



Datenschutzschulung für Mitarbeitende



Evangelische Kirche
in Deutschland

DER BEAUFTRAGTE FÜR DEN
DATENSCHUTZ DER EKD

Themenschwerpunkte

- Einführung in den rechtlichen Datenschutz
- Datenschutz im beruflichen Alltag
- Einführung in den technischen Datenschutz



Einführung in den rechtlichen Datenschutz

Inhaltsübersicht

1

Überblick über das
Datenschutzrecht

2

Verarbeitung
personenbezogener Daten

3

Grundsätze der
Datenverarbeitung

4

Rechte der betroffenen
Personen

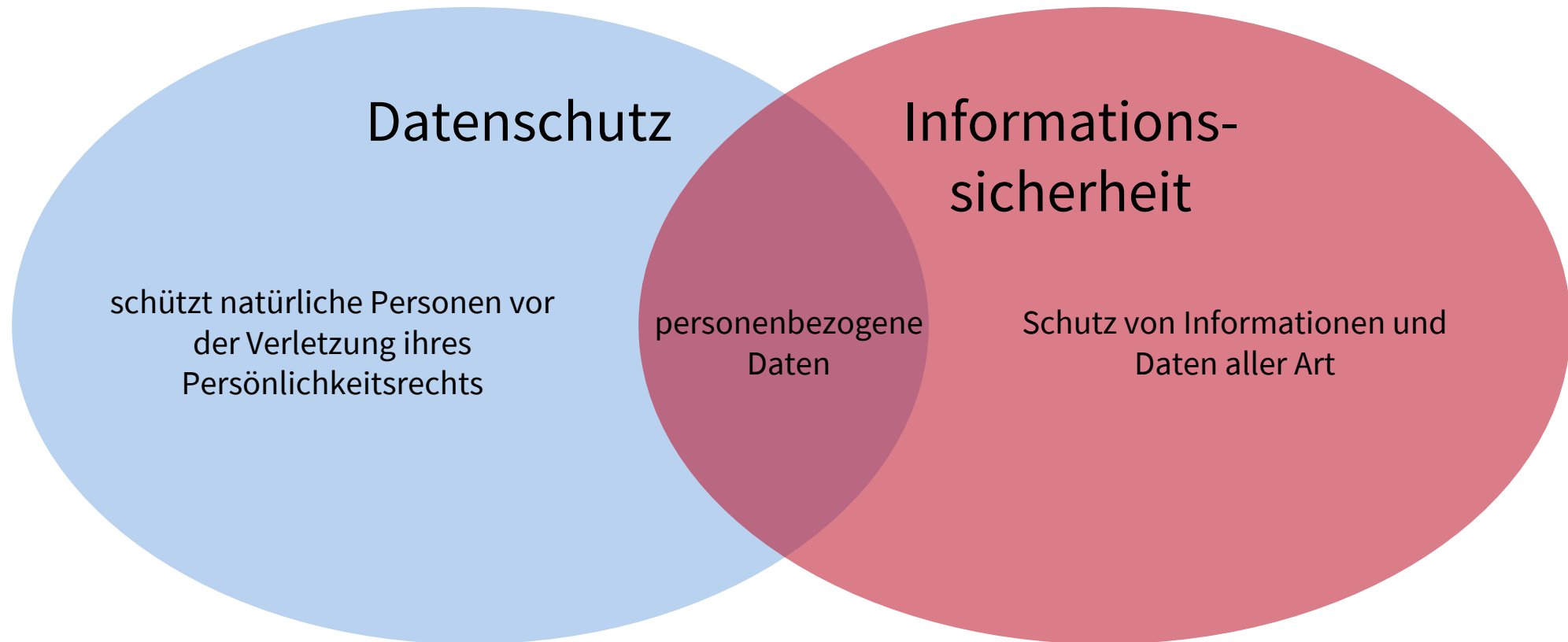
The background consists of numerous overlapping white squares, each containing a large, bold, black German character, either an uppercase 'S' or a lowercase 's'. The squares are scattered across the frame, creating a dense, textured effect. The text 'Überblick über das Datenschutzrecht' is overlaid on the left side of the image.

