Nichtamtliche Begründung zum Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz - DSG-EKD) in der Bekanntmachung der Neufassung vom 1. Januar 2013

Lfd.	Begründung	Datum
1	Begründung und Erläuterung zum Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz - DSG-EKD) in der Bekanntmachung der Neufassung vom 1. Januar 2013 (ABl. EKD 2013 S. 2, S. 34) Die Neufassung erfolgte auf Grund des Artikel 3 des Kirchengesetzes zur Änderung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland und zur Änderung des Kirchengerichtsgesetzes der Evangelischen Kirche in Deutschland vom 7. November 2012 (ABl. EKD 2012, S. 452) und berücksichtigt das Kirchengesetz zur Änderung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland vom 7. November 2002 (ABl. EKD 2002 S. 381) und Artkel 1 des Kirchengesetzes zur Änderung des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland und zur Änderung des Kirchengerichtsgesetzes der Evangelischen Kirche in Deutschland vom 7. November 2012 (ABl. EKD 2012, S. 452)	Stand 1. Januar 2013

Begründung und Erläuterungen zum Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz - DSG-EKD) in der Bekanntmachung der Neufassung vom 1. Januar 2013

I. Allgemeine Bemerkungen

1. Ausgangslage

Das Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD) ist eines der wenigen Gesetze, das nach Artikel 10a Absatz 1 der Grundordnung der EKD eine für alle Gliedkirchen verbindliche, einheitliche Regelung trifft. Der Geltungsbereich, der auch die kirchlichen Werke und Einrichtungen umfasst, schließt insbesondere die Diakonie mit ein, die es oftmals mit besonders sensiblen Patienten- und Sozialdaten zu tun hat.

Seit der letzten Novellierung vom 7. November 2002 (ABl.EKD 2002, S. 381) haben sich in datenschutzrechtlicher Hinsicht mehrere Novellierungsnotwendigkeiten ergeben:

- Die technische Fortentwicklung im Bereich der elektronischen Datenübermittlung hat sich auch im kirchlichen Bereich niedergeschlagen. Sie hat zu drei Novellen beim Bundesdatenschutzgesetz (BDSG) geführt, die am 1. April 2010 und am 11. Juni 2010 in Kraft getreten sind. Sie betreffen insbesondere die Rechtsgrundlagen der Datenverarbeitung und die Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten.
- Im Weiteren ist am 9. März 2010 ein Urteil des EuGH (NJW 2010 S. 1265) ergangen, dies hat eine entsprechende Fortschreibung der Datenschutzgesetze auf Bundes- und Landesebene von Nöten gemacht. In dem Urteil des EuGH wird der Bundesrepublik eine nicht mit der EU-Richtline übereinstimmende Umsetzung hinsichtlich der Unabhängigkeit der Kontrollstellen vorgehalten.
- Die Kirche trifft dieses EuGH-Urteil insofern, als den Kirchen die Meldedaten zulässiger Weise nur übermittelt werden dürfen, wenn sichergestellt ist, dass ausreichende Datenschutzmaßnahmen getroffen sind. Die Feststellung hierüber trifft die zuständige Landesbehörde. Dies ist so in den Landesmeldegesetzen und im Melderechtsrahmengesetz des Bundes geregelt und wird sich in gleicher Weise im neuen Bundesmeldegesetz wiederfinden. Dem gestiegen Datenschutzniveau ist also kirchlicherseits Rechnung zu tragen, will man nicht den Zusammenbruch des kirchlichen Meldewesens, des Kirchensteuereinzugsverfahrens und des kirchlichen Mitgliedschaftsrechtes riskieren.
- Darüber hinaus liegt seit dem 25. Januar 2012 ein Vorschlag der Europäischen Kommission für eine "Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung von personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)" vor. Diese EU-Rechtsverordnung wird, sobald sie verabschiedet und in Kraft gesetzt ist, in allen ihren Teilen verbindlich und gilt damit unmittelbar in jedem Mitgliedstaat der EU, insoweit auch für

die Kirche. Der Zeitplan für die Umsetzung dieser EU-Verordnung sieht zurzeit wie folgt aus: Zunächst wird sich der Europäische Rat und das EU-Parlament dieses Entwurfs in seinen Ausschüssen ab März/April 2012 annehmen und mit einer entsprechenden Stellungnahme versehen. Der Rat der EU, das heißt konkret jedes Mitgliedsland der EU wird votieren und mit entsprechenden Änderungsvorschlägen aufwarten können. Das Ganze wird von der EU-Kommission ausgewertet und mit einem veränderten Verordnungsvorschlag zur erneuten Zustimmung in die EU-Gremien zurückgespielt. Dies soll innerhalb einer Jahresfrist, spätestens vor Ende der laufenden Legislaturperiode des Europäischen Parlamentes, das heißt spätestens bis Anfang 2014, zum Abschluss gebracht werden. Falls dies nicht möglich ist, müsste der gesamte Verordnungsentwurf in der sich anschließenden Legislaturperiode neu eingebracht werden.

In dem vorliegenden Entwurf der EU-Verordnung wird größtenteils auf das Bundesdatenschutzgesetz als Maßstab zurückgegriffen. Die Ausformung des Datenschutzgesetzes in der Bundesrepublik Deutschland stellt nach Auffassung der EU-Kommission das am besten ausformulierte Schutzniveau dar, dessen sich die EU-Kommission bedient hat. Darüber hinaus werden einige Bereiche, insbesondere was die Stellung und die Einbindung der Datenschutzbeauftragten und der Aufsichtsbehörden betrifft, im Sinne der o.g. EuGH-Entscheidung festgeschrieben und weiter ausgeformt. An diesen Grundsätzen wird sich nichts ändern, zumal dies durch die Rechtsprechung des EuGH weitgehend vorgegeben ist. Welche weiteren konkreten, materiellen Inhalte letztlich aus dem Verordnungsentwurf später im endgültigen Text zustehen kommen, ist zum jetzigen Zeitpunkt noch schwer abzuschätzen. Doch sieht der Entwurf in seinen Artikeln 9 und 85, sowie in seinem Erwägungsgrund 128, eine Festschreibung der bisherigen kirchlichen Position vor, die den Erhalt des eigenen kirchlichen Datenschutzes in materieller Hinsicht sowie den Erhalt der eigenen Datenschutzaufsicht festschreibt. Der Entwurf geht damit über das hinaus, was den Kirchen bisher im Bundesdatenschutzgesetz als Normierung zugestanden wurde. Hier musste immer mit dem "beredten Schweigen" des Gesetzgebers argumentieren werden, um unsere eigenständige Regelungskompetenz zu begründen.

Der Wortlaut des Artikels 85 des EU-Entwurfs lautet:

"Artikel 85

Bestehende Datenschutzvorschriften von Kirchen und religiösen Vereinigungen oder Gemeinschaften.

(1) Wendet eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten an, dürfen diese Regeln weiter angewandt werden, sofern sie mit dieser Verordnung in Einklang gebracht werden.

(2) Kirchen und religiöse Vereinigungen oder Gemeinschaften, die gemäß Absatz 1 umfassende Datenschutzregeln anwenden, richten eine unabhängige Datenschutzaufsicht im Sinne des Kapitel VI ein."

Hier ist normiert, dass eine Kirche den Datenschutz eigenständig regeln kann, sofern bereits zum Zeitpunkt des Inkrafttretens der Verordnung ein umfassender Schutz existiert und dieser zukünftig konkret im Einklang mit dem Schutzniveau der EU-Verordnung steht. Auch die unabhängige Datenschutzaufsicht für die Kirchen wird gewährt, soweit es den Anforderungen des Kapitels 6 der Verordnung Rechnung getragen ist, die das aufnehmen, was durch das o.g. EuGH-Urteil bereits jetzt Geltung besitzt. Dies alles wird noch verdeutlicht durch den Erwägungsgrund 128 in dem es heißt:

"Im Einklang mit Artikel 17 des Vertrages über die Arbeitsweise der Europäischen Union achtet diese Verordnung den Status, den Kirchen und religiöse Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren Rechtsvorschriften genießen, und beeinträchtigt ihn nicht. Wendet eine Kirche in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten an, sollten diese Regeln weiter gelten, wenn sie mit dieser Verordnung in Einklang gebracht werden. Kirchen und religiöse Vereinigungen und Gemeinschaften sollten verpflichtet werden, eine völlig unabhängige Datenschutzaufsicht einzurichten".

Von einem Kenner der Materie, von einem Landes-Datenschutzbeauftragten, wurde auf eine entsprechende Anfrage, wie hiermit seitens der Kirchen umzugehen ist, der dringende Ratschlag gegeben, die Novellierung des kirchlichen Datenschutzes schnellstmöglich voranzutreiben, und die völlige Unabhängigkeit der Datenschutzaufsicht bereits jetzt zu normieren, damit zum Inkrafttreten der EU-Datenschutzverordnung keine offene Flanke besteht, und nur noch in einzelnen Bereichen eine evtl. notwendige materielle Anpassung an die dann gegebene konkrete Ausformung des EU-Datenschutzrechtes vorgenommen werden muss. Da auch der EU-Verordnungsgeber sich inhaltlich sehr stark an das Bundesdatenschutzgesetz angelehnt habe, sei das kirchliche Schutzniveau für die jetzt entstehende Novellierung im materiellen Bereich an dem des Bundesdatenschutzgesetzes und dem der Bundesländer auszurichten.

