Datenschutz-Richtlinie

Der Landeskirchenrat hat in seiner Sitzung am 31. März 2020 folgende Datenschutz-Richtlinie mit unmittelbar geltendem Charakter für alle kirchlichen Stellen im Bereich der Landeskirche, die mit personenbezogenen Daten umgehen, erlassen.
Die Datenschutz-Richtlinie ersetzt das derzeitige Merkblatt zum Datenschutz. Sie bildet zusammen mit der IT-Sicherheitsverordnung die Grundlage für gelebten Datenschutz in der Landeskirche und betrifft

1. Einführung - Ziele der Datenschutz-Richtlinie

Verschiedene internationale und nationale gesetzliche Grundlagen (insb. die EU-Datenschutzgrundverordnung (DSGVO), das Bundesdatenschutzgesetz (BDSG -neu), das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG)) sowie das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) regeln die Verarbeitung (u.a. Erhebung, Speicherung und Verwendung) personenbezogener Daten, die Rechte der Betroffenen und die Pflichten des jeweils Verantwortlichen sowie Datensicherungsmaßnahmen.
Ein Verstoß gegen Datenschutzvorschriften kann erhebliche Folgen für die verantwortliche Stelle bzw. den jeweilig pflichtwidrig handelnden Beschäftigten haben, wie z.B.

- Kosten für erforderliche Verfahrensänderungen, um diese datenschutzkonform zu gestalten,
- Kosten durch Schadensersatz- und Bußgeldzahlungen in Höhe von bis zu 500.000 Euro
- Strafbarkeiten (z.B. § 42 BDSG, §§ 202, 202a, 203, 263a, 269, 303a, 303b StGB) und
- das Eintreten von Image-/ Reputationsschäden.

Angemessener Datenschutz ist daher ein „Muss“ für die verantwortliche Stelle und ihre Mitarbeitenden. Diese Richtlinie hat daher zum Ziel, den Mitarbeitenden das Thema Datenschutz bei der Dienststelle zu erläutern, um Verstöße gegen Datenschutzvorschriften zum Schutze der kirchlichen Stelle sowie seiner Beschäftigten zu verhindern. Dazu werden unter Ziffer 2 der Richtlinie die allgemeinen Grundlagen des Datenschutzes dargestellt, unter Ziffer 3 der Richtlinie die Maßnahmen der Dienststelle zum Umgang mit personenbezogenen Daten verbindlich für die Mitarbeitenden der Dienststelle geregelt und unter Ziffer 4 auf die besonderen datenschutzrechtlichen Verfahren hingewiesen.

Alle Beschäftigten sind verpflichtet, den in dieser Datenschutzrichtlinie beschriebenen Maßnahmen sowie den daraus resultierenden Anforderungen und Leitsätzen Folge zu leisten. Ein Verstoß gegen die Regelungen (und Verbote) dieser Datenschutzrichtlinie kann arbeitsrechtliche und u.U. auch strafrechtliche Folgen für die betreffenden Beschäftigten haben.

2. Datenschutz bei der Dienststelle sowie allgemeine Grundlagen des Datenschutzes

2.1 Vorstellung der externen Datenschutzbeauftragten

Zur Sicherstellung der Einhaltung der gesetzlichen Datenschutzvorschriften hat die Evangelische Kirche der Pfalz (Protestantische Landeskirche) einen externen Datenschutzbeauftragten bestellt. Der externe Datenschutzbeauftragte ist von der Geschäftsleitung bestellt, der Geschäftsleitung unmittelbar unterstellt und weisungsfrei bei der Ausübung seiner Tätigkeit.

Datenschutzbeauftragter ist: Dr. Karsten Kinast
KINAST Rechtsanwaltsgesellschaft mbH
Hohenzollernring 54
D-50672 Köln
Telefon: +49 (0)221 -222 183 -0
Telefax: +49 (0)221 -222 183 -10
kinast@kinast-partner.eu

Der externe Datenschutzbeauftragte steht den Mitarbeitenden als Ansprechpartner für sämtliche Belange des Datenschutzes zur Verfügung.
Ebenso können sich die Mitarbeitenden jederzeit an

Die Datenschutzbeauftragte der Evangelischen Kirche der Pfalz
Verwaltungsrätin i. K. Pia Schneider
Dezernat 6
Roßmarktstraße 4
67346 Speyer
Telefon: 06232 667-434
E-Mail: pia.schneider@evkirchepfalz.de

wenden.

Aufgabe der Beauftragten für den Datenschutz ist es, u.a. auf die Einhaltung des DSG-EKD hinzuwirken, d.h. darauf zu achten, dass die jeweilige kirchliche Stelle bei der Erfüllung ihrer Aufgaben die gesetzlichen Vorschriften beachtet und die Beschäftigten zu schulen.

2.2 Grundlagen des Datenschutzrechts

Die Grundlage des deutschen Datenschutzrechts bilden die EU Datenschutzgrundverordnung (DSGVO) sowie das Bundesdatenschutzgesetz (BDSG-neu).
Nach Artikel 91 der DSGVO ist es den Kirchen jedoch erlaubt, eigene Regelungen zu schaffen, die die staatlichen Regelungen nicht ergänzen, sondern für den kirchlichen Bereich ersetzen. Grundlage des Datenschutzrechts in der Evangelischen Kirche ist daher das Datenschutzgesetz der EKD (DSG-EKD), das im kirchlichen Bereich ausschließlich gilt.