Überblick über das
Datenschutzrecht

Worum geht's beim Datenschutz?

- Im Mittelpunkt des Datenschutzes steht der einzelne Mensch (und nicht die Daten eines Menschen).
- Das Persönlichkeitsrecht umfasst die unantastbare Würde des Menschen und das Recht auf freie Entfaltung.
- In Datenschutzgesetzen (oder anderen Datenschutzbestimmungen) ist daher geregelt, welcher Umgang mit Daten erlaubt ist. Mit Datenschutz wird erreicht, dass der einzelne Mensch durch den Umgang mit seinen Daten in seinem Persönlichkeitsrecht nicht beeinträchtigt wird.
- Jede/r Einzelne darf selbst über die Preisgabe und Verwendung ihrer/seiner persönlichen Daten bestimmen.

Datenschutz und Informationssicherheit



EKD-Datenschutzgesetz

- Eigenes kirchliches Datenschutzgesetz aufgrund von Art. 91 Abs. 1 Datenschutzgrundverordnung (DSGVO), welches in Einklang mit der DSGVO gebracht wurde.
- EKD-Datenschutzgesetz (DSG-EKD) findet nur Anwendung, wenn keine spezielleren Regelungen bestehen, § 2 Abs. 6 DSG-EKD.
- Neben dem EKD-Datenschutzgesetz finden sich anwendbare datenschutzrechtliche Vorschriften auch in (landes-) kirchlichen (z. B. landeskirchlichen Durchführungsbestimmungen) und staatlichen Regelungen (z. B. Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG)).

Anwendungsbereich EKD-Datenschutzgesetz

„Kirchliche Stellen“, § 2 Abs. 1 DSGVO-EKD





Verarbeitung
personenbezogener
Daten

Personenbezogene Daten

§ 4 Nr.1 DSGVO-EKD

Der Ausdruck „personenbezogene Daten“ bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen.

Name, Anschrift,
Telefonnummer, E-Mail-Adresse,...

Geburtsdatum, Familienstand,...

Staatsangehörigkeit

Beruf, vertragliche oder
sonstige Verbindungen zu Dritten

Besondere Kategorien personenbezogener Daten,

§ 4 Nr. 2 DSGVO-EKD



- a)** 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,
- b)** alle Informationen, aus denen die rassische oder ethnische Herkunft, politische Meinungen oder die Gewerkschaftszugehörigkeit einer natürlichen Person hervorgehen,
- c)** genetische Daten,
- d)** biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
- e)** Gesundheitsdaten,
- f)** Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Verarbeitung, § 4 Nr. 3 DSGVO-EKD

- Das EKD-Datenschutzgesetz findet Anwendung, wenn personenbezogene Daten verarbeitet werden.
- Der Begriff der Verarbeitung ist in § 4 Nr. 3 DSGVO-EKD definiert.
- weiter Verarbeitungsbegriff
 - fast jeder Umgang mit personenbezogenen Daten umfasst
 - Erheben, Erfassen, die Organisation, das Ordnen, die Speicherung, Anpassung, Veränderung, Offenlegung und Übermittlung von personenbezogenen Daten, etc.
 - Aufzählung von Verarbeitungsformen in § 4 Nr. 3 DSGVO-EKD nur beispielhaft
 - Alle Verarbeitungsphasen unterliegen identischen rechtlichen Anforderungen (keine Differenzierung nach Erhebung, Verarbeitung und Nutzung).


Verbot mit Erlaubnisvorbehalt § 6 DSG-EKD

Grundsatz

Die Verarbeitung personenbezogener Daten ist rechtswidrig, es sei denn sie ist von einem gesetzlichen Erlaubnistatbestand gedeckt.

