nichtsdestoweniger falsch.

Eine aktuelle Studie (Februar 2005) der US-Regierung bestätigt, was schon frühere Untersuchungen immer wieder aufgezeigt haben:

1. Kommt es zu Angriffen, sind es in 4 von 5 Fällen autorisierte Anwender mit gültigen Zugängen.
2. In 2 von 3 Fällen erfolgt der Angriff während der normalen Arbeitszeiten.
3. In 9 von 10 Fällen werden einfache und zulässige Eingaben benutzt, um sich Zugang zu sensiblen Daten zu verschaffen.
4. Das Motiv, dem Dienst- oder Arbeitgeber Schaden zuzufügen, ist relativ selten. Vorwiegend geht es darum, sich finanzielle Vorteile zu verschaffen.

So weit, (nicht) so gut. Allerdings wäre es nicht mit dem Datenschutz vereinbar, wenn daraus die Konsequenz gezogen würde, nun jede Aktivität von Mitarbeitern und Mitarbeiterinnen im Netzwerk oder auf einem dienstlichen Einzelplatz-PC in systemseitigen Protokolldateien zu erfassen.

Das Misstrauen von Mitarbeitern, hinsichtlich ihrer Arbeit bzw. ihrer Arbeitsergebnisse vom System beobachtet zu werden ist teilweise erheblich, ob zu Recht oder zu Unrecht. Hier sollte eine Dienststellenleitung aus eigenem Interesse mit offenen Karten spielen.

Der erste Schritt dazu ist, dass das Risiko, gegen das man sich mit erweiterten Protokollierungen schützen will, genau benannt wird. Der zweite Schritt, dass die Möglichkeiten, nicht personenbezogen zu protokollieren, so weit wie möglich genutzt wird.

Gibt es beispielsweise Anlass zur Vermutung, dass Internetzugänge dazu missbraucht werden, Pornoseiten herunter zu laden, muss sich das Ziel der erweiterten Protokollierung darauf beschränken, genau dies zu verhindern. Dazu würde es zunächst genügen, temporär mitzuprotokollieren, ob solche Seiten aufgerufen werden, allerdings ohne im Protokoll zu erfassen, von welchem Rechnern im Netzwerk die Aufrufe ausgingen. Ergibt dann eine stichprobenartige Auswertung tatsächlich, dass unerwünschte Aufrufe von Internetseiten stattfinden, könnte die Mitarbeiterschaft darüber informiert und die Unterlassung gefordert werden. Ergibt eine Nachkontrolle, dass dies weiterhin geschieht, könnte angekündigt werden, dass nun auch protokolliert wird, von welchen Rechnern aus die Aufrufe stattfinden.

In diesem Zusammenhang sei darauf verwiesen, dass nach einem Urteil des Bundesarbeitsgerichts jemand, der während der Arbeitszeit auf Pornoseiten im Internet surft, mit der fristlosen Kündigung rechnen muss, es bedarf nicht unbedingt einer vorherigen Abmahnung. Für die Beurteilung, ob in einem konkreten Fall tatsächlich fristlos gekündigt werden kann, spielt auch eine Rolle, ob ein Imageverlust des Arbeitgebers zu gegenwärtigen ist, was bei kirchlichen Einrichtungen wohl immer der Fall ist. Allerdings wird für die Beurteilung, ob eine fristlos Kündigung angemessen ist, auch eine Rolle spielen, in welchem Umfang während der Arbeitszeit unzulässigerweise im Internet gesurft wurde. Das kann man aber nur anhand von Protokollen nachweisen, so dass in der Praxis trotz der Klarstellung des Bundesarbeitsgerichts wie oben vorgeschlagen verfahren werden sollte.

Tritt zu irgendeinem Zeitpunkt die Situation ein, dass bestimmte Aktivitäten an einem PC gerichtsverwertbar dokumentiert werden müssen, sollte rechtzeitig der Rat einer kundigen Person eingeholt und umgehend und professionell gehandelt werden.

### 4.9 Kennwörter

Der Systemadministrator einer größeren kirchlichen Stelle wollte es einmal genauer wissen und sah nach, ob denn wie verlangt das anfänglich vergebene Initialkennwort „123“ auch tatsächlich geändert wurde. Das Ergebnis war erschreckend aber eigentlich nicht verwunderlich: Nur etwa die Hälfte war dieser Aufforderung tatsächlich nachgekommen. Ich selbst hatte vor einiger Zeit einmal die Lücke genutzt und mir im Zusammenhang mit der Einführung einer neuen Software ebenfalls angesehen, was denn so alles als Kennwort dient. Ein guter Teil war von der Kategorie „Vorname“, was auch nicht viel besser als „123“ ist. Bei Besuchen von kirchlichen Stellen konnte mit einer gewissen Häufigkeit für Kirchenpfleger „Kipfl“ als Kennwort festgestellt werden. Dieses Problem scheint sich mit einer erstaunlichen Zähigkeit zu halten, auch die Landesdatenschutzbeauftragten kommen nicht umhin, diesen Blick in die informationstechnische Steinzeit immer wieder zum Thema zu machen. Im Datenschutzweb stehen im Praxisteil unter Allgemeines auch Hinweise, wie man zu akzeptablen Kennwörtern kommt, schwierig ist das nicht.

Zweierlei erscheint in diesem Zusammenhang wichtig: Besteht eine Benutzeranmeldung, ist auch mit einer mehr oder weniger umfangreichen Protokollierung dessen zu rechnen, was eine Benutzerin oder ein Benutzer tut. Weiß man das Kennwort einer anderen Person, kann man unter deren Namen agieren. Kommt es zu Schwierigkeiten, wird zunächst diese zur Rechenschaft gezogen. Diese wird sich dem mit dem Hinweis zu entziehen suchen, dass sie wohl etwas schludrig mit dem Kennwort war<sup>1</sup>, aber mit den Schwierigkeiten

---

<sup>1</sup>Der Fall, dass das Kennwort eines Kollegen oder einer Kollegin mit Hilfe von Soft-

nichts zu tun hat. Damit war es dann Herr oder Frau Niemand, wenn nicht aufgrund anderer Umstände auf eine bestimmte Person geschlossen werden kann.

Unter solchen Umständen kann aber der Datenschutz nicht mehr gewährleistet werden, es liegt ein Organisationsversagen der Stellenleitung vor. Der Datenschutz verlangt nämlich, dass jederzeit festgestellt werden kann, wer welche Einträge oder Änderungen an einem bestehenden Datenbestand vornimmt.

Dazu vielleicht folgende Auszüge aus dem Urteil eines Landesarbeitsgerichts (AG Köln, 15.12.2003 - 2 Sa 816/03 -): *Die Klägerin verkennt, dass die Ausgabe eines Passworts durch den Arbeitgeber nicht dazu dient, der Arbeitnehmerin eine private „Ecke“ der arbeitgeberseitigen Computeranlage zur Verfügung zu stellen. Vielmehr sind die Passworte erforderlich, um einzelne Eingaben den jeweiligen Sachbearbeitern mit Computerzugang zuordnen zu können. Gäbe es Passworte nicht, so könnten böswillige Arbeitnehmer unerkannt Daten ihrer Kollegen löschen, um diesen Schaden zuzufügen. Unsorgfältig oder langsam arbeitende Arbeitnehmer könnten behaupten, sie hätten die Daten bereits eingegeben gehabt und diese seien durch Dritte gelöscht worden. Passworte dienen damit der Zuordnung von Arbeitsergebnissen und der Sicherung von Arbeitsergebnissen. Allein zu diesem Zwecke, also zum Schutz der redlichen Arbeitnehmer müssen sie vergeben werden.*

Man mag sich fragen, wie denn Administratoren feststellen können, dass bestimmte Kennworte nicht geändert wurden: sind diesen vielleicht alle Kennworte bekannt? Ein solches EDV-System wäre umgehend zu beanstanden. Stand der Technik ist, dass Kennworte einwegverschlüsselt abgespeichert werden. Es ist nicht möglich, anhand des Ergebnisses der Einwegverschlüsselung auf das Kennwort zu schließen. Bei einer Benutzeranmeldung werden die Ergebnisse der Einwegverschlüsselung verglichen und müssen übereinstimmen, nicht die Kennworte. Ein Administrator kann aber hergehen, einen Testbenutzer anlegen, diesem das Kennwort „123“ geben und dann prüfen, wie oft das Ergebnis einer Einwegverschlüsselung von „123“ sonst noch im System geführt wird. Insoweit kann er dann feststellen, wie viele Benutzer ein bestimmtes Kennwort haben, ohne alle Kennworte zu kennen. Dieses Verfahren funktioniert allerdings nur bei bestimmten Systemen. Speichert das System etwa Benutzernamen und Kennwort zusammen verschlüsselt in einer nicht ohne weiteres zugänglichen Datenbank ab, wird eine solche Kontrolle schon schwieriger.

