

IT-Sicherheitskonzept

Evangelische Kirchengemeinde

xxxGemeindexxx

**Stand: 12. Februar 2019**

1. Einleitung

Alle kirchlichen Einrichtungen[[1]](#footnote-1) sind für IT-Sicherheit verantwortlich. 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).

Die Vorgaben des Datenschutzes sind im EKD-Datenschutzgesetz (DSG-EKD) in der Novellierung aus dem Jahre 2013 formuliert. Aufgabe des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch die Verarbeitung und den Umgang seiner personenbezogenen Daten in dem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen ("informationelles Selbstbestimmungsrecht").

Alle Beschäftigten und festgelegte ehrenamtlich Tätige (siehe Anlage 1), im Folgenden: Mitarbeitende, sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten bzw. darüber zu unterrichten.

Es sind technisch-organisatorische Verfahren gemäß § 9 Absatz 1 DSG-EKD zu entwickeln, um die Durchsetzung der Rechte der Betroffenen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht in bestehende Bestandsverzeichnisse sicherzustellen.

Somit müssen auch die kleinen kirchlichen Einrichtungen Maßnahmen zur Informationssicherheit umsetzen. Mit diesem IT-Sicherheitskonzept werden die notwendigen Maßnahmen und Vorkehrungen festgelegt. Es ist regelmäßig fortzuschreiben und mit der/dem zuständigen IT-Sicherheitsbeauftragten abzustimmen.

Die Evangelische Kirchengemeinde xxxGemeindexxx gehört in der Landeskirche Berlin-Brandenburg-Schlesische Oberlausitz (EKBO) aus IT-Sicht zu den sogenannten kleinen Organisationen, die wie folgt definiert werden: kleinste und kleine Einrichtungen ohne geschultes IT-Personal, nur eine minimale IT-Infrastruktur und eine überwiegend dezentrale Datenhaltung, z. T. zentrale Anwendungen (Melde-, Finanz- und Personalwesen). Zudem existiert z. T. keine ausreichende Abgrenzung zu privaten Bereichen (Räume und Geräte). Bislang gibt es keine IT-Standards (Datensicherung, Kennwortregelungen) und auch keine Server.

Informationssicherheit sorgt dafür, dass die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit gewahrt werden. Vertraulichkeit schützen bedeutet, die IT-Systeme und Anwendungen so zu sichern, dass nur autorisierte Personen auf die verarbeiteten Daten Zugriff haben. Integrität schützt die Daten vor Manipulationen. Verfügbarkeit hingegen sorgt dafür, dass Daten im gewünschten Zeitraum zur Verfügung stehen und darauf zugegriffen werden kann.

1. Sensibilisierung der Mitarbeitenden

Besonders wichtig ist die Sensibilisierung aller relevanten Mitarbeitenden. Nur mit informierten und achtsamen Mitarbeitenden können Sicherheitsmaßnahmen wirksam umgesetzt und eventuelle Sicherheitsvorfälle rechtzeitig erkannt werden.

Sobald die Ursache eines Sicherheitsvorfalls identifiziert wurde, müssen Maßnahmen zu dessen Behebung ergriffen werden. Häufig ist es notwendig, die betroffenen IT-Systeme oder Standorte zu isolieren, um die Auswirkung des Sicherheitsvorfalls einzudämmen. Die Behebung von Sicherheitsvorfällen muss ausführlich dokumentiert werden.

Eine regelmäßige und detaillierte Sensibilisierung der Mitarbeitenden erfolgt mit dem „Merkblatt über den Datenschutz für Haupt-/Ehrenamtliche“, der zugehörigen Verpflichtungserklärung sowie der „Dienstanweisung über die Nutzung elektronischer Kommunikationssysteme und den Umgang mit mobiler IT am Arbeitsplatz“ (Anlagen 2-4).

1. Datensicherungskonzept

Computersysteme und Datenträger (z. B. Festplatten, Speicherkarten) können ausfallen oder manipuliert werden. Durch Verlust oder Veränderungen von gespeicherten Daten können mitunter gravierende Schäden verursacht werden. Durch regelmäßige Datensicherungen werden Schäden durch Ausfälle von Datenträgern, Schadsoftware oder Manipulationen an Datenbeständen nicht verhindert, deren Auswirkungen können aber minimiert werden.

