Merkblatt über den Datenschutz für Mitarbeitende

In diesem Merkblatt erhalten Sie Informationen über den wesentlichen Inhalt des Datengeheimnisses und den Sinn der Verpflichtungserklärung. Die Erläuterungen und Hinweise müssen im jeweiligen Zusammenhang, der sich aus Anwendungsfragen aus der täglichen Arbeit sowie den jeweils geltenden Rechtsvorschriften ergibt, gesehen werden.

Welche rechtlichen Grundlagen gelten für den Datenschutz?

1) Zunächst gelten die allgemeinen Datenschutzbestimmungen. Dies sind jeweils in ihrer geltenden Fassung

   a) das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD; https://www.kirchenrecht-ekd.de/document/41335,

   b) die IT-Sicherheitsverordnung der Evangelischen Kirche in Deutschland (ITSVO-EKD),

   c) [Bestimmungen der Landeskirche zum DSG-EKD],

   d) [Bestimmungen der Landeskirche zur ITSVO oder zur IT-Sicherheit],

   e) [Dienst- und Organisationsanweisungen zum Datenschutz oder zur IT-Sicherheit, soweit sie von einer kirchlichen Stelle erlassen wurden].

2) Außerdem gelten den allgemeinen Regelungen zum Datenschutz vorgehende Bestimmungen. Dieses sind

   a) besondere Bestimmungen über den Schutz des Beicht- und Seelsorgegeheimnisses, die Amtsverschwiegenheit sowie sonstige gesetzliche Geheimhaltungs- und Verschwiegenheitspflichten oder von Berufs- bzw. besonderen Amtsgeheimnissen, die nicht auf gesetzliche Vorschriften beruhen, und

   b) andere Rechtsvorschriften, die die Verarbeitung personenbezogener Daten regeln.

Sie finden diese Vorschriften in der Rechtssammlung Ihrer Landeskirche. In gleicher Weise sind künftige Rechts- und Verwaltungsvorschriften sowie Veröffentlichungen der Evangelischen Kirche in Deutschland und Ihrer Landeskirche zu den Bereichen Datenschutz und IT-Sicherheit zu beachten.

Warum ist Datenschutz wichtig?

Niemand darf durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt werden. Jeder hat das Recht, über den Umgang mit seinen personenbezogenen Daten grundsätzlich selbst zu bestimmen. Das Ziel des Datenschutzes ist es, den Einzelnen vor einer Beeinträchtigung zu schützen.

Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden "betroffene Person") beziehen; identifizierbar ist eine natürliche Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen,

physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Personenbezogene Daten sind (z. B. Geburtsdatum, Anschrift, Konfession, Beruf, Familienstand, Gesundheitszustand, Fotos, Videoaufzeichnungen, Grundbesitz, Einkommen oder Rechtsbeziehungen zu Dritten).

Nach § 2 Absatz 2 DSG-EKD können sie in Akten und Aktensammlungen enthalten sein oder bei automatisierten Verarbeitungen anfallen. Beispiele für automatisierte Verarbeitungen sind Programme aus den Bereichen Textverarbeitung, Tabellenkalkulation und Datenbanken. Zu beachten ist, dass personenbezogene Daten auch beim Einsatz von mobilen Endgeräten, Videoüberwachungen, automatischen Schließsystemen und weiteren technischen Anwendungen anfallen.

Welche grundsätzlichen Regelungen gelten für den Datenschutz?

Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn das DSG EKD oder eine Rechtsvorschrift dies erlaubt oder anordnet oder soweit die betroffene Person eingewilligt hat (Grundsatz des Verbots mit Erlaubnisvorbehalt).

Personenbezogene Daten dürfen für die Erfüllung kirchlicher Aufgaben verarbeitet werden. Maßgebend sind die herkömmlichen oder durch das kirchliche Recht bestimmten Aufgaben auf dem Gebiet der Verkündigung, Seelsorge, Diakonie und Unterweisung sowie der kirchlichen Verwaltung (einschließlich Gemeinde- und Pfarrbüro).