Moderne Systeme bieten durchweg die Option, dass ein vergebenes Initialkennwort automatisch geändert werden muss, d.h. den Benutzern wird der Zugang zum System erst freigeschaltet, wenn sie dieses Kennwort ersetzt ha-

---

oder Hardware ausgespäht wurde, ist mir noch nicht untergekommen. Allerdings wurde mir erst kürzlich auch im Bereich der Landeskirche ein Fall bekannt, wo ein durch Kennwort geschützter Programmteil mit Hilfe frei erhältlicher Hacker-Software geknackt wurde.

ben. Dies kann man heute als Stand der Technik voraussetzen. Des Weiteren können Kennworte mit einer bestimmten Lebensdauer versehen werden, sie müssen dann nach Ablauf dieser Frist von den Benutzern geändert werden. Ein solches System merkt auch, wenn ein Benutzer meint, sich dem dadurch entziehen zu können, indem er ständig zwischen zwei Kennworten hin und her wechselt oder wenn er Trivialkennwörter verwenden will. Auch dies ist Stand der Technik. Man kann solche Mechanismen aktivieren oder nicht. Das immer wieder feststellbare faktische Benutzerverhalten zeigt, dass sie aktiviert werden müssen, ansonsten liegt wiederum ein Organisationsversagen der Stelle vor.

Ein weiterer Missstand bei der Verwendung von Kennwörtern ist die Unsitte, Vertretungen dadurch zu regeln, dass man diese mitteilt. Damit wird es zweifelhaft, wer was an dem edv-System gemacht hat, die eine oder die andere Person, und dies ist datenschutzrechtlich unzulässig. Grundsätzlich muss vielmehr so verfahren werden, dass die für die Systembetreuung zuständige Person kontaktiert und um Zuteilung der entsprechenden Berechtigungen gebeten wird, um den Vertretungsaufgaben nachkommen zu können. Das Vorhalten einer solchen Möglichkeit gehört zum originären Betrieb einer EDV-Anlage und muss organisatorisch gewährleistet werden.

# Kapitel 5

## Sonstiges

### 5.1 Künftige Entwicklungen

Welche für die Kirchen besonders relevanten Entwicklungen im Bereich Datenschutz sind in absehbarer Zeit zu erwarten? Dies dürften im Wesentlichen sein:

#### 5.1.1 Arbeitnehmerdatenschutzgesetz:

Auf den Bedarf einer Schaffung eines bereichsspezifischen Arbeitnehmerdatenschutzgesetzes weisen die Datenschutzbeauftragten von Bund und Land immer dringender hin. Dabei geht es darum, dass in Arbeitsverhältnissen Grundsätze berücksichtigt werden, die sich im Datenschutzrecht bereits bewährt haben:

- Die Datenerhebung hätte danach grundsätzlich beim Arbeitnehmer selbst erfolgen; Ausnahmen wären gesetzlich zu regeln.
- Regelungen über die Einwilligung eines Arbeitnehmers oder eines Bewerbers in eine Datenerhebung würden nur dann als Grundlage einer Datenerhebung, -verarbeitung oder -nutzung akzeptiert, wenn ihre Freiwilligkeit sichergestellt ist. Die Einwilligung könnte demgemäß ohne Furcht vor Nachteilen auch verweigert werden. Desgleichen wäre es nicht mehr möglich, allein aufgrund einer Einwilligung Gesundheitszeugnisse, Ergebnisse von Genomanalysen oder ähnliche Unterlagen zu verlangen, wenn sie den Rahmen des Befragungsrechts des Arbeitgebers überschreiten.
- Die strikte Zweckbindung der erhobenen Daten wäre gesetzlich verankert. Personenbezogene Arbeitnehmerdaten dürften nur für den Zweck, für den sie erhoben worden sind, verwendet werden. Daten, die für diesen Zweck nicht mehr erforderlich sind, wären zu löschen.

- Die Schaffung von Persönlichkeitsprofilen der Arbeitnehmer wäre grundsätzlich verboten.
- Aus Gründen der Transparenz wären Arbeitnehmer umfassend darüber zu informieren, welche Daten zu welcher Zeit, auf welche Weise und zu welchem Zweck über sie erhoben sowie in welcher Art und Weise ausgewertet werden. Dies würde umfassende Auskunfts- und Einsichtsrechte des Arbeitnehmers einschließen.
- Die Mitbestimmungsrechte von Betriebs- und Personalräten bei der Einführung, Anwendung und bei wesentlichen Änderungen automatisierter Dateien mit personenbezogenen Daten für Zwecke der Personalverwaltung würden gestärkt werden.
- Das Gesetz würde auch Regelungen zur Nutzung von E-Mail und Internetdiensten am Arbeitsplatz enthalten.

Solchen Anliegen werden sich auch die Kirchen bei ihren Beschäftigungsverhältnissen nicht verschließen können. Allerdings darf festgestellt werden, dass § 24 DSGVO Bestimmungen zum Umgang mit Daten bei Dienst- und Arbeitsverhältnissen enthält, die einen Teil der Anforderungen bereits abdecken, allerdings nicht in dem Umfang, wie es ein Arbeitnehmerdatenschutzgesetz vorsehen würde. Möglicherweise würde für die evangelischen Kirchen eine Novellierung ihres Datenschutzgesetzes genügen, falls ein Arbeitnehmerdatenschutzgesetz in Deutschland geltendes Recht wird.

### 5.1.2 Informationszugangsgesetz

Am 03.06.2005 hat der Bundestag beschlossen, ein Informationsfreiheitsgesetz (IFG) auf Bundesebene einzuführen. *Als einer der letzten Staaten in der Europäischen Union hat Deutschland endlich diese Reform gewagt und damit den obrigkeitstaatlichen Zopf des Amtsgeheimnisses abgeschnitten*, kommentierte der DJV-Vorsitzende Michael Konken die Entscheidung (Deutscher Journalisten Verband). *Wir sind erleichtert, dass dieses wichtige Transparenzgesetz in der laufenden Legislaturperiode noch verabschiedet worden ist*. In einigen Bundesländern sind solche Akteneinsichts- und Informationszugangsgesetze mit dem Ziel einer gesetzlichen Verankerung eines Rechts auf einen allgemeinen, voraussetzungslosen Zugang zu Informationen der öffentlichen Verwaltung bereits Realität. Worum geht es dabei im Kern? Nicht mehr die Interessenten sollen begründen müssen, warum sie welche Informationen bekommen wollen, sondern die Verwaltungen müssen darlegen, warum sie bestimmte Informationen nicht zur Verfügung stellen (z.B. weil Datenschutzbestimmungen entgegenstehen). Den von manchen befürchtete Ansturm von Querulanten, die nun auf einmal alles mögliche wissen wollten, hat es nach bisherigen Erfahrungen nicht gegeben, vielmehr wurde von dem Recht nur sparsam aber sinnvoll Gebrauch gemacht.

Der folgende Auszug der Empfehlung Rec (2002) 2 des Ministerausschusses an die Mitgliedstaaten zum Zugang zu amtlichen Dokumenten fasst den Zweck zusammen:

...

in der Erwägung der Bedeutung der Transparenz der öffentlichen Verwaltung und der leichten Verfügbarkeit von Informationen von öffentlichem Interesse in einer pluralistischen, demokratischen Gesellschaft;

in der Erwägung, dass ein weitgehender Zugang zu amtlichen Dokumenten, auf der Grundlage der Gleichbehandlung und in Übereinstimmung mit klaren Regeln:

- die Bürgerinnen und Bürger in die Lage versetzt, den Zustand der Gesellschaft, in der sie leben, und die Behörden, die sie regieren, angemessen zu beurteilen oder sich eine kritische Meinung über sie zu bilden;

- die Effizienz und Effektivität der Verwaltungen erhöht und die Aufrechterhaltung ihrer Integrität durch die Vermeidung des Korruptionsrisikos unterstützt;

- zur Bestätigung der Legitimität von Regierungen als öffentlicher Dienstleister und zur Stärkung des Vertrauens der Öffentlichkeit in die öffentliche Verwaltung beiträgt

in der Erwägung, dass deshalb die größte Anstrengung von den Mitgliedstaaten unternommen werden sollte, um die Verfügbarkeit von Informationen in amtlichen Dokumenten für die Öffentlichkeit zu gewährleisten, unter der Voraussetzung, dass andere Rechte und berechnigte Interessen geschützt werden;

...