Die zu sichernden Speicherorte, die für die Datensicherung Verantwortlichen sowie die Aufbewahrungsorte der Backup-Datenträger sind in der Anlage 5 aufgelistet. Die Datensicherung erfolgt wöchentlich auf einem externen Datenträger. Das zu verwendende Backup-Programm ist in Anlage 6 aufgeführt.

1. Schutz vor Schadprogrammen

Wenn IT-Systeme mit Schadsoftware (Viren, Würmer, Trojanische Pferde usw.) befallen werden, kann dies die Verfügbarkeit, Integrität und Vertraulichkeit der Systeme und der darauf gespeicherten Daten gefährden.

Daher sind die genutzten IT-Systeme (z. B. PC, Laptop) mit Viren-Schutzprogrammen ausgestattet. Automatische Updates müssen aktiviert sein. Dabei muss sichergestellt werden, dass auch die mobilen Endgeräte ausreichend geschützt sind.

Infizierte IT-Systeme müssen unverzüglich von allen Datennetzen getrennt und dürfen bis zur vollständigen Bereinigung nicht mehr produktiv genutzt werden.

Auf allen IT-Systemen müssen für die Betriebssysteme sowie für alle installierten Treiber und Programme zeitnah die jeweils hierfür veröffentlichten sicherheitsrelevanten Updates und Patches eingespielt werden. Dies gilt besonders für Programme, mit denen auf Fremdnetze zugegriffen wird (z. B. Webbrowser).

1. Regelungen für Hard- und Software

Für den sicheren Einsatz von IT-Systemen und IT-Anwendungen ist es erforderlich, dass Abläufe und Vorgänge, die diese IT-Systeme berühren, so gestaltet werden, dass das angestrebte Niveau der Informationssicherheit erreicht bzw. beibehalten wird.

Es darf nur explizit freigegebene und korrekt lizensierte (Standard-) Software eingesetzt werden, für die noch regelmäßig Sicherheitsupdates und -patches ausgeliefert werden. Eine Aufstellung der zulässigen und in der Evangelischen Kirchengemeinde xxxGemeindexxx genutzten Software, einschl. der Werkzeuge und Tools für das sichere Löschen von Daten auf Datenträgern, enthält Anlage 6.

Durch eine geeignete Benutzerkonten- und Rechteverwaltung wird sichergestellt, dass nur diejenigen Personen Zugriff auf IT-Systeme, Applikationen und Informationen haben, die aufgrund ihrer Aufgaben dazu berechtigt sind.

Bei der normalen Nutzung der Clients darf nicht mit administrativen Rechten (Admin-Benutzer) gearbeitet werden. Dies ist nur zu administrativen Tätigkeiten zulässig, die unbedingt von normalen Aufgaben getrennt durchzuführen sind.

Um sicherzustellen, dass nur Befugte auf Systeme und Informationen zugreifen können, ist es wichtig, dass sich die Mitarbeitenden vor der Nutzung per Passwort authentisieren müssen.

Das Passwort bei IT-Systemen muss aus mindestens 8 Zeichen bestehen. Es muss sich aus Klein- und Großbuchstaben sowie aus Zahlen oder Sonderzeichen zusammensetzen.

Bei der Beendigung von Arbeitsverhältnissen ist die geordnete Über- und Rückgabe der Geräte und Daten sicherzustellen.

Das sichere Löschen und Vernichten von Daten auf Datenträgern (z.B. Server, Clients, Netzkomponenten, Smartphones) muss vor der Aussonderung oder vor einer Weitergabe der Datenträger und Geräte vorgenommen werden.

Eine Übersicht über Nutzer und IT-Funktionspersonal enthält Anlage 7.

1. Büroraum/lokaler Arbeitsplatz

Der Büroraum ist ein Raum, in dem sich eine oder mehrere Personen aufhalten, um dort der Erledigung ihrer Aufgaben nachzugehen. Diese Aufgaben können (auch IT-unterstützt) aus den verschiedensten Tätigkeiten bestehen: Erstellung von Schriftstücken, Bearbeitung von Karteien und Listen, Durchführung von Besprechungen und Telefonaten, Lesen von Akten und sonstigen Unterlagen.

