



Datenschutz-Information für Mitarbeitende

Merkblatt zum Datenschutz nach DSGVO-EKD



WAS IST ...
DATENSCHUTZ?!



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 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



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.

Mit dem DS-EKD wird seit dem 24.05.2018 dieses Recht umgesetzt.

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 DSGVO

„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.“

§ 4 NR. 1 DSGVO

„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)

Was sind personenbezogene Daten?

Personenbezogene Daten sind Angaben über eine bestimmte oder eine bestimm- bare natürliche Person.



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 Befugnis für die Verarbeitung von personenbezogenen Datenverarbeitung einer rechtlichen Grundlage. Dies ist im Kirchenrecht im Rahmen des DSGVO geregelt und wird durch bereichsspezifische Normen ergänzt. (siehe Seite 9)

Wer schützt das DSGVO?

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 DSGVO BEACHTEN?

Evangelische Kirche in Deutschland, die Gliedkirchen und die kirchliche Zusammenschlüsse

Alle weiteren kirchlichen juristischen Personen des öffentlichen Rechts z.B. Kirchengemeinden, sowie für Ihnen zugeordneten kirchlichen und diakonischen Dienste, Einrichtungen und Werke ohne Rücksicht auf deren Rechtsform (Kirchliche Stifte).

Die Vorschriften des Kirchengesetzes, neben denen des Verfassungsaufgaben- und Zustellungsgesetzes der Evangelischen Kirche in Deutschland vor, soweit bei der Anwendung des nachwebsites personenbezogene Daten verarbeitet werden.

KONTROLLE DURCH DIE UNABHÄNGIGE AUFSICHTSBEHÖRDE

Die Aufsichtsbehörde hat insbesondere die unmittelbare Anwendung und Durchsetzung des kirchlichen Datenschutzes in ihrem Zuständigkeitsbereich zu überwachen und sicherzustellen. Sie sensibilisiert, informiert und berät die kirchliche Öffentlichkeit sowie die Verantwortlichen 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 dem Kirchenrecht und bei spezifische Maßnahmen für Minderjährige besondere Beachtung finden.

Die kirchlichen Aufsichtsbehörden für den Datenschutz arbeiten zusammen und bilden sie Datenschutzkonferenzen ab, die gemeinsame Stellungnahmen und Handreichungen zu Datenschutz- und Kohärenzfragen beschlossen werden können. Sie tauschen mit der staatlichen Datenschutzbehörden über Datenschutz-Erkenntnisse und zweifelhafte Informationen aus und geben im Bedarfsfall Unterstützung ab.



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

<p>Geldbußen</p> <p>Verstößt eine verantwortliche Stelle über ein kirchlicher Auftragsverarbeiter vorwiegend oder fast ausschließlich gegen Bestimmungen dieses Kirchengesetzes, so können die Aufsichtsbehörden Geldbußen verhängen, die für den Wiederholungsfall androhen.</p>	<p>Schadensersatz durch verantwortliche Stelle</p> <p>Jede Person, die vorsätzlich oder fahrlässig die Bestimmungen des kirchlichen Datenschutzes verletzt, ist nach dem Kirchengesetz Anspruch auf Schadensersatz gegenüber der verantwortlichen Stelle. Wenn ein Schaden, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.</p>	<p>§ 45 (3) DSGVO-EKD</p> <p>sieht Bußgelder im Einklang mit § 45 (3) DSGVO von bis zu 500.000 € vor. Aber keine Geldbußen gegen die Landeskirche, Kirchengemeinden, Kirchenstiftungen und Kirchengemeindev Verbände, soweit sie nicht als Unternehmen am Markt tätig sind.</p>
<p>Straftaten</p> <p>Sind vorsätzliche Handlungen des Mitarbeiters durch rechtswidrige Datenverarbeitungen, die gegen Erlöse oder zu Bereicherungsabsicht begangen werden. Hierzu zählen insbes:</p> <ol style="list-style-type: none"> 1 Verschaffung unberechtigter Zugang: (§202c StGB) 2 Passwortüberlassung: (§ 202 StGB) 3 Berufsgeheimnisträger (§ 203 (1) StGB) 4 rechtswidrige Datenlöschung (§ 303 a StGB) 	<p>Schadensersatzpflichten</p> <p>entsteht für Umstände, auch für den verantwortlichen Mitarbeiter gegenüber seinem Arbeitgeber, wenn er sich nicht an seine Pflichten zur Beachtung des Datenschutzes gehalten hat.</p>	<p>EINIGUNGSSCHLÜSSEL FÜR DIE EKD UND DIE GLEICHKIRCHEN SIND REPUTATIONSBÜHMESSTÄBE</p> <p>§ 47 DSGVO-EKD</p> <p>Der Rechtsweg zur ordentlichen Verwaltungsgewalt gerichten ist eröffnet.</p>
<p>Arbeitsrechtliche Konsequenzen</p> <p>Verstöße gegen den Datenschutz können für die Mitarbeiter auch arbeitsrechtliche Konsequenzen von der Abmahnung bis zur Kündigung haben.</p>		