Es ist meiner Auffassung nach auch für die Kirchen eine Überlegung wert, ob solche Erwägungen nicht auch in ihrem Bereich positive und wünschenswerte Effekte haben könnten. Nach außen würden sie das Image der Transparenz erwerben, nach innen würde man wohl einiges rationeller machen, wenn beim Speichern in Akten oder Dateien ein mögliches Auskunftersuchen immer mitbedacht werden muss.



## Kapitel 6

# Anlage: Kirchlicher Datenschutz - Warum?

### 6.1 Vorbemerkung

Diese Anlage enthält die Abschnitte

- Das Bundesverfassungsgericht - die Kernsätze
- Beweggründe des kirchlichen Datenschutzes
- Überlegungen zur Eigenständigkeit des kirchlichen Datenschutzes

Kirche und Staat sind darauf angewiesen, dass möglichst viele derjenigen, die mit den Daten anderer umgehen, die Datenschutzgrundsätze aus eigenem Antrieb und eigener Einsicht befolgen (was Immanuel Kant dann „Moralität“ nennt). Dies löst unweigerlich die Frage nach dem *Warum?* aus. Der schlichte Verweis auf Verfassungsgericht oder EKD-Synode genügt in einer alles hinterfragenden Gesellschaft nicht mehr. Das es nicht rein *akademische* Fragestellungen sind wird spätestens dann klar, wenn hinterfragt wird, mit welcher Begründung etwa im Bereich der Diakonie das kirchliche Datenschutzgesetz gilt.

Die nachfolgenden Abschnitte enthalten deshalb zunächst Kernsätze aus dem Volkszählungsurteil des Bundesverfassungsgerichts, die nach wie vor richtungweisend sind und recht klar umschreiben, was Datenschutz ist. Daran schließt sich ein Abschnitt an, wo versucht wird, mögliche Zusammenhänge von christlichem Menschenbild und Datenschutzes aufzuzeigen. Der dann folgende Abschnitt setzt sich mit der Frage auseinander, inwieweit die Kirche tatsächlich befugt ist, ihren Datenschutz selbst zu regeln.

Zweck dieser Anlage ist, die bei der Frage nach dem *Warum?* sich bislang zeigenden maßgebenden Denkstrukturen übersichtlich zu versammeln und damit einen Ort zu schaffen, auf den bei solchen Fragen verwiesen werden kann.

## 6.2 Das Bundesverfassungsgericht - die Kernsätze

Die nachfolgenden Auszüge aus dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 (auch *Bergpredigt des Datenschutzes* genannt) formulieren, wofür *Datenschutz* steht:

*Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt. Ihrem Schutz dient - neben speziellen Freiheitsverbürgungen - das in Art 2 Abs. 1 in Verbindung mit Art 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeitsrecht, das gerade auch im Blick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen der menschlichen Persönlichkeit Bedeutung gewinnen kann (vgl. BVerfGE 54, 148 [153]).*

*Es umfasst ... auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.*

*Diese Befugnis bedarf unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes. Sie ist vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muss, vielmehr heute mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmaren Person (personenbezogene Daten (vgl. § 2 Abs. 1 BDSG)) technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Sie können darüber hinaus - vor allem beim Aufbau integrierter Informationssysteme - mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekanntem Weise die Möglichkeiten einer Einsichtnahme und Einflussnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen.*

...

*Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.*

...

*Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art 2 Abs. 1 in Verbindung mit Art 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die*

*Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.*

...

*Angesichts der bereits dargelegten Gefährdungen durch die Nutzung der automatischen Datenverarbeitung hat der Gesetzgeber mehr als früher auch organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.*

...

*Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses“ Datum mehr. Wieweit Informationen sensibel sind, kann hiernach nicht allein davon abhängen, ob sie intime Vorgänge betreffen. Vielmehr bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs: Erst wenn Klarheit darüber besteht, zu welchem Zweck Angaben verlangt werden und welche Verknüpfungsmöglichkeiten und Verwendungsmöglichkeiten bestehen, lässt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten.*

...

*b) Dieses Recht auf informationelle Selbstbestimmung ist nicht schrankenlos gewährleistet. Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über „seine“ Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann. Das Grundgesetz hat, wie in der Rechtsprechung des Bundesverfassungsgerichts mehrfach hervorgehoben ist, die Spannung Individuum - Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden (BVerfGE 4, 7 [15]; 8, 274 [329]; 27, 1 [7]; 27, 344 [351 f.]; 33, 303 [334]; 50, 290 [353]; 56, 37 [49]). Grundsätzlich muß daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen.*

...

*Ein überwiegendes Allgemeininteresse wird regelmäßig überhaupt nur an Daten mit Sozialbezug bestehen unter Ausschluss unzumutbarer intimer Angaben und von Selbstbezeichnungen. Nach dem bisherigen Erkenntnisstand und Erfahrungsstand erscheinen vor allem folgende Maßnahmen bedeutsam: Ein Zwang zur Angabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbareren Zwecken nicht zu vereinbaren. Auch werden sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum*

*beschränken müssen. Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt. Schon angesichts der Gefahren der automatischen Datenverarbeitung ist ein - amtshilfefester - Schutz gegen Zweckentfremdung durch Weitergabeverbote und Verwertungsverbote erforderlich. Als weitere verfahrensrechtliche Schutzvorkehrungen sind Aufklärungspflichten, Auskunftspflichten und Löschungspflichten wesentlich. Wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatischen Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen ist die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung.*

### 6.2.1 Ergänzende Anmerkungen

Dass diese damals richtungweisenden Feststellungen des Bundesverfassungsgerichts mittlerweile auch europäischer Standard sind, zeigt die CHARTA DER GRUNDRECHTE DER EUROPÄISCHEN UNION (2000/C 364/01, proklamiert in Nizza am 07. Dezember 2000, letzte Änderung am 02.08.2001):

Artikel 8 [Schutz personenbezogener Daten]

- (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
- (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
- (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Richtungweisend ist auch nach wie vor die EU-Richtlinie zum Datenschutz, die durch die Novellierung des Bundesdatenschutzgesetzes in nationales Recht umgesetzt und seitens der evangelischen Landeskirchen durch eine Novellierung des Datenschutzgesetzes der Evangelischen Kirche in Deutschland nachvollzogen wurde.

In einigen Landesdatenschutzgesetzen wird direkt die Bewahrung der informationellen Selbstbestimmung und nicht der Schutz des Persönlichkeitsrechts als Zweck des Datenschutzgesetzes genannt. So lautet etwa § 1 des sächsischen Datenschutzgesetzes: *Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er im Freistaat Sachsen durch Behörden und*

*sonstige öffentliche Stellen bei der Verarbeitung personenbezogener Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird.*

Das Bundesverfassungsgericht hat mit der Entwicklung des Begriffs des informationellen Selbstbestimmungsrechts die Vorstellung aufgegeben, dass man zwischen einer Intimsphäre als unantastbarem Bereich privater Lebensgestaltung und einem Verhalten in der gesellschaftlichen Sphäre unterscheiden könne. Eine solche Differenzierung erschien deshalb als nicht möglich, weil jedes noch so belanglose Datum in einem bestimmten Zusammenhang hoch sensibel werden kann. Auch unter diesem Gesichtspunkt erscheint dann eine umfassende Selbstbestimmung über die Verwendung der eigenen Daten als unumgänglich. Der Einzelne soll nicht immer warten müssen, bis der Gesetzgeber auf in bestimmten Zusammenhängen sensibel gewordene Daten reagiert (und dies wird in einer komplexen Gesellschaft unüberschaubar oft vorkommen), und bis dahin die sein Persönlichkeitsrecht beeinträchtigende Datenverwendung hinnehmen müssen. Unter der Voraussetzung der Selbstbestimmung kehrt sich dieses Verhältnis um. Nun muss der Gesetzgeber reagieren, wenn er meint, ein Allgemeininteresse wahrzunehmen, das diesem Recht auf informationelle Selbstbestimmung vorgeht. Mehr wäre wohl auch schlichtweg nicht leistbar.