2.2.1 Datenschutz - was bedeutet das eigentlich

Gemäß § 1 DSG-EKD soll das Gesetz die Grundrechte und Grundfreiheiten der Einzelnen schützen, insbesondere das Recht auf Schutz personenbezogener Daten. Der Datenschutz regelt die Verarbeitung und damit u.a. die Erhebung, Speicherung und Verwendung personenbezogener Daten.
Einfacher ausgedrückt bedeutet dies: Das Datenschutzrecht dient vor allem dazu, das Persönlichkeitsrecht einer jeden einzelnen Person (z.B. eines Interessenten oder Website-Nutzers) zu schützen. Geschützt werden also nicht die Daten von Personen, sondern die Personen selbst, und zwar im Zusammenhang mit dem Umgang der auf diese Person bezogenen Daten.

2.2.2 Abgrenzung: Datenschutz vs. IT-Sicherheit

Der Datenschutz bezweckt demnach den Schutz der Privatsphäre, d.h. die Freiheit jedes Einzelnen zu bestimmen, ob und wie seine persönlichen Daten offenbart oder verwendet werden. Er stellt damit einen Schutz vor Verletzungen und Eingriffen in die Persönlichkeitsrechte dar.
Das Thema Informationssicherheit bezweckt dagegen den Schutz von Informationen/Daten und ist daher unerlässlich, um den Schutz von Daten in technischer und organisatorischer Hinsicht zu gewährleisten.

2.2.3 Schutzobjekt des DSG-EKD - Personenbezogene Daten und besondere Kategorien personenbezogener Daten

Personenbezogene Daten im Sinne von § 4 Nr. 1 DSG-EKD sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar gilt eine Person dann, wenn sie direkt oder indirekt (z.B. mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind) identifiziert werden kann. Erfasst sind insbesondere Daten wie Name, Anschrift, Familienstand, Geburtsdatum, Staatsangehörigkeit, Beruf, Konfession, Einkommen- und Vermögensverhältnisse. Die Verarbeitung (u.a. Erhebung, Speicherung, Verwendung) von personenbezogenen Daten ist nur zulässig, soweit das DSG-EKD oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder die/der Betroffene eingewilligt hat.

Das DSG-EKD hat besondere Kategorien personenbezogener Daten im Sinne von § 13 DSG-EKD unter besonderen Schutz gestellt. Dazu gehören Angaben über:

- die rassische und ethnische Herkunft,
- politische Meinung,
- religiöse oder weltanschauliche Überzeugungen,
- Gewerkschaftszugehörigkeit,
- genetische und biometrische Daten
- Gesundheit oder
- Sexualleben oder der sexuellen Orientierung.

Vorstehende besondere Kategorien personenbezogener Daten dürfen nur unter engen Voraussetzungen verarbeitet werden und unterliegen u.U. einer vorherigen Datenschutz-Folgenabschätzung des externen Datenschutzbeauftragten nach § 34 DSG-EKD.

2.3 Grundzüge des Datenschutzes

2.3.1 Zweckbindung

Es gilt der Grundsatz der Zweckbindung, d.h. der Zweck für die Verarbeitung personenbezogener Daten muss im Voraus bestimmt werden. Jede weitere Verarbeitung oder Nutzung muss im Einklang mit diesem Zweck stehen, sofern das DSG-EKD nicht die Verwendung für einen anderen Zweck erlaubt.

2.3.2 Verbot mit Erlaubnisvorbehalt

Ferner gilt das sog. Verbot mit Erlaubnisvorbehalt, wonach jede Form der Verarbeitung personenbezogener Daten – und zwar vom Erheben, Speichern, Verwenden, Verändern, Abfragen bis hin zum Übermitteln oder Löschen – als Eingriff in die Grundfreiheiten und die Privatsphäre der betroffenen Person gilt und deshalb einer Legitimation bedarf. Als Folge des grundsätzlichen Verbotes mit Erlaubnisvorbehalt bedarf es für die rechtmäßige Verarbeitung personenbezogener Daten einer Einwilligung oder einer gesetzlichen Rechtfertigungsgrundlage (z.B. § 6 Nr. 2 bis 8 DSG-EKD).

2.3.3 Rechte des Betroffenen

Den Betroffenen (z.B. den Gemeindemitgliedern oder Website-Nutzern) stehen die nachstehenden Rechte zu:

- Information, wenn die Erhebung der personenbezogenen Daten beim Betroffenen erfolgt (§ 17 DSG-EKD).

- Information, wenn die Erhebung der personenbezogenen Daten nicht beim Betroffenen erfolgt (§ 18 DSG-EKD). Auskunftsrecht, ob bzw. welche personenbezogenen Daten verarbeitet werden einschließlich Herkunft, Verarbeitungszweck und ggf. Empfängerin/Empfänger der Daten (§ 19 DSG-EKD)
- Berichtigungsrecht, d.h. Daten sind unverzüglich zu berichtigen, wenn sie unrichtig sind (§ 20 DSG-EKD).
- Löschungsrecht, z.B. bei unzulässiger Datenverarbeitung und bei nicht mehr notwendigen Daten (§ 21 DSG-EKD).
- Einschränkung der Verarbeitung, z.B. wenn die/der Betroffene die Richtigkeit der Daten bestreitet oder wenn die/der Verantwortliche, anders als der Betroffene, die Daten nicht mehr benötigt (§ 22 DSG-EKD).
- Mitteilung, d.h. die/der Verantwortliche teilt allen Empfängerinnen/Empfängern der Daten grundsätzlich jede Berichtigung, Löschung oder Einschränkung der Verarbeitung mit; Unterrichtung über diese Empfängerinnen/Empfänger, wenn die betroffene Person dies verlangt (§ 23 DSG-EKD).
- Datenübertragbarkeit, d.h. das Recht, die Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten (§ 24 DSG-EKD). Widerspruchsrecht, d.h. keine (weitere) Verarbeitung wenn die/der Betroffene aus besonderen Gründen widerspricht und die/der Verantwortliche keine schutzwürdigen Gründe nachweisen kann, die die Interessen der betroffenen Person überwiegen (§ 25 DSG-EKD).