DIE VERANTWORTUNG DER VERANTWORTLICHEN STELLE

DATAKONTEXT DATAKONTEXT D

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

ATAKONTEXT DATAKONTEXT DA

TAKONTEXT DATAKONTEXT DAT

§ 5 DSG-EKD

Wann muss die verantwortliche Stelle das DSG-EKD beachten?

(Grundsätze der Verarbeitung personenbezogener Daten)

Rechtmäßigkeit, Verhältnismäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

■ Zweckbindung

Bestimmtheit

■ Rechtfertigung

■ Speicher(dauer-)begrenzung

■ Integrität und Vertraulichkeit

Das Kirchengesetz greift überall dort, wo personenbezogene Daten verarbeitet werden, sei es mittels IT oder in strukturierten Datenansammlungen, wie z.B. Karteikarten oder Adressen. Das betrifft die kirchliche verantwortliche Stelle genauso wie die von Gemeindegliedern, Mitarbeitern... Die Zulässigkeit der Verarbeitung von Mitarbeiterdaten ist nicht an Dienstverhältnis gebunden. Jede Information über Zirkel, Mitarbeiterkreis, Pastoralstellen, Familienring und Erfasst werden.

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 sind von der verantwortlichen Stelle nachgewiesen zu werden.

XT DATAKONTEXT DATAKONTEXT

Wer trägt die Verantwortung für die Verarbeitung der personenbezogenen Daten?

T DATAKONTEXT DATAKONTEXT

Die Leitung der verantwortlichen Stelle trägt die Verantwortung für die Umgestaltung des Datenschutzes. Für die Umsetzung sind die Leiter und Mitarbeiter der Fachbereiche in Abstimmung mit dem jeweiligen örtlichen Beauftragten für den Datenschutz als sogenannte Datenschutzorganisation verantwortlich.

DATAKONTEXT DATAKONTEXT D

Für Mitarbeiter von Dienstleistern im Rahmen der Auftragsverarbeitung ist diese Verpflichtung nach dem DSG-EKD obligatorisch.

ATAKONTEXT DATAKONTEXT DA

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 DSGVO-EKD

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- 1 eine Rechtsvorschrift erlaubt die Verarbeitung der personenbezogenen Daten (pBD) oder ordnet sie an,
- 2 die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden pBD 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 für die Wahrnehmung einer sonstigen Aufgabe erforderlich, die im kirchlichen Interesse liegt,
- 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 die Verarbeitung ist zur Wahrung der berechtigten Interessen eines Dritten erforderlich, sofern nicht die schutzwürdigen Interessen der betroffenen Person überwiegen, insbesondere dann, wenn diese minderjährig ist.

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 DSGVO-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 DSGVO-EKD, eine andere Rechtsvorschrift oder durch Einwilligung der betroffenen Person gestattet sein.

Der Begriff der Verarbeitung im Sinne des DSGVO-EKD umfasst 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



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 Vertragsbeziehung erfolgt.

Die verantwortliche Stelle verspricht Mailings per Post an ihre Gemeindeglieder, 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 Diakollege teilt die Adressdaten seiner Patienten an einen Arzneimittelhersteller weiter, damit dieser gezielt seine Medikamente bewerben kann.

