Datenschutz-Information für Mitarbeitende

Merkblatt zum Datenschutz nach DSG-EKD 2025

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Liebe Kolleginnen und Kollegen*,

die Menschenwürde ist Grundlage für das gesamte kirchliche und staatliche Handeln (s.a. Der Beauftragte für den Datenschutz: EKD – warum kirchlicher Datenschutz? Sie wirkt sich auf alle Lebensbereiche aus – auch auf den Umgang mit Daten: aus dem Grundsatz der Menschenwürde leitet sich das Grundrecht auf informationelle Selbstbestimmung ab. Das bedeutet, dass jeder Mensch grundsätzlich selbst darüber bestimmen kann, welche Daten über ihn erhoben werden (personenbezogene Daten). Beim Umgang mit diesen Daten muss also immer darauf geachtet werden, dass sie sorgfältig behandelt und geschützt werden.

Datenschutz ist ein Thema, das uns alle angeht!

Für die evangelische Kirche hat der Schutz personenbezogener Daten schon immer eine besondere Rolle gespielt: Die Daten von Gemeinde-Mitgliedern und Mitarbeitenden sowie von Menschen, die kirchliche Einrichtungen in Anspruch nehmen, müssen vor dem Hintergrund des kirchlichen Auftrags und des christlichen Menschenbildes besonders geschützt werden.

Der Zweck des Datenschutzes, den Einzelnen davor zu schützen, dass er im Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird, erfordert ein verantwortliches Handeln beim Umgang mit personenbezogenen Daten, aber auch eine risikobewusste Nutzung von IT-Systemen und -Anwendungen.

Die aktuelle Novellierung des DSG-EKD zielt darauf ab, das kirchliche Datenschutzrecht im Einklang mit europäischen Anforderungen weiterzuentwickeln, um die speziellen Belange der kirchlichen Arbeit weiterhin berücksichtigen zu können.

Die Wahrung der Vertraulichkeit ist eine arbeits- und datenschutzrechtliche Pflicht.

Rechtliche Grundlage hierfür ist das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD). Es regelt die Datenverarbeitung im kirchlichen und diakonischen Bereich (s.a. Seite 6 DSG-EKD und DS-GVO).

Die Aufsicht über die Einhaltung der Vorschriften zum Datenschutz obliegt einer eigenen kirchlichen Aufsichtsbehörde.

In meiner Funktion als örtlich Beauftragter für den Datenschutz stehe ich Ihnen selbstverständlich in allen Zweifelsfragen zur Verfügung. Bitte wenden Sie sich vertrauensvoll an mich.

Ihr örtlich Beauftragter für den Datenschutz

*

Hinweis: Aus Gründen der Lesbarkeit wird auf die Aneinanderreihung von männlichen und weiblichen Personenbezeichnungen verzichtet und stattdessen jeweils nur eine Form verwendet. Selbstverständlich richten sich alle Ausführungen gleichermaßen an Mitarbeiterinnen und Mitarbeiter.

DATENSCHUTZ IM ÜBERBLICK

Die betroffene Person

... übt ihre Rechte aus

Sie kann Auskunft über gespeicherte Daten beantragen und ggf. Berichtigung, Löschung, Sperrung oder Portierung ihrer Daten erwirken.

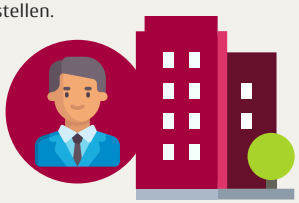
ab Seite 16

Die unabhängige Aufsichtsbehörde

... kontrolliert die Einhaltung

Die Aufsichtsbehörde kann unzulässige Verarbeitungstätigkeiten beanstanden, Bußgelder verhängen und einen Antrag auf gerichtliche Entscheidung stellen.

ab Seite 6



Die kirchliche Stelle oder Organisation

... hat die Verantwortung

dafür, dass die Verarbeitung personenbezogener Daten nur entsprechend dem Datenschutzrecht (DSG-EKD) erfolgt.

ab Seite 8

... passt Prozesse und Vorgehensweise an das novellierte DSG-EKD an.

Die EKD macht die Vorgaben, wie und unter welchen Voraussetzungen personenbezogene Daten erhoben und verarbeitet werden dürfen.

ab Seite 12

... sichert die Daten

Personenbezogene Daten müssen vor unbefugtem Zugriff, Verlust und Zerstörung ausreichend geschützt werden.

ab Seite 14

DSG-EKD – DATENSCHUTZ-GESETZ DER EVANGELISCHEN KIRCHE UND DIE DS-GVO

Die großen Amtskirchen – und andere anerkannte Religionsgemeinschaften – haben in Deutschland eine rechtliche Sonderstellung. Bereits in der Weimarer Verfassung von 1919 wurde den Kirchen weitreichende Befugnisse eingeräumt.