2. Datenschutzaufsicht durch die Beauftragten für den Datenschutz

Das EuGH-Urteil vom 9. März 2010 bezieht sich zwar formal auf die bei den Bundesländern angesiedelte Datenschutzaufsicht für den nicht – öffentlichen Bereich, bekommt jedoch hinsichtlich des öffentlichen Bereichs in noch viel stärkerem Maße zur Anwendung, weil die Exekutive keinerlei Einfluss auf die Aufgabenwahrnehmung der Kontrollbehörde nehmen darf, weil die Exekutive ihrerseits durch die Datenschutzkontrollbehörde überwacht wird.

So hat die 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder auf ihrer Sitzung am 17./18. März 2010 die Gesetzgeber aufgerufen, die Datenschutzaufsicht schnellstmöglich im Sinne der Vorgaben des EU-Rechts zu novellieren:

"Die Ausgestaltung der Unabhängigkeit der Datenschutzkontrollinstanzen muss insbesondere folgenden Kriterien entsprechen:

- Die Datenschutzkontrollstellen müssen ihre Aufgaben ohne jegliche unmittelbare und mittelbare Einflussnahme Dritter wahrnehmen können.
- Es darf keine Fach- und Rechtsaufsicht geben.
- Auch eine mögliche Dienstaufsicht darf nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzkontrollstellen führen.
- Eine Einflussnahme seitens der kontrollierten Stellen ist auszuschließen.
- Zu einer unabhängigen Amtsführung gehören ausreichende Eingriffs- und Durchsetzungsbefugnisse.
- Um eine unabhängige Wahrnehmung der Tätigkeit der Datenschutzkontrollstellen zu gewährleisten, muss ihnen die notwendige Entscheidungshoheit bei Personal, Haushalt und Organisation zustehen."

Entsprechende Nachbesserungen sind bereits in fast allen Bundesländern erfolgt, beispielsweise in Brandenburg im Juli 2010, in Hamburg zum 21. September 2010, in Baden-Württemberg mit Gesetz vom 7. Februar 2011, in Berlin zum 16. Februar 2011, in Hessen am 20. Juni 2011, in Niedersachsen zum 8. Juli 2011 und in Nordrhein-Westfalen mit Wirkung vom 16. Juli 2011.

Durchgängig ist die vollkommene Unabhängigkeit in einer eigenständigen Behörde normiert, das Amt ist hauptamtlich auszuüben und wird in ein Beamtenverhältnis auf Zeit gekleidet.

Darüber hinaus sieht die Datenschutz-Grundverordnung der EU-Kommission in ihrem Entwurf einen Artikel 46 mit folgendem Wortlaut vor:

"Artikel 46
Aufsichtsbehörde

(1) Jeder Mitgliedstaat trägt dafür Sorge, dass eine oder mehrere Behörden für die Überwachung der Anwendung dieser Verordnung zuständig sind und einen Beitrag zu ihrer einheitlichen Anwendung in der gesamten Union leisten, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung ihrer Daten geschützt und der freie Verkehr dieser Daten in der Union erleichtert werden. Zu diesem Zweck bedarf es der Zusammenarbeit der Aufsichtsbehörden untereinander und mit der Kommission.

(2) Gibt es in einem Mitgliedstaat mehr als eine Aufsichtsbehörde, so bestimmt dieser Mitgliedsstaat die Aufsichtsbehörde, die als zentrale Kontrollstelle für die wirksame Beteiligung dieser Behörden im Europäischen Datenschutzausschuss fungiert und führt ein

Verfahren ein, mit dem sicher gestellt wird, dass die anderen Behörden die Regeln für das **Kohärenzverfahren** nach Artikel 57 einhalten…"

Hierin wird die eindeutige Tendenz sichtbar, dass die Kirchen in der Bundesrepublik Deutschland, denen die eigenständige Regelung des Datenschutzes und deren Überwachung zugestanden wird, dafür Sorge zu tragen haben, dass eine einheitliche Anwendung des Datenschutzrechtes für ihren Bereich sichergestellt sein muss. Dies hat organisatorisch die Auswirkung, dass es auf EKD-Ebene eine gemeinsame Einrichtung geben muss, die für eine einheitliche Anwendung des kirchlichen Datenschutzrechtes in allen Gliedkirchen und in allen den Kirchen zugeordneten Diakonischen Werken und Einrichtungen Sorge trägt.

Dass die Kirchen bei alle dem auch innerstaatlich bereits in einem besonderen Fokus stehen, zeigen Beispiele aus jüngster Zeit:

- Im Bericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vom 14. April 2011 findet die Kirche erstmals ausdrücklich Erwähnung (S. 26):

  Bei der Reflektion zum o.g. EuGH-Urteil wird ausgeführt: "darüber hinaus muss auch **die autonome Datenschutzaufsicht bei den Religionsgemeinschaften** und im Verwaltungsbereich der öffentlich-rechtlichen Rundfunkanstalten **auf den Prüfstand**, da auch hier eine völlige Unabhängigkeit im Sinne der Europäischen Vorgaben nicht gegeben ist."
- Bei den Gesprächen im Bundesministerium am 12. Juli 2011 zu den kirchlichen Petita zum Entwurf des Bundesmeldegesetzes wurde hinsichtlich des kirchlichen Wunsches, hierin einen Anspruch der Kirchen auf Datenübermittlung festzuschreiben, entgegnet, dass kein expliziter Anspruch festgeschrieben wird. Es könnten sich Fallkonstellationen ergeben, die es aus datenschutzrechtlichen Gründen verbieten, entsprechende Daten an die Kirchen weiterzuleiten.
- Auch die Möglichkeit der Teilnahme an einem im Entwurf zum Bundesmeldegesetzes vorgesehenen automatisierten Abrufverfahren von Meldedaten wird den Kirchen verweigert mit der Begründung, dass staatlicherseits keine Kontrollmöglichkeit bestehe, was im weiteren bei Gewährung eines direkten Zugangs der Kirchen zu den staatlichen Datenbanken mit den Daten im kirchlichen Bereich geschehe. Man habe die Befürchtung, "etwas in eine Wolke zu geben ohne Kontrollmöglichkeit".
- In alldem wird die Notwendigkeit deutlich, die Unabhängigkeit der Datenschutzbeauftragten im kirchlichen Bereich gemäß den Kriterien des nationalen- und des EU-Rechtes zu erfüllen und dies nach innen und nach außen deutlich zu machen. Auch an dieser Umsetzung wird in Zukunft gemessen werden, ob die Kirchen weiterhin Meldedaten erhalten, wie es § 19 Absatz 3 des Melderechtsrahmengesetzes, bzw. § 33 Absatz 13 des Entwurfs des Bundesmeldegesetzes vorsehen, die festschreiben, dass die Kirchen die Meldedaten nur erhalten, "wenn sichergestellt ist", dass bei Ihnen

"ausreichende Datenschutzmaßnahmen getroffen sind". Nach den geltenden Landesmeldegesetzen trifft diese "Feststellung hierüber die zuständige oberste Landesbehörde". Es zeichnet sich ab, dass sich das jeweilige Landesinnenministerium als oberste Landesbehörde dieser Aufgabe intensiver als bisher zuwenden wird und etwa alle zwei Jahre eine entsprechende Kontrolle vorsehen könnte. Andeutungen in dieser Hinsicht wurden an uns herangetragen. Die Notwendigkeit, datenschutzrechtlich auf der Höhe der Zeit zu sein, ist evident, will man nicht den Zusammenbruch des kirchlichen Meldewesens riskieren.

3. Folgerungen für die Umsetzungsnotwendigkeiten im kirchlichen Datenschutzrecht

- In der jetzt anstehenden Novellierung des DSG-EKD müssen zum einen die Bereiche, die durch die letzten Novellierungen des Bundesdatenschutzgesetzes, wie sie zum 1. April 2010 und zum 11. Juni 2010 in Kraft getreten sind, aufgegriffen werden. Diese Dinge stellen mehr oder weniger Selbstverständlichkeiten dar.
- Hinzu tritt die Umsetzung des EuGH-Urteils vom 10. März 2010, was insbesondere in den Landesmeldegesetzen ihren Ausdruck und auch als vom Europäischen Gesetzgeber zu beachtendes Recht in der EU-Datenschutz-Grundverordnung bereits ihren Niederschlag gefunden hat. Dies betrifft hauptsächlich die Unabhängigkeit der Datenschutzkontrollstellen, für die Kirchen der kirchlichen Datenschutzbeauftragten. Dies stellt einen großen Kraftakt dar, da sich nach den eingeholten Befragungsergebnissen in den meisten Landeskirchen ein erheblicher Nachbesserungsbedarf zeigt.
- Grundsätzlich kann dies auf drei unterschiedlichen Wegen erreicht werden:

1. Jede Gliedkirche und die gliedkirchlichen Zusammenschlüsse können versuchen, diese rechtlichen Vorgaben alleine umzusetzen.
2. Die rechtlichen Vorgaben können in Kooperation mehrerer Gliedkirchen in Angriff genommen werden und
3. als Aufgabenübertragung von einzelnen Gliedkirchen und gliedkirchlichen Zusammenschlüssen an die EKD oder als Aufgabenwahrnehmung in Gänze durch die EKD.