➤ **Unzulässig**,

weil das Arzneimittelgesetz im Strafrecht die Weitergabe verbietet.

Die verantwortliche Stelle regelt in einer Betriebsvereinbarung die Einsatz- und Freizeit und die Nutzung der anfallenden Daten zur Abrechnung von Gehalt, Urlaub und Überstunden.

➤ **Zulässig**,

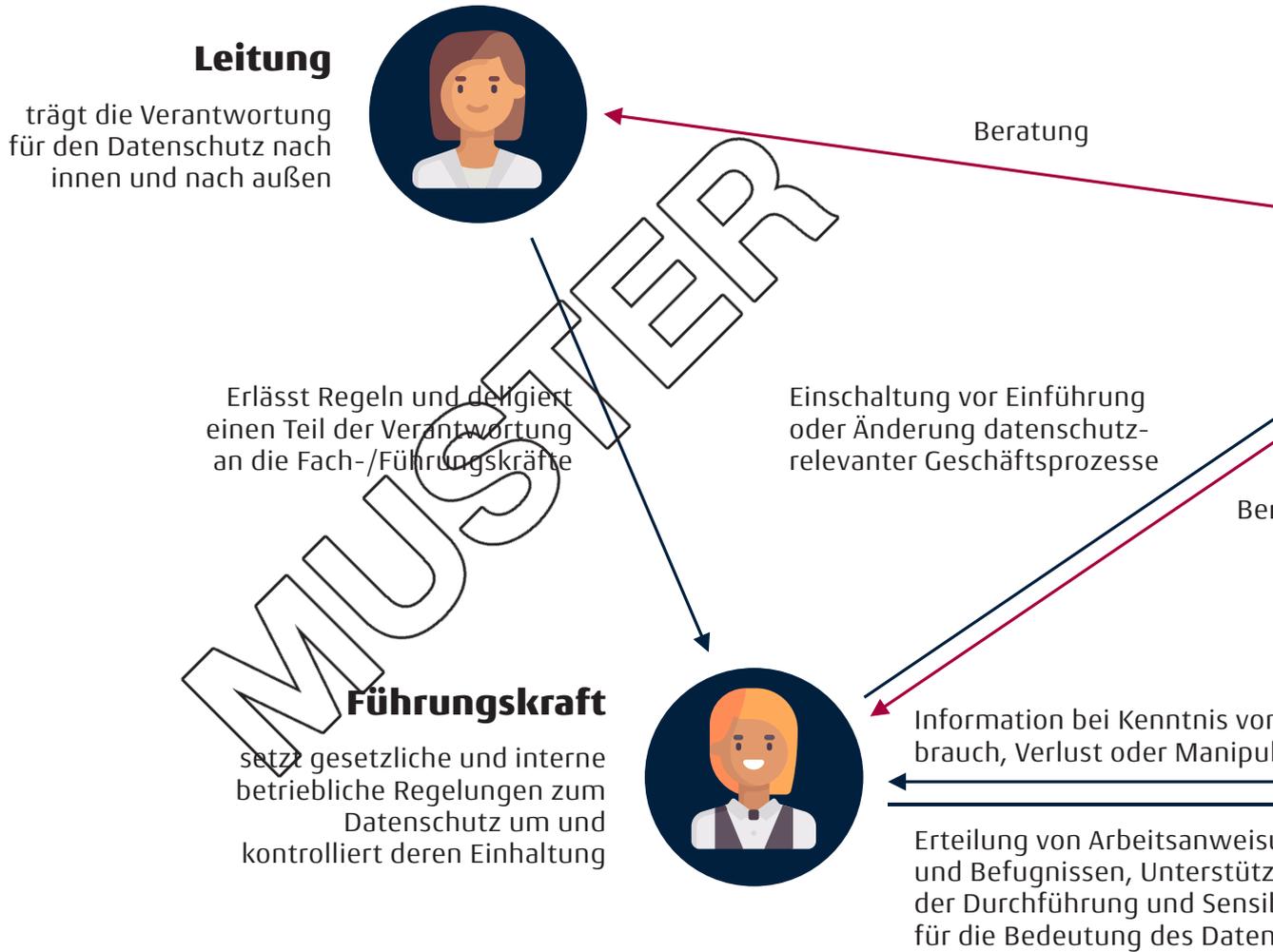
weil nach dem DSG-EKD die Beschäftigten-Datenverarbeitung durch eine Betriebsvereinbarung geregelt werden kann.

