Nichtamtliche Begründung zur Verordnung zur Sicherheit der Informationstechnik (IT-Sicherheitsverordnung - ITSVO-EKD) Vom 29. Mai 2015

Lfd.	Begründung	Datum
1	Begründung zur Verordnung zur Sicherheit der Informationstechnik (IT-Sicherheitsverordnung - ITSVO-EKD) vom 29. Mai 2015 (ABl. EKD 2015 S. 146)	Stand 30. April 2015

Begründung zur Verordnung zur Sicherheit der Informationstechnik (IT-Sicherheitsverordnung - ITSVO-EKD)

I. Allgemeine Erläuterungen:

1. Grundsätzliches

Gemäß § 9 Abs. 2 Satz 1 EKD-Datenschutzgesetz (DSG-EKD) ist jede kirchliche Stelle verpflichtet, IT-Sicherheit zu gewährleisten. Die diesbezügliche Konkretion regelt der Rat der EKD gemäß § 9 Abs. 2 Satz 2 DSG-EKD durch den Erlass einer Rechtsverordnung mit Zustimmung der Kirchenkonferenz.

Das Vertrauen der Kirchenmitglieder in die Sicherheit ihrer Daten aufrecht zu erhalten, ist eine wichtige Aufgabe der EKD und ihrer Gliedkirchen. Dazu gehört, dass die in den Kirchen vorhandenen sensiblen Daten und Aufzeichnungen (z.B. Mitgliederdaten, Personaldaten, Inhalte aus Seelsorgegesprächen) nicht in unbefugte Hände geraten und sicher sind. Insofern besteht eine Verpflichtung zur Gewährleitung von Datensicherheit. Andererseits haben die Kirchen auch ein großes Eigeninteresse an der Sicherheit ihrer Daten. Es sind gerade die hier genannten kirchenspezifischen Daten, die es erforderlich machen, eine kircheneigene Datensicherheit vorzusehen. In schwierigen Verhandlungen auf europäischer Ebene sind kürzlich Voraussetzungen geschaffen worden, nach denen die Eigenständigkeit des kirchlichen Datenschutzrechtes gesichert sein dürfte. Dies bezieht die eigenständige Regelung der IT-Sicherheit ein. Die im Entwurf vorliegende, mit Zustimmung der Kirchenkonferenz zu erlassenden Ratsverordnung verfolgt das Ziel, innerhalb der EKD und ihrer Gliedkirchen die Sicherheit in der Informationstechnik zum Schutz der Daten

durch Maßnahmen zu gewährleisten, die in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen.

2. Informationstechnik

Informations- und Kommunikationstechnik (IT) ist in heutiger Zeit ein unverzichtbares Instrument zur Erfüllung von Aufgaben kirchlicher Stellen im Bereich der evangelischen Kirchen und ihrer Diakonie.

IT-Sicherheit stellt einen Teil der Informationssicherheit dar. Diese umfasst die Sicherheit von IT-Systemen und der darin gespeicherten Daten durch Realisierung und Aufrechterhaltung geeigneter technischer und organisatorischer Maßnahmen zur Gewährleistung der Schutzziele der IT-Sicherheit (Vertraulichkeit, Integrität, Verfügbarkeit).

IT ist so auszuwählen, zu nutzen und zu administrieren, dass für die damit verarbeiteten Daten zu jeder Zeit das angemessene Maß an Vertraulichkeit, Integrität und Verfügbarkeit sichergestellt ist. Die mit der IT erhobenen oder verarbeiteten Daten sind insbesondere vor unberechtigtem Zugriff, unerlaubten Änderungen und der Gefahr des Verlustes zu schützen.

Der Stellenwert, der der IT-Sicherheit bei den kirchlichen und diakonischen Einrichtungen zugewiesen wird, ist höchst unterschiedlich. Subjektiv ist es oft schwierig, ein angemessenes Sicherheitsniveau zu erreichen und aufrecht zu erhalten. Neben der steigenden Komplexität der IT-Systeme werden die Anforderungen an IT-Sicherheit immer komplexer und umfassender.

Kirchliche Stellen sind ohne Rücksicht auf deren Rechtsform gemäß § 9 Abs. 2 EKD-Datenschutzgesetz (DSG-EKD) verpflichtet, IT-Sicherheit zu gewährleisten.

Der Begriff der kirchlichen Stelle ist in § 1 Abs. 2 Satz 1 DSG-EKD (und wortgleich § 1 Abs. 2 der Verordnung) definiert und umfasst auch die rechtlich selbstständigen Einrichtungen der Diakonie, somit sind auch die Kirchengemeinden, Kirchenkreise und die entsprechenden Verbände eingeschlossen.

Bei Nichtbeachtung oder Vernachlässigung der IT-Sicherheit besteht die Gefahr massiver Beeinträchtigung der betroffenen Personen sowie das Risiko von Reputations- oder wirtschaftlichen Verlusten für die jeweilige kirchliche Stelle, aber auch darüber hinaus. IT-Sicherheitsvorfälle können nur durch ein aktives IT- und Handlungsmanagement verhindert werden.

Die Zuständigkeit hierfür geht über die jeweilige IT-Fachabteilung hinaus und bezieht alle handelnden Personen, Akteure und Dienststellen im Rahmen ihrer Tätigkeit mit ein. Jede Person kann und muss durch ihr Verhalten dazu beitragen.

IT-Sicherheit ist eine Aufgabe von hoher Priorität, für die das jeweilige Leitungsorgan der kirchlichen Stelle Verantwortung tragen muss und für Mitarbeitende eine obliegende Ver-

pflichtung im Sinne der § 33 Abs. 1 Kirchenbeamtengesetz der EKD (KBG.EKD), § 46 Abs. 1 Pfarrdienstgesetz der EKD (PFDG.EKD) auslösen kann.

3. Zielsetzung

§ 9 Abs. 1 DSG-EKD verpflichtet alle kirchlichen Stellen, technische und organisatorische Maßnahmen zu treffen, die die in der Anlage zu § 9 Abs. 1 beschriebenen IT-Sicherheitsanforderungen erfüllen.

Durch den Erlass der Verordnung durch den Rat der EKD werden die Einheitlichkeit und die Effizienz der IT-Sicherheit gefördert.

Eine einheitliche Ausrichtung von IT in rechtlicher, organisatorischer und technischer Hinsicht erzielt darüber hinaus folgende Vorteile:

- Ein vergleichbares Sicherheitsniveau für Patienten- und Klientendaten in Kirche und Diakonie,
- einen gesetzeskonformen Schutz der Meldedaten sowie
- eine Nutzung von ressourcensparenden Standardschnittstellen.