- Einige Landeskirchen und diakonische Werke lassen die Aufgaben der Datenschutzbeauftragten nach § 18 durch externe Personen und Stellen wahrnehmen. Dies ist solange unbedenklich, solange dies durch einen anderen kirchlichen Datenschutzbeauftragten geschieht. Unter Berücksichtigung der Vorgaben des EU-Rechtes sowie der gängigen Praxis beim Staat ist festzustellen, dass die Sicherstellung der Einhaltung des Datenschutzrechtes auf der Ebene der Beauftragten für den Datenschutz, anders als bei den örtlichen und Betriebsbeauftragten für den Datenschutz, grundsätzlich eine hoheitliche Aufgabe ist, die nicht in einen privaten Sektor ausgegliedert werden kann. Auch dürfte angesichts der zukünftig sehr viel größeren Kompetenzen der Datenschutzbeauftragten die Durchsetzung der "hoheitlichen Maßnahmen" in Form von Verwaltungsakten von privaten externen Personen und Stellen schwierig werden, zum

Einen wegen der Akzeptanz, zum Anderen ist es fraglich, ob diese - allenfalls als beliehener Unternehmer - Verwaltungsakte erlassen können und dagegen der Rechtsweg eröffnet ist. Soweit in der Rechtsliteratur die Auffassung vertreten wird, dass die Datenschutzaufsicht auch durch private Externe betrieben werden kann, bezieht sich dies auf die **Betriebsbeauftragten oder die örtliche Beauftragten für den Datenschutz** (z.B. § 4f BDSG). Deshalb stellen die Beauftragten für den Datenschutz durchgängig bei den Bundesländern und bei dem Bundesbeauftragten für den Datenschutz eine staatliche, hoheitliche Struktur dar, der sich auch die Kirche - wie es auf staatlicher Seite geschieht – aus Gründen der Gleichwertigkeit stellen muss.

- Die Ausstattung der Datenschutzbehörden auf staatlicher Seite ist - bezogen auf das Jahr 2011 - auch beim Zugrundelegen der weitaus größeren Aufgabengebiete wesentlich umfänglicher (z.B. NRW 50 Mitarbeitende, Nds. ca. 30 Stellen). EKD-weit einschließlich Diakonie kommen wir insgesamt knapp auf einen zweistelligen Wert, die die Stadt Bremen allein – wahrlich bei anderen Datenströmen - für ihren Bereich vorhält. Hamburg weist 16,7 Stellen aus, davon 13,45 Stellen als Beamte und 3,25 für Angestellte. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) weist 44 Beschäftigte, davon 8 Teilzeitkräfte auf.
- Um eine **eigenständige Amtsstellenstruktur** zu gewährleisten, sind aufgrund datenschutzrechtlicher Erwägungen als Mindestausstattung eine halbe Stelle für den Datenschutzbeauftragten und eine viertel Mitarbeiterstelle sowie eine Schreibkraft vorzusehen. Darunter lässt sich keine sinnvolle Einheit bilden und eine unabhängige Arbeitsweise garantieren. Gleichwohl zeigt sich, dass die Schaffung solcher Kleinstbehörden in mehrfacher Zahl über die EKD verteilt, Schwierigkeiten hervorrufen wird, auch bei der einheitlichen Anwendung und Überwachung des Datenschutzes. Von daher liegt eine größtmögliche Zusammenarbeit in diesem Bereich nahe.
- **Bei einer Million Kirchenmitgliedern** ist nach realistischer Einschätzung des Arbeitsvolumens und im Abgleich mit den Aufgaben und der Ausstattung der Landesdatenschutzbeauftragten als Mindestausstattung eine volle Stelle eines/einer Datenschutzbeauftragten und eine halbe Mitarbeiterstelle sowie eine Stelle für eine Schreibkraft vorzusehen.
- Bei einer höheren Kirchenmitgliederzahl oder bei gleichzeitiger Zuständigkeit für die Diakonie, ist eine entsprechende prozentuale Aufstockung vorzunehmen. Für die Arbeitsbereiche der Diakonie sollten die überschlagmäßige Anzahl der Klientel und der Mitarbeitenden sowie die Anzahl der Einrichtungen, zugrunde gelegt werden, bei der personenbezogene Daten anfallen.
- Soweit Gliedkirchen sich zur Wahrnehmung der Aufgabe des Datenschutzes zusammenschließen und größere Einheiten bilden, können erhebliche **Synergieeffekte** entstehen, die größten bei einer EKD-weiten Wahrnehmung: Hier könnten dann vier bis sechs dezentrale Datenschutzzentren vorgehalten werden, die eine möglichst ortsnahe

Anbindung sicherstellen und einige der bisherigen Strukturen nutzen. Daneben sind die örtlichen oder die Betriebsbeauftragten für Datenschutz als Ortskräfte einzusetzen, die diese Aufgaben neben weiteren erfüllen können und nicht die ansonsten für die Datenschutzbeauftragten erforderliche Unabhängigkeit vorzuweisen haben.

- Bei 23 Millionen Kirchenmitgliedern EKD-weit und unter Beibehaltung der gliedkirchlichen Einzelstruktur errechnen sich EKD-weit 23 Vollzeitstellen, 12 Mitarbeiterstellen und etwa gleich viele Sekretariats-Arbeitsplätze.
- **Soweit die Aufgaben gemeinschaftlich von den Gliedkirchen wahrgenommen werden**, können bei Ausnutzung aller Synergieeffekte und bei der Bestellung eines gemeinsamen EKD-Datenschutzbeauftragten plus einem ständigen Vertreter neben zwei weiteren IT-Fachkräften und zwei Schreibkräften beispielsweise mit Standort Hannover bis zu sechs weitere Standorte gebildet werden. Hier wären über die EKD verteilt nochmals sechs juristische und sechs IT-Vollzeitfachkräfte neben sechs Schreibkräften anzusiedeln. Bei der Finanzierung könnte neben einem Sockelbetrag eine anteilige Kostenumlage nach den Mitgliedern nach Beschäftigtenzahlen der jeweiligen Gliedkirche vorgesehen werden, die sich damit an dem tatsächlichen Aufwand orientiert. Hierzu sind die weiteren Konzepte und die finanziellen Belastungen parallel zum Gesetzgebungsverfahren auszuarbeiten.

II. IT-Sicherheitskonzept

1. Allgemeines:

Informationstechnologie ist ein Instrument zur Erfüllung von wichtigen Aufgaben und zur Unterstützung von Funktionen auf allen Ebenen der Evangelischen Kirche. IT-Systeme und dienstliche Daten sind vor unberechtigtem Zugriff und vor unerlaubter Änderung zu schützen (IT-Sicherheit). Jede kirchliche Körperschaft ist verpflichtet, IT-Sicherheit zu gewährleisten.

Wachsende Verwundbarkeit und die Gefahr massiver Imageschäden oder wirtschaftlicher Schäden in Folge von IT-Risiken erhöhen den Handlungsdruck, durch aktives IT-Sicherheitsmanagement Schäden zu verhindern und das Restrisiko zu minimieren. Die Verantwortung beschränkt sich keineswegs auf die jeweiligen IT-Fachabteilungen. Vielmehr gilt: IT-Sicherheit ist eine Aufgabe hoher Priorität, dafür muss das jeweilige Leitungsorgan der kirchlichen Stelle Verantwortung tragen.

2. Rechtsgrundlage, Veränderungen; Zielsetzung [1]

§ 9 Absatz 1 DSG-EKD schreibt allen kirchlichen Stellen bereits jetzt vor, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Kirchengesetzes, insbesondere die in der Anlage zu diesem Kir-

1 Benutzte Quellen: „IT-Sicherheitskonzepte – Planung, Erstellung und Umsetzung“ aus Magazin für IT-Sicherheit „Backup“, Herausgeber Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein; „Leitfaden IT-Sicherheit“ IT-Grundschutz kompakt, Herausgeber Bundesamtes für Sicherheit und Informationstechnik (BSI); div. Materialien der Ev. Kirche von Westfalen

chengesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Schon alleine zur Erreichung dieser Ziele ist jede kirchliche Körperschaft verpflichtet, IT-Sicherheit zu organisieren.

Bisher gelten schon folgende Vorgaben: Die Daten und IT-Systeme sollen in ihrer Verfügbarkeit so gesichert werden, dass die zu erwartenden Stillstandszeiten toleriert werden können. Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen sind nur in geringem Umfang und nur in Ausnahmefällen akzeptabel (Integrität). Die Anforderungen an Vertraulichkeit haben ein normales, an Gesetzeskonformität orientiertes Niveau. In den Bereichen, in denen Programme mit schutzbedürftigen Daten eingesetzt werden, insbesondere Meldewesen, Kirchenbuchwesen, Personalwesen, Haushalts-, Kassen- und Rechnungswesen, Patientenbetreuung und -verwaltung, sind die IT-Sicherheitsziele (Verfügbarkeit, Integrität und Vertraulichkeit) unbedingt zu beachten.

