Bischöfliches Generalvikariat Trier
Betrieblicher Datenschutz

Daten schützen?
Aber sicher!

BISTUM
TRIER

Bischöfliches Generalvikariat Trier
Betrieblicher Datenschutz

Datenschutz im Bistum Trier

Die haupt- und ehrenamtlichen Mitarbeiter*innen in allen Einrichtungen und Dienststellen im Bistum Trier tragen die Verantwortung für die datenschutzkonforme Ausübung ihrer Tätigkeit *(vgl. § 17 KDG-DVO)*! Für die Umsetzung der rechtlichen Anforderungen sind die Dienststellenleitungen vor Ort zuständig.

Datenschutz ist im Kirchenrecht (Can. 220 CIC) ein Fundamentalrecht!

Wir alle schützen, bei der Erfüllung unserer Aufgaben, die uns anvertrauten personenbezogenen Daten ernsthaft und intensiv, damit niemandem durch die Verletzung des Schutzes seiner Daten ein Schaden entsteht oder zugefügt wird.

Die Betrieblichen Datenschutzbeauftragten wirken auf die Einhaltung der geltenden Rechtsnormen hin und stehen Ihnen auf Anfrage beratend und unterstützend zur Seite.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen.
Jede/jeder von uns hat eine **Verpflichtungserklärung** zum Thema Datenschutz und Geheimhaltung unterzeichnet.

Wir nehmen uns Zeit für den Datenschutz und werden feststellen:
Manches ist längst geübte Praxis, manches ist neu und bedarf etwas guten Willen und Übung. Die Lektüre dieser Informationen ist ein Schritt in die richtige Richtung. So entsteht aus einer erhöhten allgemeinen Sensibilität im Umgang mit den uns anvertrauten Daten ein gelebter Datenschutz. Dabei sollen uns die, von den verantwortlichen Stellen und Dienststellenleitungen getroffenen, technischen und organisatorischen Maßnahmen unterstützen.

Sensibilität
+ technische und organisatorische Maßnahmen
+ angepasste Arbeitsprozesse
= gelebter Datenschutz und Rechtskonformität

Datenschutz: Gut zu wissen!

Das Kirchliche Datenschutzgesetz wurde am 24.05.2018 durch Bischof Dr. Stephan Ackermann in Kraft gesetzt und löste die bisherige Anordnung für den kirchlichen Datenschutz (KDO) ab!
Die Bekanntmachung hierzu finden Sie im Kirchlichen Amtsblatt (KA 2018 Nr. 65).

KDG
KA 2018 Nr. 65

Besondere kirchliche oder staatliche Rechtsvorschriften, z. B. § 203 Strafgesetzbuch zur Vertraulichkeit des Wortes oder auch das Kunsturhebergesetz zum Umgang mit Bildnissen, Fotos etc., gehen dem Kirchlichen Datenschutzgesetz (KDG) vor, sofern sie das Datenschutzniveau des KDG nicht unterschreiten.

Am 1. März 2019 wurde die Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) in Kraft gesetzt.
Die Bekanntmachung hierzu finden Sie im Kirchlichen Amtsblatt (KA 2019 Nr. 9).

KDG-DVO
KA 2019 Nr. 9

Daten schützen? Aber sicher!

✕ Beim Datenschutz geht es auch um eine **grundsätzliche Haltung Ihren Mitmenschen gegenüber**, die das Recht haben, selbst zu entscheiden, was sie anderen von sich mitteilen wollen.

✕ Datenschutz schützt in unserem Rechtsstaat unsere im Grundgesetz verankerten Persönlichkeitsrechte und sichert mit der Datenschutzgesetzgebung **jeder/m Einzelnen von uns das Recht auf informationelle Selbstbestimmung** zu.

✕ **Datenschutzkonformität beim Arbeiten ist eine gesetzliche Verpflichtung für uns alle!** Deshalb achten wir alle selbstverständlich auf die Rechtmäßigkeit zur Verarbeitung personenbezogener Daten und prüfen aufgrund welcher Rechtsgrundlage wir personenbezogene Daten verarbeiten dürfen, sollen oder sogar müssen.

✕ **Wir arbeiten datensparsam**. Am Beginn jeder Verarbeitung von personenbezogenen Daten steht die grundsätzliche Frage:
Welche Daten sind tatsächlich erforderlich und unverzichtbar um den Zweck zu erfüllen und das Ziel des Projektes zu erreichen?

Datenschutz – Ein Aufwand, der sich lohnt!

Datenschutz?! Um was geht es?

✕ Datenschutz meint den Schutz personenbezogener Daten. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen *(§ 1 i.V.m. § 4 Nr. 1 KDG)*.

✕ Gelebter Datenschutz schützt nicht nur die betroffenen Personen, deren Daten uns anvertraut werden, sondern auch uns alle, die haupt- und/oder ehrenamtlichen Mitarbeiter*innen im Bistum Trier.