### 6.3 Beweggründe des kirchlichen Datenschutzes

*A man convinced against his will is of the same opinion still* (Jemand, der von einer Sache nicht wirklich überzeugt wurde, hängt faktisch immer noch seiner alten Meinung an). Der Datenschutz wird im kirchlichen Bereich immer noch viel zu oft als etwas von außen über gestülptes wahrgenommen oder grundsätzlich in Frage gestellt. So stellte etwa der Oberkirchenrat einer Landeskirche in einer Stellungnahme fest, dass *die Regelung des Datenschutzes im innerkirchlichen Bereich weniger einem kirchlichen Anliegen (...) entspricht, als vielmehr einer 'Auflage' des § 17 des Entwurfs eines Bundesmeldegesetzes und des Entwurfs eines Bundesdatenschutzgesetzes, welche die Datenübermittlung an Stellen der öffentlich-rechtlichen Religionsgesellschaften davon abhängig machen, dass diese ausreichende Datenschutzmaßnahmen getroffen haben.*

Zur Abwehrreaktion gesellt sich dann schnell inhaltliche Kritik:

*Kirchliche Daten seien viel zu harmlos, als dass ein nennenswertes Risiko für die Betroffenen bestünde, der Datenschutz würde den Betroffenen letztlich nur schaden, da er die Vereinzeltendenzen fördere und Hilfe und Zuwendung erschwere, die Kirchen würden sich angesichts des Rückgangs ihrer Gemeindegliederzahlen hüten, irgend jemanden in seiner Persönlichkeitsentwicklung zu verunsichern, ein Pochen auf ein Recht, und sei es das, selbst über seine Daten zu bestimmen, sei etwas dem Wesen der Kirche völlig fremdes, Datenschutz brems die Effizienz im Verwaltungshandeln, Datenschutz*

*untergräbt das Ehrenamt, ...*

Bleibende Erinnerung ist mir das vertrauliche Eingeständnis eines Kollegen, dass er sich schon nicht mehr traue, gegenüber der Kirchenleitung etwas für den Datenschutz zu verlangen.

Hinter den vorgebrachten Argumenten steht meiner Wahrnehmung nach ein mehr oder weniger eingestandener Unmut darüber, nicht mehr ungestört nach eigenem *gut gemeinten?! Gutdünken* agieren zu können, sondern Betroffene fragen zu müssen oder allgemein gefasste Beschlüsse (Rechtsgrundlagen) zu benötigen. Vielen Kirchenmitgliedern ist die Vorstellung, dass es zunächst die Betroffenen sind, die über die Verwendung ihrer Daten bestimmen, nach wie vor fremd.

Mit dem Verweis auf das Recht können sich Datenschutzbeauftragte in konkreten Streitfällen vielleicht hin und wieder durchsetzen, überzeugen tut man so wohl nur bedingt. Der Hinweis, dass die Kirchen Datenschutz betreiben müssen, weil der Staat eben Datenschutz betreibt und sie sonst Gefahr laufen, keine Meldedaten mehr zu bekommen mag ein Druckmittel sein, motiviert und überzeugt aber nicht. Auch das Argument, dass die Kirchen überhaupt nur deshalb nicht dem Bundesdatenschutzgesetz unterliegen, weil die Verfassung ihnen ein *Selbstbestimmungsrecht* garantiert und es wohl etwas widersprüchlich wäre, würden sie ihrerseits ihren Gemeindegliedern eben ein solches Selbstbestimmungsrecht verweigern, erreicht nur unwirksam die logische Sphäre aber nicht die Beweggründe.

Wirklichen Datenschutz gibt es jedoch nur, wenn hinreichend viele davon auch überzeugt sind. Die Datenschutzbeauftragten können im Rahmen ihrer Möglichkeiten die Legalität von Datenverwendungen überprüfen und einfordern, haben aber nicht die Machtmittel (und wollen sie auch nicht haben, schon gar nicht in der Kirche), diese allumfassend *durchzusetzen*. Sie können nur erfolgreich tätig sein, wenn von hinreichend vielen Personen verstanden wird, um was es dem Datenschutz geht, und wenn sie dessen Anliegen innerlich als eine Art *Ethik der Informationsgesellschaft* akzeptieren. In der Hoffnung, damit das eine oder andere Kirchenmitglied, vielleicht sogar den einen oder anderen Theologen oder die eine oder andere Theologin zum Nachdenken anzuregen, hier einige rhapsodistisch zusammengestellte Gedankengänge:

**Umgang mit Macht:** Das menschliche Spezifikum *Machtrieb* kann abstrakt verstanden werden als der Trieb, Mitteln für freigehaltene Zwecke zu akkumulieren, etwa Gefolgschaft, Vorräte, Waffen oder eben auch Wissen. Dies ist wesensmäßig etwas ganz anderes als Herrschaft oder Führung, auch wenn in vielen Fällen die angehäuften Mittel zum Zweck der Herrschaft von Menschen über Menschen eingesetzt werden. Einer der zentralen Grundsätze aller Datenschutzgesetze ist, dass Daten nur für bestimmte Zwecke verwendet werden dürfen (Zweckbindungsgrundsatz). Die geistigen Väter des Bundesdatenschutzgesetzes

und die Verfassungsrichter haben hier scharf gesehen und genau getroffen. Wie verhindert man in der aufgehenden Informationsgesellschaft die sich abzeichnenden Machtpotentiale, die durch das immer leichter werdende unbegrenzte Sammeln und Verknüpfen von Informationen, insbesondere über Personen, zwangsläufig entstehen. Wie verhindert man, dass sich die Gesellschaft in solche, die über Informationsmacht verfügen, und solche, die als Datenobjekte nur noch Opfer oder Betroffene sind, aufspaltet. Es war dann konsequent, dieser Besorgnis im Rahmen des Grundgesetzes durch eine Rückführung auf das Persönlichkeitsrecht und dessen Gefährdung eine konkrete Gestalt zu geben. Der alte Satz *Wissen ist Macht* kann man heute auch als *Information ist Macht* schreiben, setzt man sich naturwissenschaftlich und philosophisch mit dem auseinander, was *Information* eigentlich ist. Es stellt sich dann als Christ die Frage, ob Macht (im oben genannten Sinne) als *an sich böse* zu beurteilen ist bzw. ob *Macht an sich* nicht als höchst bedenklich angesehen werden muss. Verantwortung bedeutet dann, den Gebrauch der Macht durch die Erkenntnis der Folgen des Gebrauchs dieser Macht zu begrenzen. Dass man nicht einfach vom *guten Menschen* ausgehen kann, zeigt auch der Satz von Paulus: *Denn das Gute, das ich will, das tue ich nicht; sondern das Böse, das ich nicht will, das tue ich (Römer 7,19)*<sup>1</sup>. Dass alle Technik machtförmig ist, lässt sich nicht bezweifeln. Sie ist Macht über die Natur, immer auch über Menschen, letzteres als Informationstechnik in besonderem Maße. Hieße dann Nachfolge Christi konsequenterweise nicht auch Wachsamkeit und kritischen Abstand gegenüber Macht? Wäre dann kirchlicher Datenschutz nichts anderes als schlichte Wahrnehmung christlicher Verantwortung in der Informationsgesellschaft?

**Big Brother:** Datenschutz wird gelegentlich als Abwehr der Orwells'schen Vision 1984 verstanden (Big Brother). Dieser Roman schildert eine Wirklichkeit, die im Christentum vielleicht unter dem Begriff des Antichristen gefasst wird. C.F. von Weizsäcker schreibt dazu (Die Geschichte der Natur, S. 125 ff): *Die christliche Liebe ist zwar eine Zuwendung zum Menschen, wie es sie vorher nicht gegeben hat. Diese Zuwendung will sie sein. Sie schafft aber zugleich eine Distanz zum instinktgebundenen Mitmenschen, wie es sie auch vorher nicht gegeben hat. Diese Distanz will sie nicht, aber sie kann sie nicht vermeiden. Die instinktive Liebe und der instinktive Hass sind gleichermaßen blind an ihren*

---

<sup>1</sup>Allerdings wäre eine theologische Polemik gegen grenzenloses Machtstreben, das real wohl allenfalls in psychisch gestörten Einzelpersonen existiert, wohl zu einfach. Machtkonkurrenz ist zunächst Kampf um knappe Güter, in der Gesellschaft oder zwischen Gesellschaften, Machtstreben ist so gesehen vor allem Sicherheitsbedürfnis. Es ist nahe liegend, den unbegrenzten Machtdrang von Menschen als den Versuch zu werten, allmächtig wie Gott zu sein, ohne zugleich gut wie Gott zu sein. Aber erst die Folgerungen, die aus dieser Feststellung gezogen werden, zeigen auf, ob diese Deutung einen Wert hat oder nicht.

