

# Merkblatt<sup>1</sup> zur Verpflichtung auf das Datengeheimnis für Mitarbeitende<sup>2</sup>

## Welchen Grund hat die Verpflichtung auf das Datengeheimnis?

Wer seine persönlichen Daten einer kirchlichen Stelle anvertraut, hat einen Anspruch darauf, dass mit diesen Daten verantwortungsvoll umgegangen wird. Aus diesem Grund sind kirchliche Einrichtungen gesetzlich verpflichtet, alle für sie tätigen Personen zur Verschwiegenheit zu verpflichten.

Alle personenbezogenen Informationen, die Sie im Rahmen Ihrer Tätigkeit erhalten, sind grundsätzlich vertraulich zu behandeln. Diese Pflicht besteht auch nach Beendigung Ihrer Tätigkeit fort.

## Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen. Dazu gehören z. B. Name, Geburtsdatum, Anschrift, Beruf, Familienstand, Religion, Gesundheitszustand sowie Fotos und Videoaufzeichnungen. Wenn Sie etwa als Mitglied eines Besuchskreises Gespräche mit einem Gemeindeglied führen, handelt es sich bei dem, was Ihr Gesprächspartner Ihnen über sich selbst oder über eine andere Person erzählt, um personenbezogene Daten. Diese Daten werden durch die Datenschutzregelungen geschützt.

## Welche rechtlichen Grundlagen gelten für den kirchlichen Datenschutz?

Durch das Datengeheimnis wird es denjenigen, die mit personenbezogenen Daten umgehen, untersagt, diese Daten unbefugt zu verarbeiten. Was dies im Einzelnen bedeutet, wird durch die jeweils geltenden Datenschutzbestimmungen festgelegt. Es sind insbesondere die folgenden grundlegenden Bestimmungen zum Datenschutz zu beachten:

- das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD)<sup>3</sup>,
- Bestimmungen der Landeskirche zum DSG-EKD,
- die IT-Sicherheitsverordnung der Evangelischen Kirche in Deutschland (ITSVO-EKD)<sup>4</sup>.
- Sie finden diese und weitere Vorschriften in der Online-Rechtssammlung der EKD<sup>5</sup>.

## Datenverarbeitung

Die Verarbeitung personenbezogener Daten umfasst jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Dazu gehören **insbesondere das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung**, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung von Daten. Auch die Einschränkung der Verarbeitung, das **Löschen** oder die Vernichtung von Daten gehören dazu. **Der Begriff der „Verarbeitung“ erfasst damit jede Form des Umgangs mit personenbezogenen Daten.** Die Verarbeitung beginnt mit der Erhebung und endet mit der Löschung. Dies gilt unabhängig davon, ob die Daten automatisiert oder manuell verarbeitet werden.

---

<sup>1</sup> Version 2.1. vom 10.03.2026

<sup>2</sup> Ursprüngliches Musterdokument: <https://datenschutz.ekd.de/infotehek-items/verpflichtungserklaerung-von-mitarbeitenden-auf-das-datengeheimnis/>

<sup>3</sup> <https://www.kirchenrecht-ekd.de/document/58309>

<sup>4</sup> <https://kirchenrecht-ekd.de/document/32147>

<sup>5</sup> <https://datenschutz.ekd.de/datenschutzrecht/ds-ost/>

## Grundsätze der Datenverarbeitung

Folgende Grundsätze sind bei der Verarbeitung personenbezogener Daten einzuhalten (§ 6 DSGVO):

- **Rechtmäßigkeit:** Die Verarbeitung darf nur auf einer gesetzlichen Grundlage erfolgen.
- **Transparenz:** Die Datenverarbeitung muss für die betroffene Person nachvollziehbar sein.
- **Zweckbindung:** Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden. Eine Weiterverarbeitung zu anderen, damit unvereinbaren Zwecken ist unzulässig.
- **Datenminimierung:** Es dürfen nur solche Daten verarbeitet werden, die für den jeweiligen Zweck erforderlich sind.
- **Richtigkeit:** Personenbezogene Daten müssen sachlich richtig und auf dem neuesten Stand sein. Unrichtige Daten sind unverzüglich zu berichtigen oder zu löschen.
- **Speicherbegrenzung:** Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke der Verarbeitung erforderlich ist oder gesetzliche Aufbewahrungsfristen bestehen.
- **Integrität und Vertraulichkeit:** Daten müssen durch technische und organisatorische Maßnahmen so verarbeitet werden, dass sie vor unbefugtem Zugriff, Verlust oder Zerstörung geschützt sind.
- **Rechenschaftspflicht:** Die kirchliche Stelle ist verpflichtet, die Einhaltung dieser Grundsätze nachweisen zu können.