2.4 Verpflichtung auf den Datenschutz

Den mit der Datenverarbeitung befassten Personen ist untersagt, personenbezogene Daten in unzulässiger Weise zu verarbeiten.
Jeder Mitarbeitende der Dienststelle wurde daher auf den Datenschutz hingewiesen und ist diesem verpflichtet. Demnach ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu speichern, zu verändern, zu verwenden, ihre Verarbeitung einzuschränken, sie zu löschen oder diese Daten Dritten bekanntzugeben oder zugänglich zu machen. Die Verpflichtung auf den Datenschutz besteht auch nach Beendigung des Arbeitsverhältnisses mit der Dienststelle fort.

2.5 Technische und organisatorische Umsetzung des Datenschutzes

Die Dienststelle hat nach § 27 DSG-EKD die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des DSG-EKD zu gewährleisten. Insgesamt müssen die Maßnahmen geeignet sein, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme (einschließlich rascher Wiederherstellung der Verfügbarkeit bei einem physischen oder technischen Zwischenfall) im Zusammenhang mit der Verarbeitung auf Dauer sicher zu stellen. Insbesondere sind nachstehende Maßnahmen bei der Verarbeitung von personenbezogenen Daten risikobasiert zu ergreifen, um ein angemessenes Schutzniveau zu erreichen (§ 27 DSG-EKD):

- Pseudonymisierung und Verschlüsselung personenbezogener Daten.
- Zutrittskontrolle, zur Verhinderung des physischen Zugangs zu Datenverarbeitungsanlagen (Beispielmaßnahme: Gebäudesicherung, Wachdienst, Schlüsselsystem).
- Zugangskontrolle, zur Verhinderung der unbefugten Nutzung des Systems (Beispielmaßnahme: Authentifizierung, Passwortregeln, Benutzerverwaltung).
- Zugriffskontrolle, zur Gewährleistung einer ausschließlich berechtigten Nutzung (Beispielmaßnahme: gesonderte Zugriffsrechte, Passwortschutz, Verschlüsselung).
- Weitergabekontrolle, zur Verhinderung von unbefugter Kenntnis bei Transport, Speicherung und Übertragung (Beispielmaßnahme: Verschlüsselung von Daten, Transportsicherung).
- Eingangskontrolle, zur nachträglichen Prüfung und Feststellung, wer was und wann in das System eingegeben hat (Beispielmaßnahme: Protokollierung, Logfiles).

- Auftragskontrolle, um zu gewährleisten, dass die Auftragnehmerin/der Auftragnehmer mit Daten weisungsgemäß umgeht (Beispielmaßnahme: Verträge, Überprüfung von Auftragnehmern/ Subauftragnehmern).
- Verfügbarkeitskontrolle, zum Schutz gegen Zerstörung, Verlust und vor Elementarschäden (Beispielmaßnahme: Back-Ups, Firewalls, Virenschutzsoftware, Feuermelder).
- Getrennte Verarbeitung/Trennungsgebot, damit Daten entsprechend ihres Zweckes getrennt voneinander verarbeitet werden können (Beispielsmaßnahmen. Physische Trennung in unterschiedlichen Systemen oder Datenbanken).

Die Einhaltung dieser Anforderungen stellt die Dienststelle durch die Einführung entsprechender Verfahren und Prozesse sicher, auf die in Teil 2 dieser Richtlinie Bezug genommen oder im Einzelnen eingegangen wird.

3. Maßnahmen der Dienststelle zur Sicherstellung des Datenschutzes

Zur Sicherstellung der Anforderungen der geltenden Datenschutzgesetze hat die Dienststelle die nachstehenden Prozesse und Verfahren definiert, die von den Mitarbeiterinnen und Mitarbeitern (nachstehend zusammen „MA“ genannt) zu beachten und einzuhalten sind.

3.1 Umgang mit personenbezogenen Daten

Für den Umgang mit vertraulichen Informationen gelten folgende Regeln:

3.1.1 Grundsätzliche Regelung für die Weitergabe von personenbezogenen Daten

Personenbezogene Daten dürfen nur an MA oder Dritte weitergegeben werden, wenn dazu aufgrund der Zuständigkeit oder Aufgabenstellung der Empfängerinnen/Empfänger eine Berechtigung besteht oder eine vertragliche oder gesetzliche Grundlage die Weitergabe erforderlich macht. Auch mündliche Auskünfte stehen unter diesem Vorbehalt, insbesondere bei telefonischen Anfragen Dritter. Vertrauliche Telefonate über ein Festnetztelefon oder von einem Mobiltelefon aus, dürfen nur unter Ausschluss der Öffentlichkeit und so geführt werden, dass ein Mithören Unbefugter ausgeschlossen ist. Ein Zugriff auf die persönliche Telefon-Mailbox der MA darf nur durch den jeweiligen MA erfolgen.

3.1.2 Aufbewahrung von anvertrauten Dokumenten

Die MA haben die ihnen anvertrauten Dokumente mit personenbezogenem Inhalt vor dem Zugriff Unbefugter geschützt aufzubewahren. Dazu sind verschließbare Schränke, Rollcontainer oder verschließbare Büroräume (nachstehend „Schutzvorkehrungen“ genannt) zu nutzen. Wenn diese den MA zur Verfügung gestellten Schutzvorkehrungen nicht oder nicht mehr funktionstüchtig sind, ist dies der/dem Vorgesetzten mitzuteilen, die/der die Behebung dieses Mangels unverzüglich zu veranlassen hat.