- In der Praxis ist der **Stellenwert**, der der IT-Sicherheit bei den kirchlichen Stellen zugewiesen wird, **höchst unterschiedlich**. Es ist oft schwierig, ein angemessenes Sicherheitsniveau zu erreichen und aufrecht zu erhalten. Die Gründe dafür sind vielfältig: fehlende Ressourcen, zu knappe Budgets und nicht zuletzt die steigende Komplexität der IT-Systeme. Analog zur Entwicklung in der Informationstechnik sind die Anforderungen an IT-Sicherheit immer komplexer und umfassender geworden. Eine Vielzahl von IT-Sicherheitsprodukten und -beratern bieten unterschiedlichste Lösungen an. Da haben selbst Experten Mühe, den Überblick zu behalten.

  Seitens der kirchlichen Datenschutzbeauftragten muss es deswegen bei den Prüfungen vor Ort nicht nur um die einzelnen IT-Komponenten mit mehr oder weniger abgeschlossenen Maßnahmenpakete gehen, sondern es ist ein abgeschlossenes IT-Sicherheitskonzept für die jeweilige kirchliche Stelle vorzulegen. Dabei wird der im staatlichen Bereich zu Grunde gelegte Standard herangezogen.

  Seitens der Verantwortlichen aus den Leitungsorganen hört man zum Teil weit verbreitete Fehleinschätzungen zum eigenen Schutzbedarf. Die Aussage „Bei uns ist noch nie etwas passiert“ ist mutig. Die Einschätzung „Was soll bei uns schon zu holen sein, so geheim sind unsere Daten nicht“ ist in den meisten Fällen zu oberflächlich. Externe Überprüfungen decken nahezu immer ernste Schwachstellen auf und sind ein guter Schutz vor „Betriebsblindheit“. Auch die Aussage „Unsere Mitarbeiter unterliegen dem Datenschutz und sind vertrauenswürdig“ ist zwar grundsätzlich richtig, doch verschiedene Statistiken zeichnen ein anderes Bild: Die Mehrzahl der Sicherheitsverstöße wird durch Innentäter verursacht. Dabei muss nicht immer Vorsatz im Spiel sein. Auch durch Versehen, Übereifer oder Neugierde gepaart mit mangelndem Problembewusstsein (zu wenig oder keine Schulungen) entstehen manchmal große Schäden.
- **Sicherheit ist kein statischer Zustand**, sondern ein ständiger Prozess. Für die kirchlichen Stellen sind immer wieder die folgenden Fragen zu beantworten:

• Welche Formen von Missbrauch wären möglich, wenn vertrauliche Informationen aus ihrer kirchlichen Stelle in die Hände Dritter gelangten?

• Welche Konsequenzen hätte es für die kirchliche Stelle, wenn wichtige Informationen - z. B. während einer Datenübertragung oder auf ihrem Server - verändert würden? Als Ursache kann nicht nur böse Absicht unbekannter Dritter, sondern auch technisches Versagen in Frage kommen.

• Was würde geschehen, wenn in Ihrer Organisation wichtige Computer oder andere IT-Komponenten plötzlich ausfielen und für einen längeren Zeitraum (Tage, Wochen, ...) nicht mehr nutzbar wären? Könnte die Arbeit fortgesetzt werden? Wie hoch wäre der mögliche Schaden?

Es bietet sich daher an, in einem gut durchdachten IT-Sicherheitskonzept die Antworten auf diese Fragen zur Hand zu haben. § 9 Abs. 2 DSG-EKD schreibt dem Rat der EKD eine entsprechende Regelungskompetenz zu.

- Eine solche Rechtsverordnung des Rates der EKD könnte sich an den **Empfehlungen des Bundesamtes für Sicherheit und Informationstechnik (BSI)** zur Informationssicherheit und zum IT-Grundschutz orientieren. Dies sorgt für eine anerkannte Basis und gewährt eine größtmögliche Einheitlichkeit innerhalb der EKD. Das BSI bietet seit vielen Jahren Informationen und Hilfestellungen rund um das Thema IT-Sicherheit: Als ganzheitliches Konzept für IT-Sicherheit hat sich das Vorgehen nach IT-Grundschutz zusammen mit den IT-Grundschutz-Katalogen des BSI als Standard etabliert. Diese vom BSI seit 1994 eingeführte und weiterentwickelte Methode bietet sowohl eine Vorgehensweise für den Aufbau einer Sicherheitsorganisation als auch eine umfassende Basis für die Risikobewertung, die Überprüfung des vorhandenen IT-Sicherheitsniveaus und die Implementierung der angemessenen IT-Sicherheit. Die IT-Grundschutz-Kataloge dienen außerdem zahlreichen Unternehmen und staatlichen Behörden als wichtiges Fundament eigener Maßnahmenkataloge. Im Rahmen der Umsetzung der im IT-Sicherheitskonzept enthaltenen Maßnahmen ist zu beachten, dass die IT-Sicherheitsmaßnahmen in einem angemessenen Verhältnis zum Wert der schützenswerten Daten und IT-Systeme stehen müssen. Die Verantwortung für die IT-Sicherheit obliegt dem Leitungsorgan; daher ist das IT-Sicherheitskonzept sowie alle wesentliche Maßnahmen **durch das Leitungsorgan zu beschließen.**

Die Umsetzung eines einheitlichen IT-Sicherheitskonzeptes hat neben dem Sicherheitsgewinn häufig weitere Vorteile:

• Die Mitarbeiter sind zuverlässiger, die Arbeitsqualität steigt. Gelebte IT-Sicherheit kann das verantwortungsbewusste Handeln fördern und die Identifikation mit den Zielen der kirchlichen Stelle stärken.

• Wartungsarbeiten an IT-Systemen erfordern deutlich weniger Zeit und die IT-Administratoren können effektiver arbeiten. IT-Administratoren und IT-Anwender kennen sich

besser mit ihren Systemen aus. Die IT-Systeme sind gut dokumentiert, was Administrationsarbeiten, Planung, Neuinstallation von Software und Fehlerbeseitigung erleichtert. Ein gutes IT-Sicherheitskonzept vermeidet zudem einige Probleme unter denen IT-Administratoren normalerweise besonders leiden: Anwender setzen verschiedene Programme für den gleichen Zweck ein, unterschiedliche Betriebssysteme müssen betreut werden, verschiedene Versionen der gleichen Software sind im Einsatz, jeder Anwender hat individuelle Rechte, Anwender nutzen private Software und gestalten ihren Arbeitsplatz-PC selbst, ohne entsprechendes Know-how zu haben. Eine zentrale Administration des „Rechnerzoos“ ist so kaum möglich. Jeder Rechner muss mit hohem Aufwand individuell analysiert und betreut werden.

III. Die Änderungsvorschläge im Einzelnen:

Überschrift

Der Überschrift des Gesetzes wird eine Kurzbezeichnung und eine Abkürzung als Klammerzusatz angefügt. Dies erleichtert die eindeutige Zitierfähigkeit und trägt dem bisherigen Sprachgebrauch Rechnung.

Inhaltsverzeichnis

Dem Gesetzestext wird ein Inhaltsverzeichnis vorangestellt. Dies erleichtert die Lesbarkeit des Gesetzes und das Auffinden der gesetzlichen Normierungen, insbesondere für solche Personen, die nicht tagtäglich mit diesen Vorschriften arbeiten.

§ 1 Zweck und Anwendungsbereich

Der Anwendungsbereich des DSG-EKD wurde in **Absatz 2** konkretisiert: „Dieses Kirchengesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Evangelische Kirche in Deutschland, ihre Gliedkirchen und ihre gliedkirchlichen Zusammenschlüsse sowie die ihnen zugeordneten kirchlichen und diakonischen Werke und Einrichtungen ohne Rücksicht auf deren Rechtsform und rechtsfähige evangelische Stiftungen bürgerlichen Rechts (kirchliche Stellen). Die Evangelische Kirche in Deutschland und ihre Gliedkirchen und ihre gliedkirchlichen Zusammenschlüsse haben sicherzustellen, dass auch in den ihnen organisatorisch zugeordneten Werken und Einrichtungen dieses Kirchengesetz sowie Ausführungsbestimmungen und seine ergänzenden Durchführungsbestimmungen Anwendung finden...“

- In Satz 1 wird eine Legaldefinition normiert. Dies erlaubt, den Anwendungsbereich des Gesetzes klarer als bisher abstecken zu können. Die Zuordnungsrichtlinie der EKD leistet hierzu eine entscheidende Hilfestellung: Der Kirche und der Diakonie sind solche Werke und Einrichtungen zuzuordnen, bei denen der kirchliche oder der diakonische Zweck überwiegt.

  In Satz 2 wird die Verantwortlichkeit der EKD, der Gliedkirchen und ihrer gliedkirchlichen Zusammenschlüsse für die Einhaltung der datenschutzrechtlichen Vorschriften auch der ihnen jeweils zugeordneten Werke und Einrichtungen klargestellt.