Das Grundgesetz nimmt in Art. 140 GG hierauf Bezug und verankert das Kirchenrecht in unserer heutigen Verfassung. Aufgrund dessen sind die Kirchen befugt, eigene sie betreffende Rechtsvorschriften zu erlassen.

Auch europarechtlich genießen die Kirchen eine besondere Stellung. Art. 17 AEUV legt den Schutz des Religionsverfassungsrechts der Mitgliedsstaaten fest und trägt den unterschiedlichen Verhältnissen zwischen Staat und Kirche der Mitgliedsstaaten Rechnung. Das hat auch Folgen für den Datenschutz

Nach Art. 91 DS-GVO ist den Kirchen oder religiösen Gemeinschaften erlaubt, eigene Datenschutzregelungen anzuwenden, sofern diese mit der DS-GVO in Einklang gebracht werden.

Wichtige Neuerungen im DSG-EKD ab 01.05.2025:

1. Wegfall des Rechtsgrunds der kirchlichen Interessen (§ 6 Nr. 4 DSG-EKD):
   geht in der Regelung zum neuen berechtigten Interesse auf.
2. Erweiterung des Rechts auf Datenkopie für Betroffene (§19DSG-EKD):
   Annäherung an Art. 15 DS-GVO
3. Profiling (§25a DSG-EKD): erstmals aufgeführt
4. Auftragsverarbeiter (§30 (5) DSG-EKD):Die bisherige Verpflichtung des weltlichen Dienstleisters, sich der kirchlichen Aufsicht zu unterwerfen, entfällt.
5. Erhöhung des kirchlichen Bußgeldrahmens (§45 DSG-EKD)
   Der Maximalrahmen wird nunmehr auf 6 Mio € festgelegt.
6. Neuregelung des Kreises der Schuldner (§48 (1) DSG-EKD)
   Für die Haftung zum Schadenersatz tritt nunmehr ausschließlich die verantwortliche Stelle ein, nicht der Auftragsverarbeiter.
7. einheitliche Regelung für Minderjährige (§12 DSG-EKD)
   Galt die bisherige Regelung nur für elektronische Angebote, so gilt die neue Regelung für sämtliche Einwilligungen.
8. Einwilligung im Beschäftigten-Datenschutz (§49 (3) DSG-EKD)
   Ab sofort gilt die Textform.

DIE BEDEUTUNG DES KIRCHLICHEN DATENSCHUTZES

Warum ist Datenschutz notwendig?

Die technologische Entwicklung der automatisierten Datenverarbeitung führt zu steigenden Gefahren des Datenmissbrauchs. Es fallen immer mehr Daten an, die nahezu unbegrenzt gespeichert, verknüpft und ausgewertet werden können. Der Einzelne wird dadurch in seinen Persönlichkeits- und Freiheitsrechten beeinträchtigt, insbesondere wenn er nicht weiß, wer welche Daten über ihn hat, was dieser mit diesen macht und an wen er sie weitergibt.

§ 1 DSG-EKG

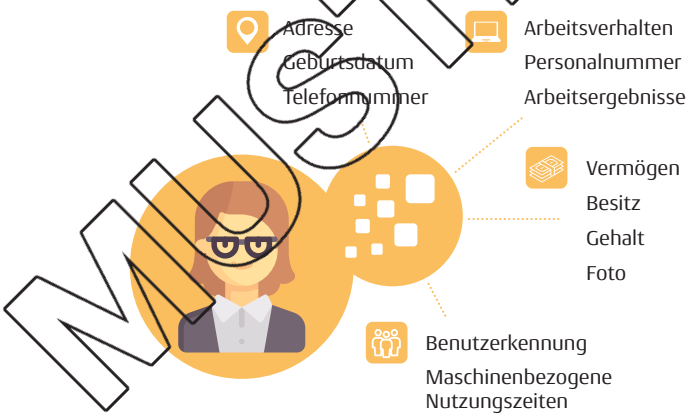
„Zweck dieses Kirchengesetzes ist es, die einzelne Person davor zu schützen, dass sie durch den Umgang mit ihren personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt wird."

Was sind personenbezogene Daten?

Personenbezogene Daten sind Angaben über eine bestimmte oder eine bestimmbare natürliche Person.

§ 4 NR. 1 DSG-EKG

„Personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, [...] identifiziert werden kann;"



MERKSATZ

Jeder Mitarbeiter muss mit personenbezogenen Daten sorgfältig und achtsam umgehen!
(siehe Seite 7/8)

Besondere Kategorien personenbezogener Daten sind alle Informationen, aus denen religiöse oder weltanschauliche Überzeugungen einer natürlichen Person hervorgehen, ausgenommen Angaben über die Zugehörigkeit zu einer Kirche oder einer Religions- oder Weltanschauungsgemeinschaft, ebenso alle Informationen, aus denen die rassische und ethnische Herkunft, politische Meinung oder Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben sowie biometrische und genetische Daten hervorgehen. Ihre Verarbeitung ist nur unter strengen Regeln erlaubt, ihre Verwendung z.B. für Marketingzwecke in der Regel unzulässig.