Nur die Vorgesetzten, Stellvertretungen und weitere im Arbeitsablauf eingebundene Personen dürfen neben der verantwortlichen MA im Rahmen des Erforderlichen und der ihnen eingeräumten Zugriffsrechte in Dokumente mit personenbezogenem Inhalt Einblick nehmen. Bei besonders schutzbedürftigen und/oder vertraulichen Daten ist durch die jeweilige Organisationseinheit zu entscheiden, ob diese Daten darüber hinaus gegen unberechtigten Zugriff (z.B. durch externe Dritte, durch Systemadministratoren etc.) zu schützen sind, indem die jeweiligen Dateien passwortgeschützt oder verschlüsselt im Netzwerk gespeichert werden. Hierbei ist aber zu beachten, dass dadurch nicht nur ein Schutz gegen unberechtigte Zugriffe geschaffen wird, sondern auch das Risiko, dass berechtigte Personen keinen Zugriff mehr auf die Daten haben, wenn das jeweilige Passwort nicht oder nicht mehr in der jeweiligen organisatorischen Einheit bekannt ist. Um diesem Risiko zu begegnen, dürfen betriebliche Daten nur passwortgeschützt oder verschlüsselt gespeichert werden, wenn in der jeweiligen organisatorischen Einheit ein Verfahren gilt (möglichst schriftlich fixiert), das sicherstellt, dass Vorgesetzte und/oder Stellvertretungen eine Entschlüsselung vornehmen können. Dies gilt nicht für die Fälle, in denen Daten allein für die Weitergabe passwortgeschützt oder verschlüsselt werden, sofern die Datei zusätzlich noch unverschlüsselt im Netzwerk gespeichert ist.

3.1.3 Papierkörbe

Papierkörbe zählen zu den unter Datenschutzgesichtspunkten sensiblen Einrichtungen, da die Entsorgung des Inhalts regelmäßig über die Müllabfuhr erfolgt, ohne dass eine vorherige Vernichtung vertraulicher Informationen durchgeführt wurde. Vertrauliche Dokumente und papiergebundene personenbezogene Informationen sind deshalb stets in dafür gesondert vorgesehene verschlossene Entsorgungsbehälter zu geben oder mit einem Schredder (mindestens Stufe 3 DIN 66399 = Materialteilchenlänge max. 60 mm, Materialteilchenbreite bis max. 4 mm oder Streifenbreite max. 2 mm) zu vernichten. Die Schlüssel für Entsorgungsbehälter dürfen nur autorisierten Personen zugänglich sein. Ein Öffnen der verschlossenen Entsorgungsbehälter, um Unterlagen die ggfs. versehentlich entsorgt wurden, wieder zu entnehmen, ist nicht erlaubt.

3.1.4 Entsorgung elektronischer Datenträger

Mit personenbezogenen Daten beschriebene elektronische Datenträger (z.B. CDs, DVDs, externe Festplatten, Speicherkarten, USB-Sticks) dürfen nicht in den Hausmüll gegeben werden. Vielmehr müssen sie zur fachkundigen Vernichtung an die IT-Abteilung gegeben werden. Die Entsorgung nicht mehr funktionsfähiger oder nicht mehr benötigter PCs darf nur durch die IT-Abteilung unter Berücksichtigung angemessener Sicherheitsverfahren durchgeführt werden. Kirchliche Stellen außerhalb des Landeskirchenrates wenden sich dazu an Ihren IT-Dienstleister, mit dem sie einen Vertrag nach § 30 DSG EKD (AV) geschlossen haben. Einzelheiten zur Entsorgung sollten in eigenen Arbeitsanweisungen geregelt werden.

3.2 Clean Desk

Soweit MA kein eigenes und in ihrer Abwesenheit durchgängig verschlossenes Büro haben, ist jeder Arbeitsplatz stets aufgeräumt zu hinterlassen. Bei Verlassen des Arbeitsplatzes ist sicherzustellen, dass personenbezogene Daten, gleich ob papiergebunden oder auf elektronischen Datenträgern, Unbefugten nicht zugänglich sind und kein Verlust an Verfügbarkeit oder Integrität entstehen kann (siehe dazu auch ergänzend Ziffer 3.1.2 dieser Richtlinie). Es ist zu verhindern, dass Unbefugte am Arbeitsplatz auf Datenträger (z.B. CDs, DVDs, USB-Sticks oder externe Festplatten) oder papiergebundene Unterlagen zugreifen können. Dokumentierte Passwörter dürfen für Unbefugte nicht zugänglich am Arbeitsplatz aufbewahrt werden (z.B. auf Klebezetteln am Monitor, unter der Schreibtischauflage oder in unverschlossenen Schreibtischschubladen). Entsprechendes gilt für Schlüssel zu besonders vertraulichen Bereichen (z.B. Geschäftsführung, IT-Abteilung, Personalabteilung, Finanzabteilung, Rechtsabteilung, Aktenarchive). Unterlagen sind bei Verlassen von Besprechungsräumen vollständig zu entfernen. Dies gilt insbesondere auch für Schriftstücke auf Flipcharts.

3.3 PC-Bildschirm, Drucker und Kopierer

Bildschirme und Drucker sind so aufzustellen, dass ein unberechtigter Einblick und Zugriff Dritter ausgeschlossen ist. Die MA sind verpflichtet, bei jedem auch nur kurzfristigen Verlassen des Arbeitsplatzes die Arbeitsstation zu sperren, soweit sie kein eigenes und in ihrer Abwesenheit verschlossenes Büro haben (siehe nähere Erläuterung dazu unter Ziffer 3.4.2). Die Dienststelle muss zusätzlich dazu sicherstellen, dass sich die Arbeitsstation spätestens 15 Minuten nach der letzten Tastatureingabe bzw. der letzten Verwendung der Maus automatisch selbst sperrt. Ausdrucke mit personenbezogenen Daten oder anderen vertraulichen Informationen dürfen nicht unbeaufsichtigt im Drucker verbleiben, sondern müssen direkt nach dem Ausdruck aus dem Drucker entnommen werden. Gleiches gilt für Kopiergeräte, worin keine Fehlkopien oder Originaldokumente mit vertraulichem Inhalt unbeaufsichtigt verbleiben dürfen.