IT-Sicherheit definiert sich über drei grundlegende Schutzziele: Vertraulichkeit, Integrität und Verfügbarkeit.

Bezüglich der Vertraulichkeit muss festgelegt werden, wer auf welche Daten zugreifen darf (Rechte- und Rollenkonzept für das jeweilige IT-System), eine unbefugte Preisgabe der Daten muss möglichst ausgeschlossen werden.

Hinsichtlich der Integrität muss eine unbefugte oder unkontrollierte Veränderung der Daten, der Software und Hardware möglichst ausgeschlossen sein.

Bezüglich der Verfügbarkeit muss sichergestellt werden, dass Daten dann zur Verfügung stehen, wenn sie zur Aufgabenerfüllung gebraucht werden; gegebenenfalls eintretende Stillstandzeiten müssen in Ausnahmefällen toleriert werden können.

In den Bereichen, in denen hochsensible schutzbedürftige Daten erhoben, verarbeitet oder genutzt werden, insbesondere im Melde-, Kirchenbuch-, Personalwesen, Haushalts-, Kassen- und Rechnungswesen, im Gesundheitssektor und bei der Patientenbetreuung und -verwaltung sowie bei der Verwaltung von Klientendaten sind an die drei Schutzziele (Vertraulichkeit, Integrität und Verfügbarkeit) in der Regel hohe Anforderungen zu stellen.

Sicherheitsprüfungen vor Ort sollen umfassend durchgeführt werden und nicht nur einzelne IT-Komponenten betrachten. Dies erfordert ein auf die Gegebenheiten der jeweiligen kirchlichen Stelle abgestimmtes Gesamt-IT-Sicherheitskonzept.

Für Kirche und Diakonie liegt es nahe, sich dieser Problematik gemeinschaftlich und mit einer einheitlichen - den besonderen kirchlichen und diakonischen Gegebenheiten Rechnung tragenden - Grundausrichtung anzunehmen. Dies eröffnet zudem Synergien, spart personelle und finanzielle Ressourcen und bietet an vielen Stellen Arbeitserleichterungen.

Dabei zeigt sich, dass die Vielfalt kirchlicher Strukturen und Aufgaben unterschiedliche Risiken mit sich bringen. Neben der Betrachtung der Schutzwürdigkeit der Daten sind hierbei auch die Zugriffe auf diese mittels der IT-Systeme und deren Organisation zu betrachten. Soweit hierbei größere einheitliche Strukturen zu Grunde liegen, kann der Aufwand über Baukastensysteme vereinfacht und reduziert werden. So sind beispielsweise für den Gesamtbereich der EKHN maximal 5 Vollzeitstellen angedacht, die unter anderem mit bereits bestehenden Stellen in der Kirchenverwaltung sowie in den Regionalverwaltungen unter anderem durch Veränderungen der Aufgaben der EDV-Koordinatoren umgesetzt werden können. Für nicht auf zentrale IT-Steuerung zurückgreifende Gliedkirchen erhöht sich der Aufwand entsprechend und gibt eventuell Anlass, über entsprechende Veränderungen nachzudenken.

Für die Berechnung des jeweiligen Aufwandes für die einzelnen kirchlichen Stellen können auch die Arbeitshilfe und das Schätztool des BSI kostenfrei genutzt werden. Diese sind unter https://www.bsi.bund.de/Personalschaetzung zum freien Download verfügbar. Weitere Informationen erhalten Sie beim Bundesamt für Sicherheit in der Informationstechnik, E-Mail: sicherheitsberatung@bsi.bund.de.

Angemessene Maßnahmen müssen zum Ziel haben, die Risiken bezogen auf den Schutzbedarf der Daten und IT-Systeme zu minimieren. Die Angemessenheit dieser Maßnahmen leitet sich einerseits vom Schutzbedarf der genutzten Daten und andererseits von den örtlichen Gegebenheiten ab.

Die Evangelische Kirche in Deutschland bietet im Rahmen Ihrer Möglichkeiten dazu ihre Unterstützung auch in Form von Muster IT-Sicherheitskonzepten an.

Kirchliche Stellen garantieren durch die Anwendung dieser Verordnung unter Verwendung der Muster IT-Sicherheitskonzepte ausreichende Maßnahmen zur IT-Sicherheit und zum Datenschutz. Den staatlichen Anforderungen von § 42 Abs. 5 des Gesetzes zur Fortentwicklung des Meldewesens (MeldFortG) und den ausfüllenden Regelungen auf Länderebene wird damit Rechnung getragen.

Da die Bestellung eines IT-Sicherheitsbeauftragten als Option normiert ist und für kleine Einrichtungen ohne eigene IT und ohne Verarbeitung von Daten mit hohem Schutzbedarf vor Ort in den Muster-IT-Sicherheitskonzepten ein vereinfachtes Verfahren mittels "Check-Listen" vorgesehen ist, können dies auch die Pfarrstellen vor Ort bewältigen.

4. Grundausrichtung der IT-Sicherheit

Hinsichtlich der Grundausrichtung und zur Gewährleistung der Gleichwertig- und der Vergleichbarkeit von kirchlichen IT-Sicherheitskonzepten mit staatlichen IT-Sicherheitskonzepten hat sich der Rat der EKD dazu entschlossen, unter Berücksichtigung der kirchlichen und diakonischen Besonderheiten, sich bei seiner Normierung der IT-Sicherheitsverordnung am IT-Grundschutz und den weiteren Empfehlungen des Bundesamtes für

Sicherheit und Informationstechnik (BSI) zur Informationssicherheit (BSI-Grundschutz) oder an einem vergleichbaren Standard zu orientieren.

Als vergleichbarer Standard kommt unter anderem die ISO 27001-Zertifizierung in Betracht. Ein Zertifikat kann sowohl gegenüber Dritten im Bereich der verfassten Kirche als auch gegenüber Kunden (zum Beispiel Patienten im Bereich der Diakonie) oder Geschäftspartnern (Dienstleistungen im Rahmen der Datenverarbeitung im Auftrag) als Qualitätsmerkmal dienen.