In Satz 3 wurde die bisherige Verpflichtung zur Anfertigung von Übersichten zur Geltung des kirchlichen Datenschutzes verstärkt: Aus der Soll-Vorschrift ist eine Muss-Vorschrift geworden, insbesondere vor dem Hintergrund, dass zukünftig größere Bereiche einer datenschutzrechtlichen Aufsicht unterstehen.

- **Absatz 5** nimmt die Regelung des BDSG (§ 1 Absatz 4) auf und bezieht es parallel zum staatlichen Verwaltungsverfahrensgesetz auf das eigenständige kirchliche Verwaltungsverfahrens- und -zustellungsgesetz. Dies hat beispielsweise zur Folge, dass bei der Ermittlung personenbezogener Daten im Rahmen des Verwaltungsverfahrens der Handlungsspielraum der kirchlichen Behörde in gleicher Weise wie der der staatlichen erheblich eingeschränkt ist:

  Sie muss in aller Regel versuchen, benötigte Daten bei Betroffenen selbst zu erfragen, bevor sie dritte Informationsquellen nutzt. Vergleichbare Beschränkungen gelten auch bei der weiteren Bearbeitung des Vorgangs im Verwaltungsverfahren, etwa die Bindung der Datenverwendung an den ursprünglichen Erhebungs- bzw. Speicherungszweck oder für eine Datenübermittlung zwischen öffentlichen (kirchlichen) Stellen, auch im Rahmen der "Amtshilfe".

  Ferner hat die Auskunftserteilung bzw. die Akteneinsicht zu unterbleiben, wenn sie zu einem unzulässigen Eingriff in das informationelle Selbstbestimmungsrecht des Dritten führen würde (Vgl. zum Ganzen, Simitis, BDSG, 7. Auflage 2011, zu § 1, Rdr. 191 ff).

§ 2 Begriffsbestimmungen

- Neu aufgenommen wurde als Erweiterung der Begriffsbestimmungen ein **Absatz 13**, der weitgehend wortgleich wie § 3 Absatz 11 des Bundesdatenschutzgesetzes definiert, was unter den Begriff „Beschäftigte“ fällt. Vorangestellt wurde "1. In einem Pfarrdienst oder in einem kirchlichen Beamtenverhältnis stehende Personen", die als kirchliche Spezifika nicht im BDSG normiert sind.

Die unter 3. getroffene Definition "zu ihrer Berufsbildung Beschäftige", geht dabei weit über die in § 1 Berufsbildungsgesetz Gemeinten hinaus und erfasst auch Volontäre, Praktikanten und Anlernlinge, soweit sie sich nicht bereits in einem Arbeitsverhältnis befinden.

Unter 6. war der Änderung des Freiwilligendienstes, die u.a. im Bundesfreiwilligendienst, im Freiwilligen Sozialen- und Ökologischen Jahr bei Wegfall des Zivildienstes ihren Ausdruck gefunden hat, Rechnung zu tragen. Diese Dienste finden sich alle in der Begriffsbestimmung wieder.

- Im Weiteren wurde ein **Absatz 14** angefügt, der eine Begriffsbestimmung zur IT-Sicherheit vornimmt. Damit wird die in § 9 Absatz 2 getroffene Regelung eindeutig, weil diese Definition des Begriffs der IT-Sicherheit zugrunde gelegt wird.

§ 2a Datenvermeidung und Datensparsamkeit

Die neugefasste Regelung übernimmt wortgleich die Regelung des § 3a BDSG und erweitert damit die hierin niedergelegte Datenvermeidung und Datensparsamkeit. In Satz 2 wird dieses Ziel konkretisiert, es soll insbesondere mittels Anonymisierung und Pseudonymisierung erreicht werden. Damit kann bereits im Vorfeld bei der Auswahl der Technik und der Ausgestaltung der IT-Systeme der Einsatz datenschutzfreundlicher Technik zielführend sein.

§ 3 Erhebung, Verarbeitung und Nutzung

§ 3 hat keine Änderung erfahren, es ist jedoch darauf hinzuweisen, dass unter dem Begriff "eine andere Rechtsvorschrift" eine abstrakt generelle Regelung zu verstehen ist, die in einem förmlichen Gesetzgebungsverfahren normiert wurde, und somit keine Verwaltungsanordnungen betrifft.

§ 7 Unabdingbare Rechte der betroffenen Person

Hier wurde ein Absatz 3 angefügt. Er dient zur Klarstellung und Erweiterung der unabdingbaren Rechte der betroffenen Person und soll seine Stellung bei der Ausübung gesetzlicher Rechte durch ein striktes Zweckbindungsgebot stärken. Grundsätzlich fallen beispielsweise bei einem mündlichen Auskunftsersuchen oder bei der persönlichen Einsicht in die eigene Personalakte keine zu dokumentierenden Daten an. Sollte dies gleichwohl der Fall sein, darf dies nicht zu negativen Bewertungskriterien führen durch entsprechende Vermerke in den Personalakten.

§ 7a Videobeobachtung und Videoaufzeichnung (Videoüberwachung)

§ 7a wurde wesentlich erweitert und der entsprechenden Regelung des Bundesdatenschutzgesetzes angepasst, insbesondere der ausführlichen Regelung des Hamburgischen Datenschutzgesetzes (§ 30) entnommen, dem sich auch weitere Landesdatenschutzgesetze nach und nach angleichen. Von daher war für das kirchliche Datenschutzrecht diese ausführlichere und detailliertere Regelung der Ausgangspunkt. Die detailierte Regelung erfüllen zugleich eine Hilfestellung zur Anwendung und zum Umgang mit Videobeobachtung. Weiterhin ausgenommen bleibt eine Videoüberwachung des Gottesdienstes.

- Mit dieser detaillierten Regelung wird auch der Fortentwicklung der Informationsverarbeitungstechnologie und der Wahrung der informationellen Selbstbestimmung durch einen angemessen Interessensausgleich Rechnung getragen.
- In Absatz 1 erfährt die Beobachtungserlaubnis bereits Einschränkungen, sie ist nur in Ausübung des Hausrechtes erlaubt unter dem Gesichtspunkt des Personen- und Sachschutzes und zur Überwachung von Zugangsberechtigungen. Dies alles steht unter der Voraussetzung, dass keine schutzwürdigen Interessen des Betroffenen höher zu bewerten sind.
- Absatz 2 setzt der darüber hinausgehenden Videoaufzeichnung dahingehend Grenzen, dass auch sie nur unter der Voraussetzung gestattet ist, dass mit einer Verletzung der Rechtsgüter nach Absatz 1 zukünftig gerechnet werden muss und keine höher einzu-

stufenden Interessen der Betroffenen vorliegen. Nur zur Verfolgung von Straftaten oder zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person oder bedeutender Sach- und Vermögenswerte dürfen sie einem anderen Zweck zugeführt werden.

- Absatz 3: Auf eine Videoüberwachung und -aufzeichnung ist erkennbar hinzuweisen und die verantwortliche Stelle anzuzeigen.
- In Absatz 4 ist die Benachrichtigungspflicht normiert, in Absatz 5 die Löschungsverpflichtung, in Absatz 6 werden die technischen und organisatorischen Maßnahmen angesprochen, die bei einer Videoüberwachung einzuhalten sind.
- Absatz 7 legt der diese Daten verarbeitenden Stelle eine umfängliche Dokumentationspflicht auf und bindet die örtlich Beauftragten bzw. die Betriebsbeauftragten für den Datenschutz nach § 22 DSG-EKD mit ein.
- In Absatz 8 findet sich eine Erforderlichkeitsüberprüfung alle zwei Jahre und in Absatz 9 werden auch für Videokamera-Attrappen grundsätzliche Regelungen zur entsprechenden Anwendung gestellt.

§ 8 Schadensersatz durch kirchliche Stellen

Hier wurden die bisherigen Beträge von 125.000,- auf 130.000,- Euro erhöht, übernommen aus § 8 Bundesdatenschutzgesetz. Ferner wird auf die (neuen) Verjährungsfristen des BGB verwiesen (Absatz 5).

§ 9 Technische und organisatorische Maßnahmen, IT-Sicherheit

Absatz 2 ist neu eingefügt und stellt die Verpflichtung zur Gewährleistung eines IT-Sicherheitskonzeptes auf. Jede kirchliche Stelle ist dazu verpflichtet.

Zur Vereinheitlichung der Sicherheitsstandards ist dem Rat der EKD eine Verordnungsermächtigung gegeben.

§ 10 Einrichtung automatisierter Abrufverfahren

In Absatz 3 wurde zur Klarstellung, ob es sich um Beauftragte für den Datenschutz oder um Betriebsbeauftragte oder örtlich Beauftragte für den Datenschutz handelt, der jeweilige Paragraph durch die Benennung des § 18 und des § 22 des Datenschutzgesetzes hinzugefügt.

Eine Klarstellung enthält auch die Neuformulierung in Absatz 5, der bei Einrichtung automatisierter Abrufverfahren die vorgenannten Voraussetzungen dann nicht aufstellt, soweit es sich um allgemein zugängliche Daten handelt.