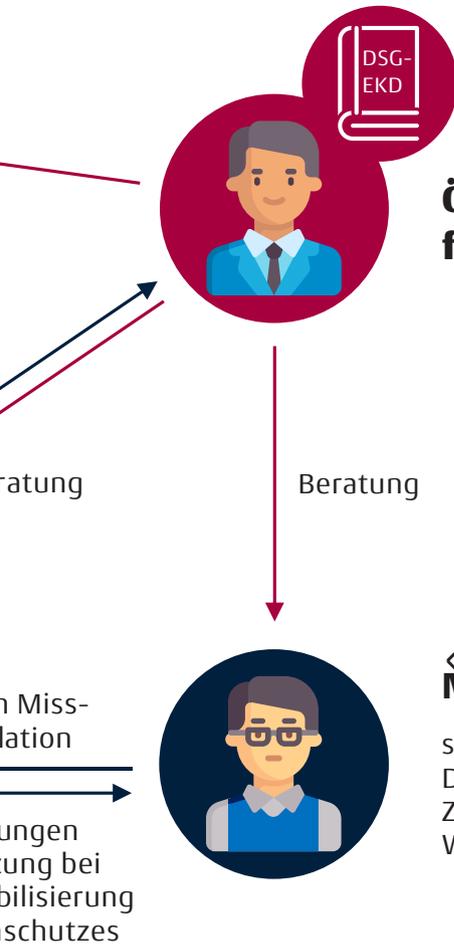
Die verantwortliche Stelle veröffentlicht das Foto eines Mitarbeiters auf der Homepage.

➤ **Nur Zulässig**,

wenn der Mitarbeiter zuvor in die Veröffentlichung eingewilligt hat.

VERANTWORTUNG FÜR DEN DATENSCHUTZ





Örtlich Beauftragter für den Datenschutz

Mitarbeiter

schützt personenbezogene Daten vor unbefugtem Zugriff und unzulässiger Weitergabe

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.

2. Integrität

§ 28 DSGVO-EKD

3

• Weitergabekontrolle

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

Verhaltensmaßnahmen durch Technikgestaltung (privacy by design) und datenschutzfreundliche Voreinstellungen (privacy by default).

• Eingabekontrolle

Beispielung: Daten von wenn personentbelegte Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind z.B.: Protokollierung, Dokumentenmanagement

3. Verfübarkeit und Belastbarkeit

• Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backupstrategie (online/offline; onsite/offsite), Stromerreichungszeit, Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne

• Rasche Wiederherstellbarkeit

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

• Datenschutz-Folgenanalyse

• Incident-Response-Management

• Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

• Auftragskontrolle

Keine Auftragsüberantwortung ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen

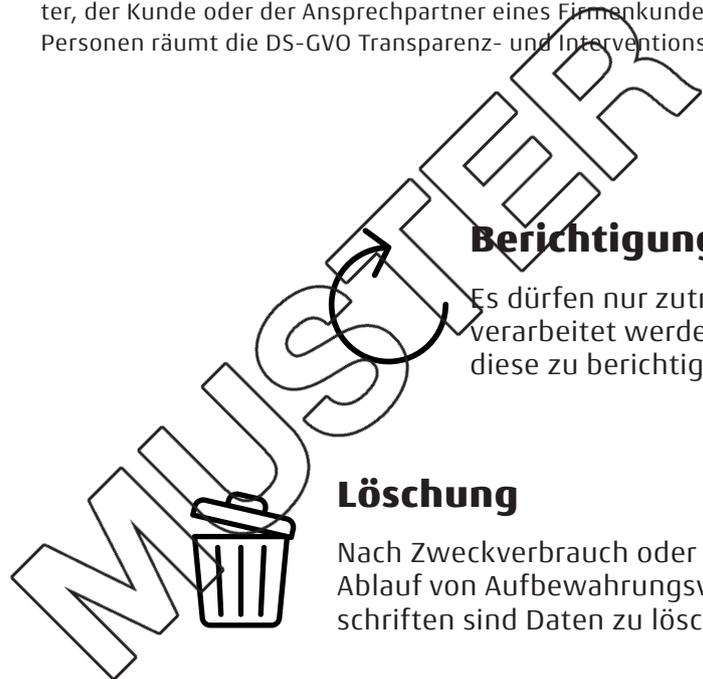
DIE RECHTE DER BETROFFENEN PERSON

Diejenige natürliche Person, deren Daten verarbeitet werden und deren Persönlichkeitsrechte Schutzobjekt des Gesetzes sind, bezeichnet das BDSG 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 die DS-GVO Transparenz- und Interventionsrechte ein.



ACHTUNG

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.

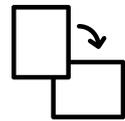
Löschung

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.



Datenübertragung

Die betroffene Person hat das Recht, die Daten an eine andere Stelle zu übertragen, wenn dies technisch machbar ist.



INTERVENTIONSRECHTE

Die betroffene Person soll wissen, für welche Zwecke ihre Daten verarbeitet werden und welche Datenschutzrechte sie hat. Dies löst Transparenzpflichten beim Unternehmen aus.

Vertragbarkeit

Die betroffene Person hat das Recht, die sie betreffenden zugehörigen Daten, die sie der verantwortlichen Stelle gestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einer anderen verantwortlichen Stelle zu übermitteln, ohne 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 Rechtsverfolgung benötigt, sind diese in der Verarbeitung einzuschränken. Dasselbe gilt für gesetzliche Aufbewahrungspflichten der verantwortlichen Stelle.

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 Mitglieder-
daten zu Werbezwecken für eigene
Werbekampagnen ist grundsätzlich

- a) zulässig
- b) unzulässig

5 Daten die nicht mehr benötigt
werden, sind

- a) zu löschen
- b) einzuschränken

6 Die Zugangskontrolle kann Daten
anderem erreicht werden durch

- a) Abschließen von Räumen
- b) Passwortschutz

7 Die Datenschutzaufsicht wird
ausgeübt durch

- a) die Mitarbeitervertretung
- b) die unabhängige Aufsichtsbehörde
- c) der örtlich zuständigen 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 Umklassifizieren von Daten in eine niedrigere Vertraulichkeitsstufe
- b) die Wahrung der Vertraulichkeit auch nach Beendigung des Arbeitsverhältnisses

PRAXISTIPPS ZUM DATENSCHUTZ

Jeder Haupt- und Nebearbeitende Mitarbeiter ist für den Datenschutz seiner Einrichtung 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

Im Aufgeklärter und bürokratisch Clean-Desk-Prinzip, sowohl 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 jede Auskunftserlaubnis per Anruf ist mit Blick auf die Person des Anrufenden und den Inhalten Vorsicht geboten und in der Regel auf den Schriftweg zu verweisen.



Abmeldung im 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, Besucher oder sonstigen Dritten geschützt ist. Auf Reisen hilft ein sogenanntes Blickschutzfilter.



Sichere Übermittlung von E-Mails

Wenn vertrauliche E-Mails sicher übermittelt werden sollen, müssen sie verschlüsselt sein. Erkundigen Sie sich bei Ihrer IT-Sicherheits- oder IT-Abteilung über die für den Datenschutz nach geeigneten Verschlüsselungsverfahren.



Öffnen von E-Mails

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



MEPKE:

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 DSGVO-EKD

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

978-3-89577-964-0

GDD – Gesellschaft für Datenschutz und Datensicherheit e.V.

1. Auflage (unveränderter Nachdruck 2024)

© 2023 DATAKONTEXT GmbH, Frechen

www.datakontext.com

Dieses Werk, einschließlich aller seiner Teile, ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen. Lizenzangaben sind nach Vereinbarung möglich.

Herausgeber: Gesellschaft für Datenschutz und Datensicherheit e.V., Bonn

Illustration: Evelyn Kläber, 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

MUSTER

GDD

Gesellschaft für Datenschutz
und Datensicherheit e.V.



DATAKONTEXT