Noch intensiveren Schutz genießen die besonderen personenbezogenen Daten (Datenschutzklasse 3). Dazu zählen z. B. die rassische und ethnische Herkunft, Gesundheitsdaten oder Daten zum Sexualleben, politische Meinungen und religiöse Überzeugung *(§ 4 Nr. 2 KDG)*.

Hinweis: Die Zugehörigkeit zu einer Kirche oder Religionsgemeinschaft (z. B. bei der Nutzung des Merkmals „rk“) gehört hier nicht dazu.

Datenschutz!
Darum geht es!

Wie stark müssen wir schützen?

Daten werden in 3 Schutzklassen (je nach Risiko) eingeteilt *(vgl. §§ 9 – 14 KDG-DVO)*:

Datenschutzklassen

1

Datenschutzklasse 1
z. B. Adressen, die so auch in Telefonbüchern oder anderen öffentlichen Quellen stehen, Berufs-, Branchen- oder Geschäftsbezeichnungen

2

Datenschutzklasse 2
z. B. Daten zum Beschäftigungsverhältnis, Kontaktdaten von haupt- und ehrenamtlichen Mitarbeitenden, z. B. Handynummer, Vertragsdaten, Mietverhältnisse, Geburts- und Jubiläumsdaten

3

Datenschutzklasse 3
besonders sensible Daten wie z. B. Daten zur Gesundheit, zum Sexualleben, alle Bank- und Kreditkartendaten, politische Meinungen, rassische und ethnische Herkunft, religiöse und philosophische Überzeugungen, Hinweise oder Angaben zu Ordnungswidrigkeiten oder Straftaten, Namens- und Adressangaben mit Sperrvermerken

*Je nach Datenschutzklasse sind technische und organisatorische Maßnahmen dem Schutzzweck angemessen zu intensivieren. Hierzu nutzen Sie innerhalb des Cloud-Computings und im E-Mailing die Funktion Vertraulichkeitsklassifizierung. Beachten Sie die im System hinterlegte Kurzanleitung zu dieser Funktion! In Zweifelsfällen fragen Sie bitte Ihre*n Betriebliche*n Datenschutzbeauftragte*n. Zuständigkeiten siehe unter www.bistum-trier.de/datenschutz.*

Grundsätze des Datenschutzes:
(§§ 6–8 KDG)

1. **Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ist verboten**, es sei denn, eine Rechtsvorschrift erfordert oder erlaubt es oder der/die Betroffene hat eingewilligt!

2. Personenbezogene Daten dürfen **nur für eindeutig festgelegte und legitime Zwecke** erhoben werden!

3. **Datensparsam arbeiten:** so wenige Daten wie möglich, so viele Daten wie nötig!

4. **Sachlich richtige und aktuelle Daten** verarbeiten. Unrichtige Daten sind unverzüglich zu löschen oder zu berichtigen.

5. **Identifizierung der betroffenen Person?** Nur so lange, wie es zur Zweckerfüllung erforderlich ist. Prüfen Sie die Möglichkeiten zur Pseudonymisierung *(§ 4 Nr. 6 KDG)* oder Anonymisierung *(§ 4 Nr. 7 KDG)*!

6. Personenbezogene Daten müssen in einer Weise verarbeitet werden, die **eine angemessene Sicherheit** gewährleistet. Im Blick sind dabei auch der **Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, Zerstörung oder Schädigung** der Daten *(§§ 26 – 30 KDG)*.

7. Wir gewährleisten und dokumentieren die zur Erfüllung unserer kirchlichen Aufgaben erforderlichen Verarbeitungsprozesse im Bistum Trier in der Weise, dass die **Einhaltung der Grundsätze jederzeit nachgewiesen werden kann**.

Datensicherheit: Unsere Ziele

Wir tun alles, was uns möglich ist, um Vertraulichkeit, Integrität, Authentizität und Revisionsfähigkeit der uns anvertrauten Daten zu gewährleisten.

Wir prüfen regelmäßig unsere Arbeitsweise und die technischen und organisatorischen Maßnahmen zur Gewährleistung eines angemessenen Schutzes und passen sie den Erfordernissen an.

Zur Datensicherheit gehören alle technischen und organisatorischen Maßnahmen, mit denen die Einhaltung der datenschutzrechtlichen Vorgaben gewährleistet wird.

Datensicherheit
Unsere Ziele!

Datenschutz: Gut zu wissen!

✕ **Das Gesetz verpflichtet das Bistum Trier auch dazu, alle Mitarbeiter*innen zu sensibilisieren und zu schulen. Hierzu stehen zahlreiche Schulungsformate zur Verfügung.**

Die erste Schulung der hauptamtlichen Mitarbeitenden wird online organisiert und ist über einen Nachweis in der Personalakte oder in der Aktenführung der jeweiligen Einsatzstelle (z.B. im Pfarrbüro für ehrenamtliche Mitarbeitende) **zu belegen.** Weitere Fortbildungen zum Thema Datenschutz finden Sie im Fortbildungsprogramm der Personalentwicklung im Bistum Trier.