Was sind die rechtlichen Grundlagen?

Wegen der Gefahren für das Persönlichkeitsrecht bedarf jede personenbezogene Datenverarbeitung einer rechtlichen Grundlage. Dies ist im Kirchenrecht im Rahmen des DSG-EKD geregelt und wird durch bereichsspezifische Normen ergänzt. (siehe Seite 9).

Wen schützt das DSG-EKD?

Zweck dieses Kirchengesetzes ist es, die einzelne Person davor zu schützen, dass sie durch den Umgang mit ihren personenbezogenen Daten in ihrem Persönlichkeitsrecht beeinträchtigt wird.

WER MUSS DAS DSG-EKD BEACHTEN?

1

Evangelische Kirche in Deutschland, die Gliedkirchen und die gliedkirchlichen Zusammenschlüsse

2

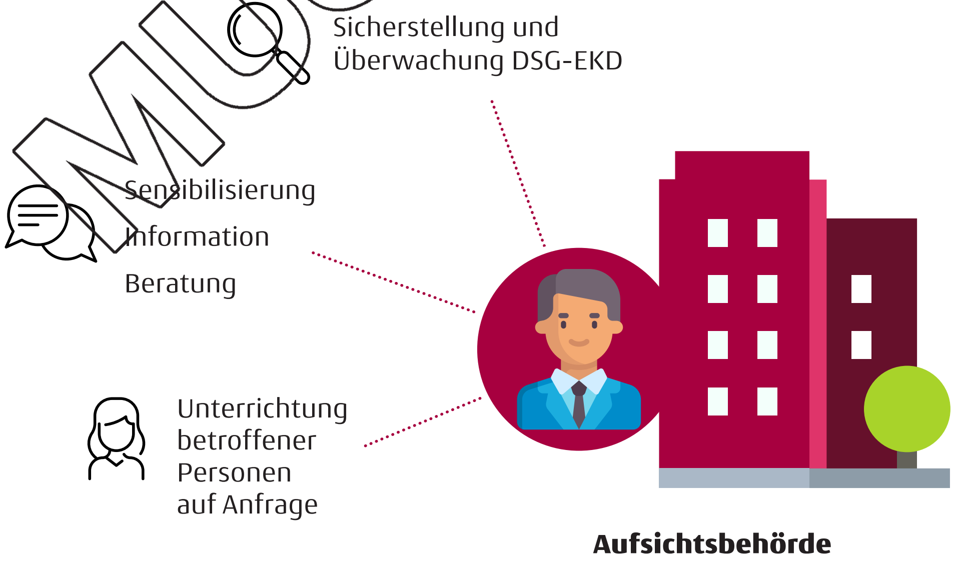
Alle weiteren kirchlichen juristischen Personen des öffentlichen Rechts z. B. Kirchengemeinden sowie die ihnen zugeordneten kirchlichen und diakonischen Dienste, Einrichtungen und Werke ohne Rücksicht auf deren Rechtsform (kirchliche Stelle).

3

Die Vorschriften des Kirchengesetzes gehen denen des Verwaltungsverfahrens- und -zustellungsgesetzes der Evangelischen Kirche in Deutschland vor, soweit bei der Ermittlung des Sachverhaltes personenbezogene Daten verarbeitet werden.

KONTROLLE DURCH DIE UNABHÄNGIGE AUFSICHTSBEHÖRDE

Die Aufsichtsbehörde hat insbesondere die einheitliche Anwendung und Durchsetzung des kirchlichen Datenschutzrechts in ihrem Zuständigkeitsbereich zu überwachen und sicherzustellen. Sie sensibilisiert, informiert und berät die kirchliche Öffentlichkeit sowie die verantwortlichen Stellen und kirchlichen Auftragsverarbeiter über Fragen und maßgebliche Entwicklungen des Datenschutzes sowie über die Vermeidung von Risiken. Sie unterrichtet betroffene Personen auf Anfrage über deren persönliche Rechte aus diesem Kirchengesetz, wobei spezifische Maßnahmen für Minderjährige besondere Beachtung finden.
Sie tauscht mit den staatlichen Aufsichtsbehörden für den Datenschutz Erfahrungen und zweckdienliche Informationen aus und gibt im Bedarfsfall Stellungnahmen ab.
Seit 1. Januar 2025 wird die Datenschutzaufsicht innerhalb der EKD nur noch von einer Behörde vorgenommen:
Evangelische Datenschutzaufsicht aus einer Hand – Der Beauftragte für den Datenschutz der EKD-



KONSEQUENZEN FÜR DIE VERANTWORTLICHEN STELLEN DER EVANGELISCHE KIRCHE IN DEUTSCHLAND UND IHRER GLIEDKIRCHEN

Geldbußen

Verstößt eine verantwortliche Stelle oder ein kirchlicher Auftragsverarbeiter vorsätzlich oder fahrlässig gegen Bestimmungen dieses Kirchengesetzes, so können die Aufsichtsbehörden Geldbußen verhängen oder für den Wiederholungsfall androhen.