## Neue Prozesse, Software oder Dienstleister

Vor der Nutzung neuer Prozesse, der Einbindung neuer Software oder neuer Dienstleister in Bezug auf die Verarbeitung kirchlicher Daten ist der Datenschutzbeauftragte zur Prüfung der datenschutzrechtlichen Bewertung und der Einhaltung der gesetzlichen Anforderungen zu konsultieren.

## Wann ist die Verarbeitung personenbezogener Daten zulässig?

Im Datenschutz gilt das sogenannte „Verbot mit Erlaubnisvorbehalt“. Das bedeutet, dass eine Verarbeitung personenbezogener Daten nur zulässig ist, sofern mindestens eine der folgenden Anforderungen („Rechtsgrundlagen“) gem. § 6 DSGVO erfüllt wird:

Die Datenverarbeitung

- ist **aufgrund** einer kirchlichen oder staatlichen **Rechtsvorschrift erlaubt**,
- erfolgt **auf Grundlage der Einwilligung** der betroffenen Person,
- ist zur **Erfüllung einer kodifizierten kirchlichen Aufgabe** erforderlich,
- erfolgt **aufgrund eines berechtigten Interesses** der kirchlichen Einrichtung an der Verarbeitung, sofern nicht die Interessen der betroffenen Person überwiegen,
- ist zur **Erfüllung eines Vertrags** erforderlich,
- ist zur **Erfüllung rechtlicher Verpflichtungen** notwendig oder
- ist zum Schutz **lebenswichtiger Interessen** erforderlich.

Das kirchliche Datenschutzrecht sieht zudem vor, dass

- Daten auch innerhalb der verantwortlichen Stelle nur solchen Personen bereitgestellt werden dürfen, die sie zur Erfüllung ihrer Aufgaben benötigen und zur Verschwiegenheit verpflichtet sind,

- Datenauskünfte an Dritte außerhalb der verantwortlichen Stelle nur vorgenommen werden dürfen, wenn eine Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat.

Grundsätzlich haben Sie über alle personenbezogenen Daten, die Sie aufgrund Ihrer kirchlichen Tätigkeit zur Kenntnis nehmen, Verschwiegenheit zu wahren. Es ist nicht zulässig, Familienmitglieder oder andere Personen zu informieren. Unabhängig davon dürfen Daten in keinem Fall an Dritte, z.B. zum Zweck der Werbung an Versicherungen, Zeitungen oder Firmen herausgegeben werden.

## Welche Schutzmaßnahmen sind umzusetzen?

Zur Gewährleistung der Vertraulichkeit sind die Daten durch technische und organisatorische Maßnahmen zu schützen. Bitte bewahren Sie aus diesem Grund alle Informationen, wie z.B. Dokumente, Notizen, Karteikarten oder USB-Speicher, stets sicher und verschlossen auf, damit ein unbefugter Zugriff Dritter nach Möglichkeit ausgeschlossen wird. In Bezug auf die Speicherung der Daten sind die folgenden Maßnahmen umzusetzen:

- Grundsätzlich dürfen **keine kirchlichen Daten in privaten Endgeräten gespeichert** werden. Die Speicherung sollte ausschließlich in der (Cloud)-Infrastruktur des Kirchenkreises erfolgen.
- Primäre Arbeitsmittel zur Kommunikation und Speicherung sind hierbei Microsoft Teams, Outlook, Online-Office, Sharepoint und OneDrive.
- Sofern die **lokale Speicherung** kirchlicher Daten in Ihrem privaten Endgerät notwendig sein sollte, ist dies vorab mit der verantwortlichen kirchlichen Stelle zu klären und eine entsprechende **Genehmigung einzuholen**.
- Auch eine Weiterleitung an die private E-Mail-Adresse oder die Speicherung in privat genutzten Cloud-Infrastrukturen, wie z.B. Dropbox oder iCloud, sind nicht gestattet.
- **Private E-Mail-Postfächer dürfen nicht für die dienstliche Tätigkeit genutzt werden**. Hiervon ausgenommen sind die automatisierten Benachrichtigungs-Mails, die darüber informieren, dass Sie in Ihrem dienstlichen Postfach ungelesene E-Mails gespeichert haben.