*Partner gebunden. Die christliche Liebe sieht den anderen Menschen und ist ihm gegenüber eben deshalb frei. Fast jeder von uns hat aber einen Punkt, an dem er noch lieber blind gehasst als durchschaut sein möchte. Die sehende Liebe stellt den Menschen, den sie sieht, durch ihre bloße Gegenwart vor eine Entscheidung. Deshalb trifft sie, wo sie nicht wieder Liebe wecken kann, auf Widerstand. Dieser Widerstand ist solange schwächer als die Liebe selbst, als er blind mit den Waffen der instinktiven Natur kämpft. So hat das Christentum einen großen Teil der Welt erobert, freilich nicht, ohne an vielen Stellen sein Wesen preiszugeben. Der Widerstand aber wird der christlichen Liebe gewachsen, ja überlegen, wo er die Waffe der Erkenntnis von ihr übernimmt und bedenkenloser als sie führt. Christus ermöglicht den Antichrist. Scheinbar neutral in diesem Kampf, aber erst durch ihn ermöglicht, ist das rationale Denken der Neuzeit. Ich glaube, dass die Distanz, die in seinem Denkschema zwischen Subjekt und Objekt besteht, ein unmittelbares Erbe der christlichen Distanz von der Welt ist. Der eigentliche Christ steht als Ich dem Du frei gegenüber. Er sieht den Mitmenschen und liebt ihn in dieser sehenden Freiheit. Wenn aus dieser Haltung die Liebe fortfällt, aber die Erkenntnis bleibt, so wird der andere nicht mehr als Subjekt angesprochen. Diese Haltung kann alles in unbeteiligter Freiheit untersuchen. Nun steht das Subjekt dem Objekt gegenüber.*

...

Vielleicht war es das, was George Orwell literarisch verarbeiten wollte. Es ist ein zentrales Anliegen des Datenschutzes, dass Menschen ihre Stellung als Subjekte behalten und nicht zu Datenobjekten werden. Das auch hinter der Informationstechnik stehende rationale Denken der Neuzeit könnte sich hier als besonders gefährlich erweisen. Deshalb sah wohl auch das Bundesverfassungsgericht in der „informationelle Gewaltenteilung“ das entscheidende „Unterpfand“ für den dauerhaften Erhalt unserer Demokratie; es ist nicht schwer, sich auszumalen, was uns blühen würde, wenn Gruppen machtbewusster aber gewissenloser Menschen maßgebliche Verfügung über Informationstechnik bekämen. Glaubt man den obigen Ausführungen Weizsäckers, ginge es unterschwellig allerdings um weit mehr als um das Überleben einer bestimmten Staatsform; der Datenschutz wäre dann lediglich eine der vielen Gelegenheiten, wo ein tiefer gehender Konflikt deutlicher wahrnehmbar wird. Die Frage nach Wert und Stellung des Subjekts erweist sich immer mehr als die zentrale Frage der technischen Welt. Der Datenschutz leistet hierzu einen wesentlichen Beitrag, indem er Verhältnisse durchsetzen will, wo die Menschen möglichst weitgehend selbst über die Verwendung ihrer Daten bestimmen.

**Glaubwürdigkeit:** Gibt man den Begriff „Informationstechnik“ im Internetauftritt der Landeskirche ein, erhält man die Mitteilung „Kein Er-

gebnis“. Gibt man „Gentechnik“ ein, erhält man eine lange Liste. Die Kirchen sehen sich zur Recht verpflichtet, sich bei der Nutzung der Gentechnik in die gesellschaftliche Diskussion einzumischen. Bei der Gentechnik richten sich Forderungen und Kritik jedoch an andere, eine Verflechtung der Kirchen etwa mit der dahinter stehenden Wirtschaft besteht nicht. Auf die Informationstechnik jedoch haben sie sich zum Teil in erheblichem Umfang und mit erheblichen finanziellen Mitteln selbst eingelassen. Man könnte es wohl nicht ganz zu Unrecht als „Wasser predigen und selber Wein trinken“ ansehen, wollen die Kirchen bei dieser Technik dann auf einmal nichts mehr von der Wahrnehmung von Verantwortung wissen oder allenfalls von einer, die nichts kostet und keine Umstände macht. Es geht hier nicht um eine Nebensächlichkeit: Die Frage nach einer Ethik der technischen Welt wird auch an die Kirchen gerichtet, und die Antwort heißt vielleicht schlicht „Wahrnehmung der Verantwortung“. Sich davon treiben lassen, das jeweils technisch Mögliche zu tun weil es technisch möglich ist, ist untechnisch und widersinnig im Sinne vernünftiger Macht. Ohne dass ein moralischer Fortschritt wenigstens einigermaßen mithält kann dies nur in einer Katastrophe enden. Äußern sich die Kirchen hier nicht, werden sie unglaubwürdig (und verfehlen wohl auch ihren Auftrag). Äußern sie sich, wird man hinsehen, wie sie es selbst mit der Technik halten. Dabei ist es eine relativ einfache Entscheidung: Spart man in den Kirchen an den Kosten für den Datenschutz, um umso mehr EDV betreiben zu können, oder betrachtet man diesen als originären Kostenfaktor eines verantwortlichen Einsatzes von Informationstechnik und rechnet konsequenterweise von vornherein die damit verbundenen Kosten und Umstände mit ein (jemand, der Auto fährt, muss auch akzeptieren, dass damit Kosten für Steuern, Versicherung, TÜV und ASU anfallen, was alles seinen Sinn hat). Es ist durchaus denkbar, dass man in absehbarer Zeit die Kirchen nicht daran misst, mit welchem Eifer sie Informationstechnik zu nutzen wussten, sondern wie verantwortlich sie an der Gestaltung der Informationsgesellschaft mitgewirkt haben. Dabei ist anerkennend festzustellen, dass die evangelische Landeskirche Württemberg durchaus etwas für den Datenschutz getan hat und auch weiterhin tut, dazu gehört auch das besondere Engagement vieler kirchenbezirklicher Datenschutzbeauftragten.

**Verantwortung:** *Verantwortung des Menschen in der technischen Welt heißt also zum mindesten: er muss inmitten der Planung und der Apparate lernen, Mensch zu bleiben. Vielleicht muss er in entscheidenden Punkten erst lernen, Mensch zu werden. So Mensch zu werden, dass er der Herr des Plans und der Apparate bleibt. Das etwa wäre der Inhalt einer Ethik der technischen Welt (C.F.v. Weizsäcker, Die Verantwortung der Wissenschaft). Vielleicht machen diese Gedanken die Vorstellung einer*

Befugnis des einzelnen, selbst über die Verwendung seiner Daten zu bestimmen, etwas eingängiger. *Eine allgemein verbindliche Ethik des Lebens inmitten der Technik muss entwickelt werden. Man kann von den Menschen nicht verlangen, sich in der technischen Welt sinnvoll zu verhalten, wenn sie nicht Normen dieses Verhaltens haben, die den tatsächlichen Verhältnissen angepasst sind; Normen, die zwar vielleicht streng, aber für den gutwilligen Durchschnittsmenschen erfüllbar sind. Die moralische Forderung, die Straßenverkehrsordnung zu respektieren, ist ein alltägliches, der Gedanke einer Übertragung des hippokratischen Eids von der Medizin in die Technik und Naturwissenschaft ein heute noch fern liegendes Beispiel* (C.F.v.Weizsäcker, Der ungesicherte Friede). Datenschutzbestimmungen sind solche Normen, gültig für den Bereich der Informationstechnologie, zumindest wenn es um personenbezogene Daten geht. Der Gedanke einer Übertragung des hippokratischen Eides auf ihre im Bereich der Informationstechnik tätige Mitarbeiterinnen und Mitarbeiter böte für die Kirchen vielleicht sogar die Chance, nicht nur hinterher zu hinken, sondern selbst ein Zeichen zu setzen und Verantwortung zu demonstrieren. Martin Heidegger verwendet in seinem Büchlein *Die Technik und die Kehre* den Begriff eines *freien Verhältnisses* um die anzustrebende Art der Beziehung des Menschen zur Technik zu benennen. Gemeint ist damit keine völlige Ablehnung (Maschinenstürmerei) und keine naive Fortschrittsgläubigkeit. Gemeint ist auch keine Gleichgültigkeit der Technik gegenüber. Es soll ein Verhältnis sein, der Mensch soll sich darauf einlassen, aber es soll ein freies Verhältnis sein. Herauszuarbeiten, was das genau heißt, ist wohl auch für Christen eine unverzichtbare Aufgabe. Als Martin Heidegger einmal gefragt wurde, ob es denn realistisch sei, anzunehmen, die Menschen könnten, so wie sie sind, die Technik zu etwas Gutem wenden, antwortete er: *Hier hilft nur ein Gott*.

