Vorblatt

zum Entwurf eines Kirchengesetzes über den Einsatz von Informationstechnik in der Evangelischen Kirche in Hessen und Nassau (IT-Gesetz)

A. Problemlage und Zielsetzung

In der Evangelischen Kirche in Hessen und Nassau wird – wie in allen anderen Lebensbereichen auch – zunehmend mit vernetzter Informationstechnik gearbeitet. Mit diesem Gesetzentwurf soll klargestellt werden, dass Informationstechnik der Erfüllung des kirchlichen Auftrags dient. Zur Verbesserung der Zusammenarbeit, der Gewährleistung einheitlicher Sicherheitsstandards und der Wirtschaftlichkeit soll zunehmend auf allen Ebenen der EKHN einheitliche Informationstechnik entwickelt und eingesetzt werden. Diese Informationstechnik muss sicher sein, d. h. alle vertraulichen Daten müssen vor unbefugter Preisgabe geschützt werden. Die Daten müssen integer sein, d.h. sie müssen korrekt und frei von Manipulationen bleiben und verfügbar sein.

B. Lösung

Mit diesem Gesetz sollen die rechtlichen Rahmenbedingungen dafür geschaffen werden, dass zum einen die Kirchenleitung einheitliche informationstechnische Verfahren für bestimmte Bereiche der EKHN verbindlich festlegen kann. Zum anderen sollen die rechtlichen Rahmenbedingungen für die Umsetzung der IT-Sicherheit in der einheitlichen Informationstechnik geschaffen werden, u.a. durch die Berufung eines Beauftragten/ einer Beauftragten für Sicherheit in der Informationstechnik für die EKHN.

C. Alternativen

Es werden keine Alternativen vorgeschlagen.

D. Finanzielle Auswirkungen

Die finanziellen Auswirkungen können schwer eingeschätzt werden. Die Kosten sind in jedem Fall deutlich geringer als die möglichen Kosten durch schwere Schäden in der Informationstechnik, wie zum Beispiel durch den Totalverlust von Daten.

E. Beteiligung

Kirchenleitung
Datenschutzbeauftragter der EKHN

Referenten/in: KRin Langmaack (federführend)
OKR Heine
KR Karsten Schmitz

F. Anlagen

1. Wortlaut § 2 BSIG,
2. § 9 DSG-EKD und Anlage zu § 9 DSG-EKD

Kirchengesetz über den Einsatz von Informationstechnik in der Evangelischen Kirche in Hessen und Nassau (IT-Gesetz)

Vom ...

Die Kirchensynode der Evangelischen Kirche in Hessen und Nassau hat das folgende Kirchengesetz beschlossen:

(Stand 24.3.2011)

§ 1. Anwendungsbereich. (1) Dieses Kirchengesetz regelt den Einsatz von Informationstechnik in der Evangelischen Kirche in Hessen und Nassau (EKHN). Zum Einsatz von Informationstechnik gehören im Wesentlichen folgende Bereiche:

1. Einheitlichkeit,
2. Sicherheit in der Informationstechnik,
3. Intranet.

(2) Der EKHN organisatorisch zugeordnete rechtlich selbstständige Werke und Einrichtungen können dieses Kirchengesetz ganz oder in Teilen für anwendbar erklären.

(3) Die Regelungen des Datenschutzgesetzes der Evangelischen Kirche in Deutschland und des Mitarbeitervertretungsgesetzes bleiben unberührt.

§ 2. Grundsätze. (1) Der Einsatz von Informationstechnik dient der Erfüllung des kirchlichen Auftrags.

(2) Informationstechnik hat die Sicherheit der automatisierten Verarbeitung von Daten zu gewährleisten.

(3) Zur Verbesserung der Zusammenarbeit, der Gewährleistung eines einheitlichen Sicherheitsstandards und der Wirtschaftlichkeit auf allen Ebenen der EKHN wird zunehmend einheitliche Informations- und Kommunikationstechnik entwickelt und eingesetzt.

§ 3. Begriffsbestimmungen. (1) Die Informationstechnik im Sinne dieses Kirchengesetzes umfasst alle technischen Mittel zur automatisierten Verarbeitung von Daten.

(2) Sicherheit in der Informationstechnik (IT-Sicherheit) bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Daten betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen, Komponenten oder Prozessen oder
2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.