Führungskräfte und Fachvorgesetzte werden darüber hinaus gezielt geschult und informiert. Bitte achten Sie auf Hinweise zur Online-Schulung und weitere Informationsveranstaltungen zum Thema Datenschutz. Weitere Termine zur individuellen Sensibilisierung, gerne auch für ganze Arbeitsbereiche, Abteilungen bzw. Einrichtungen können jederzeit erfragt und organisiert werden.

Die ehrenamtlichen Mitarbeiter*innen werden über die Pfarrbüros informiert *(§ 7 i.V.m. § 38 KDG)*. Bitte fordern Sie in diesem Zusammenhang gerne unsere Broschüre *„Handlungsempfehlungen zum Kirchlichen Datenschutz – im Ehrenamt“* an.

Datenschutz: Gut zu wissen!

Recht auf Auskunftserteilung *(§ 17 KDG i.V.m. § 14 Abs. 3 KDG)*

✕ **Vor** jeder Erhebung personenbezogener Daten für Ihren Arbeitsauftrag steht die Aufklärung der Betroffenen. Es besteht eine **umfassende Transparenz- und Informationspflicht** hinsichtlich der Verarbeitung ihrer jeweiligen personenbezogenen Daten *(§§ 14 – 16 KDG)*.

✕ Jeder hat das Recht auf eine **unverzügliche** Information, die in jedem Fall **innerhalb eines Monats nach Eingang des Antrags auf Auskunft** zu erfolgen hat.

✕ Wir informieren **schriftlich** darüber, welche personenbezogenen Daten der*des Antragstellenden zu welchem Zweck und aufgrund welcher Rechtsgrundlagen verarbeitet werden oder wurden. Die gesetzlichen Anforderungen finden Sie in § 17 KDG.

Datenschutz: Gut zu wissen!

Recht auf Auskunftserteilung

✕ Für den Fall, dass das Auskunftsersuchen nicht nur ein bestimmtes Projekt sondern mehrere Fachabteilungen/Einrichtungen innerhalb des Bistums Trier betreffen könnte, muss die Auskunft des Bistums **koordiniert** erfolgen. Bitte wenden Sie sich für weitere Informationen unverzüglich an Ihre*n zuständigen Datenschutzbeauftragte*n.

✕ Achten Sie vor der Auskunftserteilung auf die **Legitimation und zweifelsfreie Feststellung der Identität** der betroffenen Person. Falls erforderlich ist in Ausnahmefällen eine **Fristverlängerung** um weitere zwei Monate **möglich**. Die Gründe der Verzögerung sind darzulegen.

Datenschutz: Gut zu wissen!

Informationspflicht vor der Datenerhebung *(§§ 15 und 16 KDG)*

✕ Das Datenschutzrecht stärkt erheblich die Rechte der Menschen, mit deren personenbezogenen Daten wir zur Erfüllung unserer kirchlichen Aufgaben und im Rahmen unserer Zuständigkeiten umgehen, und es verpflichtet die verantwortlichen Stellen zur **proaktiven und umfassenden Information der Betroffenen** *(§§ 14–25 KDG)*.

Wir informieren über:

- Name und Kontaktdaten der verantwortlichen Stelle bzw. Einrichtung
- Name und Kontaktdaten der/des betrieblichen Datenschutzbeauftragten
- Zweck und Rechtsgrundlage zur geplanten Datenverarbeitung
- Gegebenenfalls Begründung der berechtigten Interessen *(vgl. § 6 Abs. 1 lit g KDG)*
- Gegebenenfalls Empfänger oder Kategorien von Empfängern im Falle von Offenlegung der Daten
- Gegebenenfalls Absichtserklärung zur Weiterleitung von Daten in ein Drittland
- Vorgesehene Dauer der Speicherung der personenbezogenen Daten
- Rechte der betroffenen Personen

Datenschutz: Gut zu wissen!

✕ Das Bistum Trier steht in der **Rechenschaftsverpflichtung**, d.h. es muss die Einhaltung der gesetzlichen Regelungen im KDG und der KDG-DVO (z. B. der Nachweis, dass die Informationsverpflichtung erfüllt wurde) nachweisen können.
Wir dokumentieren und halten die erforderlichen Nachweise revisionsfähig in den einzelnen Fachbereichen/Einrichtungen vor.

✕ Jede Person, der wegen eines Verstoßes gegen das KDG ein materieller oder immaterieller Schaden entstanden ist, hat **Anspruch auf Schadensersatz** gegen die kirchliche Stelle als Verantwortlicher oder Auftragsverarbeiter *(§ 50 KDG)*.

✕ Die Höhe des Bußgeldes wird durch die Datenschutzaufsicht festgelegt und beträgt je nach Schwere des Verstoßes unter Umständen bis zu 500.000 € *(§ 51 KDG)*.

Datenschutz: Gut zu wissen!