§ 11 Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten im Auftrag

- Absatz 2 stellt für die beauftragende Stelle bei der Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten klar, dass ein solcher Auftrag aus Gründen der Wahrung des hohen Datenschutzniveaus nicht außerhalb der Mitgliedsstaaten der Eu-

ropäischen Gemeinschaft vergeben werden soll. Zur Überwachung dieses Standards ist die oder der Beauftragte für den Datenschutz mit verantwortlich, daher sollte ein solcher Auftrag möglichst in der Bundesrepublik Deutschland ausgeführt werden. Hier kann eine durchaus notwendige Prüfung vor Ort ohne größeren zeitlichen und finanziellen Aufwand durchgeführt werden. Soweit besondere Fallkonstellationen ausnahmsweise eine Beauftragung außerhalb der EU für notwendig erachten, stellt Satz 2 die Voraussetzungen auf, die erfüllt sein müssen. Dies sollte nach einheitlichen Kriterien erfolgen und das entsprechende Wissen wird nicht an mehreren Stellen vorzuhalten sein, sondern für alle abrufbar bei der EKD.

- Absatz 3 stellt im Wesentlichen eine Übernahme der neu getroffenen Regelung in § 11 Absatz 2 des BDSG dar und legt die einzelnen Voraussetzungen fest, die bei der Auftragsdatenverarbeitung einzuhalten sind.
- Absatz 7 sieht die Möglichkeit vor, dass das Recht der EKD, der Gliedkirchen oder der gliedkirchlichen Zusammenschlüsse Genehmigungen vor einer Fremdvergabe vorsehen können. In der Praxis einiger Gliedkirchen, die das Genehmigungsverfahren in ihren bisherigen Durchführungsbestimmungen vorgesehen haben, hat sich herausgestellt, dass viele Verträge mit Fremdfirmen nicht den gesetzlichen Vorgaben entsprechen und nachgebessert werden müssen. Die Betriebsbeauftragten und örtlich Beauftragten für den Datenschutz sind vielfach überfordert, die Verträge inhaltlich zu prüfen und der Leitung der kirchlichen Stelle deutlich zu machen, welche Regelungen nachzubessern oder neu aufzunehmen sind. Eine Erleichterung kann auch die Verwendung von Muster-Vereinbarungen darstellen, die die Kirchen vorgeben und so ggf. einzelnen Gemeinden oder sonstigen kirchlichen Dienststellen das Verfahren verkürzen und vereinfachen können. Wenn mit der Beauftragung eine andere kirchliche Stelle betraut wird, die der Geltung des DSG-EKD untersteht, kann von den genannten Voraussetzungen abgesehen werden.

§ 12 Datenübermittlung an kirchliche oder sonstige öffentliche Stellen

Die Anfügung des neuen Absatzes 8 stellt klar, dass bei der Datenübermittlung nach außerhalb des Geltungsbereiches des DSG-EKD, auch zu anderen Religionsgemeinschaften und in den staatlichen Bereich eine besondere Zweckbindung zu beachten ist, auf die gesondert hingewiesen werden muss. Ein Hinweis genügt, da auch dort vergleichbares Datenschutzrecht gilt.

§ 14 Durchführung des Datenschutzes

Hier konnte eine wesentliche Straffung zur Durchführung des Datenschutzes vorgenommen werden, weil andere Regelungen zur Dateiübermittlung (§§ 11, 12, 13, 21, 21a) dem Datenschutzanliegen Dritter detaillierter gerecht werden. Die Pflege der bisher in § 14 vorgesehenen Übersichten einen hohen Aufwand, der in keinem Verhältnis zu dem Einsichtsrecht des Dritten stand.

§ 17 Anrufung der Beauftragten für den Datenschutz

Absatz 2 ist angefügt und trägt der Tatsache Rechnung, dass es für den Meldenden keinen Nachteil mit sich bringen darf, wenn er entsprechende Anhaltspunkte über Rechtsverstöße seinen Dienstvorgesetzen meldet. Auch darf er den direkten Weg zum Beauftragten für den Datenschutz wählen. Zur effektiven und schnellen Gewährung des Datenschutzes ist diese "Meldepflicht" ein wichtiger Baustein (vergleichbare Regelung in § 26 Absatz 2 HmbDSG).

§§ 18 ff.

Wie bereits in den allgemeinen Ausführungen oben unter I. ausgeführt ist es nötig, die Stellung des Beauftragten für den Datenschutz und die der örtlichen Beauftragten oder Betriebsbeauftragten für den Datenschutz entscheidend zu verbessern. Dies betrifft in der Novelle hauptsächlich die völlige Unabhängigkeit in organisatorischer und sachlicher Hinsicht (**§ 18** Rechtsstellung der Beauftragten für den Datenschutz). Hinsichtlich des **Beanstandungsrechtes (§ 20)** wird zurzeit noch keine Befugniserweiterung vorgesehen. Dies beruht auf der Tatsache, dass weder die Landesdatenschutzgesetze noch das Bundesdatenschutzgesetz Anordnungs- und Durchgriffsbefugnisse vorsehen und noch nicht absehbar ist, ob und wie die diesbezüglichen Anforderungen im Entwurf der EU-Datenschutzgrundverordnung umgesetzt werden. **Eine weitergehende Anordnungs- und Durchgriffsbefugnis** erscheint jedoch vielfach angebracht und wird **wohl bei einer nächsten Novellierung zum Tragen kommen.**

Zum Einzelnen:

§ 18 Rechtsstellung der Beauftragten für den Datenschutz

- In Absatz 1 Satz 1 verbleit es bei der bisherigen Regelung, dass sowohl die EKD als auch die Gliedkirchen für ihren Bereich jeweils Beauftragte für den Datenschutz bestellen können, soweit sie die Wahrnehmung nicht nach § 18b Absatz 1 übertragen haben. An dieser Weichenstellung wird auch in Zukunft festgehalten. Ob sich zukünftig eine eigenständige Organisationsstruktur für einzelne Gliedkirchen als sinnvoll erweist, oder ob eine starke Kooperation untereinander oder sogar die gemeinsame hoheitliche Aufgabenwahrnehmung des Datenschutzes insgesamt von der EKD anzustreben ist, bleibt damit offen. In **§ 18b** wird dieser Grundgedanke noch einmal aufgegriffen und die hier in § 18 Absatz 1 angelegte Weichenstellung noch im Weiteren konkretisiert.
- In Absatz 2 wird eine Amtszeitbegrenzung als "Soll-Vorschrift" normiert. Alle Datenschutzgesetze auf staatlicher Ebene sehen Begrenzungen vor. Darüber hinaus ist festgehalten, dass die Tätigkeit hauptberuflich auszuüben ist, das ist der Eigenständigkeit der Aufgabe geschuldet und soll verhindern, dass bei weiteren Tätigkeiten ein möglicher Interessenskonflikt auftreten kann. Soweit Nebentätigkeiten ausgeübt werden, sind diese nur dann möglich, wenn die Unabhängigkeit und die Unparteilichkeit

der Aufgabenwahrnehmung des Datenschutzes dadurch nicht gefährdet werden und den Anforderungen der §§ 46 bis 48 Kirchenbeamtengesetz der EKD Rechnung getragen ist. Vergleichbare Regelungen finden sich in den Datenschutzgesetzen in Berlin (§ 22), in Brandenburg (§ 22), in Hessen (§ 21) sowie auch im BDSG (§ 23) beispielhaft wieder.

- Der bisherige Absatz 2 wird zu Absatz 3 und um einen neuen Satz 2 ergänzt, der besagt, dass die Stellung des Datenschutzbeauftragten neben den bereits im Vorsatz erwähnten Sachkunde und Zuverlässigkeit auch die Befähigung zum Richteramt oder zum höheren Dienst beinhaltet und dass die entsprechende Person zur Wahrnehmung der Aufgabenfülle das Spektrum des Evangelischen Protestantismus in Deutschland nachvollziehen können muss, das heißt, aus einer Gliedkirche der EKD stammt. Hinsichtlich der Befähigung ist eine Öffnung gegeben, da nur der höhere Dienst und nicht der höhere Verwaltungsdienst vorausgesetzt wird. Eine weitere Abschwächung hin zu einer "Soll-Vorschrift" wurde vielfach abgelehnt, da weitere IT-Fachkompetenz durch die weiteren Mitarbeiter abgedeckt werden kann und soll.
- In den neuen Absatz 4 wird die Anbindung an die bisherige Struktur der kirchlichen Verwaltungsämter aufgehoben und als neue Regelung die organisatorische und sachliche Unabhängigkeit festgelegt, die sich auch darin äußert, dass die Beauftragten für den Datenschutz einer eigenen Behörde vorstehen. Soweit eine Dienstaufsicht notwendig ist, darf sie die Unabhängigkeit jedoch nicht beeinträchtigen. Es finden sich vergleichbare Regelungen in BDSG und in den Landesdatenschutzgesetzen.
- In Absatz 5 ist der besondere Kündigungsschutz niedergelegt. Es kann nur eine außerordentliche Kündigung erfolgen und der Kündigungsschutz wirkt auch entsprechend nach, soweit sich ein kirchliches Beschäftigungsverhältnis anschließt.
- In Absatz 6 ist eine vergleichbare Regelung für beamtete Beauftragte des Datenschutzes vorgesehen, die unter den erschwerten Bedingungen des Kirchenbeamtengesetzes der EKD §§ 76, 77, 79 oder 80 und einem entsprechenden Urteil der Disziplinargerichte aus dem Dienst entfernt werden können.
- Die Absätze 5 und 6 machen deutlich, dass es sich um eine hoheitliche Aufgabe handelt, die durch kirchliche Mitarbeitende oder kirchliche Stellen und nicht durch private Personen und Stellen wahrzunehmen sind (siehe auch die ausführlichen Hinweise oben unter I. 3., S. 5f).
- In Absatz 7 ist die notwendige Eigenständigkeit auch der Personal- und Sachausstattung normiert, beides kann nur im Einvernehmen mit den Beauftragten für den Datenschutz geschehen. Die Haushaltsmittel sind separat auszuweisen und öffentlich.
- In Absatz 8 findet die konsequente Fortentwicklung der Eigenständigkeit darin ihren Ausdruck, dass auch entsprechende Aussagegenehmigungen von Mitarbeitenden in der Datenschutzaufsichtsbehörde von den Beauftragten für den Datenschutz zu treffen

sind und es wird festgestellt, dass die Beauftragten für den Datenschutz auch als oberste Dienstaufsichtsbehörde nach § 99 Verwaltungsgerichtsordnung gelten.