(3) Kommunikationstechnik der Evangelischen Kirche in Hessen und Nassau ist die Informationstechnik, die von einer oder mehreren kirchlichen Einrichtungen oder im Auftrag einer oder mehreren kirchlichen Einrichtungen betrieben wird und der Kommunikation oder dem Datenaustausch untereinander oder mit Dritten dient.

(4) Sicherheitsrisiken sind Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion informationstechnischer Systeme beeinflussen können.

§ 4. Aufgaben der Kirchenverwaltung. Die Kirchenverwaltung fördert die Sicherheit in der Informationstechnik. Hierzu nimmt sie folgende Aufgaben wahr:

1. Abwehr von Gefahren für die Sicherheit der Informationstechnik der EKHN;
2. Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen, soweit dies zur Erfüllung der Aufgaben der EKHN erforderlich ist;
3. Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen und Komponenten sowie Prüfung und Bewertung der Konformität im Bereich der IT-Sicherheit;
4. Prüfung, Bewertung und Entscheidung über die Einführung einheitlicher informations- und kommunikationstechnischer Systeme für alle Ebenen der EKHN;
5. Sicherung der Datenqualität bei einheitlichen Lösungen und
6. Sicherstellung des laufenden Betriebes bei einheitlichen Lösungen.

§ 5. Einheitlichkeit. (1) Die Kirchenleitung kann einheitliche Lösungen in der Informationstechnik festlegen, um die Ziele des § 2 Absatz 3 zu erreichen. Kirchliche Einrichtungen sind verpflichtet, die von der Kirchenleitung festgelegten einheitlichen informationstechnischen Lösungen für ihren Bereich einzusetzen. Solange die Kirchenleitung von dieser Regelung keinen Gebrauch macht, sind die eingesetzten informationstechnischen Lösungen der Kirchenverwaltung zu melden.

(2) Kirchliche Einrichtungen haben vor wesentlichen Entscheidungen auf dem Gebiet der Informationstechnik die Beratung der Kirchenverwaltung in Anspruch zu nehmen.

§ 6. Sicherheit in der Informationstechnik. (1) Jede kirchliche Einrichtung ist verpflichtet, Sicherheit in der Informationstechnik zu gewährleisten. Hierfür ist das jeweilige Leitungsorgan verantwortlich.

(2) Die Kirchenleitung beschließt eine IT-Sicherheitsrahmenrichtlinie. Diese konkretisiert die Anforderungen der Anlage zu § 9 des Datenschutzgesetzes der EKD.

(3) Zur Gewährleistung der Sicherheit in der Informationstechnik ist jede kirchliche Einrichtung verpflichtet, ein IT-Sicherheitskonzept zu erstellen, wenn sie eigene informationstechnische Lösungen verwendet. Die Sicherheitsrahmenrichtlinie ist zu beachten. Das IT-Sicherheitskonzept muss Maßnahmen gegen Gefährdungen von innen und außen enthalten. Die IT-Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Daten und informationstechnischen Systeme stehen. In Dekanaten können einheitliche IT-Sicherheitskonzepte eingeführt werden. Das IT-Sicherheitskonzept bedarf der Genehmigung der Kirchenverwaltung.

§ 7. Kommunikationstechnik. (1) Das Internet darf nur im Rahmen des kirchlichen Auftrags genutzt werden. Soweit die private Nutzung gestattet wird, sind die Einzelheiten im Rahmen einer Dienstvereinbarung zu regeln.

(2) Die Nutzung des gesamtkirchlichen Intranets dient zur Bereitstellung und zum Austausch dienstlicher Daten.

(3) Die Nutzung des gesamtkirchlichen E-Mail-Systems dient der dienstlichen Kommunikation.

§ 8. Beauftragte oder Beauftragter für Sicherheit in der Informationstechnologie (IT-Sicherheitsbeauftragte/ IT-Sicherheitsbeauftragter). (1) Die Kirchenleitung beruft für die Dauer von jeweils sechs Jahren eine Beauftragte oder einen Beauftragten für Sicherheit in der Informationstechnik. Die oder der Beauftragte für Sicherheit in der Informationstechnik ist bei einheitlichen Verfahren für die Sicherheit der Informationstechnik im Sinne dieses Kirchengesetzes zuständig.