✕ Die verantwortlichen Dienststellen müssen ein Verzeichnis ihrer Verarbeitungstätigkeiten erstellen. Den hierfür zu nutzenden Vordruck **„Verfahrensbeschreibung/ Beschreibung der Verarbeitungstätigkeit", in dem die Prozesse zu den Arbeitsabläufen in Ihren Zuständigkeitsbereichen beschrieben werden**, finden Sie im Portal oder erhalten Sie auf Anfrage bei den betrieblichen Datenschutzbeauftragten in der Stabsstelle Justiziariat.

✕ Es ist erforderlich für das Bistum Trier eine Übersicht über **ALLE „Verfahrensbeschreibungen/Beschreibungen von Verarbeitungstätigkeiten"** zu haben.

Bitte beachten Sie die hierzu ergehenden Hinweise, die Sie über die Leitung Ihrer Organisationseinheit (Stabsstelle, Bereich, Servicestelle) oder Ihre Einrichtung/Dienststellenleitung erhalten *(§ 31 KDG i.V.m. § 1 KDG-DVO)*.

Datenschutz: Gut zu wissen!

Auftragsverarbeitung *(§§ 29 und 30 KDG i.V.m. § 21 KDG-DVO)*

✕ Verträge zur Auftragsverarbeitung nach § 57 KDG sind in jedem Fall mit folgenden Dienstleistern abzuschließen: Rechenzentren, externen Agenturen (Leiharbeit, Headhunter, Assessment-Center), externe Dienstleister mit „Remote-Zugriff" (Server, Wartungsverträge, Softwarepflege), externe Dienstleister für Peripherie-Geräte (Fax, Drucker, Multifunktionsgeräte, Scanner, Kopierer), Entsorger (IT, Aktenentsorgung), externe Berater mit Zugriff auf Software und personenbezogene Daten, Internet-Service-Provider (Fremdsoftware als Dienstleistung), Dienstleister für Heizkostenabrechnungen ...

✕ **Auftragsverarbeitung im Sinne des Datenschutzrechts bedeutet die Einschaltung eines Dienstleisters bei der Verarbeitung personenbezogener Daten.** Von Datenverarbeitung im Auftrag spricht man, wenn die datenverarbeitende Stelle (verantwortliche Stelle) sich einer Stelle bedient (Dienstleister), die für die Einrichtung im Auftrag und weisungsabhängig personenbezogene Daten erhebt, verarbeitet oder nutzt. **Dabei haftet der Auftraggeber (die Einrichtung) dem Dateneigentümer (Betroffener) gegenüber.**

*Auf Anfrage erhalten Sie Unterstützung sowie Musterverträge durch die betriebliche*n Datenschutzbeauftragte*n.*

Datenschutz: Gut zu wissen!

✕ Datenpannen, d. h. Datenschutzverletzungen (Verlust, Offenlegung der Daten oder Fremdzugriff), werden **unverzüglich** (innerhalb von 72 Stunden nach Bekanntwerden) von der/dem Verantwortlichen an die Überdiözesane Aufsichtsstelle (gemeinsame Datenschutzstelle in Frankfurt) und an die/den zuständige*n betriebliche*n Datenschutzbeauftragte*n gemeldet *(§§ 33, 34 KDG)*. Beachten Sie hierzu auch den „**72 Std.-Notfallplan im Falle einer Datenpanne (Ziel und Prozessbeschreibung)" unter www.bistum-trier.de/datenschutz.**

✕ Die Meldung an die Überdiözesane Aufsichtsstelle (Datenschutzaufsicht) hat immer zu erfolgen, wenn die Datenschutzverletzung eine Gefahr für die Rechte und Freiheiten der/des Betroffenen darstellt (z. B. die Verletzung der Vertraulichkeit, Verlust der Hoheit über die persönlichen Daten des Betroffenen).

✕ Verantwortlich für die Meldung ist im hauptamtlichen Bereich zunächst die Dienststellenleitung, deren/dessen Stellvertreter*in bzw. die/der verantwortliche Mitarbeiter*in. Im ehrenamtlichen Bereich ist der Verantwortliche der Pfarrer bzw. die/der Vorsitzende des Entscheidungsgremiums im Bereich, in dem Sie Ihr ehrenamtliches Engagement ausüben.

Dabei gilt: Niemand ist frei von Fehlern! Wir stehen zu unseren Fehlern und tun alles, um mögliche Schäden und Folgeschäden zu vermeiden, abzuwenden oder zumindest zu begrenzen.

Im Dienstgebäude oder beim mobilen Arbeiten:

- ✓ Bürotüren bei eigener Abwesenheit immer abschließen.
- ✓ Zugangstüren und -tore außerhalb der Rahmenarbeitszeiten immer abschließen.
- ✓ Nach Dienstschluss keine Gäste oder Besucher alleine im Gebäude zurücklassen.
- ✓ Schlüssel und/oder Transponder nicht verleihen.