- In Absatz 9 wird die Bestellung des Vertreters geregelt. Soweit es sich um eine Aufgabenwahrnehmung über einen größeren EKD-Bereich handelt, ist eine ständige Vertretung angezeigt, ansonsten kann eine Vertretung im Verhinderungsfalle ausreichend sein.
- In Absatz 10 bleibt es bei der bisherigen Regelung (alt Abs. 7), jedoch waren die Mitarbeitenden ausdrücklich mit einzubeziehen.

§ 18a Der oder die Beauftragte für den Datenschutz der Evangelischen Kirche in Deutschland

Die Bestimmung sieht vor, dass das Aufgabenspektrum "Datenschutz" des Evangelischen Werkes für Diakonie und Entwicklung neben den gesamtkirchlichen Werken und Einrichtungen gemeinschaftlich von der EKD wahrzunehmen ist. Darin wird deutlich, dass verfasste Kirche und Diakonie sehr eng miteinander verbunden sind, es keine unterschiedliche Aufgabenwahrnehmung geben kann, vielmehr eine einheitliche Anwendung des Datenschutzrechtes sichergestellt sein muss.

§ 18b Beauftragte für den Datenschutz der Gliedkirchen der EKD

Die Weichenstellung, in § 18 angesprochen, dass die Gliedkirchen einzeln oder gemeinschaftlich Beauftragte bestellen können, oder diese Aufgaben insgesamt gemeinschaftlich ausführen zu lassen, indem man diese Aufgabenbereiche dem oder der Beauftragten für den Datenschutz der EKD überträgt, wird hier näher ausgeführt. Ein entsprechendes Grundkonzept ist ausgearbeitet.

- In Absatz 2 wird noch einmal aufgenommen, dass auch der Bereich der Diakonie grundsätzlich unter den Anwendungsbereich des kirchlichen Datenschutzes fällt und nur, soweit erforderlich, die Möglichkeit einer besonderen Bestellung von Datenschutzbeauftragten eröffnet ist. Das bedeutet, nach den vorherigen Ausführungen, dass auch im diakonischen Bereich mindestens eine halbe Stelle für den Datenschutzbeauftragten und eine viertel Mitarbeiterstelle sowie eine Schreibkraft vorzusehen sind. Darunter lässt sich keine sinnvolle eigenständige Einheit bilden und keine unabhängige Arbeitsweise garantieren. Es ist davon auszugehen, dass die Schaffung solcher „Kleinstbehörden“ in mehrfacher Zahl über die "Diakonielandschaft" verteilt, gleichfalls wie bei der verfassten Kirche Schwierigkeiten hervorrufen wird, ebenso bezüglich der einheitlichen Anwendung und Überwachung des Datenschutzes, verbunden mit einem sehr hohen Abstimmungsbedarf (siehe auch die ausführlichen Hinweise oben unter I. 3., S. 5f).

- Sofern die diakonischen Werke ermächtigt werden, eigene Beauftragte zu bestellen, ist für größere diakonische Werke eine – über die Mindestausstattung hinausgehende - prozentuale Aufstockung unter Berücksichtigung der Anzahl der Einrichtungen, der Beschäftigten- und der Klientelzahl vorzusehen.

§ 19 Aufgaben der Beauftragten für den Datenschutz

- Durch die neue Konzeption und Ausstattung der Datenschutzaufsicht wird diese zukünftig auch in der Lage sein, die Einhaltung der Datenschutzvorschriften allumfassend und unangekündigt untersuchen zu können. Dies war bisher so meist nicht der Fall. Das ist jedoch für eine effektive Gewährung des Datenschutzes unumgänglich.
- In Absatz 2 wird das Wort "insbesondere" eingefügt, um den Beispielscharakter zu verdeutlichen; die Vorschrift ermöglicht auch eine anlasslose Überprüfung.
- In Absatz 4 ist geregelt, dass Beauftragte für den Datenschutz auf Anforderung der kirchenleitenden Organe tätig werden können. Daneben ist es angezeigt, dass die frühzeitige Beteiligung, z.B. bei Stellungnahmen zu aktuellen datenschutzrelevanten Gesetzesvorhaben, genutzt werden sollte.
- In Absatz 5 ist die öffentliche Darstellung der Datenschutzaufsicht in entsprechenden (Tätigkeits-)Berichten analog der Regelung des § 26 Absatz 1 Bundesdatenschutzgesetz normiert. Hier sieht der Entwurf der EU-Verordnung im Artikel 54 einen jährlichen Tätigkeitsbericht vor. Dies ist personalintensiv und war deshalb mit einer offenen Frist zu versehen.
- In Absatz 10 ist die Zusammenarbeit der kirchlich Beauftragten für den Datenschutz als verpflichtend normiert und im Hinblick auf die staatlichen Beauftragten als eine Soll-Vorschrift zum Erfahrungsaustausch vorgesehen. Die Praxis hat gezeigt, dass ein regelmäßiger Erfahrungsaustausch mit allen kommunalen staatlichen Beauftragten für den Datenschutz nicht praktizierbar ist, daher kann dieser Passus gestrichen werden. Darüber hinaus ist ein neuer Satz 2 angefügt, dass auch eine Verpflichtung besteht, die einheitliche Anwendung und Durchführung des kirchlichen Datenschutzrechtes sicherzustellen. Dies wird Auswirkungen für die praktische Zusammenarbeit der Beauftragten, etwa in regelmäßigen Treffs oder im Aufbau einer zentralen Datenbank und gemeinschaftlich organisierte Fortbildungsveranstaltungen, beinhalten.

§ 21 Meldepflicht

In § 21 sind die zum Teil im Bundesdatenschutzgesetz (BDSG) geänderten Vorschriften des § 4d aufgenommen und auf die Kirchen-Spezifika zugeschnitten. Der sich hierin zeigende Novellierungsbedarf ist dem gestiegenen Datenschutzbewusstsein und dem technischen Fortschritt geschuldet, obgleich die praktischen Fälle aufgrund der Einschränkungen hinsichtlich der vorausgesetzten Personenzahl kaum auftreten dürften: Es besteht bereits per Gesetz (§ 22) eine Verpflichtung zur Bestellung von Betriebsbeauftragten oder örtlich Beauftragten für den Datenschutz. Es gilt die weitere Entwicklung zu beobachten, sodass zukünftig auch eine Streichung der §§ 21 und 21a erwogen werden könnte, unter Beibehaltung der Vorabkontrolle.

- Absatz 1 beinhaltet die Vorabkontrolle, Absatz 2 die Einschränkungen sofern ein Beauftragter nach § 22 bestellt ist oder kleinere kirchliche Einrichtungen und Kirchen-

gemeinden unter der neuen Personengrenze liegen, wie sie sie zur Zeit auch noch das BDSG vorsieht (§ 4d Abs. 3).

- In Absatz 3 sind besondere Risiken benannt, bei denen eine Vorabkontrolle verpflichtend ist.
- Absatz 4 regelt die Zuständigkeit der nach § 22 Beauftragten, die sich in Zweifelsfällen mit dem oder der für sie zuständigen Beauftragten für den Datenschutz (§ 18) in Verbindung setzen können.

§ 21a Inhalt der Meldepflicht

Der neu formulierte § 21a ist inhaltlich weitestgehend identisch mit § 4e Bundesdatenschutzgesetz (BDSG). Diese Vorschrift ist an die kirchlichen Notwendigkeiten angepasst und trägt der praktischen Handhabung nun besser Rechnung. Die bisherige Verpflichtung der kirchlichen Stellen, vor Inbetriebnahme eine entsprechende Meldung an den Beauftragten für den Datenschutz abzugeben, kann nun entfallen, da insbesondere durch die Novellierung des § 22 auch örtlich Beauftragte bzw. Betriebsbeauftragte für den Datenschutz zu bestellen sind, die diese Aufgaben ortsnah wahrnehmen. Zum Einen sind sie von der Dienststellenleitung bzw. von der IT-Stelle regelmäßig über wesentliche Veränderungen zu informieren (dazu zählt auch die Einführung neuer DV-Programme), zum Anderen stehen ihnen nach § 21 mehr Rechte im Wege der Vorabkontrolle von neuen DV-Verfahren zu.