Büroräume in der Evangelischen Kirchengemeinde xxxGemeindexxx sind: Kirchenbüro, Arbeitszimmer des Pfarrers bzw. der Pfarrerin, Leitungsbüro Kita xxxBitteExaktDefinierenxxx.

Fenster und Türen sind zu verschließen, wenn ein Raum nicht besetzt ist. Schutzbedürftige Datenträger und Dokumente sind bei Nichtnutzung bzw. nach Beendigung der Aufgabe wegzuschließen. Dazu sind verschließbare Schreibtische, Rollcontainer und Schränke vorhanden.

In den Büroräumen müssen die vorhandenen IT-Geräte, Zubehör, Software oder Daten ausreichend gegen Diebstahl, Zerstörung und Veränderungen geschützt werden.

In Büros mit Publikumsverkehr sind Diebstahlsicherungen zum Schutz von IT-Systemen (z. B. Laptops) einzusetzen, da andernfalls die Gefahr besteht, dass solche Geräte in einem unbewachten Augenblick abhandenkommen.

1. Mobiler Arbeitsplatz

Ein mobiler Arbeitsplatz im Sinne dieses IT-Sicherheitskonzepts ist eine weitgehend ortsungebundene IT-Ausstattung (z.B. Laptop, Tablet). Bei einem mobilen Arbeitsplatz kann die infrastrukturelle Sicherheit nicht so vorausgesetzt werden, wie sie in einer Büroumgebung innerhalb der Räumlichkeiten einer Institution anzutreffen ist.

Dienstliche Aufgaben werden häufig auch an wechselnden Arbeitsplätzen und in unterschiedlichen Umgebungen durchgeführt. Die dabei verarbeiteten Informationen müssen angemessen geschützt werden (z. B. durch Sperren des Bildschirms oder Anbringen eines Sichtschutzes).

An mobilen Arbeitsplätzen sollten weder dienstliche Unterlagen noch mobile IT-Systeme unbeaufsichtigt bleiben. Sie sollten zumindest gegen einfache Wegnahme gesichert, z. B. mit einer Diebstahlsicherung versehen oder in Schränke geschlossen werden.

Beim Einsatz mobiler Geräte sind die Festplatten der Rechner grundsätzlich immer zu verschlüsseln.

1. Arbeitsplatz-Rechner

Als Arbeitsplatz-Rechner wird ein IT-System mit einem beliebigen Betriebssystem bezeichnet, das die Trennung von Benutzern zulässt.

Eine Bildschirmsperre muss eingerichtet werden, die sich sowohl manuell vom Benutzer aktivieren lässt, als sich auch nach einem vorgegebenen Inaktivitäts-Zeitraum automatisch aktiviert.

Alle Mitarbeitenden sind dazu zu verpflichten, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden.

E-Mails müssen verschlüsselt von und zu Mail-Servern übertragen werden (z. B. mittels SSL/TLS). Die entsprechenden Einstellungen bei E-Mailprogrammen (SSL/TLS) sind standardmäßig vorzunehmen.

Ein Laptop oder Notebook ist ein IT-System mit einer transportfreundlichen, kompakten Bauform, welches aufgrund dieser mobil genutzt werden kann. Ein Laptop ist ein vollwertiger Arbeitsplatz-Rechner und kann über Akkus zeitweise unabhängig von externer Stromversorgung betrieben werden.

Bei diesen Geräten sind die Festplatten grundsätzlich zu verschlüsseln.

Zugriffe von einem Laptop von außerhalb auf das interne Netz müssen abgesichert erfolgen (über SSL/TLS oder VPN verschlüsselt).

1. Mobiltelefon/Smartphone

Mobiltelefone bzw. Smartphones sind inzwischen alltäglicher Bestandteil der kirchlichen Kommunikationsinfrastruktur geworden. Neben herkömmlichen Telefongesprächen bieten die Geräte meist noch eine Vielzahl an zusätzlichen Funktionen wie das Verschicken von SMS, MMS, E-Mails, die Nutzung des Internets über WLAN oder Mobilfunk. Zudem existieren auch Apps, wie z. B. Whatsapp oder Threema, die Funktionalitäten zur Datenübertragung ermöglichen.