- Verbot mit Erlaubnisvorbehalt ist zwar im Gesetz nicht ausdrücklich benannt, folgt jedoch aus § 6 DSG-EKD.
- Folge: Jeder Umgang mit personenbezogenen Daten bedarf einer Rechtfertigung!

Rechtmäßigkeit der Verarbeitung, § 6 DSG-EKD (1)

Nr.	Rechtfertigungsgrund für die Verarbeitung	Erläuterung
1	Eine Rechtsvorschrift erlaubt die Verarbeitung der personenbezogenen Daten oder ordnet sie an.	<p>Prüfungsschritte:</p>  <pre>graph LR; A["bereichsspezifische Regelung (z.B. Datenschutz-Durchführungs-VO, TTDSG)"] --> B["DSG-EKD"]; B --> C["Dienstvereinbarung"]</pre>
2	Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben.	Dabei müssen die Anforderungen an eine wirksame Einwilligung aus § 11 DSG-EKD beachtet werden.

Rechtmäßigkeit der Verarbeitung, § 6 DSGVO-EKD (2)

Nr.	Rechtfertigungsgrund für die Verarbeitung	Erläuterung
3	Die Verarbeitung ist zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich, einschließlich der Ausübung kirchlicher Aufsicht.	Betrachtung des spezifischen Aufgabenbereichs der jeweiligen Einrichtung notwendig (Kirchengemeinde, Diakoniestation, Schule, Kita usw.).
4	Die Verarbeitung ist für die Wahrnehmung einer sonstigen Aufgabe erforderlich, die im kirchlichen Interesse liegt.	Tatbestand muss aufgrund allgemeiner gesetzlicher Formulierung eng ausgelegt werden.

Rechtmäßigkeit der Verarbeitung, § 6 DSGVO-EKD (3)

Nr.	Rechtfertigungsgrund für die Verarbeitung	Erläuterung
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.	Umfang der zulässigen Datenverarbeitung ist anhand des konkreten Vertragszwecks zu bestimmen (Erforderlichkeitsgrundsatz).
6	Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der die kirchliche Stelle unterliegt.	Verpflichtung im Sinne der Vorschrift kann sich sowohl aus kirchlichem, als auch aus staatlichem Recht ergeben.

Rechtmäßigkeit der Verarbeitung, § 6 DSGVO-EKD (4)

Nr.	Rechtfertigungsgrund für die Verarbeitung	Erläuterung
7	Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.	<ul style="list-style-type: none">• Begriff der „lebenswichtigen Interessen“ ist eng auszulegen.• Körperliche Unversehrtheit und Leben natürlicher Personen müssen betroffen sein.• Beispiele: Hilfe bei Katastrophen und humanitären Notfällen (einwilligungsunfähiger Patient).
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.	<ul style="list-style-type: none">• Regelung erfordert aufgrund sehr weiter gesetzlicher Formulierung eine sorgfältige Abwägung der kollidierenden Interessen.

Einwilligung, § 11 DSGVO-EKD

- Wirksamkeitsvoraussetzungen der Einwilligung, § 11 in Verbindung mit § 4 Nr. 13 DSGVO-EKD:
 - freiwillig (ohne Zwang)
 - problematisch bei Über-Unterordnungs-Verhältnissen (z. B. im Beschäftigungsverhältnis)
 - „Kopplungsverbot“, § 11 Abs. 4 DSGVO-EKD
 - konkret („für einen oder mehrere bestimmte Zwecke gegeben“, § 6 Nr. 2 DSGVO-EKD)
 - informiert (hinreichende Vorab-Information, auch über die Widerrufsmöglichkeit)
 - unmissverständlich (eindeutig).
- Schriftform empfehlenswert wegen Nachweispflicht der verantwortlichen Stelle, § 11 Abs. 1 DSGVO-EKD.
- Betroffene Person ist vor Abgabe der Einwilligung über jederzeitige Möglichkeit des Widerrufs in Kenntnis zu setzen, § 11 Abs. 3 Satz 2 DSGVO-EKD.