Schadensersatz durch verantwortliche Stelle

Jede Person, der wegen einer Verletzung der Regelungen über den kirchlichen Datenschutz ein Schaden entstanden ist, hat nach diesem Kirchengesetz Anspruch auf Schadensersatz gegen die verantwortliche Stelle. Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

§ 45 (3) DSG-EKD

Bei Verstößen werden im Einklang mit §45 (3) DSG-EKD Geldbußen von bis zu 6 Mio € verhängt. Aber keine Geldbußen gegen die Landeskirche, Kirchengemeinden, Kirchenstiftungen und Kirchengemeindeverbände, soweit sie nicht als Unternehmen am Markt teilnehmen.

EINE GROSSE GEFAHR

für die EKD und ihre Gliedkirchen sind Reputations- und Imageschäden.

KONSEQUENZEN FÜR DEN MITARBEITER

Straftaten

sind vorsätzliche Handlungen des Mitarbeiters gegen rechtswidrige Datenverarbeitungen, die gegen Entgelt oder in Bereicherungsabsicht begangen werden. Hierzu zählen insbes.:

1 Verschaffung unbefugten Zugang: (§202c StGB)
2 Passwort-Überlassung: (§ 202 c StGB)
3 Berufsgeheimnisträger (§ 203 (1) StGB)
4 rechtswidrige Datenlöschung (§ 303 a StGB)

Schadensersatzpflichten

entstehen unter Umständen auch für den verantwortlichen Mitarbeiter gegenüber seinem Arbeitgeber, wenn er sich nicht an seine Pflichten zur Beachtung des Datenschutzes gehalten hat.

Arbeitsrechtliche Konsequenzen

Verstöße gegen den Datenschutz können für die Mitarbeiter auch arbeitsrechtliche Konsequenzen von der Abmahnung bis zur Kündigung haben.

§ 47 DSG-EKD

Die Zuständigkeit der Klagen gegen die Aufsichtsbehörde nach §39 (2) DSG-EKD richtet sich nach § 5 Kirchengerichtsgesetzes der EKD in der jeweils geltenden Fassung. Vor der Erhebung einer solchen Klage ist kein Vorverfahren durchzuführen.

DIE VERANTWORTUNG DER VERANTWORTLICHEN STELLE

Die jeweilige kirchliche Stelle hat die Verantwortung für den Datenschutz. Das DSG-EKD spricht deshalb von verantwortlichen Stellen. Dienstleister, die lediglich Datenverarbeitung im Auftrag betreiben (z.B. Service-Rechenzentren, Entsorger), werden der verantwortlichen Stelle zugeordnet.

§ 5 DSG-EKD
(Grundsätze der Verarbeitung personenbezogener Daten)

Wann muss die verantwortliche Stelle das DSG-EKD beachten?

Das Kirchengesetz greift überall dort, wo personenbezogene Daten verarbeitet werden, sei es mittels IT oder in strukturierten Datensammlungen, wie z.B. Karteikarten oder Akten. Dabei ist es egal, die Daten der verantwortlichen Stelle genutzt wie die von Gemeindegliedern, Mitarbeitern... Die Zulässigkeit der Verarbeitung von Mitarbeiterdaten ist nicht auf Dateien beschränkt. Jede Information über einen Mitarbeiter muss datenschutzkonform erhoben und erfasst werden.

- Rechtmäßigkeit, Verhältnismäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicher(dauer)-begrenzung
- Integrität und Vertraulichkeit

Datenschutzmanagement

Das DSG-EKD fordert von in Abhängigkeit vom Risiko für die betroffenen Personen ein Datenschutzmanagement. Technische und organisatorische Maßnahmen müssen umgesetzt, regelmäßig überprüft und gegebenenfalls aktualisiert werden. Die Beachtung der Grundsätze der Datenverarbeitung und das Datenschutzmanagement müssen von der verantwortlichen Stelle nachgewiesen werden.

Wer trägt die Verantwortung für die Verarbeitung personenbezogenen Daten?