Achten sie auch beim mobilen Arbeiten und im Ehrenamt darauf, dass die Vertraulichkeit gewährleistet ist und ein unberechtigter Zugriff auf die Ihnen anvertrauten personenbezogenen Daten nicht erfolgen kann. Datenschutz gilt immer und gleichermaßen für haupt- und ehrenamtliche Mitarbeitende, egal wo und bei welcher Tätigkeit.

Im Dienstgebäude

Am Arbeitsplatz, egal ob im Büro oder beim mobilen flexiblen Arbeiten, am Telefon, auf dem Flur, ... :

- ✓ Keine unbefugten Personen alleine im Büro lassen.
- ✓ Keine sensiblen Unterlagen bei eigener Abwesenheit offen auf dem Schreibtisch liegen lassen.
- ✓ Drucker/Kopierer in Sichtweite aufstellen. Ausdrucke direkt abholen und im Folgenden vor dem unberechtigten Zugriff Dritter schützen.
- ✓ Sensible Unterlagen und Akten nach Beendigung der Tätigkeit in verschlossenen Schränken aufbewahren.
- ✓ Wenn die/der Gesprächspartner*in nicht bekannt ist, Authentizität oder Identität sicherstellen.
- ✓ In Gesprächen Vertraulichkeit gewährleisten: ohne Einverständnis kein Mithören von Dritten ermöglichen.
- ✓ Personenbezogene Daten gehören nicht in öffentliche Foren.

Im Arbeitsalltag

Im Umgang mit der Technik:

- ✓ Verwenden Sie schlaue und sichere Passwörter.
  Am besten anhand eines für Sie persönlich gut einprägsamen Satzes unter Verwendung von Sonderzeichen, Groß- und Kleinbuchstaben sowie Zahlen.
  Je mehr Zeichen umso sicherer!

  Beispiel: #Datenschutz im Bistum Trier ist uns nicht erst seit dem 24.5.2018 wichtig!
  => Passwort: #DiBTiunesd24.5.w!

- ✓ Geben Sie Passwörter niemals weiter (auch nicht unbeabsichtigt über den hinterlegten Spickzettel).

- ✓ Sperren Sie bei eigener Abwesenheit Ihren Bildschirm/PC.

- ✓ Fahren Sie nach Dienstschluss den PC runter und schalten Sie die Geräte aus.

Technik

Im Umgang mit der Technik:

- ✓ Für den Fall, dass Sie durch dienstliche Gründe dazu gezwungen sind, Daten der Datenschutzklasse III auf mobilen Geräten zu speichern, darf dies nur **verschlüsselt** erfolgen *(vgl. hierzu § 13 Abs. 2 a KDG-DVO)*.

- ✓ Die technische Umsetzung erfolgt über die **Vertraulichkeitsklassifizierung** und Ihrer Auswahl der Datenschutzklasse I, II oder III. Zur korrekten Einordnung orientieren Sie sich immer am verarbeiteten personenbezogenen Datum mit der höchsten Datenschutzklasse. Eine entsprechende Kurzanleitung und FAQs sind für Sie im IT-System des Bistums Trier hinterlegt.

- ✓ Die Verarbeitung personenbezogener Daten auf privaten IT-Systemen zu dienstlichen Zwecken ist grundsätzlich unzulässig.
Ausnahmeregelungen können durch den Verantwortlichen, unter Beachtung der jeweils geltenden gesetzlichen Regelungen, schriftlich zugelassen werden *(vgl. hierzu § 20 Abs. 1–3 KDG-DVO)*.

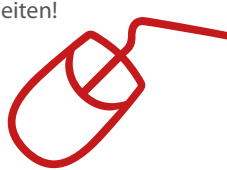
- ✓ Die **automatische Weiterleitung** dienstlicher E-Mails auf private E-Mail-Konten ist in jedem Fall unzulässig *(vgl. hierzu § 20 Abs. 4 KDG-DVO)*.

Im Umgang mit der Technik:

- **Dienstliche Kommunikation erfolgt ausschließlich über die Bistums-IT.**
  Alle Mitarbeitenden im Anstellungsverhältnis zum Bistum Trier nutzen stets die dienstliche E-Mailadresse (....@bgv-trier.de oder ....@bistum-trier.de).
  *Beachten Sie die Nutzungsbedingungen der IT-Systeme des Bistums Trier und der spezifischen Anlagen in der jeweils geltenden Fassung. Zu finden im Portal oder anzufordern bei **digitalisierung@bistum-trier.de**.*

- Eine **Datenschutz-Folgenabschätzung** *(vgl. hierzu § 35 KDG)* ist immer dann vorzunehmen, wenn mindestens eines der nachfolgend aufgeführten Kriterien zutrifft bzw. ein **hohes Risiko** zu Lasten der betroffenen Personen gegeben ist. Von einem Risiko ist auszugehen, wenn die Datenverarbeitung zu einem physischen, materiellen oder immateriellen Schaden führen könnte.