Verlorene Geräte müssen über den Mobilfunkanbieter umgehend gesperrt werden.

Es muss sichergestellt werden, dass die Sicherheitsmechanismen von Mobiltelefonen (z. B. Eingabe einer PIN oder eines Passworts, Fingerabdruck, etc.) genutzt werden.

Bei der Verwendung von Mobiltelefonen muss entschieden werden, ob und wie zusätzliche Dienste wie MMS, Bluetooth oder WLAN genutzt werden dürfen. Nicht benötigte Dienste sollten deaktiviert werden.

Vertrauliche Daten, wie personenbezogene Daten oder Zugangsdaten zum Netz der Institution, sind prinzipiell nicht auf den Geräten zu speichern. Eine unumgängliche Speicherung auf dem Gerät (inklusive Speicherkarte) muss ausschließlich in verschlüsselter Form erfolgen. Das Senden von vertraulichen Daten ist nur über gesicherte, von der kirchlichen Organisation bereitgestellte Transportwege, z.B. über das landeskirchenweite Intranet oder in verschlüsselter Form erlaubt. Nicht zulässig ist ein offener, unverschlüsselter Versand von vertraulichen Daten.

1. Netzwerke

Funknetzwerke (WLAN) bieten die Möglichkeit, mit geringem Aufwand drahtlose lokale Netze aufzubauen oder bestehende drahtgebundene Netze zu erweitern. WLAN können aufgrund der einfachen Installation nicht nur dauerhaft, sondern auch für temporär zu installierende Netze, wie z. B. für Veranstaltungen, verwendet werden. Eine weitere Möglichkeit zur aufwandsarmen Vernetzung sind sogenannte Power-LAN, bei denen vorhandene elektrische Leitung für den Aufbau eines Netzwerks genutzt werden.

Die Kommunikation im WLAN sowie im Power-LAN muss verschlüsselt werden. Für WLAN ist WPA2 zu verwenden. Für Power-LAN ist mindestens eine Verschlüsselung mit AES-128 zu verwenden.

Die Netzwerkschlüssel für den Zugriff auf ein WLAN sind regelmäßig zu wechseln. Sie müssen aus mindestens 12 Zeichen bestehen und Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen enthalten. Voreingestellte Standardpasswörter sind vor Inbetriebnahme unbedingt zu wechseln.

Bei der Aussonderung von WLAN-Komponenten müssen die Authentifizierungsinformationen für den Zugang zum WLAN und andere erreichbare Ressourcen, die in der Sicherheitsinfrastruktur und anderen Systemen gespeichert sind, entfernt bzw. als ungültig deklariert werden. Hierzu ist die Komponente auf die Werkseinstellung zurückzusetzen.

1. Mobile Datenträger

Mobile Datenträger werden für eine Vielzahl von Zwecken eingesetzt, beispielsweise für den Datentransport, die Speicherung von Daten oder die mobile Datennutzung. Es gibt eine Vielzahl verschiedener Varianten von mobilen Datenträgern. Hierzu gehören unter anderem Disketten, externe Festplatten, CD-ROM, DVD, Magnetbänder und USB-Sticks.

Die Mitarbeitenden müssen über die Risiken in Hinblick auf mobile Datenträger und über die erforderlichen Sicherheitsmaßnahmen informiert werden. Das erfolgt mit der „Dienstanweisung über die Nutzung elektronischer Kommunikationssysteme und den Umgang mit mobiler IT am Arbeitsplatz“ (Anlage 1).

Bei mobilen Datenträgern besteht ein hohes Verlust- und Diebstahlsrisiko. Damit die auf verlorenen oder gestohlenen Datenträgern enthaltenen Daten nicht in falsche Hände geraten, sind die Dateien zu verschlüsseln. Insbesondere vertrauliche Dateien auf mobilen Datenträgern müssen zwingend verschlüsselt werden.

Für die Verschlüsselung ist entweder die in bestimmten Programmen integrierte Verschlüsselungsfunktion (z. B. in Microsoft Word) oder die freie Software 7zip mit AES-256 Bit Verschlüsselung zu nutzen.