Verarbeitung besonderer Kategorien personenbezogener Daten, § 13 DSGVO-EKD

Verarbeitung besonderer Kategorien personenbezogener Daten (§ 4 Nr. 2 DSGVO-EKD) ist aufgrund hohen Schutzbedarfs an strengere Anforderungen geknüpft.

- Grundsätzliches Verarbeitungsverbot, § 13 Abs. 1 DSGVO-EKD.
- Abschließender Katalog von Erlaubnistatbeständen in § 13 Abs. 2 Nr. 1 bis 10 DSGVO-EKD.
- Strengere Anforderungen bzgl. Verarbeitung nach § 13 Abs. 3 Nr. 8 DSGVO-EKD (Verarbeitung für Zwecke der Gesundheitsvorsorge, der Arbeitsmedizin, usw.): Fachpersonal, das nach kirchlichem oder staatlichen Recht der Berufsgeheimnispflicht unterliegt oder eine andere Person, die nach kirchlichem oder staatlichen Recht einer Geheimhaltungspflicht unterliegt, § 13 Abs. 3 DSGVO-EKD.

Offenlegung, §§ 8 und 9 DSGVO-EKD

unterschiedliche Zulässigkeitsanforderungen
je nach Empfänger der Offenlegung

Offenlegung an kirchliche oder öffentliche Stellen
(§ 8 DSGVO-EKD)

Offenlegung an sonstige Stellen
(§ 9 DSGVO-EKD)

Offenlegung an kirchliche oder öffentliche Stellen, § 8 DSGVO-EKD

- Grundsatz: Die offenlegende Stelle trägt die Verantwortung, § 8 Abs. 2 S. 1 DSGVO-EKD.
- Offenlegung an kirchliche Stellen: zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der offenlegenden oder der empfangenden kirchlichen Stelle liegenden Aufgaben erforderlich ist und die Zulässigkeitsvoraussetzungen des § 6 DSGVO-EKD erfüllt sind.
- Zulässigkeit bei Offenlegung an Behörden und sonstige öffentliche Stellen, § 8 Abs. 7 DSGVO-EKD:
Alt. 1 durch Rechtsvorschrift oder Alt. 2 bei Erforderlichkeit zur Erfüllung der Aufgaben, die der offenlegenden Stelle obliegen und kein Entgegenstehen offensichtlich berechtigter Interessen der betroffenen Person.

Offenlegung an sonstige Stellen, § 9 DSGVO-EKD

- Zulässigkeitsvoraussetzungen der Offenlegung an sonstige Stellen, § 9 Abs. 1 DSGVO-EKD.
- Strengere Anforderungen für Offenlegung nach § 9 Abs. 1 Nr. 3 DSGVO-EKD, wenn diese besondere Kategorien personenbezogener Daten umfasst, § 9 Abs. 2 DSGVO-EKD:

Offenlegung nur soweit zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich!

- Verantwortung für Zulässigkeit der Offenlegung trägt offenlegende kirchliche Stelle, § 9 Abs. 3 DSGVO-EKD.
- Offenlegung kann durch Rechtsverordnung von Genehmigung einer anderen kirchlichen Stelle abhängig gemacht werden, § 9 Abs. 3 DSGVO-EKD.
- Offenlegende Stelle muss datenempfangende Stelle und Personen auf besondere Zweckbindung hinweisen, § 9 Abs. 5 DSGVO-EKD.
- Im Zweifel immer nach Absprache mit dem oder der örtlich Beauftragten für den Datenschutz!