**Rechtfertigung:** Technik löst Begeisterung aus. Viele gehen ausgesprochen gerne damit um, üben mit Engagement ihren technischen Beruf aus. Andererseits ist die Technik ambivalent, sie kann viel Gutes, aber auch viel Unheil anrichten. Ist es dann, bezogen etwa auf die Informationstechnik, verantwortbar, durch Entwicklung oder Anwendung von Hard- und Software daran mitzuwirken, dass diese immer weitere gesellschaftliche Bereiche durchdringt, oder spielt man hier Russisch Roulette? Dass die Skepsis nicht nur am heute besonders deutlich wahrnehmbaren Gefährdungspotential liegt, zeigt die alte chinesische Geschichte von dem Weisen, der es ablehnt, einen Ziehbrunnen zu benutzen und stets in den Brunnen hinab stieg um Wasser zu holen: *Wer Maschinen benutzt, bekommt eine Maschinenseele*. Carl F. von Weizsäcker schildert in *Zeit und Wissen* (S. 1046) folgende Begegnung mit Karl Barth: *Ich frage ihn: Von Galilei führt ein schnurgerader Weg zur Atombom-*

*be. Darf ich die von mir geliebte Physik weiter treiben? Er: Wenn Sie glauben, was alle Christen bekennen und keiner glaubt, dass nämlich Christus wiederkommt, dann dürfen Sie, ja dann sollen Sie weiter Physik treiben. Glauben Sie es nicht, so müssen sie sofort damit aufhören.* Man wird wohl nicht annehmen können, dass dies nur für die Physik als den Kern der neuzeitlichen Naturwissenschaft gilt, die anderen Wissensgebiete wie die Informatik und die daraus folgenden Techniken jedoch davon entlastet sind, ihr Tun zu rechtfertigen. Eine Kirche, die eine solche Technik bedenkenlos nutzt, erweckt den Anschein einer bedenkenlosen Rechtfertigung und ist dafür verantwortlich. Die Nähe des Dichters Stefan George zum katholischen Christentum deutend, beschreibt Carl F. Weizsäcker dessen Wahrnehmung mit den Worten (ebenda S. 998): *Heute haben wir die Wiederkehr des Herrn zu erwarten, denn die bisherige Welt gräbt sich im Taumel ihrer technischen Macht sichtbar ihr Grab.* Es sei auch an die Euphorie zum Beginn der zivilen Nutzung der Kerntechnik erinnert, heute ist hier eher betretene Unauffälligkeit angesagt. Informations- und Gentechnik haben die Stafette übernommen, und die Informationstechnik nutzen nun auch die Kirchen. Sie müssen dann aber auch rechtfertigen, wieso sie dies trotz der erkennbaren Ambivalenz dieser Technik tun.

**Vernunft:** Immanuel Kant unterscheidet Legalität, als Handeln vor dem Gesetz, von Moralität als Handeln aus Achtung vor dem Gesetz. Das Gesetz ist hier das Gebot der Vernunft: Handle so, dass die Maxime deines Handelns jederzeit zum Prinzip einer allgemeinen Gesetzgebung werden könnte. Angewendet auf die Informationstechnik und dort auf den Bereich persönlicher Daten heißt das: Dass jede Person oder Stelle nach ihrem Gusto mit den Daten anderer macht was sie will, kann nicht Prinzip einer allgemeinen Gesetzgebung sein. *Verwende Daten anderer immer mit deren Billigung, es sei denn, du kannst auf ein geltend gemachtes Interesse der Allgemeinheit verweisen,* dagegen schon. Gerade Kirchen können es nicht einfach beim legalen Handeln bewenden lassen, sie müssen sich schon mit der Frage auseinandersetzen, ob ihre Handlungsweise eine allgemeine Richtlinie für die Allgemeinheit sein kann. Eigentlich ist es auch ihre Aufgabe, solche Richtlinien zu entwickeln.

**Fazit:** Die oben aufgeführten Überlegungen zeigen, dass eine *informationelle Selbstbestimmung* und eine *informationelle Gewaltenteilung* wohl kaum im Gegensatz zur Wahrnehmung des kirchlichen Auftrags stehen. Das dahinter stehende Anliegen ist keine Nebensächlichkeit, immerhin nennt man die kommende Art und Weise des Zusammenlebens die Informationsgesellschaft. Eine diese aktiv mitgestaltende Kirche hätte vermutlich eine gute Chance, wieder etwas mehr wahrgenommen zu

werden.

## 6.4 Überlegungen zur Eigenständigkeit des kirchlichen Datenschutzes

Der Gesetzgeber hat bei der Formulierung des Bundesdatenschutzgesetzes nicht eindeutig geregelt, ob dieses auch für kirchliche Verwendungen personenbezogener Daten gilt oder nicht. Die Kirchen haben dann ihre eigenen Datenschutzbestimmungen erlassen. Dabei gehen sie davon aus, dass der Staat sie durch *beredtes Schweigen* deshalb aus dem Bundesdatenschutzgesetz ausgenommen habe, um ihrem Selbstbestimmungsrecht gem. Art. 140 Grundgesetz i.V.m Art. 137 III Weimarer Reichsverfassung Rechnung zu tragen, das es ihnen erlaube, innerhalb der Schranken des geltenden Rechts den Datenschutz in ihrem Bereich selbst zu betreiben. Die staatliche Sicht dazu gibt bezeichnend wohl eine frühere Aussage des Vertreters des Bundesdatenschutzbeauftragten Hertel wieder: *Ich möchte mich [...] nicht festlegen. Für uns ist wichtig, dass kein datenschutzfreier Raum entsteht, dass also entweder staatliches Datenschutzrecht gilt oder dass sich nahtlos das kirchliche Datenschutzrecht daran anschließt* (in Lorenz, Datenschutz im kirchlichen Bereich, S.140).

Die Umsetzung dieser Grundsätze im Bereich der Kirchen bringt es mit sich, dass ihre Ressourcen in Anspruch genommen werden, typischerweise bezahlte Zeit, etwa von Datenschutzbeauftragten, zusätzliche EDV-Technik oder die Umgestaltung organisatorischer Umstände. Oder Mitarbeiter oder andere Personen müssen ihr Verhalten in einer bestimmten Weise ändern bzw. machen die Erfahrung, dass eine Datenverwendung gar nicht geht oder nicht so, wie sie es sich vorgestellt hatten. Einige Kirchenleitungen und Kirchenmitglieder standen dieser Entwicklung deshalb teilweise skeptisch gegenüber.

Die Herausnahme der Kirchen aus dem Regelungsbereich des Bundesdatenschutzes wurde und wird immer wieder angezweifelt. So führt ein namhafter Datenschutzkommentator zur jüngsten Rechtsprechung des Europäischen Gerichtshofs (Urteil vom 6. November 2003 - C- 101/01-) folgendes aus: *3. Für die Religionsgesellschaften ergeben sich dagegen neue Anforderungen. Laut EuGH werden 'religionsgemeinschaftliche Tätigkeiten ... von dieser Ausnahme (es geht um Art. 3 Abs. 2 erster Gedankenstrich EG-DSRL, der Rez.) nicht erfasst'. Damit steht fest: Sie fallen unter die Richtlinie. Ein wie auch immer abgesenkter Datenschutz ist nicht mehr ausreichend. Ausnahmen können nur noch gemeinschaftsrechtlich begründet werden. Die (in ihrer Reichweite schon bisher umstrittene) innere Berechtigung für innerkirchliche Datenschutzregelungen, die das (staatliche) Gesetz verdrängen (vgl. etwa Simitis-Dammann, BDSG-Kommentar, § 2 Rdnrn. 82 ff.), ist entfallen.* (in RDV 2004 Heft 1 Seite 19). Die Kirchen müssen angesichts solcher

Kommentierungen schon etwas fundierter begründen, wieso für die von ihnen verwendeten Daten nicht auch das staatliche Datenschutzrecht gilt.