## Verstöße hiergegen können einen meldepflichtigen Datenschutzvorfall zur Folge haben.

Des Weiteren sind die nachfolgenden Maßnahmen zur Gewährleistung eines Mindestmaßes an Datensicherheit umzusetzen:

- Der Zugang zum Computer muss durch eine Benutzerkennung und ein Passwort geschützt sein.
- Familienangehörige oder andere Personen dürfen keinen Zugriff auf die kirchlichen Daten haben.
- Das Betriebssystem und die Programm- sowie Browserversionen sind stets aktuell zu halten. Die Nutzung veralteter Systeme kann zu einem Einbruch in Ihr IT-System und Datenabfluss führen.
- Schutzsoftware (Virenschutzprogramme, Firewall, etc.) ist regelmäßig zu aktualisieren.
- Nicht mehr benötigte Daten, die nicht einer Aufbewahrungspflicht unterfallen und vom kirchlichen Archiv nicht benötigt werden, sind sicher zu löschen.
- Die Daten sind durch Datensicherungen vor einem etwaigen Verlust zu schützen.
- Kirchliche Daten sollten auf verschlüsselten Datenspeichern gespeichert werden. Sensible Informationen müssen verschlüsselt werden.

## Datenschutzfolgenabschätzung bei hohem Risiko für Betroffene

Hat eine Datenverarbeitung ein hohes Risiko für die Betroffenen und ist eine Bewertung der Datenschutzfolgen nicht erfolgt, ist vorab eine Datenschutzfolgenabschätzung (DSFA) vorzunehmen. Hierzu ist der örtlich Beauftragte für Datenschutz zu konsultieren.

Beispiele für risikobehaftete Verarbeitungstätigkeiten, die eine vorherige Datenschutzfolgenabschätzung notwendig machen: Videoüberwachung, GPS-Tracking, Einsatz künstlicher Intelligenz, Verarbeitung medizinischer, biometrischer oder genetischer Daten, Verarbeitung von Daten zur sexuellen Orientierung, usw.

## **Strafrechtlichen Konsequenzen**

Verstöße gegen das Datengeheimnis können Straftatbestände darstellen. Mit einer Freiheits- oder Geldstrafe könnte jemand bestraft werden, der:

- 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 Berufsheimnisträger i. S. v. § 203 Absatz 1 StGB, als dessen berufsmäßig tätige Gehilfen (z. B. Sekretärin, Verwaltungsfachkraft), als beim Berufsheimnisträger 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 Berufsheimnisträgers 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 Privatheimnissen“),
- 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.

**Verstöße gegen das Datengeheimnis können Disziplinarmaßnahmen und Schadensersatzforderungen nach sich ziehen.**

## **Datenschutzverletzungen**

**Haben Sie den Eindruck, dass eine Datenschutzverletzung vorliegt, sind sofort die Verwaltungsleitung und der örtlich Beauftragte für Datenschutz zu informieren.**

Datenschutzverletzungen liegen unter anderem vor, wenn

- Unberechtigte in das Netzwerk eingedrungen sind,
- Daten an Unberechtigte (versehentlich oder absichtlich) übermittelt oder offenbart wurden **oder**
- Daten abhandengekommen (z.B. durch den Verlust von Geräten) sind,

## **Weitere Informationen**

Zur Veröffentlichung von Meldungen und Bereitstellung von Formularen sowie weiteren Unterlagen hat der Datenschutzbeauftragte ein Datenschutzportal eingerichtet. Dieses Portal können Sie über die folgende Internetadresse aufrufen: <https://kkrm.datenschutzbuero.hamburg>

Bei Fragen zum Datenschutz können Sie sich an den örtlich Beauftragten für Datenschutz wenden:

Mag. jur. Djoko Lukic  
datenschutzbuero.hamburg | Suhrenkamp 59 – 22335 Hamburg

Email (Ticketsystem): [kkrm@datenschutzbuero.hamburg](mailto:kkrm@datenschutzbuero.hamburg)

Telefon: 040 – 414 313 070

# Information über die Verarbeitung von Personaldaten gem. § 17 DSGVO

## Kommunikation

Um mit Ihnen kommunizieren zu können, verarbeiten wir Ihre Kontaktdaten (Adresse, Telefonnummer, E-Mail-Adresse). Sofern wir uns mit Ihnen per E-Mail austauschen, verarbeiten wir die Kommunikationsinhalte sowie technische Protokolldaten in unserem E-Mail-Server.