(2) Die oder der IT-Sicherheitsbeauftragte hat auf der Grundlage der Sicherheitsrahmenrichtlinie das Sicherheitskonzept zu erstellen, anzupassen sowie Erweiterungen aufzunehmen und der Kirchenleitung zur Beschlussfassung vorzulegen. Die Kirchenleitung verantwortet die Umsetzung.

(3) Der oder dem IT-Sicherheitsbeauftragten ist auf Verlangen Auskunft sowie Einsicht in alle Unterlagen und Akten über IT-sicherheitsrelevante Vorgänge zu geben; ihr oder ihm ist jederzeit Zutritt zu allen Diensträumen und Anlagen zu gewähren.

§ 9. Datenverarbeitung im Auftrag. Die Kirchenverwaltung schließt im Rahmen von einheitlichen informationstechnischen Lösungen als gesetzliche Stellvertreterin Vereinbarungen über die Auftragsdatenverarbeitung personenbezogener Daten mit dem oder den Auftragsnehmern für die beteiligten kirchlichen Einrichtungen ab.

§ 10. Weitere Aufgaben der Kirchenverwaltung. (1) Die Kirchenverwaltung ist berechtigt, im Rahmen ihrer gesetzlichen Aufgaben bei einheitlichen Verfahren die Daten automatisiert zu verarbeiten.

(2) Der Kirchenverwaltung obliegt weiterhin

1. die Erhebung, Verarbeitung und Übermittlung der für die gesetzliche Prüfung erforderlichen Daten der Kirchengemeinden, Dekanate
   und der Gesamtkirche an die staatliche Finanzverwaltung sowie die staatlichen Sozialversicherungsträger. Die kirchlichen Einrichtungen sind zur Übermittlung der für die gesetzliche Prüfung erforderlichen Daten an die Kirchenverwaltung verpflichtet;

2. die Übermittlung von personenbezogenen Daten an andere Evangelische Kirchen, die Mitglied der Evangelischen Kirche in Deutschland sind, und die Evangelische Kirche in Deutschland im Rahmen des kirchlichen Meldewesens, von statistischen Daten im Rahmen der staatlichen Statistikgesetze an staatliche Behörden sowie die automatisierte Verarbeitung von statistischen Daten im Rahmen des Controllings.

§ 11. Verwaltungsvorschriften. Die Kirchenleitung kann ergänzende Regelungen zu diesem Kirchengesetz im Rahmen einer Rechtsverordnung sowie Verwaltungsvorschriften zur Ausführung dieses Kirchengesetzes erlassen.

§ 12. Inkrafttreten. Dieses Kirchengesetz tritt am... in Kraft.

Begründung:

A. Vorbemerkung

Bei allen Diskussionen um Datenschutz und automatisierte Datenverarbeitung wird gerne übersehen, dass die traditionelle Bearbeitung von Daten in Papierform ein hochkomplexes System erfordert, um drei Grundwerte sicherzustellen:

1. Vertraulichkeit, d. h. vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.
2. Integrität, d. h. Korrektheit, Manipulationsfreiheit und Unversehrtheit von Schriftstücken und Akten.
3. Verfügbarkeit, d. h. die schriftlich gesammelten Informationen müssen zum geforderten Zeitpunkt und für den gewünschten Zeitraum immer zur Verfügung stehen.

In der EKHN werden diese Ziele durch ein umfassendes Regelungswerk wie die Schriftgutordnung, die Kassationsordnung, das Kirchenarchivgesetz und die Personalaktenordnung geregelt und auf gesamtkirchlicher Ebene durch die Schriftgutverwaltung der Kirchenverwaltung und das Zentralarchiv sichergestellt. Nur so kann sichergestellt werden, dass Informationen zunächst einmal schriftlich niedergelegt werden, wieder gefunden werden können und nach Ablauf von Aufbewahrungsfristen vernichtet werden durch einen zertifizierten Aktenvernichtungsbetrieb. Das Zentralarchiv stellt sicher, dass Archivgut sachgemäß auf Dauer aufbewahrt wird und zugänglich bleibt. Diese Verwaltungsabläufe müssen zudem noch zweckmäßig und rationell erledigt werden. Zur Unterstützung arbeitsteiligen Handelns müssen sie auch einheitlich sein.
Die automatisierte Verarbeitung von Informationen erleichtert Arbeitsabläufe. Es müssen jedoch dieselben Grundwerte der Vertraulichkeit, Integrität und der Verfügbarkeit sichergestellt werden. Um diese Grundwerte umzusetzen, bedarf es ebenfalls organisatorischer Maßnahmen. Diese werden im vorliegenden Gesetzentwurf geregelt.