Die Leitung der verantwortlichen Stelle trägt die Verantwortung für die Umsetzung des Datenschutzes. Für die Umsetzung sind die Leiter und Mitarbeiter der Fachbereiche in Abstimmung mit dem jeweiligen örtlichen Beauftragten für den Datenschutz als sogenannte Datenschutzkoordinatoren verantwortlich. Für Mitarbeiter von Dienstleistern im Rahmen der Auftragsverarbeitung ist diese Verpflichtung nach dem DSG-EKD obligatorisch.

WANN IST DATENVERARBEITUNG ZULÄSSIG?

Jede Verarbeitung von personenbezogenen Daten bedarf einer gesetzlichen Rechtfertigung. Bei der Erhebung der Daten ist außerdem der Zweck, für den die Daten verarbeitet werden sollen, konkret festzulegen.

und

Erlaubnis durch das DSG-EKD

1. Eine kirchliche oder staatliche Rechtsvorschrift erlaubt die Verarbeitung der personenbezogenen Daten oder ordnet sie an;
2. Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
3. Die Verarbeitung ist zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich, einschließlich der Ausübung kirchlicher Aufsicht;
4. Die Verarbeitung ist zur Wahrung der berechtigten Interessen der verantwortlichen Stelle oder eines Dritten erforderlich, sofern nicht die Interessen der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn diese minderjährig ist;
5. Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgt;
6. Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der die kirchliche Stelle unterliegt;
7. Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
8. Weitere Rechtsgrundlagen für die Zulässigkeit einer Verarbeitung personenbezogener Daten sind: § 49, § 50a, § 50b DSG-EKD.

Erlaubnis durch andere kirchliche oder staatliche Rechtsvorschriften: z.B.:

1 Kirchenmitgliedschaftsgesetz EKD

2 Kirchensteuergesetz

3 Bundes-Meldegesetz

4 Sozialgesetzbuch

Es gelten ggf. damit auch weitere (andere) Datenschutzvorschriften.

FORMEN DES UMGANGS MIT PERSONENBEZOGENEN DATEN

Das DSG-EKD gilt für die automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten in einem Dateisystem (z.B. Karteikarten).

MERKSATZ

Jede Datenverarbeitung muss durch das DSG-EKD, eine andere Rechtsvorschrift oder durch Einwilligung der betroffenen Person gestattet sein.

Der Begriff der Verarbeitung im Sinne des DSG-EKD erfasst jeden Vorgang des Umgangs mit personenbezogenen Daten. Die Verarbeitung beginnt bei der Datenbeschaffung beim Betroffenen (z.B. durch schriftliche oder mündliche Befragung) oder bei Dritten (Übermittlung von Personendaten durch (staatliche) Meldebehörden) und reicht über deren Verwendung (z.B. durch Auswertung oder Weitergabe) bis hin zu deren Unkenntlichmachung.

DATA-LIFE-CYCLE

Geburt
Erstellung

z.B.
- Erheben
- Erfassen
- Auslesen
- Abfragen

Leben
Verwendung

Nutzen, z.B.
- Speicherung
- Organisation
- Ordnen
- Anpassung
- Veränderung
- Verwendung
- Abgleich
- Verknüpfung

Weitergeben/ Offenlegung, z.B. durch
- Übermittlung
- Verbreitung
- andere Form der Bereitstellung

Archivieren, z.B.
- Einschränkung

Tod
Vernichtung

z.B.
- Löschen
- Vernichtung

BEISPIELE: ZULÄSSIG ODER NICHT?

Die verantwortliche Stelle speichert Vertragsdaten zur Abwicklung eines Kaufvertrages und zur Prüfung möglicher Gewährleistungsansprüche.	› Zulässig,	weil die Datenverarbeitung auf Grund einer bestehenden Vertrags-beziehung erfolgt.
Die verantwortliche Stelle verschickt Mailings per Post an ihre Community-Mitglieder, um für das nächste Ferienlager der Jugend zu werben.	› Zulässig,	weil Mitgliederdaten auch für Zwecke der Werbung verwendet werden dürfen.
Nutzung von Mitglieder-Daten für eigene Werbezwecke, obwohl der Betroffene erklärt hat, keine Werbung mehr erhalten zu wollen.	› Unzulässig,	weil bei einem Werbewiderspruch die Daten für diesen Zweck nicht genutzt werden dürfen.
Die verantwortliche Stelle übermittelt die Lohn- und Einkommensdaten seiner Mitarbeiter an das Finanzamt und an die Sozialversicherungsträger.	› Zulässig,	weil das Steuer- und Sozialversicherungsrecht die verantwortliche Stelle hierzu verpflichtet.
Ein Diakonieverein gibt die Adressdaten seiner Patienten an einen Arzneimittelhersteller weiter, damit dieser gezielt seine Medikamente bewerben kann.	› Unzulässig,	weil das Arztgeheimnis im Strafgesetzbuch die Weitergabe verbietet.
Die verantwortliche Stelle regelt in einer Betriebsvereinbarung die Erfassung der Arbeitszeit und die Nutzung der anfallenden Daten zur Abrechnung von Gehalt, Urlaub und Überstunden.	› Zulässig,	weil nach dem DSG-EKD die Beschäftigten-Datenverarbeitung durch eine Betriebsvereinbarung geregelt werden kann.
Die verantwortliche Stelle veröffentlicht das Foto eines Mitarbeiters auf der Homepage.	› Nur Zulässig,	wenn der Mitarbeiter zuvor in die Veröffentlichung eingewilligt hat.

