Merkblatt über den Datenschutz und die Datensicherheit für haupt- und ehrenamtlich Mitarbeitende des Deutschen Evangelischen Kirchentages[1]

Dieses Merkblatt enthält Informationen über den wesentlichen Inhalt des Datenschutzes und Datengeheimnisses und den Sinn der Verpflichtungserklärung. Zudem dient es der Aufklärung über die Verarbeitung von Daten der haupt- und ehrenamtlich Mitarbeitenden selbst. Es schließen sich die Verpflichtung zur Wahrung des Datengeheimnisses und die Erklärung zur Verschwiegenheit über interne Informationen des Kirchentages an.

Die Vorschriften betreffen alle Mitarbeitenden (sowohl Haupt- und Ehrenamtliche als auch Honorar-, Werks-, sonstige Vertragsmitarbeitende und Freiberufler:innen).

Welche rechtlichen Grundlagen gelten für den Datenschutz?

Für den Schutz von personenbezogenen Daten gelten die allgemeinen Datenschutzbestimmungen. Dies sind jeweils in ihrer geltenden Fassung das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) und die Verordnung zur Sicherheit der Informationstechnik (ITSVO-EKD) sowie Dienst- und Organisationsanweisungen zum Datenschutz oder zur IT-Sicherheit, die vom Deutschen Evangelischen Kirchentag erlassen wurden.

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 beim Deutschen Evangelischen Kirchentag?

1. 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).

   Der Deutsche Evangelische Kirchentag stützt den Großteil seiner Verarbeitungsvorgänge auf Einwilligung, Erfüllung der Aufgabe des Deutschen Evangelischen Kirchentages und

[1] Als Deutscher Evangelischer Kirchentag gelten hier der Verein zur Förderung des Deutschen Evangelischen Kirchentages e. V. sowie der jeweilige Durchführungsverein.

Vertragserfüllung. Weitere Informationen dazu sind in den Datenschutzhinweisen des Deutschen Evangelischen Kirchentages nachlesbar.

2. Personenbezogene Daten dürfen nur zur Erfüllung von Aufgaben aus der Geschäftsordnung des Deutschen Evangelischen Kirchentages und den korrespondierenden Vereinssatzungen verwendet werden, sofern dies im Zusammenhang mit der Vorbereitung, Durchführung und Abwicklung des jeweils aktuellen Kirchentages steht. Maßgebend für den Zugang zu den Daten ist für die Mitarbeitenden der ihnen zugewiesene Tätigkeits- und Aufgabenbereich.
3. Personenbezogene Daten sind nach den Grundsätzen gemäß § 5 DSG-EKD zu verarbeiten. Die verantwortliche Stelle muss die Einhaltung der Grundsätze nachweisen können (Rechenschaftspflicht).
4. 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 zulässig (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.
5. Alle Informationen, die Mitarbeitende aufgrund ihrer Tätigkeiten an und mit Akten, Dateien und Listen erhalten, sind von ihnen streng vertraulich zu behandeln. Diese Pflicht besteht auch nach Beendigung der Tätigkeit weiter. Personenbezogene Daten dürfen nur Mitarbeitenden zugänglich gemacht werden, die aufgrund ihrer Aufgaben zum Empfang der Daten ermächtigt, ausdrücklich über ihre Verpflichtung zum Datenschutz belehrt und zur Wahrung des Datengeheimnisses verpflichtet worden sind.
6. Die Mitarbeitenden sind für die datenschutzrechtlich korrekte Ausübung ihrer Tätigkeit verantwortlich. Die sorgsame und vertrauliche Behandlung von Daten ist ein wichtiges Gebot im Rahmen ihrer Arbeit. Daten sind im Rahmen der Möglichkeiten stets sicher und verschlossen zu verwahren und vor Einsicht oder sonstiger Verwendungen durch Unbefugte zu schützen.