Personenbezogene Daten sind gemäß § 5 DSG-EKD nach den folgenden Grundsätzen zu verarbeiten:

1. Rechtmäßigkeit, Verhältnismäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz;
2. Zweckbindung: Personenbezogene Daten werden für festgelegte, eindeutige und legitime Zwecke erhoben. Sie dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Eine Weiterverarbeitung für im kirchlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszecke oder für statistische Zwecke gilt als vereinbar mit den ursprünglichen Zwecken;
3. Datenminimierung: Die Verarbeitung personenbezogener Daten wird auf das dem Zweck angemessene und notwendige Maß beschränkt; personenbezogene Daten sind zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert;
4. Richtigkeit: Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
5. Speicherbegrenzung: Personenbezogene Daten werden in einer Form gespeichert, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Personenbezogene Daten dürfen länger gespeichert werden, soweit sie für die Zwecke des Archivs, der wissenschaftlichen und historischen Forschung sowie der Statistik verarbeitet werden;

6. Integrität und Vertraulichkeit: Personenbezogene Daten werden in einer Weise verarbeitet, die eine angemessene Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Zerstörung oder unbeabsichtigter Schädigung.

Die verantwortliche Stelle muss die Einhaltung der Grundsätze nachweisen können (Rechenschaftspflicht).

Mündliche, elektronische und schriftliche Auskünfte aus Akten oder Datenbanken sowie die Offenlegung von personenbezogenen Daten (z. B. Kopien von Listen, Datenträgern und Akten) sind zulässig an kirchliche Stellen, andere öffentlich-rechtliche Religionsgesellschaften sowie an Behörden und sonstige öffentliche Stellen des Bundes, der Länder, der Gemeinden etc., soweit eine Rechtsgrundlage für die Offenlegung der Daten vorhanden ist und sie zur Erfüllung kirchlicher Aufgaben erforderlich sind (siehe auch § 8 DSG EKD).

Die Offenlegung der Daten an sonstige Stellen oder Personen ist nur in Ausnahmefällen statthaft (siehe auch § 9 DSG-EKD). Auskünfte zur geschäftlichen oder gewerblichen Verwendung der Daten dürfen ohne Einwilligung der betroffenen Person in keinem Fall gegeben werden.

Widersprüche von betroffenen Personen, die sich gegen die Verarbeitung ihrer personenbezogenen Daten richten, sind zu beachten – Ausnahmen regeln die kirchlichen Vorschriften sowie § 25 DSG-EKD.

Alle Informationen, die Mitarbeitende auf Grund ihrer Arbeit an und mit Akten, Dateien und Listen erhalten, sind vertraulich zu behandeln. Diese Pflicht besteht auch nach Beendigung der Tätigkeit fort. Personenbezogene Daten dürfen nur kirchlichen Mitarbeitenden zugänglich gemacht werden, die auf Grund ihrer dienstlichen Aufgaben zum Empfang der Daten berechtigt sind.

Die Mitarbeitenden sind für die datenschutzrechtlich korrekte Ausübung ihrer Tätigkeit verantwortlich. Die sorgsame und vertrauliche Behandlung von Daten ist ein wichtiges Gebot im Rahmen der kirchlichen Arbeit.

Was ist aus Sicht des technischen und organisatorischen Datenschutzes zu beachten?

Wenn personenbezogene Daten verarbeitet werden, sind die technischen und organisatorischen Maßnahmen gemäß §§ 27, 28 DSG-EKD zu beachten.

Landeskirchliche Bestimmungen sowie Regelungen und Hinweise zum Datenschutz und zur Datensicherheit aus bestehenden Dienst- und Organisationsanweisungen sind zu befolgen.