Für die Bereitstellung und Administration unserer Kommunikationssysteme setzen wir technische Dienstleister ein, die bei Fehlfunktionen zur Fehleranalyse möglicherweise auch die Kommunikationsinhalte zur Kenntnis nehmen können.

Die Kommunikation erfolgt zur Erfüllung und Inanspruchnahme der vertraglichen Verpflichtungen, die sich aus der Dienst- bzw. Arbeitsvereinbarung gemäß § 6 Nr. 5 in Verbindung mit § 49 DSGVO ergeben.

In allen übrigen Fällen ist die Rechtsgrundlage unser berechtigtes Interesse an der Kommunikation gem. § 6 Nr. 4 DSGVO.

## Personaldaten

Die Kirchenkreisverwaltung verarbeitet Ihre Personaldaten zur Erfüllung und Inanspruchnahme der vertraglichen Verpflichtungen, die sich aus der Dienst- bzw. Arbeitsvereinbarung gemäß § 6 Nr. 5 in Verbindung mit § 49 DSGVO ergeben. Die Verarbeitung erfolgt ausschließlich im Rahmen der gesetzlichen Bestimmungen des DSGVO und dient der Begründung, Durchführung und Beendigung des Dienst- bzw. Arbeitsverhältnisses.

Verarbeitet werden hierbei die folgenden Datenkategorien:

- Stammdaten (z. B. Name, Geburtsdatum, Anschrift, Kontaktdaten)
- Beschäftigtendaten (z. B. Personalnummer, Vertragsdaten, Arbeitszeitmodelle, Einsatzbereich, Bewerbungsunterlagen)
- Abrechnungs- und Zahlungsdaten (z. B. Bankverbindung, Steuer- und Sozialversicherungsdaten, Gehaltsabrechnungen)
- Leistungs- und Bewertungsdaten (z. B. Beurteilungen, Qualifikationen, Fortbildungsnachweise)
- Abwesenheits- und Gesundheitsdaten, soweit für das Beschäftigungsverhältnis erforderlich (z. B. Krankmeldungen, Urlaubszeiten, Arbeitsunfähigkeitsbescheinigungen)

Ihre Daten werden ausschließlich in Erfüllung kirchlicher oder staatlicher Rechtsvorschriften gem. § 6 Nr. 1 DSGVO weitergegeben. Empfänger können insbesondere folgende Stellen sein:

- Sozialversicherungsträger (z. B. Krankenkassen, Rentenversicherungsträger),
- Finanzbehörden,
- Zusatzversorgungskassen und Versorgungseinrichtungen,
- Banken im Rahmen der Gehaltszahlung,
- Interessenvertretungen (z. B. Mitarbeitervertretung, Schwerbehindertenvertretung) sowie
- das kirchliche Archiv

Sofern wir zur Erfüllung unserer Aufgaben und Pflichten Dienstleister einsetzen, werden die Daten auch von diesen verarbeitet. Eine weitergehende Offenlegung gegenüber Dritten erfolgt ausschließlich mit Ihrer ausdrücklichen Einwilligung oder auf Grundlage einer bestehenden gesetzlichen Verpflichtung.

Ihre Personaldaten werden nur so lange gespeichert, wie es für die Durchführung des Dienst- bzw. Arbeitsverhältnisses und zur Erfüllung gesetzlicher Aufbewahrungsfristen erforderlich ist. Nach Beendigung des Beschäftigungsverhältnisses werden die Daten regelmäßig gelöscht, sobald gesetzliche oder vertragliche Aufbewahrungsfristen abgelaufen sind. Hierbei kommen unter Anderem die folgenden Löschfristen zur Geltung:

- Lohn- und Gehaltsabrechnungen: 10 Jahre
- Bewerbungsunterlagen: 6 Monate nach Abschluss des Verfahrens, sofern keine Einwilligung für längere Speicherung erteilt wurde
- Gesundheitsdaten: für die Dauer des Beschäftigungsverhältnisses, soweit erforderlich
- Archivwürdige Unterlagen: unbegrenzt (siehe Archivierungsregelung)

Welche konkreten Löschfristen zur Anwendung kommen, ist der Kassationsordnung zu entnehmen (verfügbar unter: <https://www.kirchenrecht-ekd.de/document/3432>).