B. Informationstechnik-Gesetz – IT-Gesetz

Zu § 1. Anwendungsbereich

§ 1 regelt den räumlichen und sachlichen Anwendungsbereich dieses Kirchengesetzes. In Absatz 1 wird klargestellt, dass die Informationstechnik allgemein folgende Bereiche umfasst:

- die Einheitlichkeit,
- die Sicherheit in der Informationstechnik und
- das Intranet.

Das Gesetz gilt für die Evangelische Kirche in Hessen und Nassau, d.h. die öffentlich-rechtlich verfasste Kirche.

Absatz 2 regelt, dass der EKHN organisatorisch zugeordnete rechtlich selbstständige Werke und Einrichtungen dieses Kirchengesetz ganz oder in Teilen für anwendbar erklären können. Gedacht ist dabei insbesondere an das Diakonische Werk in Hessen und Nassau.

In Absatz 3 wird klargestellt, dass die Regelungen des Mitarbeitervertretungsgesetzes und des Datenschutzgesetzes der EKD unberührt bleiben. Die Mitbestimmungsrechte der Mitarbeitervertretungen bleiben unverändert bestehen ebenso wie die Befugnisse des Datenschutzbeauftragten.

Zu § 2. Grundsätze

Absatz 1 stellt klar, dass auch die Informationstechnik der Erfüllung des kirchlichen Auftrags dient. Diese Technik muss die Sicherheit der automatisiert verarbeiteten Daten gewährleisten, Absatz 2. Zur Verbesserung der Zusammenarbeit, der Gewährleistung eines einheitlichen Sicherheitsstandards und der Wirtschaftlichkeit soll für alle Ebenen der EKHN zunehmend einheitliche Informations- und Kommunikationstechnik entwickelt und eingesetzt werden, Absatz 3.

Zu § 3. Begriffsbestimmungen

§ 3 enthält gesetzliche Definitionen der verwendeten Fachbegriffe. Diese Definitionen sind selbsterklärend. Sie entsprechen den gesetzlichen Definitionen des § 2 Absatz 1 bis Absatz 3 des Bundesgesetzes über des Bundesamt für Sicherheit in der Informationstechnik – BSIG. Der Gesetzestext des § 2 BSIG ist als Anlage beigefügt.

Zu § 4. Aufgaben der Kirchenverwaltung

§ 4 regelt die Aufgaben der Kirchenverwaltung auf dem Gebiet der Informationstechnik und der Sicherheit in der Informationstechnik. Gemäß Absatz 1 nimmt die Kirchenverwaltung folgende Aufgaben wahr:

1. Die Kirchenverwaltung ist zuständig für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik der EKHN.
2. Die Kirchenverwaltung untersucht Sicherheitsrisiken bei der Anwendung von Informationstechnik und entwickelt Sicherheitsvorkehrungen, soweit dies zur Erfüllung der Aufgaben der EKHN erforderlich ist.
3. Sie prüft und bewertet die Sicherheit von informationstechnischen Systemen und Komponenten und prüft und bewertet die Konformität im Bereich der IT-Sicherheit.
4. Sie prüft, bewertet und führt einheitliche Informations- und kommunikationstechnische Systeme auf allen Ebenen der EKHN ein.
5. Die Kirchenverwaltung ist zuständig für die Sicherung der Datenqualität bei einheitlichen Lösungen und
6. sie stellt den laufenden Betrieb bei einheitlichen Lösungen sicher.

Es ist beabsichtigt, die bislang in der Verwaltungsverordnung über den Einsatz von Informationstechnologie in der EKHN – ITVO – geregelte Arbeitsgruppe EDV – AG-EDV – weiterzuführen. Dies soll nach dem Inkrafttreten dieses Kirchengesetzes in der Ausführungsverordnung geregelt werden. Dies hat den Vorteil, dass die Zusammensetzung und Aufgaben der AG-EDV durch kurzfristige Änderung der Rechtsverordnung geänderten Bedürfnissen und Erkenntnissen angepasst werden können.