3.4 Rechner (Arbeitsplatzrechner und mobile Geräte)

3.4.1 Beschaffung und Nutzung von Hard- und Software

Die Beschaffung von Hardware jeder Art (Desktop-und Notebook-Rechner, Mobiltelefone, Smartphones, Zubehör etc.) sowie von Software obliegt ausschließlich der IT-Abteilung, in kirchlichen Stellen außerhalb des LKR bestimmt die Geschäftsleitung, wer dafür zuständig ist.
Die private Nutzung der zu dienstlichen Zwecken an die MA überlassenen Hard-und Software ist ausdrücklich untersagt, sofern nicht abweichend geregelt. Ebenso ist die Verwendung privater Hard-und Software zu dienstlichen Zwecken nicht gestattet. Insbesondere das Überspielen oder Weiterleiten von betrieblichen Daten auf private Datenträger (z.B. auf CDs, DVDs, USB-Sticks, externe Festplatten, Mobiltelefone, Smartphones) ist untersagt. Das heißt, dass auch die Weitergabe bzw. Weiterleitung von betrieblichen Daten per E-Mail auf private Datenträger/Hardware (z.B. durch Weiterleitung einer E-Mail an einen privaten E-Mailaccount) untersagt ist.
Soweit MA ausnahmsweise Administrationsrechte auf ihrem Rechner haben, ist vor jeder Installation von neuer Software die Genehmigung der IT-Abteilung - in kirchlichen Stellen außerhalb des LKR bestimmt die Geschäftsleitung wer die Genehmigung erteilen darf - einzuholen. Dateien von externen Datenträgern (z.B. CDs, DVDs, USB-Sticks, externe Festplatten, Mobiltelefonen, Smartphones) müssen vor der Speicherung auf Rechnern kirchlicher Einrichtungen und der Übermittlung über das Netzwerk kirchlicher Einrichtungen auf Viren und Würmer überprüft werden. Das Deaktivieren von Antivirenprogrammen ist untersagt.

3.4.2 Sperrung des persönlichen PC bei Verlassen des Arbeitsplatzes

Soweit MA kein eigenes und in ihrer Abwesenheit verschlossenes Büro haben, ist auch bei kurzzeitigem Verlassen des Arbeitsplatzes der Zugriff auf den persönlichen PC zu sperren. Dies kann durch eine Systemabmeldung, die Sperrung des Arbeitsplatzrechners (ggf. durch die Tastenkombination: „Windows“ + “L“) oder die Aktivierung eines passwortgeschützten Bildschirmschoners erfolgen. In jedem Falle ist sicherzustellen, dass niemand unter der Benutzerkennung eines abwesenden MA auf Systemressourcen zugreifen kann.

3.4.3 Speicherung von relevanten Daten

Relevante Daten müssen auf Netzwerklaufwerken, wo regelmäßige Sicherungen/Back Ups erfolgen, und nicht auf den lokalen Festplatten (z.B. C-Laufwerk) der PCs gespeichert werden.

3.4.4 Löschung von Daten

Sämtliche Daten, die für die Geschäftstätigkeit nicht mehr erforderlich sind und die keiner vertraglichen oder gesetzlichen Aufbewahrungspflicht unterliegen, sind umgehend zu löschen. Einzelheiten zu den Aufbewahrungspflichten sollten in entsprechenden Arbeitsanweisungen geregelt werden.

3.4.5 Nutzung von mobilen Endgeräten (Laptops, Smartphones, PDA etc.)

Bei der Nutzung von mobilen Endgeräten ist sicherzustellen, dass Unbefugte Dritte nicht vertrauliche Informationen (wie personenbezogene Daten) mitlesen oder mithören können. Die Einsichtnahme des Bildschirms durch unbefugte Dritte ist zu verhindern. Bei Bedarf ist daher mit der IT-Abteilung - in kirchlichen Stellen außerhalb des LKR mit der von der Geschäftsleitung bestimmten Stelle - abzustimmen, ob Sicherungsmaßnahmen (z. B. Blickschutzfilter) möglich sind, die die Einsichtnahme durch Dritte bei der Nutzung in der Öffentlichkeit (z.B. auf einer Zugfahrt) verhindern. Die SIM-PIN-Abfrage beim Start eines Gerätes darf nicht deaktiviert werden. Außerdem muss die automatische Bildschirmsperre mit Passwort aktiviert sein. Sollten diese Schutzmaßnahmen nicht gewährleistet sein, ist die Benutzung des Laptops zur Verarbeitung personenbezogener und anderer vertraulicher Daten in der Öffentlichkeit verboten.

3.4.6 USB-Sticks, CD/DVD, externe Festplatten, Speicherkarten und andere mobile elektronische Datenträger

Das Speichern von Daten kirchlicher Einrichtungen (wozu insb. auch personenbezogene Daten gehören) auf privaten USB-Sticks, CD/DVD, Speicherkarten, externen Festplatten und anderen mobilen Speichermedien ist untersagt. Vielmehr dürfen diese schon nicht in Rechner kirchlicher Einrichtungen eingelegt oder an diese angeschlossen werden.
Werden auf betrieblichen USB-Sticks oder anderen externen Datenträgern vertrauliche Informationen und insbesondere personenbezogene Daten gespeichert, so muss der Datenträger bzw. die darauf gespeicherten Daten vor ihrem Transport außerhalb der kirchlichen Einrichtung verschlüsselt werden. Mit solchen Daten beschriebene USB-Sticks, CD/DVD, Speicherkarten, externe Festplatten und andere mobile Datenträger sind zur fachkundigen Vernichtung an die IT-Abteilung - in kirchlichen Stellen außerhalb des LKR an die von der Geschäftsleitung bestimmte Stelle - zu geben.