Das kirchenrechtliche Institut der EKD meint dazu in einem Gutachten aus dem Jahre 1996, dass die Wurzel des kirchlichen Datenschutzrechts nicht in der Tradition der Freiheitsrechte, sondern im Beicht- und Seelsorgegeheimnis liege. Daraus wird dann ein besonderer Bedarf der Kirchen an Wissen um ihre Gemeindeglieder abgeleitet und es als übermäßige Härte angesehen, würde das Bundesdatenschutzgesetz vollumfänglich auf die kirchlichen Verhältnisse übertragen. Ein unerlässliches Minimum eines grundsätzlichen informationellen Persönlichkeitsschutzes wäre jedoch auch für die Kirchen verbindlich, dem sei die EKD durch das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland aber umfassend gerecht geworden. Sicherlich ist das Beicht- und Seelsorgegeheimnis eine wichtige Wurzel des Gedankens eines selbst bestimmten geschützten Bereichs, aber wird in dieser Formulierung nicht auch eine vielleicht nicht ganz unproblematische Abwehrhaltung deutlich? Zugespitzt könnte man dazu ja anmerken, dass ein Gemeindeglied, das mit dem kirchlich gewährten *Minimum an grundsätzlichem informationellem Persönlichkeitsschutz* nicht so ganz zufrieden ist, aus der Kirche im Gegensatz zum Staat ja austreten kann bzw. es für jemanden, der eine kirchliche oder diakonische Einrichtung in Anspruch genommen hat ja auch eine staatliche oder privatwirtschaftliche Alternative gegeben hätte. Das war mit dem genannten Gutachten so sicherlich nicht intendiert, aber gerade die Ableitung eines *besonderen Bedarfes an Wissen um die Gemeindeglieder* aus dem Beicht- und Seelsorgegeheimnis macht deutlich, dass sich diese Argumentation nur schwerlich etwa auf das Erheben von Daten einer kirchlichen Stelle zur Begründung eines Miets- oder Beschäftigungsverhältnisses ausdehnen lässt. Deutlich wird, dass die Meinungsbildung dazu sicherlich nicht als abgeschlossen angesehen werden kann.

Dass das Beichtgeheimnis nicht geeignet ist, die Eigenartigkeit des kirchlichen Datenschutzes zu begründen, wurde indes ausführlich von Ziekow dargestellt (Arne Ziekow, Datenschutz und evangelisches Kirchenrecht, Jus Ecclesiasticum 67 S. 150 ff.) Das Beichtgeheimnis schützt, sieht man einmal von der theologischen Dimension ab, ähnlich wie im weltlichen Bereich die Schweigepflicht nach § 203 Strafgesetzbuch, vor allem die Institution und nur mittelbar die Person: Ohne die absolute Wahrung des Beichtgeheimnisses würde die Beichte unglaubwürdig und die Freudigkeit der Christen zur Beichte und Absolution erschüttert (siehe ebenda S. 184). Ebenso offenbart sich jemand nur dann einem Arzt oder Psychologen, wenn er sich darauf verlassen kann, dass dieser mit seinem Wissen nicht hausieren geht. Die Wahrung von Berufs- oder Amtsgeheimnissen wurden in den Datenschutzgesetzen (Bundesdatenschutzgesetz, Landesdatenschutzgesetze) jedoch explizit als von diesen unberührt erklärt. Dem Datenschutz liegen weniger Geheimnisbrüche, sondern die Sorge vor einer nachteiligen gesellschaftlichen Entwicklung aufgrund von sich als beobachtet fühlende und dann sich als

möglichst unauffällig profilierende Personen zugrunde. Der Einzelne würde sich im gesellschaftlichen Raum nicht so entfalten, wie er ist, sondern führte ein Leben hinter Masken. Folgerichtig rekrutiert dann Ziekow auf die christlichen Wurzeln von Persönlichkeit und Menschenwürde und versucht daraus, einen Anknüpfungspunkt für den Bezug des kirchlichen Datenschutzes zum geistlichen Zentrum der Kirche zu gewinnen (siehe ebenda S. 206 ff.): Geschützt werden soll die Möglichkeit des *Sich-als-ich-Fühlens* bzw. des „Sich-seiner-selbst-bewußt-Seins“. Diese Ausführungen Ziekows sind wohl wesentlich nachvollziehbarer als eine Rückführung auf Beicht und Seelsorgegeheimnis. Allerdings schreibt Prof. Germann dazu wohl nicht ganz zu unrecht (Zeitschrift für evangelisches Kirchenrecht, Band 48 (2003) S. 474) : *Die aus der Diskussion um die rechtstheologischen Grundlagen des evangelischen Kirchenrechts angeregte Suche nach einem „eigengearteten“ Kirchenrecht mag den Versuch nahe legen, ein von den Konzepten des säkularen, staatlichen Rechts gelöstes, „genuin kirchliches“ Persönlichkeitsrecht zu konstruieren. Ein solcher Versuch wäre allerdings so voraussetzungsreich, dass er sich vor der Gefahr eines theologischen Dilettierens kaum würde bewahren können. Dogmatische Formeln wie Gottebenbildlichkeit, Schöpfungsgabe, göttliches Recht, ein „christlicher Begriff“ der Person, Persönlichkeit und Würde des Menschen lassen sich nicht aus der Dynamik und Verantwortung theologischer, insbesondere etwa exegetischer Erkenntnissuche herauslösen, als scheinbar objektive Deduktionsbasis für eine kirchenrechtliche Schutzbestimmung dienstbar machen und auf die bekannten Datenschutzmaßnahmen für das „Recht der einzelnen Person“, „selbst über die Preisgabe und Verwendung ihrer Daten zu bestimmen“, herunterrechnen.* Prof. Germann hebt dagegen (siehe ebenda S. 458) darauf ab, dass der Staat den Einzelnen auch vor einem kirchlichen Umgang mit seinen Daten schützen muss: *Des Schutzes bedarf die informationelle Selbstbestimmung auch vor dem kirchlichen Umgang mit personenbezogenen Daten. Der kirchliche Umgang mit Daten ist dabei nicht Gegenstand der grundrechtlichen Eingriffsabwehr. Die Kirchen üben keine staatliche Gewalt und sind deshalb nicht an die Grundrechte gebunden (Art. 1 III, 20 III GG). Ihre Rechtsform als Körperschaften des öffentlichen Rechts ändert daran nichts. Der kirchliche Umgang mit Daten ist stattdessen Gegenstand der Schutzpflicht-Dimension des Rechts auf informationelle Selbstbestimmung: Der Staat muss den einzelnen Betroffenen vor einem kirchlichen Umgang mit seinen Daten schützen, der seine Persönlichkeitsentfaltung zu beeinträchtigen geeignet ist. Bei diesem Schutz hat das staatliche Recht im Ergebnis einen Ausgleich zu schaffen zwischen der informationellen Selbstbestimmung des Betroffenen auf der einen Seite und dem kirchlichen Selbstbestimmungsrecht aus Art. 140 GG i. V. m. Art. 137 III 1 WRV auf der anderen Seite.*

Danach hätten die Kirchen das Recht auf informationelle Selbstbestimmung grundsätzlich zu akzeptieren und Maßnahmen zu treffen, dass es von ihren Daten verarbeitenden Stellen beachtet wird. Es ist dann nahe liegend,

das genuin kirchliche im Spektrum der vorrangigen kirchlichen Rechtsvorschriften zu sehen, die das informationelle Selbstbestimmungsrecht der einzelnen Gemeindeglieder im gesamtkirchlichen Interesse einschränken. Hier darf und muss für den kirchlichen Bereich dann das kirchliche Selbstbestimmungsrecht zum Tragen kommen. Allerdings nicht unbegrenzt: Der Staat muss die vorrangigen kirchlichen Rechtsvorschriften noch als Ausgleich zwischen dem kirchlichen Selbstbestimmungsrecht und seiner Pflicht zum Schutz der informationellen Selbstbestimmung akzeptieren können. Das Gebot der Normenklarheit und der Grundsatz der Verhältnismäßigkeit wären so auch von den vorrangigen kirchlichen Rechtsvorschriften zu verlangen. Unter Anerkennung der Befugnis der Betroffenen, grundsätzlich selbst über die Verwendung ihrer Daten zu bestimmen, ist es dann auch rechtlich unproblematisch, wenn kirchliche Einrichtungen (die unter Umständen sogar vom Staat finanziell unterstützt werden) auch Daten von Nicht-Gemeindegliedern erheben, verarbeiten und nutzen (beispielsweise Kindergärten, kirchliche oder diakonische Beratungsstellen usw.).