Im Wirtschaftsleben spielt die ISO 27001-Zertifizierung eine immer größer werdende Rolle. IT-Dienstleister führen mit Hilfe dieses Zertifikats den Nachweis, dass sie die Maßnahmen nach IT-Grundschutz realisiert haben. Auch Unternehmen und Behörden können ein Interesse daran haben, gegenüber ihren Kunden oder Bürgern ihre Anstrengungen um eine ausreichende IT-Sicherheit deutlich zu machen. Diesem Anliegen werden sich die kirchlichen Stellen, insbesondere aus dem Bereich der Diakonie, auch öffnen wollen, um ihre besondere Qualität zu unterstreichen.

Weiterführende Informationen zu einer Zertifizierung und zum ISO 27001-Grundschutz – Zertifizierungsschema sind auf der BSI-Website https://www.bsi.bund.de/ zu finden.

ISIS12 (Informations-Sicherheitsmanagement System in 12 Schritten) ist ein Modell zu Vereinfachung der Einführung des BSI-Grundschutzes für kleine und mittelständische Unternehmen im Bereich der Wirtschaft. Dieses baut für die Prozesse auf dem Service-Management nach ITIL (IT Infrastructure Library) auf, welches im Bereich von Kirche und Diakonie im Gegensatz zur Wirtschaft bisher kaum Verbreitung gefunden hat.

Für Kirche und Diakonie sind die Bedürfnisse der Vereinfachung für kleine Einrichtungen bereits durch das entsprechende Muster-IT-Sicherheitskonzept abgedeckt.

Weiterhin sieht auch der sich weiter entwickelnde BSI-Standard zukünftig mehrere Module vor, die nach und nach aufgebaut werden können und jeweils, nach Prioritäten gestaffelt, unterschiedliche Abstufungen und Teilbereiche umfassen, so dass die IT-Gesamtstrategie schrittweise vervollständigt und nach den unterschiedlich gestuften Sicherheitsanforderungen vorgenommen werden kann.

Darüber hinaus können in der Diakonie vergleichbare, die in dieser Verordnung festgelegten Mindestanforderungen einhaltende und von staatlicher Seite anerkannte Standards für IT-Sicherheitskonzepte als Grundlage herangezogen werden.

Die Möglichkeit, eine zusätzliche Zertifizierungen vornehmen zu lassen, bleibt unberührt.

Mit dem BSI-Grundschutz werden verschiedene Aspekte der IT-Sicherheit beleuchtet und entsprechende Empfehlungen ausgesprochen. Dieser kann als De-Facto-Standard für die IT-Sicherheit angesehen werden. Da der BSI-Grundschutz die IT im breiten Feld betrachtet, sind auch Kataloge für IT-Bereiche dabei, die für die im kirchlichen Umfeld verwendete IT nicht zutreffen und somit nicht einbezogen werden müssen.

Im Rahmen der Orientierung an dem IT-Grundschutz des BSI bedeutet dies für die kirchlichen Stellen im Grundsatz folgendes Vorgehen:

- Betrachtung der vorhandenen IT-Systeme,
- Einstufung des Schutzbedarfes,
- Prüfen der entsprechenden Kataloge für die ermittelnden IT-Systeme,
- Ableiten der Maßnahmen gemäß BSI-Grundschutz.

5. Schutzbedarfskategorien

Das BSI unterscheidet verschiedene Schutzbedarfskategorien, die für den kirchlichen einschließlich des diakonischen Bereichs beispielsweise folgendermaßen definiert (erweitert) werden können:

- **Offen:** Dies gilt für alle im Internet frei verfügbaren Informationen und andere frei zugängliche Daten auch für dienstliche Telefonnummern.
  Zu treffende Maßnahmen: Keine Regelung notwendig.
- **Normal oder I:** Hierunter zählt man z.B. alltägliche Vertragsbeziehungen, Einkommensverhältnisse, Sozialleistungen und mögliche Schäden für die betroffenen Personen oder für die kirchliche Stelle bis max. € 50.000,-.
  Zu treffende Maßnahmen: Der IT-Arbeitsplatz muss kennwortgeschützt und darf nicht frei zugänglich sein, er sollte sich in einem abgeschlossenen Raum oder unter ständiger Aufsicht befinden. Es sind Sicherheitskopien anzufertigen, die verschlossen aufzubewahren sind.
  Vor der Weitergabe eines bereits verwendeten Datenträgers oder Datenverarbeitungsgerätes ist durch fachgerechtes Löschen sicherzustellen, dass keine Wiederherstellung von Daten durch Dritte möglich wird. Nicht öffentlich verfügbare Daten können nur dann an Berechtigte weitergegeben werden, wenn geeignete Schutzmaßnahmen (Verschlüsselung) getroffen sind.
- **Hoch oder II:** Sämtliche Daten, die die Privatsphäre betreffen, wie Schulden und Pfändungen, dienstliche Beurteilungen, Insolvenzen, Ansehensverluste betroffener Personen und/oder kirchlicher Stellen mit Schäden bis max. € 500.000,- sowie Daten, deren Ausfallzeit max. 1 bis 24 Std. betragen darf.
  Zu treffende Maßnahmen: Zusätzlich zu den zu treffenden Maßnahmen unter I sind folgende Erweiterungen zu berücksichtigen: Der IT-Arbeitsplatz muss mit einem Kennwort geschützt sein und das Kennwort muss in regelmäßigen Abständen geändert werden, die Vorgabe ist systemseitig umzusetzen. Die Einstellungen beim BIOS sind durch ein Kennwort zu schützen, das nur dem Administrator bekannt ist. Ein Booten von einem externen Datenträger ist zu unterbinden.
- **Sehr hoch oder III:** Hochsensible Daten, wie die Unterbringung in Anstalten und Einrichtungen, Daten zur Intimsphäre, zu Straftaten, zu erzieherischen Maßnahmen, Pfle-

gedaten oder Daten von Berufsgeheimnisträgern gemäß § 203 StGB oder ein breiter öffentlicher Ansehensverlust, daneben Schäden größer als € 500.000,-, sowie Daten deren Ausfallzeit max. 1 Std. betragen darf.

Zu treffende Maßnahmen: Zusätzlich zu den zu treffenden Maßnahmen unter II sind folgende Erweiterungen zu berücksichtigen: Auf mobilen Datenträgern ist ein Speichern nur mit einer Verschlüsselung nach dem aktuellen Stand der Technik zulässig. Ein besonderer Schwerpunkt ist auf die system- und nutzerunabhängige Lesbarkeit der Daten zu legen. Die Sicherheit des Schlüssels bei einer Verschlüsselung muss seitens des Konzeptes beachtet werden, um bei einem Schlüsselverlust keinen automatischen Datenverlust zu erleiden.