1. Internetnutzung

Das Internet als wichtiges Informations- und Kommunikationsmedium ist aus dem Arbeitsalltag nicht mehr wegzudenken. Auch in der Evangelischen Kirchengemeinde xxxGemeindexxx ist die Nutzung von E-Mail, Informationsangeboten und Internet-Dienstleistungen selbstverständlich. Gleichzeitig muss verhindert werden, dass durch die Anbindung der eigenen Geräte an das Internet für die Kirchengemeinde nicht akzeptable Risiken entstehen.

Alle Mitarbeitenden sollten über das Potential, aber auch die Risiken der Internet-Nutzung informiert sein. Sie müssen wissen, welche Rahmenbedingungen bei der Nutzung von Internet-Diensten zu beachten sind. Dazu gehört insbesondere, dass sie die Regeln kennen, um Dienste sicher zu nutzen und sich korrekt im Internet zu verhalten, beispielsweise in (Web-)Blogs oder sozialen Netzwerken (z. B. Facebook, Twitter). Die wichtigsten Regelungen enthält die „Dienstanweisung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz und den Umgang mit mobilen Datenträgern“ (Anlage 4).

Bei vielen Internet-Diensten müssen sich die Benutzer mittels Benutzernamen und Passwort authentisieren. Dabei sind die allgemeinen Regeln zur sicheren Verwendung von Passwörtern (siehe Hard- und Software) einzuhalten. Wichtig ist insbesondere, dass die Passwörter nicht leicht zu erraten sind. Es sind für verschiedene Internet-Dienste verschiedene Passwörter zu verwenden. Vor allem sind dafür keine Passwörter zu nutzen, die für IT-Systeme oder IT-Anwendungen innerhalb der kirchlichen und diakonischen Einrichtungen verwendet werden.

Für die sichere Ablage von Passwörtern steht der Passwortsafe „KeePass“ allen Mitarbeitenden zur Verfügung (siehe Anlage 6).

1. Checkliste für kleine Organisationen

Die folgende Checkliste dient als Umsetzungshilfe für die Prüfung und Dokumentation des Umsetzungszustandes der Sicherheitsmaßnahmen für kleine Einrichtungen. Die Checkliste kann ebenso als Nachweis der Bemühungen zur Umsetzung der IT-Sicherheit verwendet werden.