- **Im Mittelpunkt steht der Mensch** mit seinen Rechten und Grundfreiheiten! Daher sind die Risiken aus seiner Perspektive, also aus der Sicht der/s Einzelnen zu ermitteln.



Bitte beachten Sie die nachfolgenden Kriterien, unter denen eine Datenschutzfolgenabschätzung vorgenommen werden muss.

Solche Kriterien sind zum Beispiel, wenn der Vorgang der Datenverarbeitung zu Lasten der betroffenen Personen

- eine Diskriminierung verursachen könnte;
- die Gefahr eines Identitätsdiebstahls oder -betruges darstellt;
- zu einem finanziellen Verlust oder einer Rufschädigung führen kann;
- die Vertraulichkeit personenbezogener Daten, die einem besonderen Berufsgeheimnis unterliegen, gefährden würde;
- eine unbefugte Aufhebung einer Pseudonymisierung ermöglicht;
- sie daran hindert, die Verwendung ihrer Daten zu kontrollieren;
- Persönlichkeitsprofile unter Verwendung besonderer Kategorien personenbezogener Daten erstellt;
- Daten schutzbedürftiger Personen, insbesondere Kinder betrifft;
- eine große Menge von Daten einer Vielzahl von betroffenen Personen beinhaltet.

Es müssen in jedem Fall eine genaue Risikoanalyse stattfinden und Maßnahmen zur Bewältigung der Risiken vorgesehen sein.

*Im Zweifelsfall kontaktieren Sie bitte die/den betriebliche*n Datenschutzbeauftragte*n.*

Beachten Sie folgende Grundregeln:

- ✓ Benutzen Sie keine Sticks zum Speichern oder Weitergeben von Daten.
- ✓ Wenn die Nutzung externer Laufwerke nicht vermeidbar ist, dann verwenden Sie nur verschlüsselte Laufwerke.
- ✓ Ausgediente Wechseldatenträger sind professionell zu vernichten.
- ✓ Beim Öffnen von Mails mit unbekannter Herkunft besteht Virengefahr. Bewahren Sie ein gesundes Misstrauen beim Öffnen von Mails, Links, SMS oder auch QR-Codes! Phishing, Spoofing, Quishing, egal wie sich Angriffsversuche von Trickbetrügern nennen.
  Immer gilt: **Links/QR-Codes bitte nicht anklicken wenn Sie von der Legalität/der Realität des Absenders nicht überzeugt sind!**

*In Zweifelsfällen im Umgang mit Technik, Software und E-Mail-Verkehr ist die **Abteilung B 4.3.2 Team Service und Betrieb** (helpdesk@bgv-trier.de, Telefon (06 51) 7105-123) in der Abteilung IT-Servicemanagement oder auch die **Abteilung Digitalisierung** (digitalisierung@bgv-trier.de) der richtige Ansprechpartner für Sie.*

Vor der Erhebung von Daten:

- ✓ Klären Sie die Rechtsgrundlage: Gibt es eine Rechtsvorschrift und/oder eine Einwilligung der Betroffenen *(§§ 6 – 8 KDG)*?
- ✓ Planen Sie Ihre Verarbeitungsprozesse vorausschauend und beachten Sie dabei die Grundsätze zur Verarbeitung von personenbezogenen Daten *(§ 7 KDG)*.
- ✓ Legen Sie die Zweckbestimmung fest: Welche Daten brauche ich wofür *(§§ 6 – 8 KDG)*?
- ✓ Kommen Sie Ihrer **Informationsverpflichtung** nach §§ 14 ff KDG nach.

Es gibt keinen Bestandsschutz für Datenbestände nach altem Recht. Nach Inkraftsetzung gilt das neue Kirchliche Datenschutzgesetz für bestehende und künftige Datenbestände.

Daten erheben

Vor der Weitergabe von Daten:

- ✓ Prüfen Sie Identität und Kontaktdaten des Empfängers/der Empfängerin *(vgl. §§ 9, 10 KDG)*.

- ✓ Senden Sie nur die Daten und Informationen, welche die/der Empfänger*in tatsächlich in diesem Moment für ihre/seine Arbeit benötigt.
  Schwärzen Sie die personenbezogenen Daten und Informationen, die für diese Arbeit nicht zwingend benötigt werden, **und schützen Sie damit sowohl die Rechte der betroffenen Personen als auch sich selbst als Mitarbeiter*in in Ihrem Tun**.

- ✓ Geben Sie Unterlagen und Daten nur dann weiter, wenn es erlaubt ist, und geben Sie keine Daten an unbefugte Dritte. Desgleichen gilt selbstverständlich auch für das Teilen oder die Freigabe von Dokumenten mit personenbezogenen Daten.

Offenlegung

✓ Prüfen Sie die **Zugriffsberechtigung** des Empfängers/der Empfängerin und legen Sie vor der Teilung/der Freigabe fest, welche Berechtigungen die/der Empfänger*in hat bzw. haben soll. Erstellen Sie in Ihrem Team/in Ihrer Abteilung/etc. ein Zugriffsberechtigungskonzept.