Meldedaten, die seitens des Staates (kommunale Meldebehörden) an die Kirchen (Rechenzentren) geliefert werden, sind hinsichtlich Vertraulichkeit und Integrität grundsätzlich in die Schutzbedarfskategorie hoch einzustufen. Patienten- und Klientendaten fallen in der Regel unter die Schutzbedarfskategorie sehr hoch (§ 203 StGB) oder hoch.

Diese Empfehlungen sind auch auf Grund der staatlichen Festlegungen in Zusammenhang mit OSCI/XMeld EKD-weit als verbindlich anzusehen.

Neben der Einstufung der Daten in die entsprechenden Schutzbedarfskategorien und den diesbezüglich zu treffenden IT-Sicherheitsmaßnahmen sind zusätzliche Regelungen insbesondere für die Nutzung von IT-Systemen zu treffen.

Dies umfasst u.a. Regelungen zur Verhinderung von Virenvorfällen und zum Erkennen von Angriffen zum Ausspionieren persönlicher Umfelder.

Darüber hinaus ist eine Sensibilisierung der haupt- und ehrenamtlich Mitarbeitenden notwendig, die Erlangung vertraulicher Informationen - etwa unter Vortäuschung falscher Identitäten durch Dritte - zu unterbinden. Außerdem sind Verhaltensregeln beim Verdacht eines IT-Sicherheitsvorfalls zu erlassen.

6. Verantwortung und Umsetzung

Die Verantwortung für die IT-Sicherheit obliegt in all ihren Schutzzielen dem Leitungsorgan (vgl. § 4 Abs. 2 der Verordnung) der jeweiligen kirchlichen Stelle (vgl. zur diesbezüglichen Definition § 1 Abs. 2 Satz 1 DSG-EKD und wortgleich § 1 Abs. 2 der Verordnung).

Die Umsetzung auf der technischen Ebene kann durch zentral vorgegebene Strukturen rechtlich und konzeptionell, z.B. durch ein IT-Gesetz oder ein entsprechendes Konzept, unterstützt und erleichtert werden.

Diese Strukturen gewährleisten durch zentrale Datenhaltung, Datenzugriff über gesicherte Verbindung und gleichzeitige Absicherung der Endgeräte z.B. über Festplattenverschlüsselung weitgehend die Einhaltung der Vorgaben zur IT-Sicherheit und reduzieren den finanziellen und personellen Aufwand vor Ort auf ein Minimum.

Beispiele hierfür sind die Einführung des kirchlichen Arbeitsplatzes (KirA) in der evangelischen Kirche in Hessen-Nassau, die Umsetzung des Projektes PC im Pfarramt in der Landeskirche Württemberg oder das EDV-Projekt im Ev.-luth. Kirchenkreis Mecklenburg.

Vergleichbare erleichternde konzeptionelle Schritte finden wir beispielsweise auch in der Evangelisch-Lutherischen Landeskirche Sachsens und in der Evangelischen Kirche von Kurhessen-Waldeck oder sind in anderen kirchlichen und diakonischen Einrichtungen in Planung.

Die Aufgaben, die mit der Umsetzung verbunden sind, können delegiert werden und sind von den zuständigen IT-Sicherheitsbeauftragten zu überwachen.

II. Zu den Regelungen im Einzelnen:

1. Eingangsformel

Der Rat der EKD ist durch § 9 Abs. 2 Satz 2 DSG-EKD ermächtigt, mit Zustimmung der Kirchenkonferenz für die kirchlichen Stellen (§ 1 Abs. 2 Satz 1 DSG-EKD, siehe auch oben unter I. 1.), im Verordnungswege eine verbindliche Regelung zur IT-Sicherheit zu erlassen.

Zum Erlass weitergehender Regelungen siehe § 6 der Verordnung.

2. § 1 IT-Sicherheit

Zu Absatz 1:

Im Rahmen der Verordnung wird die IT-Sicherheit gemäß § 2 Abs. 14 DSG-EKD geregelt. Die mit der IT erhobenen, genutzten oder verarbeiteten Daten sollen unter anderem vor unerlaubtem Zugriff, Veränderung und der Gefahr des Verlustes geschützt werden.

Zu Absatz 2:

Für die kirchlichen Stellen sind unter anderem folgende oder ähnliche Fragen zu beantworten:

Welche Formen von Missbrauch sind denkbar, wenn vertrauliche Informationen in die Hände unbefugter Dritter gelangen? (Vertraulichkeit)

Welche Konsequenzen sind denkbar, wenn Informationen und Daten - nicht nur in böser Absicht unbekannter Dritter sondern auch unbemerkt - durch technisches Versagen verändert werden? (Integrität)

Welche Auswirkungen sind denkbar, wenn der Zugriff auf Computer oder andere IT-Komponenten für einen längeren Zeitraum (Tage, Wochen, Monate ...) oder permanent nicht mehr möglich ist? Könnte die Arbeit fortgesetzt werden? Wie hoch wäre der mögliche Schaden oder ein Reputationsverlust? (Verfügbarkeit)

Welche Auswirkungen hat die Vielzahl unterschiedlicher Endgeräte, die dienstlich und privat eingesetzt werden?

In dem IT-Sicherheitskonzept, das überwiegend abhängig von dem Schutzbedarf der zu verarbeitenden Daten und weniger von der Größe zur Einrichtung zu gestalten ist, sind die eingesetzten IT-Systeme darzustellen und fortzuschreiben. Die Kontinuität des Fortschreibens ergibt sich aus veränderten Gegebenheiten in tatsächlicher, technischer, organisatorischer und rechtlicher Hinsicht.

Das IT-Sicherheitskonzept muss geeignete Maßnahmen gegen Gefährdungen von innen (z.B. fahrlässiger Umgang mit innerkirchlichen Daten durch Mitarbeitende) und außen (z.B. nicht autorisierter Zugriff und Abrufen von innerkirchlichen Daten durch Dritte) enthalten.

Verantwortung für die Umsetzung der IT-Sicherheit tragen die in § 1 Abs. 2 genannten kirchlichen Stellen bzw. deren Leitungsorgane (siehe auch § 4 Abs. 2 der Verordnung).

Bei der verfassten Kirche ergibt sich aus dem jeweiligen einschlägigen kirchlichen Recht, was unter einem Leitungsorgan zu verstehen ist. Besonders im Bereich der Diakonie ist es abhängig von der gewählten Organisationsform (GmbH, e.V., …).