3.5 Betriebliches E-Mail-System

3.5.1 Privatnutzung

Das E-Mail-System der Dienststelle darf nur zu betrieblichen Zwecken verwendet werden. Jede private Nutzung ist untersagt. Hiervon ausgenommen ist die private Nutzung aus einem dienstlich veranlassten Grund (z.B. die Verabredung mit anderen MA zum Mittagessen). Alle ein- und ausgehenden E-Mails werden aufgrund gesetzlicher Vorschriften elektronisch archiviert und autorisierte MA können möglicherweise Zugriff auf alle gespeicherten E-Mails nehmen. Wegen des notwendigen Schutzes des Netzwerks kann die Dienststelle daher nicht die völlige Vertraulichkeit von Informationen innerhalb des Netzwerks garantieren.

Die Nutzung des E-Mail-Systems zu betrieblichen Zwecken umfasst jegliche Nutzeraktivität, die sich entweder direkt oder indirekt auf die Dienststelle und den Betrieb oder das Verhältnis von der Dienststelle und MA beziehen. Daher muss eine betriebliche E-Mail-Nutzung in einem gewissen Zusammenhang zur Dienststelle stehen, wobei dieser Zusammenhang auch indirekt ausgestaltet sein kann oder nicht auf den ersten Blick erkennbar sein muss (z.B. E-Mail des MA an die Ehefrau, um eine Verspätung wegen Überstunden anzukündigen). Die private Nutzung des E-Mail-Systems weist hingegen keinen Zusammenhang zur Dienststelle oder Geschäftspartnern auf. Sie betrifft weder die Interessen der Dienststelle noch deren Beziehung zu der Nutzerin/dem Nutzer.

Die Nutzerinnen/Nutzer des E-Mail-Systems dürfen keine private Korrespondenz in eine betriebliche E-Mail mit aufnehmen. Entgegen dieses Verbots der Privatnutzung in den dienstlichen E-Mail-Accounts befindliche und/oder eingehende E-Mails sind von MA sofort aus dem E-Mail-Account zu entfernen. Soweit eine eingehende betriebliche E-Mail dennoch auch private Informationen zum Inhalt hat, ist sie wie eine betriebliche E-Mail einzuordnen und zu behandeln. Unter der Voraussetzung, dass ein negativer Einfluss auf den Arbeitsablauf vermieden wird, sollte die versendende Person der E-Mail dazu aufgefordert werden, keine weitere private Korrespondenz in betriebliche E-Mails einzubeziehen bzw. sollte die versendende Person darauf hingewiesen werden, dass die entsprechende Adresse nur für dienstliche Zwecke genutzt werden darf. DieDienststelle ist berechtigt, bei konkretem Verdacht auf eine missbräuchliche Nutzung, Überprüfungen anhand gespeicherter Nutzerdaten vorzunehmen.

Die Dienststelle gestattet unter dem Vorbehalt des jederzeitigen Widerrufs eine angemessene Nutzung der kirchlichen Einrichtung fremden webbasierten E-Mail-Systemen (z. B. web.de) für private Zwecke, da diese Informationen nicht im Netzwerk der kirchlichen Einrichtung gespeichert werden. Die private Nutzung von webbasierten E-Mail-Systemen ist nur zulässig, soweit dadurch weder die Interessen der Dienststelle oder die Funktionsfähigkeit der IT-Systeme negativ beeinflusst werden, noch die Arbeitsleistung der jeweiligen MA darunter leidet. E-Mail-Systeme, die nicht der Dienststelle zuzuordnen sind, dürfen nicht für die betriebliche Kommunikation eingesetzt werden.

3.5.2 Regelungen zum E-Mail - Versand

Vor Versand einer E-Mail ist darauf zu achten, dass die eingegebenen Empfängeradressen richtig sind. Gleiches gilt bei Nutzung der Antwort-Funktion des E-Mail-Programms und der damit verbundenen Übernahme der von der ursprünglichen Absenderin/ dem ursprünglichen Absender ggf. zusätzlich eingegebenen E-Mail-Adressen. Zusätzliche E-Mail-Adressen sollen nur in den Verteiler einer E-Mail aufgenommen werden, wenn die Hinzuziehung der jeweiligen Empfangenden erforderlich ist.
Wenn E-Mails an eine Gruppe der kirchlichen Einrichtung fremden Adressaten versendet werden, sind die E-Mail-Adressen grds. ins „bcc“ zu setzen, so dass die Empfänger die E-Mail-Adressen der anderen Adressaten nicht einsehen können. Eine „offene“ Eingabe der E-Mail-Adresse im „cc“ ist nur dann zulässig, wenn davon ausgegangen werden darf, dass die Betroffenen mit dieser Weiterübermittlung ihrer E-Mail-Adresse einverstanden sind.
Beispiele für ein Versenden der E-Mail-Adressen im „cc“ können insbesondere die E-Mail-Adressen von Abteilungs-oder Fachbereichsleitungen sein, wenn diese von bestimmten Vorgängen in Kenntnis gesetzt werden sollen. Aber auch bei der Kommunikation mit Vertragspartnerinnen und -partnern kann davon ausgegangen werden, dass jegliche Personen, die mit den aus dem Vertragsverhältnis hervorgehenden Aufgaben betraut sind, mit der offenen Eingabe der E-Mail-Adressen einverstanden sind. Als Faustregel kann darüber hinaus zugrunde gelegt werden, dass diejenigen, die auch bereits von der Absenderseite auf “cc“ gesetzt wurden, bei der Antwort ebenfalls auf „cc“ gesetzt werden dürfen.
Die „bcc“ -Funktion ist immer dann sinnvoll, wenn die Empfängerliste sehr umfangreich ist, die Empfangenden einer Weitergabe der eigenen E-Mail-Adresse nicht zugestimmt haben oder niemand wissen soll, an wen die E-Mail noch gegangen ist, etwa um die Privatsphäre der einzelnen Empfangenden zu schützen. Auch um zu verhindern, dass die Mail-Adressen der Empfangenden von Rundmails für Spam-Mails missbraucht werden, ist die Verwendung der „bcc“-Funktion sinnvoll. Beispiele für ein Setzen auf „bcc“ sind also vor allem die Empfangenden von Sammel-E-Mails oder Newslettern.
Seitens der MA darf nur den jeweiligen Stellvertretungen und/oder Vorgesetzten Zugriff auf die persönliche Mailbox eingeräumt werden.