✓ Achten Sie beim Versand darauf, dass Sie als **Absender*in mit Adresse für den Zusteller erkennbar** sind. So vermeiden Sie, dass die Postsendung im Falle von Unzustellbarkeit geöffnet werden muss.

✓ Prüfen Sie kritisch, ob die Inhalte in einer E-Mail versendet werden können. Eine E-Mail ist so offen wie eine Postkarte.

- Versenden Sie personenbezogene Daten oder vertrauliche Inhalte besser verschlüsselt als Anlage zur Mail oder per Post.
- Wenn Sie Inhalte verschlüsselt per E-Mail schicken, dann übermitteln Sie das Kennwort persönlich oder telefonisch.
- Senden Sie personenbezogene Daten der Datenschutzklassen II und III niemals unverschlüsselt per E-Mail außerhalb eines geschlossenen und gesicherten Netzwerks *(vgl. hierzu § 12 Abs. 2 e KDG-DVO)*.
- Hinweis für Pfarrsekretärinnen und Pfarrsekretäre: Es besteht die Möglichkeit, den gesicherten Datentransfer in „e-mip“ zu nutzen.

- ✓ Verwenden Sie bei der Bezeichnung von Dateien oder Ordnern **keine Namen/ Vornamen von betroffenen Personen**.
- ✓ Beim Versand einer E-Mail an große Empfängerkreise außerhalb des gesicherten Netzwerkes gehören alle privaten Empfängeradressen in das Bcc-Feld und die eigene E-Mail-Adresse ins Empfängerfeld.
- ✓ Geben Sie eine **aufschlussreiche Betreffzeile** an, um dem Empfänger bestenfalls eine eindeutige Identifikation des Absenders zu ermöglichen.

  (Beispiel für eine schlechte Betreffzeile: „Einladung" – Diese Betreffzeile lässt den Empfänger rätseln und zweifeln, ob der Absender real ist oder ob es sich vielleicht um eine Pishing-Mail handelt. Besserer Betreff: Einladung zur PGR-Sitzung am ...)
- ✓ Richten Sie eine **aussagekräftige dienstliche Signatur** ein, damit die/der Empfänger*in Sie als reale*n Absender*in identifizieren kann. Halten Sie sich hierzu an die Vorgaben des Bistums zur Signatur.
- ✓ Verwenden Sie auch **in der Betreffzeile keine Namen** von betroffenen Personen sondern nur ein Aktenzeichen oder das Thema, um das es gerade geht. *(Bitte nicht „Datenauskunft über Karl Mustermann", sondern einfach „Auskunftsersuchen KDG Az...".)*

Vor der Löschung von Daten:

- ✓ Zur Bewertung von auszusondernden Akten, Unterlagen und Datenbeständen ziehen Sie das Bistumsarchiv hinzu und bieten Sie diese Unterlagen vor einer Vernichtung/Löschung dem Bistumsarchiv an. Gemäß § 6 der Kirchlichen Archivordnung *(KA 2014 Nr. 60, hier S. 100)* besteht eine Anbietungspflicht für alle Unterlagen.
  Bistumsarchiv | bistumsarchiv@bgv-trier.de | Telefon (06 51) 96627-0
- ✓ Prüfen Sie die gesetzlichen und individuellen Aufbewahrungsfristen.
- ✓ Entsorgen Sie keine sensiblen Unterlagen (auch nicht die eigene Gehaltsabrechnung etc.) ungeschreddert im Papierkorb.
- ✓ Zu vernichtende Unterlagen größeren Umfangs (z. B. Altakten ohne Archivierungswürdigkeit, ausgediente Schematismen) gehören in die „silbernen Tonnen" oder in einen abgeschlossenen Container und werden einer professionellen Löschung zugeführt.

Daten löschen

Ihre Rechte als betroffene Person:

1. Recht auf Widerruf der datenschutzrechtlichen Einwilligungserklärung *(vgl. § 8 KDG)*

Für den Fall, dass die Verarbeitung Ihrer Daten auf Ihrer datenschutzrechtlichen Einwilligungserklärung beruht, haben Sie nach § 8 KDG das Recht, diese jederzeit zu widerrufen. Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung wird davon nicht berührt.

2. Auskunftsrecht *(vgl. § 17 KDG)*

Sie haben das Recht auf eine transparente Information. Auf Verlangen geben wir Ihnen darüber Auskunft, welche Ihrer personenbezogenen Daten zu welchem Zweck verarbeitet werden.

3. Recht auf Berichtigung *(vgl. § 18 KDG)*

Sie haben das Recht auf Berichtigung unrichtiger Daten, die Ihre Person betreffen.

Ihre Daten bei uns

4. Recht auf Löschung *(vgl. § 19 KDG)*

Unter den in § 19 KDG genannten Voraussetzungen (z. B. falls Sie eine erteilte Einwilligung widerrufen oder die Daten für die Zwecke, für die sie erhoben wurden nicht mehr erforderlich sind) haben Sie das Recht, eine Löschung der Sie betreffenden personenbezogenen Daten zu verlangen.