Eine Delegation auf eine andere Strukturebene ist nicht ausgeschlossen. Bei einer gemeinsamen IT-Infrastruktur bedarf es einer ausdrücklichen Festlegung der Verantwortung.

Bevor im Rahmen einer gemeinsamen IT-Infrastruktur eine Vereinbarung zwischen den beteiligten kirchlichen Stellen geschlossen wird, sollte das gemeinsame IT-Sicherheitskonzept beraten und für die Beschlussfassung im Detail ausformuliert werden. Die Vereinbarung soll dabei folgende Aspekte berücksichtigten und entsprechende Regelungen treffen:

- Alle kirchlichen Stellen müssen diesem gemeinsamen IT-Sicherheitskonzept durch Beschlüsse der jeweils zuständigen Organe zustimmen.
- Es ist durch Beschluss festzulegen, wem die Fachaufsicht über die Umsetzung und die Einhaltung des IT-Sicherheitskonzeptes übertragen wird. Des Weiteren muss auch die kontinuierliche Fortschreibung des IT-Sicherheitskonzeptes geregelt werden.
- Kirchliche Stellen, die selbst keine Aufsicht wahrnehmen, müssen diese einer anderen kirchlichen Stelle übertragen.
- Das Verfahren zur Einleitung von Sanktionen bei Verstößen des IT-Sicherheitskonzeptes muss die Frage der Verantwortlichkeit für die Meldung eines IT-Sicherheitsvorfalls an die aufsichtsführende Stelle regeln.

Man muss sich der Tatsache bewusst sein, dass IT-Sicherheit kein statischer Zustand ist, sondern sich immerwährend fortentwickelt. Deshalb sind die Regelungen in regelmäßigen Abständen, quartalsweise oder kürzer, mindestens aber einmal im Jahr, zu überprüfen und gegebenenfalls anzupassen.

In Absatz 2 ist definiert, dass die Umsetzung der IT-Sicherheit durch die Erstellung und Fortschreibung eines IT-Sicherheitskonzeptes erfolgt. Die unterschiedlichen örtlichen Gegebenheiten, insbesondere die organisatorischen, funktionalen und technischen Besonderheiten der kirchlichen Stellen sind zu berücksichtigen und die Verbindlichkeit des IT-Sicherheitskonzeptes ist sicherzustellen.

Unabhängig von der jeweiligen Verantwortungsebene erscheint eine Zusammenarbeit im IT-Bereich, beispielsweise hinsichtlich der Verwendung einer gemeinsamen IT-Infrastruktur, sinnvoll.

So bietet sich eine Zusammenarbeit zwischen der landeskirchlichen Ebene, der Kirchenkreisebene und der kirchengemeindlichen Ebene ebenso an wie auf der Ebene der unterschiedlichen diakonischen Verbände. Es kommt auch nicht auf die Organisationsform der jeweiligen Stelle an. So ist es auch möglich, dass eine Kirchengemeinde mit einer Einrichtung der Diakonie eine gemeinsame IT-Infrastruktur unterhält.

Zu Absatz 3:

Das IT-Sicherheitskonzept bildet die Grundlage aller Maßnahmen und Vorkehrungen, die zur Erfüllung der Anforderungen der IT-Sicherheit notwendig sind. Der aktuelle Sachstand zum Thema IT-Sicherheit sollte im Detail betrachtet werden: Entweder sind bestehende Regelungen anzupassen oder es ist (in Teilbereichen) auf die Muster-IT-Sicherheitskonzepte (§ 1 Abs. 4) als Mindestanforderung zurückzugreifen. Das aus den Muster-IT-Sicherheitskonzepten abgeleitete IT-Sicherheitskonzept bildet dabei die Grundlage für die Verifizierung der Einhaltung der IT-Sicherheit. Gegebenenfalls sind weitere Regelungen durch die jeweilige verantwortliche kirchliche Stelle (§ 1 Abs. 2 Satz 1 DSG-EKD) zu treffen.

Zum erforderlichen Sicherheitsstandard vergleiche oben unter I. 4. Dabei ist herauszustellen, dass mit der Orientierung an die vorhandenen BSI-Standards eine merkliche Erleichterung und Aufwandsreduzierung einhergeht.

Zur Schutzbedarfsfeststellung und Risikominimierung siehe oben unter I. 5.

Zu Absatz 4:

Die EKD stellt Muster-IT-Sicherheitskonzepte für unterschiedlich strukturierte kleine, mittlere und große kirchliche Stellen zur Verfügung. Diese Muster-IT-Sicherheitskonzepte wurden mit externer Unterstützung (HiSolutions AG) erarbeitet. Der erforderliche Aufwand einer individuellen Anpassung bei der Erstellung des eigenen IT-Sicherheitskonzeptes verringert sich beim Zugrundelegen der Muster-IT-Sicherheitskonzepte. Diese Anpassung kann überall dort notwendig werden, wo die Muster-IT-Sicherheitskonzepte die örtlichen Gegebenheiten nicht berücksichtigen konnten. Beim zugrunde legen dieser Muster kann von einer Übereinstimmung mit den kirchlichen und staatlichen Anforderungen ausgegangen werden.

Bestehende IT-Sicherheitskonzepte von anderen kirchlichen Stellen können übernommen werden, sofern die gleiche IT-Infrastruktur oder vergleichbare IT-Verfahren verwendet werden sowie eine ähnliche Organisationsstruktur vorhanden ist. Bei der Nutzung einer gemeinsamen IT-Infrastruktur ist durch entsprechende Beschlüsse der beteiligten kirchlichen Stellen die Verbindlichkeit für alle und deren Umsetzung sicher zu stellen.

3. § 2 Einsatz von IT

Zu Absatz 1:

Der Einsatz von IT muss im Einklang mit dem IT-Sicherheitskonzept erfolgen. Die eingesetzten unterschiedlichen IT-Geräte und -Verfahren sind dort abzubilden (Verfahrensverzeichnis). Die Kurzlebigkeit aktueller IT macht es notwendig, keine IT-Systeme auszuschließen, die dem Regelungsumfang unterliegen können: Mobiltelefone, Tabletts, Drucker mit eigenem Speicher oder tragbare Geräte, wie Laptops, Notebooks und Netbooks, mit denen Daten entweder empfangen, gespeichert oder verarbeitet werden können. Später aufkommende neue Entwicklungen im Bereich von Hard- und Software sind einzubeziehen.