Zu § 5. Einheitlichkeit

§ 5 enthält eine grundsätzliche Neuerung. Auf der Grundlage dieser Regelung ist die Kirchenleitung berechtigt, einheitliche Lösungen in der Informationstechnik verbindlich für die EKHN oder bestimmte Arbeitsbereiche festzulegen. Die einheitlichen Lösungen sollen den Zielen der Verbesserung der Zusammenarbeit, der Gewährleistung eines einheitlichen Sicherheitsstandards und der Wirtschaftlichkeit kirchlichen Handelns dienen. Im Gegenzug wird eine gesetzliche Pflicht begründet, die von der Kirchenleitung festgelegten einheitlichen informationstechnischen Lösungen für den eigenen Bereich einzusetzen.

Kommt beispielsweise ein Kirchenvorstand dieser Aufgabe nicht nach, so greifen die Regelungen der §§ 45, 46 der KGO ein. Beruht das Vorgehen einer Kirchengemeinde auf datenschutzrechtlichen Bedenken, so können diese im Rechtswege vor dem Kirchlichen Verfassungs- und Verwaltungsgericht geltend gemacht werden.

Solange und soweit die Kirchenleitung von der Befugnis, einheitliche Lösungen einzuführen, keinen Gebrauch macht, können individuelle informationstechnische Lösungen genutzt werden. Diese sind der Kirchenverwaltung zu melden. Kirchliche Einrichtungen haben vor wesentlichen Entscheidungen auf dem Gebiet der Informationstechnik die Beratung der Kirchenverwaltung in Anspruch zu nehmen. Die Melde- und Beratungspflicht bezieht sich nicht auf die Anschaffung einzelner Geräte. Einzelheiten werden in der Ausführungsverordnung geregelt.

Die Verpflichtung, Verfahren automatisierter Verarbeitung vor Inbetriebnahme der oder dem zuständigen Datenschutzbeauftragten zu melden, § 21 Datenschutzgesetz der EKD (DSG-EKD) bleibt bestehen. Einheitliche Lösungen müssen von der Kirchenleitung der oder dem Datenschutzbeauftragten gemeldet werden. Individuelle Lösungen einzelner Einrichtungen müssen von der oder dem Datenschutzbeauftragten gemeldet werden.

Gleiches gilt für das Mitbestimmungsrecht der Mitarbeitervertretung aus § 36 Buchst. k) MAVG. Nach dieser Regelung bestimmt die MAV mit über die Einführung von technischen Einrichtungen, die dazu geeignet sind, die Leistung oder das Verhalten von Mitarbeiterinnen und Mitarbeitern zu kontrollieren oder die die Bestimmungen des Datenschutzes der Mitarbeiterinnen und Mitarbeiter berühren. Jede kirchliche Einrichtung muss vor der Einführung die Mitarbeitervertretung beteiligen, wenn die informationstechnische Lösung den Tatbestand des § 36 Buchst. k) erfüllt. Bei der Einführung von einheitlichen informationstechnischen Systemen für Kirchengemeinden sind die Mitbestimmungsverfahren auf Dekanatsebene durchzuführen.

Als praktisches Beispiel sei die Installation einer computergesteuerten Schließanlage genannt, bei der an Stelle herkömmlicher teurer Schlüssel nur noch preiswerte Chipkarten verwendet werden. Die Einrichtungen der EKHN sind bei der Entscheidung frei, ob und wenn ja welche EDV-gestützte Schließanlage sie für ihre Gebäude einführen wollen. Vor der Einführung müssen sie die Beratung der Kirchenverwaltung in Anspruch nehmen und das Verfahren vor Inbetriebnahme der oder dem Datenschutzbeauftragten gemäß § 21 Absatz 1 DSG-EKD melden. Da diese Anlage geeignet ist, Bewegungsprotokolle der Beschäftigten zu erstellen, besteht ein Mitbestimmungsrecht der MAV bei der Einführung, § 36 Buchst. k) MAVG.

Erst wenn die Kirchenleitung gemäß Absatz 1 eine bestimmte Schließanlagentechnik verbindlich vorschreiben sollte, darf ab diesem Zeitpunkt nur noch diese Technik installiert werden. Wird diese Technik in einer kirchlichen Einrichtung eingeführt, bleiben die Meldepflicht an die oder den Datenschutzbeauftragten und das Mitbestimmungsrecht der Mitarbeitervertretung jedoch bestehen.