§ 22 Betriebsbeauftragte und örtlich Beauftragte für den Datenschutz

- In Absatz 1 ist die bisherige Soll-Vorschrift einer Bestellung für den Betriebsbeauftragten bzw. für den örtlich Beauftragten für den Datenschutz zu einer "Muss-Vorschrift" geändert worden. In den Gliedkirchen, in denen schon flächendeckend örtlich Beauftragte oder Betriebsbeauftragte für den Datenschutz bestellt worden sind, überwiegen die sehr positiven Erfahrungen. Der Datenschutz vor Ort erfährt einen höheren Stellenwert, da eine qualifizierte Person zu den Fragestellungen weiterhelfen kann. Auch ist das Handeln für die (landeskirchlichen) Beauftragten für den Datenschutz einfacher, da sie vor Ort Ansprechpersonen haben. Für alle Beteiligten ist es hilfreich, wenn die Qualifizierung der örtlich Beauftragten oder Betriebsbeauftragten für den Datenschutz durch Schulungen seitens der Gliedkirchen bzw. der Beauftragten für den Datenschutz geschieht. Zukünftig hat die Bestellung der örtlich Beauftragten oder Betriebsbeauftragten für den Datenschutz immer schriftlich zu erfolgen. Die bisher in Satz 2 vorgesehene Bestellung bei sechs Personen, die regelmäßig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zu tun haben, wurde auch hier, wie bereits bei § 21 Absatz 2, auf neun Personen angehoben. Gleiches sieht das Bundesdatenschutzgesetz vor (§ 4f Absatz 1 Satz 4 BDSG). Eine strengere Regelung, als das Bundesdatenschutzgesetz bei der Bestellungsverpflichtung vorsieht, erscheint nicht angebracht. Die im BDSG vorgesehene Grenze von 20 Personen betrifft nur den nicht öffentlichen (privaten) Bereich (§ 4f Absatz 1 Satz 3) und kann somit nicht für

die Kirche herangezogen werden. Die Bestellung kann sich auf mehrere kirchliche Stellen beziehen, sodass auch hier eine gemeinsame Wahrnehmung zu Synergieeffekten führt. Hierzu können auch Außenstehende, Dritte, bestellt werden, die z.B. aufgrund eines Werkvertrages die Aufgaben eines Betriebsbeauftragten oder eines örtlich Beauftragten für den Datenschutz wahrnehmen. Insofern unterscheiden sie sich gravierend von den Beauftragten für den Datenschutz nach § 18.

- In Absatz 3 ist die Befugnis, Auskünfte einzuholen und Einsicht in die Unterlagen zu nehmen, aufgenommen worden.
- In Absatz 4 ist ebenfalls das erschwerte Kündigungsrecht wie in § 18 Absatz 5 normiert, das nur aus einem wichtigem Grund ausgeübt werden kann, der auch zu einer fristlosen Kündigung berechtigen würde. Auch hier ist im Weiteren der Kündigungsschutz mit seiner Nachwirkung fixiert, wie es in § 4f Absatz 3 Satz 5 des Bundesdatenschutzgesetzes (BDSG) seinen Ausdruck gefunden hat.
- In Absatz 5 wurde zur Qualifizierung der örtlich Beauftragten oder Betriebsbeauftragten für den Datenschutz weitgehend die Regelung des § 4f Absatz 3 Satz 7 des Bundesdatenschutzgesetzes übernommen, in Anlehnung an § 19 Absatz 3 des Mitarbeitervertretungsgesetzes der EKD. Die örtlich Beauftragten oder Betriebsbeauftragten für den Datenschutz haben einen Rechtsanspruch auf Fort- und Weiterbildung, die Dienststelle hat die Kosten zu übernehmen.
- Absatz 8 verweist zur Verdeutlichung darauf hin, dass die Bestellung den nach § 18 Absatz 1 Beauftragten für den Datenschutz anzuzeigen ist. Sie müssen über ihre "Ortskräfte“ im Bilde sein.
- In Absatz 9 ist der Fall geregelt, dass keine Verpflichtung zur Bestellung einer örtlich Beauftragten oder Betriebsbeauftragten für den Datenschutz besteht. Da die Leitung der kirchlichen Stelle immer die Verantwortung für ein ordnungsgemäßes Handeln trägt, gilt dies erst recht für den Datenschutz. Daher verdeutlicht Abs. 9 diese Verpflichtung der Leitung der kirchlichen Stelle auf Einhaltung der Bestimmungen des Datenschutzes, sowie die ordnungsgemäße Anwendung der DV-Programme zu überwachen, für die Aufklärung und Schulung der Mitarbeitenden Sorge zu tragen. Dies gilt auch für den Fall einer vorübergehenden Vakanz, wenn zum Beispiel eine (Neu)Bestellung von örtlich Beauftragten oder Betriebsbeauftragten für den Datenschutz noch nicht erfolgt ist.

§ 24 Datenerhebung, -verarbeitung und -nutzung bei Dienst- und Arbeitsverhältnissen

In Absatz 1 konnten die Worte "Bewerber und Bewerberinnen " aufgrund der in § 2 Absatz 13 vorgenommenen Definition entfallen.

§ 27 Ergänzende Bestimmungen, Rechtsweg

Die Ermächtigungsgrundlage in Absatz 1, so hat es die Praxis in der Vergangenheit gezeigt (Durchführungsbestimmung – Fundraising), ist nicht ausreichend. Der Rat der EKD soll zukünftig mit Zustimmung der Kirchenkonferenz auch ergänzende Durchführungsbestimmungen zu diesem Kirchengesetz erlassen können, etwa um die Einheitlichkeit des kirchlichen Datenschutzrechtes sicherzustellen. Die gleiche Regelungskompetenz haben die Gliedkirchen in Absatz 2 für ihren Bereich, die oftmals differenziertere Lösungen erfordern. Diese dürfen jedoch keine dem Recht der EKD widersprechende Normierungen darstellen.

Im neuen Absatz 4 ist der Rechtsweg zu den kirchlichen Verwaltungsgerichten für Streitigkeiten auf der Grundlage dieses Gesetzes normiert. § 15 Absatz 1 Nr. 3 Verwaltungsgerichtsgesetz der EKD (VwGG.EKD) sieht diese Möglichkeit der Eröffnung des kirchlichen Verwaltungsrechtsweges vor.

Anlage (zu § 9 Absatz 1)

Hier ist nach 8. eine Ergänzung hinzugefügt worden, wie sie sich auch im Bundesdatenschutzgesetz vorfindet. Sie trägt der Tatsache Rechnung, dass Verschlüsselungsverfahren weitgehend Verwendung finden sollten, und jeweils den Stand der Technik beinhalten müssen.

Artikel 2 Änderung des Kirchengerichtsgesetzes der Evangelischen Kirche in Deutschland

Die in § 27 Absatz 4 getroffene Regelung des Rechtsweges zu dem Kirchengericht der EKD – Kammer für verwaltungsrechtliche Streitigkeiten – hat die entsprechende Anpassung des Kirchengerichtsgesetzes zur Folge, die hierin getroffen wird.

Artikel 3 Bekanntmachungserlaubnis

Die Erlaubnis, die von der EKD-Synode beschlossenen Änderungen als Fließtext bekannt zu machen, erleichtert die Lesbarkeit des Textes und schließt notwenige redaktionelle Änderungen, Fehler mit ein, die auf diese Weise mit in den Blick genommen werden können und keine erneute Befassung des Gesetzgebungsorgans von Nöten machen.

Artikel 4 Inkrafttreten, Übergangsregelungen

Folgende Inkrafttretens-Regelung ist vorgesehen:

"(1) Dieses Kirchengesetz tritt am 1. Januar 2013 in Kraft.

(2) Bisherige Bestellungen der Beauftragten für den Datenschutz bleiben unberührt, soweit hierbei die Regelungen des § 18 Absatz 3 Satz 3 und 4 und Absatz 4 Satz 1, 2. Halbsatz und die Sätze 2 bis 4, Beachtung finden."

Um den geforderten rechtlichen Anforderungen möglichst bald gerecht zu werden, ist ein schnellstmögliches Inkrafttreten erforderlich. Nach der frühestmöglichen Beschlussfassung durch die Synode im November 2012 und der sich noch anschließenden Zustim-

mungsnotwendigkeit durch die Kirchenkonferenz Anfang Dezember 2012 ist dies der 1. Januar 2013.

Bisherige Bestellungen von Beauftragten für den Datenschutz, so sieht es die Regelung in Absatz 2 vor, bleiben unberührt, soweit hierbei die Grundvoraussetzungen wie Kirchenmitgliedschaft, gewissenhafte Aufgabenwahrnehmung, Weisungsungebundenheit, organisatorische und sachliche Unabhängigkeit der Beauftragten für den Datenschutz Beachtung finden.

Diese (Alt-) Bestellungen können jedoch nicht verlängert werden und laufen somit aus. Für alle weiteren (späteren) Bestellungen gelten die Voraussetzungen des Gesetzes uneingeschränkt.