### **Verpflichtung auf das Datengeheimnis**

Wir sind gemäß § 26 Satz 2 DSGVO verpflichtet, alle Beschäftigten auf das Datengeheimnis zu verpflichten. Die Verpflichtung erfolgt somit zur Erfüllung einer gesetzlichen Pflicht gemäß § 6 Nr. 1 DSGVO. Die Verpflichtungserklärung wird durch die Personalabteilung des kirchlichen Verwaltungszentrums aufbewahrt.

Verarbeitet werden Ihr Name, der Ort und das Datum der Unterzeichnung sowie Ihre Unterschrift.

### **Kirchliches Archiv**

Das kirchliche Archiv hat die Aufgabe, das Wirken der Kirche und damit die Erfüllung des kirchlichen Auftrags zu dokumentieren. Stellt das kirchliche Archiv fest, dass die Schriftgüter archivwürdig sind, werden diese in ein Langzeitarchiv überführt und nicht vernichtet. Die Archivierung kann auch Dokumente betreffen, die personenbezogene Daten Ihnen enthalten. Hierzu gehören auch Personalakten, die aus Sicht der Archivs von Bedeutung sind.

Die Archivierung erfolgt aufgrund der Pflichten aus § 7 EKD-Archiv-DSGVO und somit in Erfüllung einer Rechtsvorschrift gem. § 6 Nr. 1 DSGVO.

## **Ihre Rechte**

- Sie haben ein Recht auf Auskunft, ob und welche Daten von Ihnen durch uns gespeichert bzw. verarbeitet werden.
- Sollten die Sie betreffenden Daten nicht richtig oder unvollständig sein, können eine Berichtigung Ihrer Daten verlangen.
- Ihnen steht ein Löschantrag zu, soweit keine rechtlichen Verpflichtungen die weitere Speicherung erforderlich machen.
- Zudem können Sie die Verarbeitung der Daten einschränken, soweit u. A. die Richtigkeit der Daten bestritten wird oder die Datenverarbeitung unrechtmäßig ist.
- Wenn Sie in die Datenverarbeitung eingewilligt haben oder ein Vertrag zur Datenverarbeitung besteht und die Datenverarbeitung mithilfe automatisierter Verfahren durchgeführt wird, steht Ihnen ein Recht auf Datenübertragbarkeit zu.
- Sie haben das Recht gegen die Verarbeitung Sie betreffender personenbezogener Daten Widerspruch einzulegen. Ihr Widerspruch verpflichtet uns dazu, die Verarbeitung zu unterlassen, soweit wir nicht an der Verarbeitung ein zwingendes kirchliches Interesse haben, das Interesse einer dritten Person überwiegt oder uns eine Rechtsvorschrift zur Verarbeitung verpflichtet.
- Sie haben das Recht eine erteilte Einwilligung zur Verarbeitung Ihrer personenbezogenen Daten jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.
- Schließlich steht Ihnen ein Beschwerderecht über die Verarbeitung Ihrer personenbezogenen Daten bei der zuständigen Datenschutzaufsicht zu.

## **Verantwortliche Stelle**

Verantwortlich für die Datenverarbeitung ist der Ev.-Luth. Kirchenkreis Rantzaу-Münsterdorf (Heinrichstraße 1, 25524 Itzehoe) als Körperschaft des öffentlichen Rechts. Der Kirchenkreis wird vertreten durch den Kirchenkreisrat (siehe: <https://www.kk-rm.de/impressum/>).

## **Örtlich Beauftragter für Datenschutz**

Mag. jur. Djoko Lukic  
datenschutzbuero.hamburg | Suhrenkamp 59 – 22335 Hamburg  
Email (Ticketsystem): kkrm@datenschutzbuero.hamburg  
Telefon: 040 – 414 313 070

## **Kirchliche Datenschutzaufsicht**

Der Beauftragten für den Datenschutz der EKD (BFD EKD)  
Außenstelle Berlin für die Datenschutzregion Ost  
Invalidenstraße 29 | 10115 Berlin