Eigenmächtige Änderungen der dienstlichen Hardware und deren Konfiguration – insbesondere der Einbau von Karten und der Anschluss von Druckern oder anderen Zusatzgeräten – sind ebenso wie das unbefugte Einspielen von privater Software nicht gestattet. Private IT Geräte dürfen eingesetzt werden, wenn diese durch Vereinbarung mit der kirchlichen Stelle zugelassen sind (§ 2 Absatz 2 ITSVO-EKD).

Soweit aus Gründen der Aufgabenerfüllung Daten mittels eines Datenträgers auf einen PC übertragen werden, ist durch geeignete Maßnahmen sicherzustellen, dass die auf dem Datenträger enthaltenen Daten nicht mit Schadsoftware befallen sind.

Es ist untersagt, Passwörter und Hardwaretoken (z. B. USB-Stick und Chipkarten) sowie Benutzerkennungen weiterzugeben.

Daten (z. B. Belege, EDV-Listen), Datenträger (z. B. Festplatten, USB-Sticks, DVDs) und Zubehör (z. B. Schlüssel) sind stets sicher und verschlossen zu verwahren und vor jeder Einsicht oder sonstigen Nutzung durch Unbefugte zu schützen.

Analoge und digitale Daten, die nicht mehr benötigt werden, müssen in einer Weise vernichtet oder gelöscht werden, die jeden Missbrauch der Daten ausschließt.

Mängel, die bei der Datenverarbeitung auffallen, müssen dem Vorgesetzten gemeldet werden. Dies gilt auch für den Fall, dass in den Bereichen Datenschutz und Datensicherheit unzureichende technische und organisatorische Maßnahmen ergriffen wurden. Es wird empfohlen, die örtlich Beauftragten für den Datenschutz zu beteiligen. Unabhängig davon können sich Mitarbeitende auch ohne Einhaltung des Dienstweges vertraulich an den Beauftragten für den Datenschutz der EKD wenden.

Welche strafrechtlichen Konsequenzen können mir im Einzelfall drohen?

Bestimmte Handlungen, die einen Verstoß gegen das Datengeheimnis beinhalten, stellen Straftatbestände dar. Danach kann mit Freiheitsstrafe oder mit Geldstrafe beispielsweise bestraft werden, wer

- unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft (§ 202a StGB „Ausspähen von Daten“),
- Passwörter Dritten verkauft oder überlässt oder entsprechende Computerprogramme installiert (§ 202c StGB „Vorbereiten des Ausspähens und Abfangens von Daten“),
- als Berufsgeheimnisträger i. S. v. § 203 Absatz 1 StGB, als dessen berufsmäßig tätige Gehilfen (z. B. Sekretärin, Verwaltungsfachkraft), als beim Berufsgeheimnisträger in Vorbereitung auf den Beruf Tätige (z. B. Praktikant, Auszubildender) oder als sonstige Personen (§ 203 Absatz 3 Satz 2 StGB), die an der beruflichen und dienstlichen Tätigkeit eines Berufsgeheimnisträgers mitwirken (z. B. IT-Administrator), unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihr oder ihm im Rahmen der beruflichen Tätigkeit anvertraut oder sonst bekannt geworden ist (§ 203 StGB – „Verletzung von Privatgeheimnissen“),
- rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert (§ 303a StGB „Datenveränderung“).

Auch weitere Verschwiegenheitsvorschriften und Geheimhaltungspflichten (z. B. dienst- und arbeitsrechtliche Regelungen, Sozialgeheimnis, Brief-, Post- und Fernmeldegeheimnis) sind zu beachten.

Wo erhält man weitere Auskünfte?

Wenn Sie weitere Fragen zum Datenschutz haben oder in einem Einzelfall eine Rechtsauskunft benötigen, wenden Sie sich an die Dienstvorgesetzten oder an die örtlich Beauftragte oder den örtlich Beauftragten für den Datenschutz.

Die Aufgabe der Datenschutzaufsicht obliegt der oder dem zuständigen Beauftragten für den Datenschutz Ihrer Landeskirche. Weitere Informationen und die Kontaktdaten erhalten Sie über das Internet unter https://datenschutz.ekd.de.