Zu Absatz 2:

Der Grundsatz lautet, dass für dienstliche Zwecke auch nur dienstliche IT eingesetzt wird. Dies hat der Dienstgeber zur Verfügung zu stellen. Sollen private IT-Geräte zu dienstlichen Zwecken genutzt werden, bedarf es einer besonderen Regelung/Vereinbarung.

Diese kann entweder in Form einer grundsätzlichen Normierung in einem IT-Gesetz/einer IT-Verordnung/einer IT-Richtlinie oder durch eine Regelung des kollektiven Arbeitsrechtes, etwa durch eine Dienstvereinbarung sowie einer individuellen Vereinbarung zwischen Dienstgeber und Dienstnehmer, geregelt werden.

Neben der Einhaltung der Mindestvoraussetzungen nach Absatz 1, die für den Einsatz von IT im ausschließlich dienstlichen Bereich erforderlich sind, werden in Absatz 2 für den Fall, dass private IT-Geräte durch eine ausdrückliche Vereinbarung zugelassen sind, weitere Voraussetzungen aufgestellt.

Mit der ausdrücklich angeführten Anwendung des kirchlichen Datenschutzes (Nr. 2.) wird deutlich, dass damit auch ein möglicher Zugriff selbst des Beauftragten für den Datenschutz (§ 18 DSG-EKD) auf die private Umgebung des IT-Gerätes eingeschlossen ist, um die Einhaltung des Datenschutzes prüfen zu können.

Somit ist auch die Haftung des Dienstgebers ausgeschlossen, wenn im Zusammenhang mit dienstlichen Anwendungen Schäden auf privaten IT-Geräten entstehen oder sogar ein Verlust privater Daten eintritt. Dies könnte jedoch unbillig sein, wenn der Einsatz der privaten IT auf Veranlassung des Dienstgebers erfolgt ist.

Bei Feststellung eines Verstoßes gegen die Voraussetzungen des Satzes 2 ist die Zulassung unverzüglich zu widerrufen. Dies gilt auch dann, wenn die IT-Sicherheit (der kirchlichen

Stelle) durch den Einsatz privater IT (Soft- und Hardware) gefährdet oder beeinträchtigt wird und andere Maßnahmen zur Behebung nicht ausreichen.

4. § 3 Beteiligung

Der oder die Betriebsbeauftragte, bzw. der oder die örtlich Beauftragte für den Datenschutz, (§ 22 DSG-EKD) sind frühzeitig bei der Erstellung des IT-Sicherheitskonzeptes zu beteiligen.

Eine effektive Beteiligung an der Erstellung und an der kontinuierlichen Fortschreibung des IT-Sicherheitskonzeptes setzen eine gute Entscheidungsgrundlage voraus. Hierzu zählt das Wissen beispielsweise über die Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung sowie die Kenntnis der Empfänger oder Kategorien von Empfängern, denen die Daten übermittelt werden sollen, einschließlich geplanter Datenübermittlungen in Drittstaaten (EU-Mitgliedsstaaten).

5. § 4 Einhaltung der IT-Sicherheit

Zu Absatz 1:

Zu einem qualifizierten Umgang mit IT ist eine entsprechende angemessene Fort- und Weiterbildung notwendig. Jede kirchliche Stelle sollte hierzu ein Angebot unterbreiten, bzw. im Rahmen der Nutzung einer gemeinsamen IT-Infrastruktur dieser Verpflichtung gemeinschaftlich nachkommen.

Die generelle Beteiligung der Mitarbeitervertretung entsprechend dem Mitarbeitervertretungsgesetz im Rahmen von Fortbildungsmaßnahmen bleibt davon unberührt.

Zu Absatz 2:

Hier wird klargestellt, dass die grundsätzliche Verantwortung, und somit auch die Haftung, für die IT-Sicherheit beim Leitungsorgan der jeweiligen kirchlichen (und diakonischen) Stelle obliegt, soweit es sich hierzu fachlich und tatsächlich in der Lage sieht. Zur Möglichkeit der Delegation siehe § 5 Abs. 1 der Verordnung.

Je nach Struktur der kirchlichen oder diakonischen Einrichtung obliegt die Einhaltung der IT-Sicherheitsverordnung einem Gremium oder einer Einzelperson.

Bei IT-Sicherheitsvorfällen sind geeignete Maßnahmen zu ergreifen. Unter "geeignete Maßnahmen" sind sowohl technische, d.h. im Rahmen einer Gefährdung eines IT-Systems z.B. die erforderliche Trennung von der restlichen IT sowie ggf. auch dienstrechtliche Maßnahmen zu verstehen, falls der/die Mitarbeitende einer Aufforderung, z.B. ein Fehlverhalten einzustellen, nicht nachkommt.

Im Zusammenhang mit technischen Schritten ist nach der Schwere des IT-Sicherheitsvorfalls zu unterscheiden. Wenn entweder die kirchliche Stelle Schaden nimmt oder Persönlichkeitsrechte verletzt werden, so hat die Sperrung des IT-Systems von der restlichen IT

oder die Sperrung der Zugangsberechtigung zum IT-System des entsprechenden Mitarbeitenden sofort zu erfolgen.

Wenn es sich um keinen schweren IT-Sicherheitsvorfall handelt, so kann auch eine Frist gesetzt werden, innerhalb derer der Verstoß abgestellt werden soll. Verstreicht diese Frist ohne Reaktion, so ist entsprechend zum schweren Verstoß zu verfahren.

Die Sperrung der Zugangsberechtigung zum IT-System bzw. die Trennung des IT-Systems von der restlichen IT kann vorübergehend erfolgen und ist wieder aufzuheben, wenn der Nachweis über die Beseitigung des Missstandes erbracht ist.

Bei den dienstrechtlichen Maßnahmen stehen folgende Möglichkeiten zur Verfügung:

- Belehrungspflicht:
  Die Mitarbeitenden sollen angeschrieben oder mündlich mit Protokoll darüber belehrt werden, welche negativen Folgen das Verhalten nach sich zieht, bzw. welche Konsequenzen oder welcher Schaden für die kirchliche Stelle auf Grund eines IT-Sicherheitsvorfalls eintreten kann.
- Aufforderungspflicht:
  Das Leitungsorgan oder die aufsichtführende Stelle soll die Mitarbeitenden auffordern, sich konform zur IT-Sicherheit zu verhalten, um eine Wiederholung des IT-Sicherheitsvorfalls zu vermeiden.