Zu § 6. Sicherheit in der Informationstechnik

Sicherheit in der Informationstechnik dient dem Schutz **aller** elektronisch gespeicherten Daten und ist Voraussetzung für den Datenschutz im Sinne des DSG-EKD, der nur dem Schutz personenbezogener Daten dient.

IT-Sicherheit hat drei Grundwerte:

1. Vertraulichkeit, d.h. vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.

2. Integrität, d.h. Korrektheit, Manipulationsfreiheit und Unversehrtheit von IT-Systemen, IT-Verfahren und Daten.
3. Verfügbarkeit, d.h. die Dienstleistungen und Funktionen eines IT-Systems und die darin enthaltenen Daten müssen zum geforderten Zeitpunkt immer zur Verfügung stehen.

Elektronisch gespeicherte Daten sollen vertraulich bleiben, integer sein und jederzeit zur Verfügung stehen, wenn sie benötigt werden. Um dies zu erreichen, müssen die Daten vor bestimmten Gefährdungen geschützt werden. Typische Gefährdungen sind

- höhere Gewalt
- organisatorische Mängel
- menschliche Fehlhandlungen
- technisches Versagen und
- vorsätzliche Schädigungen.

Für elektronisch gespeicherte Daten, seien sie personenbezogen oder nicht, gelten im Grunde dieselben Grundsätze wie für herkömmlich in Papierform gesammelte Daten. Für diese ist in der Schriftgutordnung (SGO) ebenfalls geregelt, dass vertrauliches Schriftgut vor unbefugter Einsicht zu schützen ist, § 9 SGO. Auch herkömmliche Papierunterlagen müssen so geordnet und aufbewahrt werden, dass ihre Auffindbarkeit gewährleistet ist, § 1 SGO. Dabei soll die Verwaltung des Schriftgutes insgesamt einheitlich, zweckmäßig und rationell erfolgen, § 1 SGO. In der Kassationsordnung sind darüber hinaus die Aufbewahrungsfristen geregelt.

Als praktisches Beispiel für mangelnde Sicherheit in der Informationstechnik möge eine hessische Staatsanwaltschaft dienen, bei der ein simpler Stromausfall zum dauerhaften Verlust von Beweisdaten in einem großen Ermittlungsverfahren geführt hat.

Absatz 1 stellt klar, dass es Aufgabe jeder kirchlichen Einrichtung ist, die Sicherheit in der Informationstechnik zu gewährleisten. Dies ist eine strategische Managementaufgabe, für die das jeweilige Leitungsorgan zuständig ist.

Die Kirchenleitung ist verpflichtet, die kirchlichen Einrichtungen bei dieser Aufgabe durch die Verabschiedung einer Sicherheitsrahmenrichtlinie zu unterstützen. Mit der Sicherheitsrahmenrichtlinie wird gleichzeitig die technische und organisatorische Gewährleistung des Datenschutzes konkretisiert. Gemäß § 9 DSG-EKD haben kirchliche Stellen die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung des DSG-EKD zu gewährleisten. Erforderlich sind Maßnahmen, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. In der Anlage zu § 9 DSG-EKD sind Kategorien von Maßnahmen aufgelistet, die zu treffen sind, um den Schutz personenbezogener Daten zu gewährleisten. Zu den Maßnahmen zählen die

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle

- getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.

Der Wortlaut des § 9 DSG-EKD und die Anlage zu § 9 DSG-EKD sind als Anlage beigefügt.

In Absatz 3 wird geregelt, dass jede kirchliche Einrichtung verpflichtet ist, für eigene informationstechnische Lösungen ein eigenes IT-Sicherheitskonzept zu erstellen. Das IT-Sicherheitskonzept muss die Regelungen der Sicherheitsrahmenrichtlinie beachten. Das IT-Sicherheitskonzept muss Maßnahmen gegen Gefährdungen von innen und außen enthalten. Diese müssen in einem angemessenen Verhältnis zur Bedeutung der zu schützenden Daten und informationstechnischen Systeme stehen. Dekanate können für ihre Bereiche einheitliche IT-Sicherheitskonzepte einführen. Die IT-Sicherheitskonzepte bedürfen der Genehmigung der Kirchenverwaltung.