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

1. Wenn personenbezogene Daten verarbeitet werden, sind die technischen und organisatorischen Maßnahmen gemäß §§ 27, 28 DSG-EKD zu beachten.
2. Personenbezogene Daten dürfen erst nach der Akzeptanz der Verschwiegenheitserklärung und nur im Rahmen der Erfüllung der Aufgaben auf einem persönlichen IT-Gerät gespeichert und verarbeitet werden.
3. Werden Laptops und andere Endgeräte des Deutschen Evangelischen Kirchentages für die Erfüllung der Aufgaben bereitgestellt, sind diese in erster Linie zu nutzen. Werden private Laptops oder andere Endgeräte zur Erfüllung der Aufgaben genutzt, hat die/der Benutzer:in für einen angemessenen Schutz (Virenschutz/Firewall) zu sorgen, diesen regelmäßig zu überprüfen und zu aktualisieren. Sensible personenbezogene Daten sind darüber hinaus zu verschlüsseln.
4. Es ist untersagt, Passwörter und Hardwaretoken (z. B. Chipkarten) sowie Benutzerkennungen (z. B. für Windows, Microsoft) weiterzugeben. Auch das Notieren, Speichern oder Hinterlegen von Kennwörtern ist unerwünscht und stellt ein Risiko dar.
5. Beim Verlassen des Arbeitsplatzes – auch bei kurzfristiger Abwesenheit – ist der Computer so zu hinterlassen, dass keine dritte Person Zugang zu Daten und Portalen erlangen kann. Der Zugang

zu Datenbanken und Datenbank-Tools (Wilma, Pentaho) sowie der Cloud ist unmittelbar nach der Nutzung wieder sachgemäß zu beenden.

6. Alle Arten von Datenträgern müssen bei Abwesenheit stets sicher und verschlossen verwahrt werden und vor jeder Einsicht oder sonstigen Nutzung durch Unbefugte zu schützen. Sofern die Gegebenheiten es zulassen, sind Räume insbesondere über Nacht abzuschließen.

   Der Begriff Datenträger umfasst sowohl elektronische Speichermedien (z. B. USB-Sticks, CDs, externe Festplatten, Dateien, Datenbanken, Cloud-Server) als auch schriftliche Unterlagen (z. B. Listen, Schriftverkehr, Anmeldeunterlagen, Excel-Listen, Datenbank-Exporte).

7. 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.

8. Unbeaufsichtigt aufgefundene Datenträger müssen schnellstmöglich an die/den zuständige:n Mitarbeiter:in zurückgegeben werden. Ist dies nicht möglich, sind die Datenträger an die für den Einsatzbereich zuständige hauptamtliche Ansprechperson zu übergeben oder ordnungsgemäß zu vernichten.

9. Analoge und digitale Datenbestände, die nicht mehr zur Erfüllung des zugewiesenen Aufgabenbereichs benötigt werden, sind an den Deutschen Evangelischen Kirchentag zurückzugeben oder so zu vernichten oder zu löschen, dass jeder Missbrauch der Daten ausgeschlossen ist. Dies bedeutet für elektronische Datenbestände insbesondere auch, dass diese Datenbestände aus dem Papierkorb zu löschen sind. Schriftliche Datenbestände, die personenbezogene Daten enthalten, sind im Datenmüll zu entsorgen.

10. Eigenmächtige Änderungen der dienstlichen Hardware und deren Konfiguration – insbesondere der Einbau von Karten – sind ebenso wie das unbefugte Einspielen von privater Software nicht gestattet.

11. Im Netzwerk bzw. WLAN des Kirchentages ist das private Downloaden ausführbarer Dateien, großer Datenmengen und umfassendes Medienstreaming nicht erlaubt.

12. Ist für den Mitarbeitenden ein Outlook-Zugang eingerichtet worden, ist die Nutzung dieser E-Mail-Adresse nur zu Zwecken der Aufgabenerfüllung, nicht für private Zwecke erlaubt.