VERANTWORTUNG FÜR DEN DATENSCHUTZ

Leitung

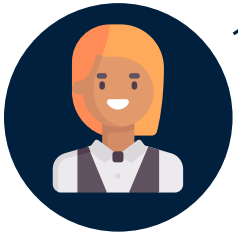
trägt die Verantwortung für den Datenschutz nach innen und nach außen

Beratung

Erlässt Regeln und delegiert einen Teil der Verantwortung an die Fach-/Führungskräfte

Einschaltung vor Einführung oder Änderung datenschutzrelevanter Geschäftsprozesse

Ber



Führungskraft

setzt gesetzliche und interne betriebliche Regelungen zum Datenschutz um und kontrolliert deren Einhaltung

Information bei Kenntnis vor
brauch, Verlust oder Manipul

Erteilung von Arbeitsanweisu
und Befugnissen, Unterstütz
der Durchführung und Sensil
für die Bedeutung des Daten

Örtlich Beauftragter für den Datenschutz

ratung

Beratung

n Miss-
dation

ungen
cung bei
bilisierung
schutzes

Mitarbeiter

schützt personenbezogene Daten vor unbefugtem Zugriff und unzulässiger Weiterfabe

Selbstkontrolle durch den örtlich Beauftragten für den Datenschutz

Der örtlich Beauftragte für den Datenschutz wirkt auf die Einhaltung der Bestimmungen für den Datenschutz hin und unterstützt die verantwortliche Stelle bei der Sicherstellung des Datenschutzes.

Er berät die verantwortliche Stelle und deren Mitarbeiter, überwacht die ordnungsmäßige Anwendung der Datenverarbeitungsprogramme, informiert und schult die bei der Verarbeitung der personenbezogenen Daten tätigen Personen, arbeitet mit der Aufsichtsbehörde zusammen und berät die verantwortliche Stelle bei der Durchführung der Datenschutz-Folgenabschätzung und überwacht deren Durchführung.

BEI FRAGEN

zum Thema Datenschutz bzw. Datensicherheit oder in Zweifelsfällen wenden Sie sich bitte an Ihren örtlich Beauftragten für den Datenschutz.

SICHERHEITSZIELE ZUR DATENSICHERHEIT

§ **§ 27 DSG-EKD**

Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung von Datenschutzverstößen hat die verantwortliche Stelle die mit der Verarbeitung verbundenen Risiken zu ermitteln und Maßnahmen zu ihrer Eindämmung zu treffen. Folgende Ziele im Sinne von § 27 (5) DSG-EKD sowie der IT-SVO sind zu erreichen:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

1. Vertraulichkeit

- **Zutrittskontrolle**
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B. Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen
- **Zugangskontrolle**
  Keine unbefugte Systembenutzung, z.B. (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern
- **Zugriffskontrolle**
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B. Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen
- **Trennungskontrolle**
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit
- **Pseudonymisierung**
  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

2. Integrität

- **Weitergabekontrolle**
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur

- **Eingabekontrolle**
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement

3. Verfüabarkeit und Belastbarkeit

- **Verfügbarkeitskontrolle**
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; onsite/offsite), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne

- **Rasche Wiederherstellbarkeit**

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- **Datenschutz-Management**
- **Incident-Response-Management**
- **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)**
- **Auftragskontrolle**
  Keine Auftragsdatenverarbeitung ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen

§ 28 DSG-EKD

fordert Datenschutz durch Technikgestaltung (privacy by design) und datenschutzfreundliche Voreinstellung (privacy by default).

DIE RECHTE DER BETROFFENEN PERSON

Diejenige natürliche Person, deren Daten verarbeitet werden und deren Persönlichkeitsrechte Schutzobjekt des Gesetzes sind, bezeichnet das DSG-EKD oder die DS-GVO als „betroffene Person“. Betroffene Personen können beispielsweise der Mitarbeiter, der Kunde oder der Ansprechpartner eines Firmenkunden sein. Den betroffenen Personen räumt das DSG-EKD Transparenz- und Interventionsrechte ein.