3.6 Internet

Die Nutzung des Internets wird in einer gesonderten Dienstvereinbarung geregelt.

3.7 Passwörter

3.7.1 Anforderungen an Passwortparameter

Soweit die Passwortparameter nicht ohnehin systemseitig vorgegeben sind, ist bei der Auswahl eines Passwortes darauf zu achten, dass es nicht leicht erraten werden kann. Ein Passwort sollte mindestens acht Zeichen lang sein und möglichst immer aus einer Kombination von Buchstaben in Groß-und Kleinschreibung, Ziffern und Sonderzeichen bestehen. Problematisch sind Trivialkennwörter wie "ABC" oder Tastaturfolgen (z.B. "qwert" oder "asdfgh"), alle Arten von Namen (etwa von Freunden, Bekannten, Kollegen/Innen, Familienangehörigen, Haustieren), Städte- und Gebäudebezeichnungen, Comic-Figuren, Automarken, Autokennzeichen, Begriffe, Geburtsdaten, Telefonnummern, gängige Abkürzungen usw.

3.7.2 Geheimhaltung von Passwörtern

Passwörter sind strikt geheim zu halten. Die Geheimhaltungsverpflichtung hinsichtlich des Passwortes gilt auch gegenüber Kolleginnen/Kollegen und Vorgesetzten. Sollte eine Weitergabe entgegen dieser Anweisung dennoch erfolgt sein, um etwa im Notfall den Zugriff auf bestimmte Datenbestände durch Dritte zu ermöglichen, ist das Passwort umgehend zu ändern. Es ist untersagt, Passwörter papiergebunden am Arbeitsplatz ohne Schutz vor unberechtigtem Zugriff (z.B. unverschlossene Schreibtischschublade, unter Schreibtischunterlage) oder elektronisch unverschlüsselt auf einem Rechner oder externen Datenträger vorzuhalten.

3.8 Telefax / Scanner

Bei Telefaxgeräten besteht ein erhöhtes Risiko der Fehlleitung von Nachrichten oder der unberechtigten Einsichtnahme in Nachrichten bei Empfangenden. Deshalb sollte auf die Nutzung von Telefaxgeräten bei der Übermittlung sensibler personenbezogener Daten und besonders vertraulicher Informationen soweit möglich verzichtet werden.
Dennoch gibt es Ausnahmen, in denen ein Verzicht auf die Nutzung von Telefaxgeräten nicht praktikabel erscheint. Dies betrifft insbesondere die Kommunikation mit Behörden (bspw. Finanzämtern und Aufsichtsbehörden), mit Rechtsanwältinnen/Rechtsanwälten und Vertragspartnerinnen und -partnern, soweit dies vertraglich vereinbart wurde.
Abgesehen von den genannten Fällen, in denen Behörden oder Berufsgeheimnisträger involviert sind, sollte vor Sendung des Telefax der Empfangenden über die Sendung informiert werden, um sicherzustellen, dass ein zugriffsbefugter MA des Empfangenden das Empfangsgerät während des Ausdrucks persönlich überwacht und das gedruckte Dokument umgehend aus dem Gerät entnimmt.
Vor Absendung eines Telefax hat sich die Bedienerin/der Bediener über die Richtigkeit der Zielwahlnummer Gewissheit zu verschaffen, um eine Fehlsendung auszuschließen. Zudem ist vor dem Starten des Sendevorgangs noch einmal die Übereinstimmung der Zielwahlnummer mit der im Display angezeigten Rufnummer zu überprüfen. Bei fehlender Übereinstimmung ist der Sendevorgang zu unterbrechen.
Soweit über einen Scanner das eingelesene Dokument direkt in einem Netzwerkverzeichnis abgelegt werden kann, ist sicherzustellen, dass dieses Netzwerkverzeichnis zugriffsgeschützt ist, so dass nur berechtigte Personen zugreifen können. Lediglich öffentliche Dokumente dürfen direkt in kirchenweit zugängliche Netzwerkverzeichnisse eingescannt werden.
Faxe mit personenbezogenen Daten oder anderen vertraulichen Informationen dürfen nicht unbeaufsichtigt im Gerät verbleiben, sondern müssen direkt nach dem Ausdruck entnommen werden.

3.9 Briefpost

Bei der Versendung von Briefpost ist möglichst die empfangsberechtigte Person oder zumindest die Abteilung, der die Person zugeteilt ist, auf der Empfängerseite anzugeben. Soweit vertrauliche Informationen enthalten sind, ist zudem der Vermerk „persönlich“ oder „vertraulich“ in das Adressfeld aufzunehmen. Wenn bereits aus den Absenderangaben Rückschlüsse auf bestimmte Tatsachen möglich sind, darf die (genaue) absendende Person nicht erkennbar sein (z.B. „Mahnabteilung"). Bei Fensterkuverts sind die Formatierung, der Umschlag, die Fenstergröße und das Papier so zu wählen, dass durch Verschiebungen keine weiteren personenbezogenen Daten erscheinen. Nur durchsichtsgeschützte Briefumschläge dürfen verwendet werden.
Da das grundrechtlich geschützte Briefgeheimnis auch im Beschäftigungsverhältnis gilt, sollte Briefpost, die im Adressfeld den Namen eines MA aufweist, diesem oder im Bedarfsfall seiner Stellvertretung ungeöffnet zugestellt werden. Dies gilt zwingend, wenn zuerst der Name des MA und dann der Name der kirchlichen Einrichtung genannt sind. Soweit ein Adressfeld den Hinweis „persönlich“, „vertraulich“, „privat“, „geheim“ o.Ä. aufweist, darf die Postsendung auch nicht durch die Stellvertretung oder Vorgesetzten geöffnet werden, sondern ist dem MA persönlich zuzustellen oder zurück zu senden. In einem solchen Falle ist die Öffnung der Postsendung durch andere Personen nur erlaubt, sofern die jeweilige mitarbeitende Person die Postöffnung durch diese andere Person explizit erlaubt hat. Eine Verletzung des Briefgeheimnisses ist ggf. strafbar, auch wenn der Brief lediglich geöffnet, aber nicht gelesen wurde.