Das Datenschutzgesetz der evangelischen Kirchen in Deutschland (DSG-EKD) trägt diesen Überlegungen mit der in § 1 Abs. 1 DSG-EKD genannten Zweckbestimmung hinreichend Rechnung, man könnte vielleicht der vorstehend formulierten Rechtsauffassung relativ zwanglos auch dadurch Ausdruck verleihen, indem man wie viele Landesdatenschutzgesetze § 1 Abs. DSG-EKD so formulierte: *(1) Zweck dieses Kirchengesetzes ist es, den einzelnen davor zu schützen, dass er durch den kirchlichen Umgang mit seinen Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird.* Soweit vorrangige kirchliche Rechtsvorschriften dieses im kirchlichen Bereich dann im kirchlichen Gesamtinteresse einschränken, wäre dies staatlicherseits als Ausdruck kirchlicher Selbstbestimmung zu akzeptieren, so dass die Formulierung auch in ihrer Bedeutung der staatlichen analog ist.

Von diesen Überlegungen könnte man sich wohl allenfalls dann distanzieren, wenn man die kirchlichen Datenbestände personenbezogener Daten als so überschaubar und abgeschlossen betrachtet, dass deren Verwendung konkret und abschließend regelbar ist. Es bedurfte dann keiner *informationellen Selbstbestimmung* mehr im Bereich der Kirchen, weil alles geregelt ist. Die Behauptung eines überschaubaren Kernbestands an Daten ginge aber wohl deutlich an der kirchlichen Wirklichkeit vorbei, betrachtet man das ganze Spektrum kirchlicher Tätigkeit und kirchlicher Ämter und Beauftragungen; mit einer Erstreckung des kirchlichen Datenschutzrechts auf den Bereich von Diakonie (oder Caritas) wäre sie überhaupt nicht zu vereinbaren. Vor allem wäre sie in sich widersprüchlich: die kirchlicherseits beanspruchte „Kompetenz-Kompetenz“ will ja Kirche gerade nicht als ein aufzählbares Spektrum von Aufgaben und Tätigkeiten definieren, sondern die Offenheit gegenüber gesellschaftlichen Entwicklungen, neuen Wahrnehmungen und neuen Erkenntnissen offen halten. Gibt es diesen überschaubaren Kernbestand an Daten aber nicht, wird man auch nicht wieder auf die vom

Bundesverfassungsgericht aufgegebene Vorstellung von Daten, die einer Intimsphäre und solchen, die der gesellschaftlichen Sphäre angehören, zurückgehen können: jedes Datum in einem bestimmten Zusammenhang kann hoch sensibel werden. Es ist dann schlichtweg nicht zu sehen, welche überzeugende und praktikable Alternative den Kirchen verbleibt, die Sache wie beim Staat so zu regeln, dass dem einzelnen die Befugnis zugesprochen wird, selbst über die Verwendung seiner Daten zu bestimmen.

Dieses Bild würde dann durch die nachfolgenden Ausführungen von Prof. Germann vollends abgerundet (siehe ebenda): *Solange die betreffende Religionsgemeinschaft durch ihre eigenen organisatorischen Strukturen, insbesondere also die Kirchen durch kirchliche Datenschutzbeauftragte und eine kirchliche Datenschutzaufsicht ausreichende Vorkehrungen zur Verwirklichung des Datenschutzes treffen, wird Art. 140 GG i.V.m. Art. 137 III WRV das Entschließungsermessen der staatlichen Datenschutzaufsicht stets auf Null reduzieren.*

Die Reduktion des *Entschließungsermessens der staatlichen Datenschutzaufsicht auf Null* nur mittels kirchlicher Datenschutzgesetze griffe allerdings zu kurz. Papier ist bekanntlich geduldig (und billig), letztlich kommt es auf die faktische Umsetzung der Datenschutzvorschriften bei kirchlichen Stellen an. Das novellierte Bundesdatenschutzgesetz enthält eine ganze Reihe von Bußgeldbestimmungen und für schwere Verstöße auch Strafbestimmungen. Der Staat hat erkannt, dass Daten verarbeitende Stellen die informationelle Selbstbestimmung nur dann hinreichend beachten, wenn Folgen in Aussicht stehen, die die *Vorteile* einer Ignoranz nicht nur zunichte machen, sondern diese überwiegen. Die Kirchen verhängen keine Bußgelder und können nicht strafen. Kommt über diese Lücke das oben genannte *Entschließungsermessen der staatlichen Datenschutzaufsicht* dann doch wieder ins Spiel? Es bedürfe dann keiner Vertiefung dieser Fragestellung, wenn kirchliche Stellen etwa mittels Datenschutz-Audits (unter § 9a in das novellierte DSG-EKD aufgenommen) aufzeigten, was sie für den Datenschutz tun. Die konkrete Gestaltung solcher Audits, etwa der damit verbundene Aufwand, würde kirchliche Verhältnisse und Leistungsfähigkeit berücksichtigen und wäre als Ausdruck kirchlicher Selbstbestimmung zu sehen, wenngleich es sich anbietet, sich an staatlichen Standards zu orientieren. Abgesehen davon, dass dies eine beachtliche Vertrauensbasis in die kirchliche Verarbeitung personenbezogener Daten bewirken würde, wäre das im Hinblick auf die Schutzpflicht-Dimension für eine staatliche Datenschutzaufsicht sprechende Argument, dass es zwar ausreichende kirchliche Rechtsvorschriften gibt, deren Umsetzung aber wegen fehlender „Druckmittel“ nur bedingt gewährleistet wäre, vollends hinfällig. In diesem Zusammenhang wäre dann auch zu überlegen, welche praktischen Anforderungen aus der Schutzpflicht-Dimension des Staats für den kirchlichen Bereich resultieren. Neben rechtlichen Regelungen gehören dazu auf alle Fälle unabhängige Stellen, also Datenschutzbeauftragte, die als internes und externes Kontrollsystem funktionieren.

Dass sich in dem Spektrum der vorrangigen kirchlichen Rechtsbestimmungen das genuin kirchliche Leben manifestiert ist wesentlich nachvollziehbarer als eine grundsätzliche pauschale Exemption vom staatlichen Datenschutz: Eine einen solch umfassenden Anspruch begründende *Eigengeartetheit* hätte gute Chancen, sich bei einer stringent geführten Argumentation als Fata Morgana zu erweisen: was soll bei einem kirchlichen Mietsvertrag oder Beschäftigungsverhältnis unter Datenschutzgesichtspunkten anders sein als bei einem der freien Wirtschaft oder beim Staat? Die Problematik würde sich auch wohl immer weiter verschärfen, etwa wenn auf EU-Ebene ein Arbeitnehmer-Datenschutzgesetz beschlossen wird und dies national umgesetzt werden muss. Ein Bestehen auf einer pauschalen Exemption könnte dann auch den *Dritten Weg* der Kirchen, der verfassungsrechtlich so unbestritten auch nicht ist, wieder zum Thema werden lassen.

Die Gretchenfrage, *Sag Kirche, wie hältst du es mit dem Recht des Einzelnen, selbst über seine Daten zu bestimmen?*, wäre nach diesen Überlegungen zwingend mit einem *Er hat dieses Recht* zu beantworten. Manche kirchliche Amtsträger scheinen damit allerdings noch ihre Schwierigkeiten zu haben, werden ihnen die Konsequenzen in aller Deutlichkeit aufgezeigt. Nur, die Frage, wer bestimmen soll, der die Daten hat oder der, den sie betreffen, muss eben auch im kirchlichen Bereich eindeutig beantwortet sein. Die obigen Ausführungen machen dies deutlich. Aber auch Seitens der Theologie wird man es mit einem pauschalen Hinweis auf die *Dynamik und Verantwortung theologischer, insbesondere etwa exegetischer Erkenntnissuche* auf Dauer nicht bewenden lassen können. Hier ist auch die Theologie gefordert, sich am Anfang des Informationszeitalters mit der Verwendung personenbezogener Daten über das Beicht- und Seelsorgegeheimnis hinaus reflektierend auseinander zu setzen.

# Linkliste

Datenschutz, [7](#)

Persönlichkeitsschutz, [7](#)