13. Die Mitarbeitenden sind verpflichtet, Datenpannen (Verlust von Laptops, Telefonen, Zugängen, Dokumenten, Ordnern, Speichermedien etc.), Mängel beim Datenschutz, der Datensicherung oder der ordnungsgemäßen Datenverarbeitung unverzüglich an die für den Einsatzbereich zuständige hauptamtliche Ansprechperson zu melden. Diese gibt die Meldung via datenschutz@kirchentag.de an die örtlich Beauftragte für den Datenschutz weiter. Unabhängig davon können sich Mitarbeitende auch ohne Einhaltung des Dienstweges vertraulich an den Beauftragten für den Datenschutz der EKD wenden.

14. Verstöße gegen die Datenschutzbestimmungen sind Pflichtverletzungen und können rechtliche Konsequenzen haben.

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, Steuer-, Brief-, Post- und Fernmeldegeheimnis) sind zu beachten.

Hinweise zur Verarbeitung der Daten von ehrenamtlich und hauptamtlich Mitarbeitenden

1. Sowohl Telefonate und weitere Kommunikation, die bei der Nutzung von Microsoft-Produkten (vor allem MS Teams) entstehen, als auch Internetzugriffe werden mit der vorhandenen Technologie gespeichert. Auswertungen werden nicht personenbezogen, nach Arbeitsplätzen oder Durchwahlnummern vorgenommen, sondern nur zu statistischen Zwecken. Personenbezogene Auswertungen sind nur nach Rücksprache mit dem Vorstand und MAV/Betriebsrat möglich, wenn ein konkreter Missbrauchsverdacht vorliegt. Die Datenschutzbeauftragte wird informiert.
2. Die Tracking-Funktionen von Microsoft, die z.B. Vorschläge zum Zeitmanagement durch MS Viva ermöglichen, können alle Mitarbeiter:innen selbstständig deaktivieren.
3. Bei längerer Abwesenheit von Mitarbeitenden (über zwei Wochen) kann das E-Mail-Postfach auf Weisung des zuständigen Vorstandes und mit Einverständnis der MAV/des Betriebsrates für andere Mitarbeitende freigeschaltet bzw. umgeleitet werden. Die Datenschutzbeauftragte wird informiert. Die technischen Möglichkeiten einer Vertretungsregelung bzw. einer Weiterleitung durch die verwendete Software Outlook sollten – soweit möglich – von den Mitarbeitenden selbst genutzt werden.
4. Nach Beendigung des Dienstverhältnisses kann das E-Mail-Postfach der Mitarbeitenden an andere Mitarbeitende bzw. der/dem dienstlich Vorgesetzten weitergeleitet werden. Das E-Mail-Postfach der Mitarbeitenden wird nach Beendigung der Tätigkeit i.d.R. 10 Jahre aufbewahrt. Die Aufbewahrungsfristen richten sich nach Handelsgesetzbuch (HGB), Abgabenordnung (AO) und Umsatzsteuergesetz (UStG).
5. Die private Dateiablage ist auf OneDrive möglich. Einsicht kann durch die Systemadministration genommen werden, falls ein berechtigtes Interesse seitens der Vorgesetzten vorliegt. Die Datenschutzbeauftragte, der Betriebsrat bzw. die Mitarbeitendenvertretung werden informiert.
6. Die Schließanlage des Deutschen Evangelischen Kirchentages in den Geschäftsräumen in Fulda und ggf. der Durchführungsstadt besitzt eine Funktion zur Aufzeichnung aller Schließvorgänge. Eine systematische Dokumentation und Auswertung dieser Daten finden nicht statt. Im Falle von missbräuchlicher Nutzung besteht die Möglichkeit in Absprache mit dem Vorstand und MAV/Betriebsrat im Einzelfall die Daten einzusehen.
7. Die Arbeitszeiterfassung erfolgt über absence. Direkte Vorgesetzte haben Einsicht in die Daten von Mitarbeitenden ihrer Abteilung. Die Personalabteilung hat Volleinsicht. Der Personalvorstand und weitere Vorstandsmitglieder nach Bedarf haben auch das Recht auf Einsicht. MAV/Betriebsrat dürfen Einsicht nehmen.
8. Hinweis: Der Betriebsrat ist nach § 79 BetrVG auf das Datengeheimnis verpflichtet. Die Mitarbeitendenvertretung ist nach § 22 MVG-EKD auf das Datengeheimnis verpflichtet.
9. Hinweis: Regelungen zur Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses sind u.a. in § 26 Bundesdatenschutzgesetz (BDSG) festgehalten.