| **Nr.** | **Frage** | **Referenz** | **Umgesetzt** |
| --- | --- | --- | --- |
| **1.** | Werden neue Mitarbeitende bei der Einstellung auf bestehende Regelungen und Handlungsanweisungen zur Informationssicherheit hingewiesen? | Kap. 1 | □ |
| **2.** | Sind die wichtigen Schlüsselpositionen (in Pfarramt und Büro) durch einen Vertreter besetzt? | Kap. 1 | □ |
| **3.** | Haben alle Mitarbeitenden eine Verpflichtung zur Wahrung des Datengeheimnisses unterschrieben? | Kap. 2 | □ |
| **4.** | Werden Backup-Datenträger in einem gesonderten Raum aufbewahrt? | Kap. 3 | □ |
| **5.** | Sind auf allen Clients Virenschutzprogramme installiert? | Kap. 4 | □ |
| **6.** | Werden Betriebssysteme und Anwendungen regelmäßig aktualisiert? | Kap. 4 | □ |
| **7.** | Gibt es eine Checkliste für Mitarbeitende zur Beendigung des Arbeitsverhältnisses? | Kap. 5 | □ |
| **8.** | Gibt es eine Benutzer- und Rechteverwaltung für IT-Systeme und Anwendungen? | Kap. 5 | □ |
| **9.** | Gibt es Passwortregelungen für IT-Systeme und Anwendungen und werden diese umgesetzt? | Kap. 5 | □ |
| **10.** | Werden alle Mitarbeitenden über die Regelungen zur Nutzung von Standardsoftware informiert? | Kap. 5 | □ |
| **11.** | Wird ausschließlich Software aus vertrauenswürdigen Quellen installiert? | Kap. 5 | □ |
| **12.** | Gibt es regelmäßige Kontrollen bezüglich der installierten Software? | Kap. 5 | □ |
| **13.** | Sind auf Clients und Servern automatische Updates aktiviert? | Kap. 5 | □ |
| **14.** | Gibt es spezielle Handlungsanweisungen und Tools zum Löschen und Vernichten von Daten? | Kap. 5 | □ |
| **15.** | Sind Türen und Fenster in der Regel verschlossen, wenn die Mitarbeitenden nicht am Platz sind? | Kap. 6 | □ |
| **16.** | Sind in den Büros verschließbare Schreibtische oder Schränke vorhanden? | Kap. 6 | □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **17.** | Gibt es in Büros mit Publikumsverkehr Diebstahlsicherungen für IT-Systeme? | Kap. 6 | □ |
| **18.** | Sind am mobilen Arbeitsplatz verschließbare Schreibtische oder Schränke vorhanden? | Kap. 7 | □ |
| **19.** | Gibt es Regelungen welche dienstlichen Unterlagen am häuslichen Arbeitsplatz bearbeitet und zwischen der Institution und dem häuslichen Arbeitsplatz hin und her transportiert werden dürfen? | Kap. 7 | □ |
| **20.** | Ist auf allen Clients die Bildschirmsperre aktiviert? | Kap. 8 | □ |
| **21.** | Ist der Zugriff von mobilen Laptops auf das LAN per VPN abgesichert? | Kap. 8 | □ |
| **22.** | Ist die Verschlüsselung von E-Mail-Kommunikation zwischen Client und Server aktiviert? | Kap. 8 | □ |
| **23.** | Ist bei allen Mobiltelefonen/Smartphones die Eingabe der Geräte-PIN aktiviert? | Kap. 9 | □ |
| **24.** | Werden alle vertraulichen Daten nur verschlüsselt auf Mobiltelefonen/Smartphones oder Speicherkarten gespeichert? | Kap. 9 | □ |
| **25.** | Wird bei WLAN das Verschlüsselungsverfahren WPA2 eingesetzt? | Kap. 110 | □ |
| **26.** | Werden die Schlüssel für den WLAN-Zugriff regelmäßig gewechselt? | Kap. 110 | □ |

1. Glossar

|  |  |
| --- | --- |
| **Begriff** | **Erläuterung** |
| WPA2 | Wi-Fi Protected Access 2 (WPA2) ist die Implementierung eines Sicherheitsstandards für Funknetzwerke. |
| AES-128 | AES steht für Advanced Encryption Standard. Dies ist ein Verschlüsselungsstandard mit einer Schlüssellänge von 128 Bit. |
| TLS/SSL | Transport Layer Security (TLS) ist ein Protokoll zur Verschlüsselung von Datenübertragungen im Internet - weitläufiger bekannt unter der Vorgängerbezeichnung Secure Sockets Layer (SSL). |
| VPN | Virtual Private Network (VPN) ist ein privates (in sich geschlossenes) Rechnernetz, das auf einer öffentlichen Netzwerk-Infrastruktur aufgebaut ist. |
| Patch | Ein Patch ist ein in der Regel kleineres Softwareupdate bzw. eine kleinere Softwarekorrektur. |

1. Anlagenverzeichnis

1 Liste der auf den Datenschutz zu verpflichtenden hauptamtlich und ehrenamtlich Tätigen

**2a** Merkblatt für **Hauptamtliche** zum Datenschutz in der Kirchengemeinde

**2b** Merkblatt für **Ehrenamtliche** zum Datenschutz in der Kirchengemeinde

**3a** Verpflichtungserklärung **Hauptamtlicher** auf das Datengeheimnis

**3a** Verpflichtungserklärung **Ehrenamtlicher** auf das Datengeheimnis

4 Dienstanweisung über die Nutzung elektronischer Kommunikationssysteme am Arbeitsplatz und den Umgang mit mobilen Datenträgern

5 Regelungen zur Datensicherung

6 Übersicht der eingesetzten Arbeitsplatzrechner und der darauf genutzten Software

7 Nutzer und IT-Funktionspersonal

8 Einbezug der Mitarbeitervertretung

1. siehe § 1 Absatz 2 DSG-EKD [↑](#footnote-ref-1)