Zu § 7. Kommunikationstechnik

In dieser Vorschrift ist geregelt, dass Internet und Intranet nur im dienstlichen Auftrag genutzt werden dürfen. Die private Nutzung des Internets kann gestattet werden im Rahmen einer Dienstvereinbarung. Das gesamtkirchliche E-Mail-System dient ausschließlich der dienstlichen Kommunikation. Dies bedeutet für kirchliche Mitarbeiterinnen und Mitarbeiter, dass das Senden und Empfangen privater E-Mails am Arbeitsplatz nicht zulässig ist. Die Inhalte privater E-Mails sind gegenüber der Einsichtnahme durch Kollegen, Vorgesetzte und Dienststellenleitung genauso einsehbar wie die dienstliche Korrespondenz. Die unzulässige Nutzung unterliegt nicht dem Datenschutz.

Zu § 8. Beauftragte oder Beauftragter für Sicherheit in der Informationstechnologie (IT-Sicherheitsbeauftragte/ IT-Sicherheitsbeauftragter)

Mit dieser Regelung wird das Amt der IT-Sicherheitsbeauftragten/ des IT-Sicherheitsbeauftragten eingeführt. Die Kirchenleitung beruft eine IT-Sicherheitsbeauftragte/ einen IT-Sicherheitsbeauftragten jeweils für die Dauer von sechs Jahren. Es ist angedacht, hierbei auf die Mitarbeiterinnen und Mitarbeiter der Kirchenverwaltung zurückzugreifen.

Der oder dem IT-Sicherheitsbeauftragten ist für die Sicherheit in der Informationstechnik bei einheitlichen Verfahren zuständig. Dabei hat sie oder er gemäß Absatz 2 auf der Grundlage der Sicherheitsrahmenrichtlinie, die die Kirchenleitung gemäß § 6 Absatz 2 zu beschließen hat, für die einheitlichen Verfahren ein Sicherheitskonzept zu erstellen, dieses anzupassen, ggf. Erweiterungen aufzunehmen und der Kirchenleitung zur Beschlussfassung vorzulegen. Die Kirchenleitung verantwortet die Umsetzung.

In Absatz 3 werden der oder dem IT-Sicherheitsbeauftragten Zutrittsrechte eingeräumt, die in ähnlicher Weise auch die Datenschutzbeauftragten nach § 19 Absatz 5 DSG-EKD haben.

Zu § 9. Datenverarbeitung im Auftrag

Werden im Rahmen einer einheitlichen informationstechnischen Lösung personenbezogene Daten im Auftrag verarbeitet, so ist jede kirchliche Einrichtung, die verantwortliche Stelle im Sinne des § 2 Absatz 8 DSG-EKD ist, gemäß § 11 DSG-EKD verpflichtet, der Stelle, die die personenbezogenen Daten im Auftrag verarbeitet, einen schriftlichen Auftrag zu erteilen, wobei die Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen festzulegen sind, § 11 Absatz 2 DSG-EKD.

In der praktischen Umsetzung bedeutet dies, dass bei einem einheitlichen Verfahren für alle Kirchengemeinden jede Kirchengemeinde als verantwortliche Stelle einzeln mit dem beauftragten Unternehmen einen Vertrag über die Auftragsdatenverarbeitung personenbezogener Daten abschließen müsste. Das Unternehmen müsste ca. 1100 Verträge abschließen! Um dies zu vermeiden, aber auch die

Anforderungen des DSG-EKD zu beachten, ist in § 10 geregelt, dass die Kirchenverwaltung diese Verträge über Auftragsdatenverarbeitung als gesetzliche Stellvertreterin im Namen und für die Kirchengemeinden abschließt. Die Kirchengemeinden als verantwortliche Stellen im Sinne des DSG-EKD werden Vertragspartnerinnen der Vereinbarungen.

Zur Zeit werden entweder keine Auftragsdatenvereinbarungen abgeschlossen oder diese werden von der Kirchenverwaltung abgeschlossen. Die Kirchenverwaltung ist jedoch nur für ihre eigenen Daten verantwortliche Stelle im Sinne des. § 2 Absatz 8 DSG-EKD.

Hält die kirchliche Einrichtung als verantwortliche Stelle die Vereinbarung für nicht datenschutzkonform, so kann sie diese gemäß § 314 BGB aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist kündigen. Sie ist dann jedoch gemäß § 11 DSG-EKD verpflichtet, eine eigene Auftragsdatenvereinbarung abzuschließen. Datenschutzrechtliche Bedenken gegen die einheitliche Lösung müssen gegenüber der oder dem Datenschutzbeauftragten geltend gemacht werden oder auf dem Rechtsweg gegenüber der Kirchenleitung.