3.10 Schutzmaßnahmen außerhalb des Betriebsgeländes

Außerhalb des Betriebsgeländes sind vertrauliche und personenbezogene Daten mit betrieblichem Bezug so zu schützen, dass ein Zugang zu den Informationen durch unbefugte Personen ausgeschlossen wird. Vertrauliche Papierdokumente müssen zugriffsgeschützt (etwa in verschlossenem Behälter oder Schrank) aufbewahrt werden. Die Regeln über den Transport von Laptops (siehe oben unter Ziffer 3.4) gelten für betriebliche Papierdokumente entsprechend.

4. Besondere datenschutzrechtliche Verfahren

Nachstehend wird auf besondere datenschutzrechtliche Verfahren hingewiesen, auf die die Mitarbeitenden im Rahmen dieser Datenschutzrichtlinie hingewiesen werden sollen.

4.1 Auskunftsrecht und Auskunftsverzeichnis

Gemäß § 19 DSG-EKD steht dem Betroffenen (z.B. Interessenten und Website-Nutzern) ein Auskunftsrecht gegenüber der Dienststelle dahingehend zu,

- welche personenbezogenen Daten zu der Person gespeichert sind,
- an welche Empfängerinnen/Empfänger oder Kategorien von Empfängerinnen/Empfängern, die Daten weitergegeben werden, und
- den Zweck der Speicherung.
- Speicherdauer
- evtl. Herkunft der Daten
- weitere Rechte des Betroffenen.

Anfragen auf Auskunft nach § 19 DSG-EKD, die an die Evangelische Kirche der Pfalz bzw. die in diesem Zusammenhang verantwortliche Stelle gerichtet sind, können an den externen Datenschutzbeauftragen (Kontaktdaten s. oben unter Ziffer 2.1) oder

Die Datenschutzbeauftragte der Evangelischen Kirche der Pfalz
Verwaltungsrätin i. K. Pia Schneider
Dezernat 6
Roßmarktstraße 4
67346 Speyer
Telefon: 06232 667-434
E-Mail: pia.schneider@evkirchepfalz.de

gegeben werden. Die Anfragen werden von dort aus beantwortet.

4.2 Melde- und Eskalationsprozess nach § 32 und § 33 DSG-EKD

Ferner ist jeder Mitarbeitende verpflichtet, einen bestimmten Melde-und Eskalationsprozess einzuhalten. Danach sind Mitarbeitende im Fall des Verdachtes, dass personenbezogene Daten verloren gegangen sind, gestohlen wurden oder durch unberechtigte Dritte eingesehen worden sind, verpflichtet, ihre direkte Vorgesetzte/ihren direkten Vorgesetzten sowie den Datenschutzbeauftragten zu informieren. Für die Meldung einer Datenpanne ist stets der Meldebogen im kirchlichen Intranet (Arbeitsplatz – Recht – Datenschutz – Muster/Vorlagen) zu verwenden. Die Meldung muss unbedingt über die Pannenhotline (0160 / 500 148 5) erfolgen. Unter dieser Telefonnummer meldet sich die Rechtsanwaltskanzlei Kinast und Partner in Köln, die für die verfasste Kirche der EKP als externer Datenschutzbeauftragter bestellt wurde. Die Übersendung des Meldebogens hat so zeitnah wie möglich zu erfolgen. Dieser Prozess soll sicherstellen, dass dieDienststelle ihren Informationsverpflichtungen gegenüber der zuständigen Aufsichtsbehörde für Datenschutz sowie den Betroffenen gem. § 32 und § 33 DSG-EKD nachkommen kann. Ein Verstoß gegen diese Verpflichtung stellt nach § 45 DSG-EKD eine Ordnungswidrigkeit dar, die mit einer Geldbuße in Höhe von bis zu 500.000 Euro geahndet werden kann.

4.3 Erstellung eines Verarbeitungsverzeichnisses bei Einführung neuer Verfahren; Datenschutz-Folgenabschätzung durch den externen Datenschutzbeauftragten

Verarbeitungsverzeichnisse und Datenschutzfolgeabschätzungen werden ggf. zentral im Landeskirchenrat geführt bzw. erstellt (z. B. KFM, DaviP, Kidicap, AHD-Formulare, MS-Office). Die beabsichtigte Einführung anderer neuer Verfahren, die nicht zentral vom Landeskirchenrat supported werden, ist dem/der Datenschutzbeauftragten zu melden. Dies dient dazu, dem externen Datenschutzbeauftragten die Möglichkeit zu geben, vor Inbetriebnahme einer automatisierten Verarbeitung von personenbezogenen Daten (Verfahren) eine erste Bewertung der datenschutzrechtlichen Zulässigkeit des beabsichtigten Verfahrens und ggf. anschließend – soweit das Verfahren ein erhöhtes Risiko für die Grundrechte und Grundfreiheiten der Betroffenen darstellen könnte – gem. § 34 DSG-EKD eine Datenschutz-Folgenabschätzung vorzunehmen.

Stand: März 2020