Generelle Zielsetzung ist, die Einhaltung der IT-Sicherheit sicherzustellen. Dienstrechtliche Maßnahmen stellen hierbei die letzte Möglichkeit dar, um durch das Fehlverhalten von Mitarbeitenden größeren Schaden für die IT und somit auch für die kirchliche Stelle abzuwenden.

Des Weiteren ist zu prüfen, inwieweit der Verstoß gegen die IT-Sicherheit nicht durch fehlende oder mangelnde Kenntnis der IT-Sicherheit bzw. entsprechender Regelungen zu erklären ist, an dieser Stelle sollte ein Schulungskonzept erarbeitet oder ein bereits bestehendes angepasst werden.

In Zusammenhang mit dienstrechtlichen Maßnahmen muss gegebenenfalls zwischen haupt- und ehrenamtlichen Mitarbeitenden unterschieden werden.

Beim Hauptamtlichen können weitergehende arbeitsrechtliche Maßnahmen ergriffen werden, z.B. Ermahnung, Abmahnung, Kündigung.

Bei Ehrenamtlichen hat das Leitungsorgan bei einem schweren Verstoß gegen die IT-Sicherheit die übertragene Aufgabe zu entziehen. Hierbei ist zu beachten, dass nach dem Ende der Aufgabenwahrnehmung auch auf privaten IT-Geräten keine dienstlichen Daten verbleiben. Hierüber muss der Ehrenamtliche der Aufsicht führenden Stelle einen geeigneten Nachweis erbringen. Geeignet sind hierfür die Erklärung, dass keine dienstlichen Daten auf privaten IT-Geräten vorhanden sind und die Zusicherung, künftig keine dienstlichen Daten auf private IT-Geräte zu übernehmen.

Zu Absatz 3:

Im Zusammenhang mit einem IT-Sicherheitsvorfall kann der oder die Beauftragte für den Datenschutz (§ 18 DSG-EKD) unabhängig von der getroffenen Maßnahme der jeweiligen kirchlichen Stelle eigene Maßnahmen anordnen (Beanstandungen aussprechen, zu Stellungnahmen auffordern, Vorschläge zur Beseitigung unterbreiten), insbesondere bei (schwerwiegenden) Verstößen gegen Persönlichkeitsrechte (§ 20 DSG-EKD).

6. § 5 IT-Sicherheitsbeauftragte

Zu Absatz 1:

Mit der Wahrnehmung der IT-Sicherheit können besondere Personen (IT-Sicherheitsbeauftragte) benannt werden. Dieser Option sollten sich vor allem größere Verbände und Einrichtungen annehmen. Auch die Möglichkeit der Zusammenarbeit mehrerer kirchlicher Stellen sieht der Verordnungstext vor, ebenso die Delegation auf eine andere Strukturebene.

Ob das Amt einer oder eines IT-Sicherheitsbeauftragten von einer Einzelperson, einer Personengruppe, in Teilzeit, im Verbund mehrerer kirchlicher Stellen oder durch externe Dienstleister wahrgenommen wird, hängt von der Größe der Einrichtung, den vorhandenen Ressourcen und dem - entsprechend der Daten einzuhaltenden - Sicherheitsniveau ab.

Als IT-Sicherheitsbeauftragter wird der IT-Administrator der eigenen Einrichtung nicht empfohlen, da dieser sich nicht selbst kontrollieren kann. Bedenken vergleichbarer Art bestehen auch, wenn diese Aufgaben durch Betriebsbeauftragte oder örtliche Beauftragte für den Datenschutz wahrgenommen werden, da hier Interessenskonflikte auftreten können.

Unter dem Aspekt der IT-Sicherheit ist es generell sinnvoll, dass kleinere kirchliche Stellen eine gemeinsame IT-Infrastruktur bilden und nutzen, die dann jeweils auch nur eine oder einen IT-Sicherheitsbeauftragten und ein IT-Sicherheitskonzept benötigen. So können dann auch die zusätzlichen Kosten und der Personalaufwand verringert werden. Der oder die IT-Sicherheitsbeauftragte hat bei der Einführung und Anpassung von IT mitzuwirken.

Zu Absatz 2:

Die Erfüllung der Aufgaben der IT-Sicherheitsbeauftragten setzt eine gute Entscheidungsgrundlage voraus. Hierzu zählen IT- und Fachverfahrenskenntnisse, das Wissen beispielsweise über die Zweckbestimmung der Datenerhebung, -verarbeitung oder -nutzung sowie die Kenntnis der Empfänger oder Kategorien von Empfängern, denen die Daten übermittelt werden sollen, einschließlich geplanter Datenübermittlungen in Drittstaaten (EU-Mitgliedsstaaten).

Hinsichtlich ihrer einzuhaltenden Qualifikation könnte sich zumindest bei größeren kirchlichen Stellen und beim Verbund einer gemeinsamen IT-Infrastruktur eine besondere Zertifizierung, wie z.B. nach Certified Information Systems Auditor (CISA) oder z.B. nach

Certified Information Security Manager (CISM) anbieten. Durch eine regelmäßige Zertifizierung ist auch eine verbindliche kontinuierliche Fortbildung sichergestellt.

Zu Absatz 3:

Die schwerpunktmäßigen Aufgaben der IT-Sicherheitsbeauftragten bestehen darin, das Leitungsorgan der kirchlichen Stelle bei dessen Wahrnehmung von Aufgaben bezüglich der IT-Sicherheit zu beraten und deren Umsetzung zu unterstützen, hierzu zählen insbesondere:

- Sachkundige Beratung für das verantwortliche Leitungsorgan bei der Festlegung des anzustrebenden IT-Sicherheitsniveaus und der IT-Sicherheitsziele.
- Unterstützung der Durchführung von Risikoanalysen im IT-Sicherheitsbereich sowie bei der Erstellung und der kontinuierlichen Fortschreibung des IT-Sicherheitskonzeptes.
- Mitwirkung bei der Anpassung der Ziele des IT-Einsatzes an die einzuhaltenden IT-Sicherheitsziele. Kontrolle und Dokumentation des Fortschritts der Realisierung von IT-Sicherheitsmaßnahmen.
- Koordinierung von Kontrollen der Effektivität von IT-Sicherheitsmaßnahmen im laufenden Betrieb.
- Schulungs- und Sensibilisierungsmaßnahmen der Mitarbeitenden zum Thema IT-Sicherheit zu initiieren und zu koordinieren.
- Regelmäßige Berichte an das Leitungsorgan über den Status Quo der IT-Sicherheit, deren möglicher Fortentwicklung und über seine oder ihre eigene Tätigkeit, ausgerichtet an der Komplexität und dem Schutzbedarf der IT-Systeme, gegebenenfalls quartalsweise oder kürzer, mindestens aber einmal im Jahr.
- Regelmäßiger Austausch und gegenseitige Information der Betriebsbeauftragten und der örtlich Beauftragten für den Datenschutz mit den IT-Sicherheitsbeauftragten.