ACHTUNG

Die betroffene Person
Die betroffene Person kann sich mit Beschwerden oder Anfragen an den örtlich Beauftragten für den Datenschutz wenden. Dieser unterliegt hinsichtlich der betroffenen Person einer Verschwiegenheitsverpflichtung, sofern diese ihn nicht davon befreit hat.

Berichtigung

Es dürfen nur zutreffende Daten verarbeitet werden. Sonst sind diese zu berichtigen.

Datenüb

Die betroffe
personenbe
Stelle bereit
und maschi
das Recht, d
Stelle ohne

Löschung

Nach Zweckverbrauch oder dem Ablauf von Aufbewahrungsvorschriften sind Daten zu löschen.

Recht auf Vergessenwerden

Wenn die verantwortliche Stelle löschpflichtige Daten veröffentlicht hat, hat sie auf Verlangen der betroffenen Person zu recherchieren, wer auf diese Daten verlinkt oder diese adaptiert hat. Diese Dritten sind über das Löschverlangen zu informieren.

INTERVENTIONSRECHTE

Die betroffene Person soll wissen, für welche Zwecke ihre Daten verarbeitet werden und welche Datenschutzrechte sie hat. Dies löst Transparenzpflichten bei den kirchlichen Stellen aus.

ertragbarkeit

ne Person hat das Recht, die sie betreffenden zogenen Daten, die sie der verantortlichen gestellt hat, in einem strukturierten, gängigen nenlesbaren Format zu erhalten, und sie hat iese Daten einer anderen verantwortlichen Behinderung zu übermitteln.

Widerspruch

Die betroffene Person kann aus Gründen, die sich aus ihrer besonderen Situation ergeben, Widerspruch gegen die Datenverarbeitung erheben, ebenso hat sie das Recht zur Beschwerde bei der Aufsichtsbehörde.

Einschränkung der Verarbeitung (Sperrung)

Wenn die Richtigkeit der Daten von betroffenen Personen bestritten wird oder die betroffene Person bei Löschpflicht die Daten zur Rechtverfolgung benötigt, sind diese in der Verarbeitung einzuschränken. Dasselbe gilt für gesetzliche Aufbewahrungspflichten der verantwortlichen Stelle.

TRANSPARENZPFLICHTEN DER VERANTWORTLICHEN STELLE

Benachrichtigung bei mittelbarer Datenerhebung

Wenn personenbezogene Daten nicht bei der betroffenen Person erhoben werden, ist die betroffene Person von der verantwortlichen Stelle zusätzlich zu den allgemeinen Informationspflichten auch über die Herkunft der Daten zu informieren.

Informationspflichten

Möglichst bei der Datenerhebung, spätestens aber auf Verlangen muss die verantwortliche Stelle die betroffene Person über ihre Identität, die Zweckbestimmungen der Datenverarbeitung sowie mögliche Kategorien von Empfängern und die Speicherdauer informieren. Zugleich ist sie eine Kontaktmöglichkeit zum örtlichen Beauftragten für den Datenschutz sowie über alle ihre Rechte zu informieren.

Auskunft

Der betroffene Person ist auf Antrag unentgeltlich Auskunft über die zu ihrer Person gespeicherten personenbezogenen Daten zu erteilen. Hierunter fallen Verarbeitungszwecke, Kategorien personenbezogener Daten, Empfänger/Kategorien von Empfängern, denen die Daten offengelegt worden sind, geplante Dauer der Speicherung, Informationen über Betroffenenrechte sowie bei mittelbarer Datenerhebung Auskunft über die Herkunft der Daten.

Meldung

Meldung von Datenpannen an die Aufsichtsbehörde und ggf. an Betroffene.

FIT FÜR DEN DATENSCHUTZ? TESTEN SIE IHR WISSEN!

(Mehrfachnennungen möglich)

1. **Das DSG-EKD schützt ...**
   a) Unternehmen ☐
   b) natürliche Personen ☐

2. **Die Datenschutzaufsichtsbehörde kann ...**
   a) Mitarbeiter kündigen ☐
   b) Bußgelder verhängen ☐

3. **Die Verantwortung für den Datenschutz in der verantwortlichen Stelle hat ...**
   a) die jeweilige Leitung ☐
   b) die Führungskraft ☐
   c) der Mitarbeiter ☐

4. **Die Nutzung von eigenen Mitgliederdaten zu Werbezwecken für eigene Veranstaltungen ist grundsätzlich ...**
   a) zulässig ☐
   b) unzulässig ☐

5. **Daten, die nicht mehr benötigt werden, sind ...**
   a) zu löschen ☐
   b) einzuschränken ☐

6. **Die Zugangskontrolle kann unter anderem erreicht werden durch ...**
   a) Abschließen von Räumen ☐
   b) Passwortschutz ☐