5. Recht auf Einschränkung der Verarbeitung *(vgl. § 20 KDG)*

Unter den in § 20 KDG genannten Voraussetzungen haben Sie das Recht, eine Einschränkung der Verarbeitung der Sie betreffenden Daten zu verlangen.

6. Recht auf Unterrichtung *(vgl. § 21 KDG)*

Haben Sie Ihr Recht auf Berichtigung, Löschung oder Einschränkung der Verarbeitung gegenüber dem Verantwortlichen geltend gemacht, ist dieser verpflichtet, allen Empfängern, denen sie betreffende personenbezogene Daten offengelegt wurden, die Berichtigung, Löschung oder Einschränkung der Verarbeitung mitzuteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Ihnen steht gegenüber dem Verantwortlichen das Recht zu, über diese Empfänger unterrichtet zu werden.

7. Recht auf Datenübertragbarkeit *(vgl. § 22 KDG)*

Ihnen steht auch das Recht zu, die Sie betreffenden personenbezogenen Daten, die Sie dem Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

8. Widerspruchsrecht *(vgl. § 23 KDG)*

In bestimmten Fällen, die in § 23 KDG näher beschrieben sind, haben Sie jederzeit das Recht, gegen die Verarbeitung der Sie betreffenden personenbezogenen Daten Widerspruch einzulegen.

9. Automatisierte Entscheidung im Einzelfall *(vgl. § 24 KDG)*

Von der Möglichkeit automatisierter Entscheidungen, die im Einzelfall zulässig wären, machen wir keinen Gebrauch.

10. Unabdingbare Rechte der betroffenen Person *(vgl. § 25 KDG)*

Über Entscheidungen zu den von Ihnen geltend gemachten Rechten werden Sie regelmäßig schriftlich informiert.

Datenschutz konkret: Ihre Daten bei uns

Wir tun alles, um Ihre personenbezogenen Daten zu schützen. Für den Fall, dass Sie sich jedoch von uns im Umgang mit Ihren Daten nicht gut behandelt fühlen, haben Sie auch ein Recht auf Beschwerde bei einer Aufsichtsbehörde *(vgl. § 48 KDG)*:

Überdiözesane Aufsichtsstelle im Datenschutz der (Erz-)Diözesen Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier:
Gemeinsame Datenschutzstelle
Diözesandatenschutzbeauftragte:
Ursula Becker-Rathmair
Roßmarkt 23, 60311 Frankfurt/M.
info@kdsz-ffm.de
Telefon 069 58 99 755-10
Telefax 069 58 99 755-11

Ihre Daten bei uns

Hilfe? Hilfe!

Die Betrieblichen Datenschutzbeauftragten der einzelnen Zuständigkeitsbereiche stehen Ihnen gerne beratend und unterstützend bei allen datenschutzrechtlichen Fragen und Anregungen zur Seite. Die Kontaktdaten können Sie hier erfragen:

Betrieblicher Datenschutz
Mustorstraße 2, 54290 Trier, Telefon (06 51) 7105-0

- datenschutz@bgv-trier.de
- datenschutz-pfarreien@bgv-trier.de
- datenschutz-lebensberatung@bgv-trier.de
- datenschutz-telefonseelsorge@bgv-trier.de

Weitere Informationen finden Sie auch unter:
www.bistum-trier.de/datenschutz

Kontakte

BISTUM
TRIER

Impressum

Bischöfliches Generalvikariat Trier
Betrieblicher Datenschutz
Mustorstraße 2, 54290 Trier
datenschutz@bgv-trier.de
Telefon (06 51) 7105-0

Stand Dezember 2023

Diese Informationsschrift ist beispielhaft und erhebt keinen Anspruch auf Vollständigkeit.

Redaktion Ursula Eiden | Betriebliche Datenschutzbeauftragte

Zuständigkeitsbereiche:

- Bischöfliches Generalvikariat, das Bischöfliches Offizialat, die Kanzlei der Kurie, die Diözesanstelle Weltkirche, die Geschäftsstelle der diözesanen Arbeitsgemeinschaften der Mitarbeitervertretungen (DiAG), das Büro des Bischofs und die Büros der Weihbischöfe sowie die Katholischen Büros in Mainz und Saarbrücken,
- die Bildungshäuser, Fachstellen für Erwachsenenbildung, Priesterhaus St. Thomas, Diözesanstelle für Exerzitien, geistliche Begleitung und Berufungspastoral, Fachstellen für Erwachsenenbildung,
- die Fachstellen für Jugendpastoral, Fachstellen für Kirchenmusik, Schülerzentren, Häuser der offenen Tür, Katholische Hochschulgemeinden Koblenz, Saarbrücken und Trier, das Johannes-Foyer Saarbrücken
- und die Schulen in Trägerschaft des Bistums Trier.