Angebracht erscheint, den IT-Sicherheitsbeauftragten mindestens ein Stundenkontingent von einem halben Arbeitstag pro Woche für die Wahrnehmung ihrer Aufgaben zur Verfügung zu stellen, um sich in die Materie einarbeiten und fachlich auf dem Laufenden halten zu können. Welchen Umfang dies andererseits in seinem fachlichen und örtlichen Aufgabengebiet umfasst, ist den konkreten Gegebenheiten geschuldet.

Zu Absatz 4:

Um die Einhaltung der IT-Sicherheit gewährleisten zu können, muss jedermann die die Aufgaben der IT-Sicherheit wahrnehmende Person bei ihren Aufgaben unterstützen und ihnen bekanntgewordene IT-Sicherheitsvorfälle unverzüglich melden.

IT-Sicherheitsvorfälle sind bei Gefahr im Verzuge auch ohne Einhaltung des Dienstweges in einer geeigneten Art und Weise, gegebenenfalls auch in einer dokumentationsfähigen Form umgehend an die die Aufgaben der IT-Sicherheit wahrnehmende Person zu melden.

Die Bewertung und die Einleitung weiterer Schritte obliegen dem Leitungsorgan der kirchlichen Stelle.

7. § 6 Durchführungs- und Ergänzungsbestimmungen

Zu Absatz 1:

Der Rat der EKD kann in dieser Verordnung keine abschließenden Regelungen treffen. Daher muss eine Möglichkeit zum Erlass von Durchführungs- und Ergänzungsbestimmungen gegeben sein. Diese Befugnis ist sowohl für den Bereich der EKD in ihren eigenen Belangen als auch für die Gliedkirchen und die gliedkirchlichen Zusammenschlüsse vorgesehen.

Die Regelung des § 6 Absatz 1 ist insofern vergleichbar der von § 27 Absatz 2 DSG-EKD.

Dies können beispielsweise Regelungen zur Zuständigkeit (insbesondere bei der Nutzung einer gemeinsamen IT-Infrastruktur), Musterverträge zur privaten Nutzung von IT, Organisations- und Dienstanweisungen zur IT-Sicherheit, zur Durchführung des Datenschutzes sowie Regelungen zur Bestellung, Qualifikation und zur Rechtsstellung der IT-Sicherheitsbeauftragten sein.

Der Zusatz „ergänzende Bestimmungen zur IT-Sicherheit“ gestattet es ferner, über die IT-Sicherheitsverordnung hinaus, weitere, auch verschärfende Regelungen zur IT-Sicherheit (z.B. Freigabeverfahren von Software, Genehmigungsvorbehalte, Informationsverpflichtung bei IT-Sicherheitsvorfällen, Zertifizierungsverfahren zum IT-Grundschutz) zu erlassen.

Im Rahmen der Gesetzgebung ist sicherzustellen, dass das Recht in sich schlüssig ist und den Vorgaben der IT-Sicherheitsverordnung des Rates der EKD nicht widerspricht. Der in dieser IT-Sicherheitsverordnung festgelegte (Mindest-) Standard kann durch diese zusätzlichen Regelungen nicht herabgesetzt, allenfalls erhöht werden.

Zu Absatz 2:

Hierbei handelt es sich um eine Norm, die aus Gründen einer einheitlichen Bewertungsmöglichkeit, einen möglichst einheitlichen Standard festschreibt. Das erfordert die Anpassung des kirchlichen Rechtes, soweit die bestehenden Regelungen nicht im Einklang mit dieser IT-Sicherheitsverordnung stehen. Damit wird sichergestellt, dass es auf der Ebene der EKD, ihrer Gliedkirchen und der gliedkirchlichen Zusammenschlüsse keine sich widersprechenden Regelungen gibt.

Die Jahresfrist beginnt frühestens mit dem Inkrafttreten dieser IT-Sicherheitsverordnung bzw. mit dem Hinweis der EKD, dass andere kirchliche Bestimmungen dem EKD-Recht widersprechen und einer Anpassung (Änderung, Aufhebung) bedürfen. Die Jahresfrist ist angemessen, da ausreichend Zeit verbleibt, Änderungen vorzubereiten und den in verfasster Kirche und Diakonie - dort sind Dienstanweisungen als Regelung in diesem Sinne anzusehen - zuständigen Gremien zur Beratung und Beschlussfassung vorzulegen.

8. § 7 Übergangsbestimmungen

Der IT-Sicherheitsprozess beginnt mit Erstellung des IT-Sicherheitskonzeptes, welches in ihren Grundzügen bis spätestens zum 31.Dezember 2015 beginnen und spätestens bis zum 31. Dezember 2017 abgeschlossen sein.

Die engen zeitlichen Vorgaben der Umsetzung rühren für den Bereich der verfassten Kirche auch daher, dass mit dem Projekt der OSCI-XMeld-Erweiterung um das Modul Kirche eine verstärkte Kontrolle staatlicherseits der Umsetzung entsprechender kirchlicher Regelungen einhergeht.

Die Parallelität dieser Prozesse ist einzuhalten, um nicht die Einstellung der Lieferung der Meldedaten von staatlicher Seite an die Kirche zu riskieren und damit letztlich auch das kirchliche Meldewesen mit seiner Kirchenmitgliederverwaltung sowie das Kirchensteuereinzugsverfahren zu gefährden.

Falls gleichwohl dieses Datum (31. Dezember 2015) nicht eingehalten werden kann, ist auf ein entsprechendes Signal seitens der Gliedkirchen der EKD eine Verlängerung der Umsetzungsfrist nicht auszuschließen.

9. § 8 Inkrafttreten

Das Verkündigungsorgan ist das Amtsblatt der Evangelischen Kirche in Deutschland, Erscheinungsdatum jeweils zum 15. eines Monats. Es wird auch in elektronischer Form herausgegeben (www.kirchenrecht-ekd.de) und so jederzeit über einen Internetzugang einsehbar.