Grundsätze der
Datenverarbeitung

Grundsätze der Datenverarbeitung, § 5 DSGVO-EKD

- Rechtmäßigkeit, § 5 Abs. 1 Nr. 1 DSGVO-EKD
- Verhältnismäßigkeit, insbesondere Erforderlichkeit, § 5 Abs. 1 Nr. 1 DSGVO-EKD
- Verarbeitung nach Treu und Glauben, § 5 Abs. 1 Nr. 1 DSGVO-EKD
- Transparenz, § 5 Abs. 1 Nr. 1 DSGVO-EKD
- Zweckbindung, § 5 Abs. 1 Nr. 2 DSGVO-EKD
- Datenminimierung, § 5 Abs. 1 Nr. 3 DSGVO-EKD
- Richtigkeit, § 5 Abs. 1 Nr. 4 DSGVO-EKD
- Speicherbegrenzung, § 5 Abs. 1 Nr. 5 DSGVO-EKD
- Integrität und Vertraulichkeit, § 5 Abs. 1 Nr. 6 DSGVO-EKD
- Rechenschaftspflicht, § 5 Abs. 2 DSGVO-EKD

Grundsätze – Rechtmäßigkeit, § 5 Abs. 1 Nr. 1 DSGVO-EKD

- Die Rechtsregel geht davon aus, dass grundsätzlich alle datenrelevanten Maßnahmen rechtswidrig sind, es sei denn, ein (gesetzlich normierter) Erlaubnisgrund rechtfertigt sie.

Grundsätze – Verhältnismäßigkeit, § 5 Abs. 1 Nr. 1 DSGVO-EKD (1)

- Verhältnismäßigkeitsprinzip verlangt, dass jede Maßnahme, die in Grundrechte eingreift,
 - einen legitimen öffentlichen Zweck verfolgt und außerdem
 - geeignet,
 - erforderlich und
 - verhältnismäßig im engeren Sinn („angemessen“) ist.
- Eine Maßnahme, die diesen Anforderungen nicht entspricht, ist rechtswidrig.

Grundsätze –

Verhältnismäßigkeit, § 5 Abs. 1 Nr. 1 DSGVO-EKD (2)

- Es dürfen keine überflüssigen personenbezogenen Daten verarbeitet werden. Maßstab ist die Zweckbindung: Was ist für den Zweck der Bearbeitung erforderlich?
- Personenbezogene Daten dürfen nur in dem Umfang verarbeitet werden, wie es zur Erfüllung der Aufgabe erforderlich ist.
- Bei der Verarbeitung von Daten: Reduzierung auf für den Zweck notwendige Daten
 - „need to know“, nicht „nice to have“
- Bei Zugangs-/Einsichtsrechten: Nur, wenn es zur Aufgabenerledigung erforderlich ist.
- Bei der Aufbewahrungsdauer: Solange zur Erledigung der Aufgabe erforderlich.

Grundsätze – Transparenz, § 5 Abs. 1 Nr. 1 DSGVO-EKD

- Die Erhebung und Verarbeitung personenbezogener Daten durch die verantwortliche Stelle muss dem Betroffenen gegenüber transparent sein.
- Informationspflichten bei unmittelbarer Datenerhebung auf Verlangen, § 17 DSGVO-EKD
- Informationspflichten bei mittelbarer Datenerhebung, § 18 DSGVO-EKD
- Alle Informationen und Mitteilungen an die betroffene Person müssen leicht zugänglich, verständlich und in klarer Sprache verfasst werden.

Grundsätze - Zweckbindung, § 5 Abs. 1 Nr. 2 DSGVO-EKD

- Personenbezogene Daten werden für festgelegte, eindeutige und legitime Zwecke erhoben, § 5 Abs. 1 Nr. 2 DSGVO-EKD.
- Der Zweck muss bei der Erhebung feststehen. Der Betroffene ist auf Verlangen über den Zweck zu informieren, § 17 Abs. 1 Nr. 3 DSGVO-EKD.
- Eine spätere Zweckänderung ist nur ausnahmsweise zulässig, § 7 DSGVO-EKD.
 - Weiterverarbeitungen für im kirchlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gelten als vereinbar mit den ursprünglichen Zwecken.