7. **Die Datenschutzkontrolle wird ausgeübt durch ...**
   a) die Mitarbeitervertretung ☐
   b) die unabhängige Aufsichtsbehörde ☐
   c) den örtlich Beauftragten für den Datenschutz ☐

8. **Falls ein Mitglied keine Werbung wünscht, kann es verlangen, die Daten dafür...**
   a) zu löschen ☐
   b) einzuschränken ☐

9. **Die Verpflichtung zur Wahrung des Datengeheimnisses verlangt ...**
   a) das Unterlassen unbefugter Datenverarbeitung ☐
   b) die Wahrung der Vertraulichkeit auch nach Beendigung des Arbeitsverhältnisses ☐

Auflösung: 1b, 2b, 3a/b/c, 4a, 5a, 6b, 7a/b/c, 8b, 9a/b

PRAXISTIPPS ZUM DATENSCHUTZ

Jeder haupt- und ehrenamtliche Mitarbeiter ist für den Datenschutz in seiner kirchlichen Stelle mitverantwortlich. Nicht zuletzt im eigenen Interesse gehört es zu seinen Aufgaben, sich an die Datenschutzregeln seiner verantwortlichen Stelle zu halten und seine Aufgaben mit Bezug zum Datenschutz wahrzunehmen.

Einfache Datenschutztipps sind jedoch allgemeingültig

Clean Desk
Ein aufgeräumter Schreibtisch, das Clean-Desk-Prinzip, sorgt für Datensicherheit und Vertraulichkeit. Personenbezogene Daten und Vertraulichkeit sind gewahrt und gelangen nicht in die Hände Unbefugter. Bei Abwesenheit sollten Unterlagen, USB-Sticks, Datenträger etc. eingeschlossen sein.

Auskünfte am Telefon
Personenbezogene Auskünfte, sowohl intern als auch extern, sind mit Blick auf den Datenschutz kritisch zu prüfen. Insbesondere bei Auskunftsverlangen am Telefon ist mit Blick auf die Person des Anrufenden und den Inhalten Vorsicht geboten und in der Regel auf den Schriftweg zu verweisen.

Abmeldung am System
Bei Abwesenheit vom Arbeitsplatz sollte man sich vom System abmelden und den Bildschirmschoner mit Passwortschutz aktivieren.

Sichtschutz am Bildschirm
Der Bildschirm ist so zu positionieren, dass er vor dem unbefugten Einblick durch Kollegen, Besuchern oder generell Dritten geschützt ist. Auf Reisen hilft ein sogenannter Blickschutzfilter.

Sichere Übermittlung von E-Mails
Wenn vertrauliche E-Mails sicher übermittelt werden sollen, müssen sie verschlüsselt sein. Erkundigen Sie sich bei Ihrem IT-Sicherheits- oder örtlich Beauftragten für den Datenschutz nach geeigneten Verschlüsselungsverfahren.

Öffnen von E-Mails
Die meisten Computerviren werden über E-Mail-Anhänge verbreitet. Diese enthalten Malware, wie Viren, Trojanern, Würmer oder selbst Ransomware. Falls der Virenschutz versagt, sollten Sie sich bei verdächtigen E-Mails immer durch Rücksprache vergewissern, dass der Anhang tatsächlich von der Person oder Institution verschickt wurde, die als Absender angegeben ist.

MERKE:
Datenschutz schützt Ihre Kollegen und Sie selbst!

Bibliographische Informationen der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet unter *http://dnb.ddb.de* abrufbar.
Mitarbeiterinformation Datenschutz – Merkblatt für Mitarbeitende nach DSG-EKD

Autoren: Dipl.-Kfm. Günther Otten, Köln; Diakon Peter Buck, München

978-3-98746-033-3
GDD – Gesellschaft für Datenschutz und Datensicherheit e.V.
2. aktualisierte Auflage 2025 (Stand 01.05.2025)

Herausgeber: Gesellschaft für Datenschutz und Datensicherheit e.V., Bonn
Illustration: Evelyn Klaiber, Köln
Satz: Matthias Lück, CreaTechs, Boppard
Bildnachweis (Cover): fizkes, Adobe Stock
Hersteller: DATAKONTEXT GmbH, Augustinusstr. 11A, 50226 Frechen

Kontakt und Informationen zum Thema Produktsicherheitsverordnung:
Per Telefon: 02234 9894999
Per Mail: dieter.schulz@datakontext.com
https://www.datakontext.com/produktsicherheitsverordnung

Printed in Germany

Für dieses Merkblatt werden Staffelpreise angeboten.
Informationen unter: 02234/98949-26

GDD
Gesellschaft für Datenschutz
und Datensicherheit e.V.

DATAKONTEXT

ISBN 978-3-98746-033-3