Zu § 10. Weitere Aufgaben der Kirchenverwaltung

§ 10 enthält gesetzliche Ermächtigungsgrundlagen für die Kirchenverwaltung für Aufgaben, die die Kirchenverwaltung teilweise seit Jahren erledigt, ohne jedoch über die nach dem DSG-EKD erforderliche gesetzliche Grundlage zu verfügen.

Absatz 1 stellt klar, dass die Kirchenverwaltung berechtigt ist, im Rahmen ihrer gesetzlichen Aufgaben bei einheitlichen Verfahren die Daten automatisiert zu verarbeiten. Die Kirchenverwaltung ist berechtigt, diese Daten zu erheben, zu verarbeiten oder zu nutzen unter Einsatz von Datenverarbeitungsanlagen.

Absatz 2 Buchstabe a) enthält eine gesetzliche Ermächtigungsgrundlage für die seit vielen Jahren praktizierte zentrale Betriebsstättenprüfung durch das Finanzamt Darmstadt und die Sozialversicherungsträger. Nach den Regeln der Abgabenordnung ist jede kirchliche Körperschaft öffentlichen Rechts eine eigene Betriebsstätte, die vom jeweils örtlich zuständigen Finanzamt zu prüfen wäre. Die Sozialversicherungsträger müssten ihre Betriebsprüfungen ebenfalls vor Ort, in der einzelnen Kirchengemeinde oder in den Regionalverwaltungen durchführen. Aus Gründen der Einheitlichkeit der Prüfungsstandards, der Zweckmäßigkeit und der rationelleren Prüfung ist bereits vor Jahren mit der Finanzverwaltung vereinbart worden, die gesetzlichen Betriebsprüfungen zentral für die gesamte öffentlich-rechtlich verfasste Kirche in der Kirchenverwaltung durchzuführen. Mit Absatz 2 Buchstabe a) wird zum einen geregelt, dass die kirchlichen Einrichtungen zur Übermittlung der prüfungsrelevanten Daten an die Kirchenverwaltung verpflichtet sind. Zum anderen wird klargestellt, dass die Kirchenverwaltung diese Daten den staatlichen Behörden zu den gesetzlich geregelten Prüfungszwecken übermitteln darf.

Absatz 2 Buchstabe b) regelt drei Sachverhalte. Zum einen wird die bislang schon praktizierte Übermittlung personenbezogener Daten an Gliedkirchen der EKD sowie an die EKD im Rahmen des kirchlichen Meldewesens gesetzlich geregelt. Diese Datenübermittlungen im IKIDA – innerkirchlicher Datenaustausch- und im ZWIKIDA – zwischenkirchlichen Datenaustausch – sind erforderlich, um die Mitgliederverzeichnisse zu pflegen. Diese sind Grundlage für die Erhebung der Kirchensteuer und die Steuerung kirchlichen Handelns.

Weiterhin wird der Kirchenverwaltung die Aufgabe zugewiesen, statistische Daten der Gesamtkirche im Rahmen der staatlichen Statistikgesetze an staatliche Behörden zu übermitteln. Im Rahmen staatlicher statistischer Erhebungen besteht eine bundes- bzw. landesgesetzliche Mitwirkungspflicht. Die statistischen Daten sind anonymisiert, d. h. personenbezogene Daten sind derart verändert, dass die

Einzelangabe über persönliche oder sachliche Verhältnisse nicht mehr oder nur noch mit einem unverhältnismäßigen Aufwand einer einzelnen Personen zugeordnet werden könnte.

Die Kirchenverwaltung ist auch zuständig für die automatisierte Verarbeitung von statistischen Daten im Rahmen des Controllings.

§ 11. Verwaltungsvorschriften

§ 11 gibt der Kirchenleitung die Möglichkeit, ergänzende Regelungen zu diesem Kirchengesetz im Rahmen einer Rechtsverordnung sowie Verwaltungsvorschriften zur Ausführung dieses Kirchengesetzes zu erlassen. Nach Inkrafttreten des Kirchengesetzes ist die IT-Verordnung zu überarbeiten und den Regelungen dieses Kirchengesetzes anzupassen.

§ 12 Inkrafttreten

Diese Vorschrift regelt das Inkrafttreten des Kirchengesetzes.