Grundsätze – Datenminimierung, § 5 Abs. 1 Nr. 3 DSGVO

- Beschränkung auf das dem Zweck angemessene und notwendige Maß
- Soweit mit vertretbarem Aufwand und angesichts des Verwendungszwecks möglich, sollen Daten anonymisiert oder pseudonymisiert werden.
- Präventive Zielvorgaben in § 28 DSGVO, die bei der Technikgestaltung und den Voreinstellungen zu berücksichtigen sind („Privacy by design“ und „Privacy by default“).

Grundsätze – Richtigkeit, § 5 Abs. 1 Nr. 4 DSGVO-EKD

- Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein.
- Es müssen alle angemessenen Maßnahmen getroffen werden, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

Grundsätze - Speicherbegrenzung, § 5 Abs. 1 Nr. 5 DSGVO-EKD

- Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Person nur solange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.
- Eine längere Speicherdauer ist zulässig, soweit die Daten für Zwecke des Archivs, der wissenschaftlichen und historischen Forschung sowie der Statistik verarbeitet werden.

Grundsätze –

Integrität und Vertraulichkeit, § 5 Abs. 1 Nr. 6 DSGVO-EKD

- Es ist eine angemessene Sicherheit bei der Datenverarbeitung zu gewährleisten, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Zerstörung oder unbeabsichtigter Schädigung.

Grundsätze – Rechenschaftspflicht, § 5 Abs. 2 DSGVO-EKD

- Die verantwortliche Stelle muss die Einhaltung der Grundsätze nachweisen können!
 - Daraus folgt eine Dokumentationspflicht! Der Nachweis kann nur gelingen, wenn schriftlich festgehalten ist, wie die verantwortliche Stelle mit personenbezogenen Daten umgeht.

Datengeheimnis, § 26 DSGVO-EKD

- Alle (hauptamtlichen und ehrenamtlichen) Mitarbeitenden sind auf das Datengeheimnis zu verpflichten.
- Den bei der Datenverarbeitung tätigen Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis schriftlich zu verpflichten, soweit sie nicht aufgrund anderer kirchlicher Bestimmungen zur Verschwiegenheit verpflichtet wurden. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.



Rechte der betroffenen
Person

Übersicht der Betroffenenrechte (1)

transparente Information, Kommunikation, § 16 DSGVO-EKD

Informationspflicht bei unmittelbarer Datenerhebung, § 17 DSGVO-EKD

Informationspflicht bei mittelbarer Datenerhebung, § 18 DSGVO-EKD

Auskunftsrecht der betroffenen Person, § 19 DSGVO-EKD

Recht auf Berichtigung, § 20 DSGVO-EKD

Recht auf Löschung, § 21 DSGVO-EKD

Übersicht der Betroffenenrechte (2)

Recht auf Einschränkung der Verarbeitung, § 22 DSGVO

Informationspflicht bei Berichtigung, Löschung oder Einschränkung der Verarbeitung, § 23 DSGVO

Recht auf Datenübertragbarkeit, § 24 DSGVO

Recht auf Widerspruch, § 25 DSGVO

Recht auf Beschwerde, § 46 DSGVO

Schadensersatz durch verantwortliche Stellen, § 48 DSGVO

Auskunftsrecht, § 19 DSGVO-EKD (1)

zentrales Element des Rechts auf Informationelle Selbstbestimmung

Mittel des Selbst Datenschutzes

gesetzliches Recht

unentgeltlich

Auskunftsrecht, § 19 DSGVO-EKD (2)

- Auf Antrag können Betroffene von der verantwortlichen Stelle Auskunft zu den zu ihrer Person gespeicherten Daten verlangen.
- Informationen der Auskunft
 - Verarbeitungszwecke
 - Kategorien personenbezogener Daten
 - Empfänger oder Kategorien von Empfängern
 - geplante Speicherdauer oder Kriterien für deren Festlegung
 - bestehendes Recht auf Berichtigung, Löschung, Einschränkung oder Widerspruch
 - Beschwerderecht bei der Aufsichtsbehörde
 - alle verfügbaren Informationen über Herkunft der Daten