Wo erhält man weitere Auskünfte?

Weitere Fragen zum Datenschutz, Datenpannen oder im Einzelfall die Bitte um eine Rechtsauskunft können unter datenschutz@kirchentag.de an die örtlich Beauftragte für den Datenschutz Dorothea Böhr oder den für Datenschutz zuständigen Vorstand Janine Rolfsmeyer gerichtet werden.

Die Aufgabe der Datenschutzaufsicht obliegt dem zuständigen Beauftragten für den Datenschutz der Evangelischen Kirche Deutschland, vertreten durch die zuständige Außenstelle Dortmund (Datenschutzregion Mitte-West). Weitere Informationen und die Kontaktdaten sind unter datenschutz.ekd.de einsehbar.

Verpflichtung auf das Datengeheimnis

Ich bin als haupt- oder ehrenamtliche:r Mitarbeiter:in mit der Vorbereitung und Durchführung des Deutschen Evangelischen Kirchentages betraut worden. Zur Erfüllung meiner spezifischen Aufgaben bin ich auch mit der Verarbeitung personenbezogener Daten im Vorbereitungs- und Durchführungszeitraum beauftragt. Diese Nutzungserlaubnis endet mit der Tätigkeit für den Kirchentag.

Mit Aushändigung und unter Hinweis auf das obige Merkblatt verpflichte ich mich wie folgt auf das Datengeheimnis gemäß § 26 DSG-EKD:

Es ist untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis).

Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

Verstöße gegen das Datengeheimnis sind Pflichtverletzungen und können dienstrechtlich, arbeitsrechtlich, urheberrechtlich, strafrechtlich, disziplinarrechtlich geahndet werden und Haftungstatbestände auslösen.

Verschwiegenheitserklärung

Ich verpflichte mich Stillschweigen zu wahren über vertrauliche und geheime Informationen, Erkenntnisse, Dokumente, Muster, Vorlagen etc., von denen ich im Rahmen meiner Tätigkeit Kenntnis erlange. Ich treffe alle erforderlichen Maßnahmen, um die Verwertung und Kenntnisnahme durch Dritte zu verhindern. Ohne Einwilligung des Kirchentages verwende ich die Informationen nicht eigenmächtig.

Ich habe den Inhalt des Merkblattes über den Datenschutz und die Datensicherheit für haupt- und ehrenamtlich Mitarbeitende des Deutschen Evangelischen Kirchentages zur Kenntnis genommen und akzeptiere die dort benannten Hinweise und Handlungsvorgaben.

Ich verpflichte mich, die Bestimmungen des Datenschutzes auf Grundlage der Europäischen Datenschutzgrundverordnung (EU-DSGVO) und des Datenschutzgesetzes der EKD (DSG-EKD) sorgfältig einzuhalten.

Die Verpflichtung auf das Datengeheimnis und die Verschwiegenheitserklärung gelten verbindlich ab dem Zeitpunkt der Unterschrift bzw. der digitalen Anmeldung in der Datenverwaltung des Kirchentages (Wilma) und über das Ende des Beschäftigungsverhältnisses hinaus.

Name, Vorname	Datum, Unterschrift

Stand 9.1.2024