Bischöfliches Generalvikariat Trier
Stabsstelle Betrieblicher Datenschutz

Daten schützen?
Aber sicher!

BISTUM
TRIER

Bischöfliches Generalvikariat Trier
Stabsstelle Betrieblicher Datenschutz

Datenschutz im Bistum Trier

Die haupt- und ehrenamtlichen Mitarbeiterinnen und Mitarbeiter in allen Einrichtungen und Dienststellen im Bistum Trier tragen die Verantwortung für den kirchlichen Datenschutz! Für die Umsetzung der rechtlichen Anforderungen sind die Fachvorgesetzten und 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. In der Summe entsteht so aus einer gesteigerten allgemeinen Sensibilität zur Verantwortung um den Datenschutz zusammen mit den hierfür, von den verantwortlichen Stellen und Personen, getroffenen Maßnahmen, gelebter Datenschutz.

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

Neues zum Datenschutz: Gut zu wissen!

Der kirchliche Datenschutz bekommt **eine neue Rechtsgrundlage**:
Das neue Gesetz über den Kirchlichen Datenschutz (KDG) wird am 24. Mai 2018 durch Bischof Dr. Stephan Ackermann in Kraft gesetzt und löst unsere bisherige Anordnung über den kirchlichen Datenschutz (KDO) ab!
Achten Sie bitte auf die Bekanntmachung am 1. April 2018 im Kirchlichen Amtsblatt (KA 2018 Nr. 65).

Die Durchführungsverordnung zur KDO und die IT-Richtlinien behalten übergangsweise ihre Gültigkeit. 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.

Neues Gesetz
ab 24. Mai 2018

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)*

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

Noch intensiveren Schutz genießen die besonderen personenbezogenen Daten (Datenschutzklasse 3), wie z. B. rassische und ethnische Herkunft, Gesundheitsdaten oder Daten zum Sexualleben, politische Meinungen, religiöse Überzeugung, etc. *(§ 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
Worum es geht!

Wie stark müssen wir schützen?

Daten werden in 3 Schutzklassen (je nach Risiko) eingeteilt:
(vgl. KDO/DVO, Anlage 2 zu § 6 KDO (KA 2016 Nr. 193) i.V.m. den IT Richtlinien (KA 2016 Nr. 194)

1

Datenschutzklasse 1
z. B. Adressen die so auch in Telefonbüchern oder anderen öffentlichen Quellen stehen, etc.

2

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

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 etc.

Je nach Datenschutzklasse sind die technischen und organisatorischen Maßnahmen, dem Schutzzweck angemessen, zu intensivieren. In Zweifelsfällen fragen Sie bitte Ihre Betriebliche Datenschutzbeauftragte oder Ihren Betrieblichen Datenschutzbeauftragten (Kontaktdaten über die Stabsstelle).

Datenschutzklassen

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 die ursprünglich und eindeutig festgelegten Zwecke** erhoben werden!

3. **Datensparsam arbeiten:** so wenig Daten wie möglich – so viel wie nötig!

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, die die Einhaltung der datenschutzrechtlichen Vorgaben gewährleisten.

Datensicherheit
Unsere Ziele!

Neues zum Datenschutz: Gut zu wissen!

✕ Das neue Gesetz verpflichtet auch dazu, alle Mitarbeiterinnen und Mitarbeiter zu sensibilisieren und zu schulen. **Die Schulung der hauptamtlichen Mitarbeitenden wird online organisiert und ist über einen Nachweis in der Personalakte zu belegen.** Führungskräfte und Fachvorgesetzte werden darüber hinaus gezielt geschult und informiert. Bitte achten Sie auf kommende Hinweise zur Online-Schulung und weitere Informationsveranstaltungen zum Thema Datenschutz. Die ehrenamtlichen Mitarbeiterinnen und Mitarbeiter werden über die Pfarrbüros informiert. *(§ 7 i.V.m. § 38 KDG)*

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

✕ Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine **angemessene Sicherheit** gewährleistet. Wir haben hierbei auch den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, Zerstörung oder Schädigung der Daten im Blick. *(§§ 26–30 KDG)*

Neues zum Datenschutz: Gut zu wissen!

✕ 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)*

✕ Der Bußgeldrahmen wird durch das KDG erhöht und beträgt je nach Schwere des Verstoßes unter Umständen bis zu 500.000 €. *(§ 51 KDG)*

✕ 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**, erhalten sie von der Stabsstelle Betrieblicher Datenschutz. Rückgabefrist ist der 31. Dezember 2018. *Beachten Sie bitte die hierzu ergehenden Hinweise der Stabsstelle an die Dienststellenleitungen innerhalb des Organisationserlasses des Bischöflichen Generalvikariates (vgl. hierzu die Bestimmung der Dienststellenleitungen durch Herrn Generalvikar Dr. Graf von Plettenberg: Juni 2017 ff.). (§ 31 KDG und § 3a KDO i.V.m. KDO-DVO (KA 2016 Nr. 193) sowie IT-Richtlinien (KA 2016 Nr. 194)*

✕ Verträge zur Auftragsdatenverarbeitung sind bis zum 31. Dezember 2019 der neuen Gesetzgebung anzupassen! *(§ 57 KDG)*

Neues zum Datenschutz: Gut zu wissen!

✕ Datenpannen (Verlust, Offenlegung der Daten oder Fremdzugriff) müssen unverzüglich (innerhalb von 72 Stunden nach Bekanntwerden) der/dem Verantwortlichen der Überdiözesanen Aufsichtsstelle (gemeinsame Datenschutzstelle in Frankfurt) und der Stabsstelle Betrieblicher Datenschutz gemeldet werden *(siehe Kontaktdaten)*. *(§§ 33, 34 KDG)*

✕ Die Meldung an die Überdiözesane Aufsichtsstelle (Datenschutzaufsicht) hat immer zu erfolgen, wenn die Datenschutzverletzung eine Gefahr für die Rechte und Freiheiten des/der Betroffenen darstellt.

✕ Verantwortlich für die Meldung ist im hauptamtlichen Bereich zunächst die Dienstellenleitung bzw. die/der Fachvorgesetzte, deren/dessen Stellvertreter/in bzw. der/die verantwortliche Mitarbeiter/in. Im ehrenamtlichen Bereich ist der Verantwortliche der Pfarrer des Bereichs, 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 Gebäude:

- ✓ 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.

Im Gebäude

Am Arbeitsplatz, im Home Office, am Telefon, auf dem Flur, ... :

- ✓ Keine unbefugten Personen alleine im Büro lassen.
- ✓ Keine sensiblen Unterlagen bei eigener Abwesenheit offen auf dem Schreibtisch liegen lassen.
- ✓ Ausdrucke direkt am Kopierer oder Drucker abholen.
- ✓ Sensible Unterlagen und Akten nach Beendigung der Tätigkeit in verschlossenen Schränken aufbewahren.
- ✓ Wenn die Gesprächspartnerin oder der Gesprächspartner 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 Büro

Datenschutz gilt immer und gleichermaßen für haupt- und ehrenamtliche Mitarbeitende, egal wo und bei welcher Tätigkeit.

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. 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.

- ✓ Immer dann, wenn Sie ein hohes Risiko für die Rechte und Freiheiten der Betroffenen befürchten, z. B. vor der Verwendung neuer Technologien (neue Software etc.), besteht die Verpflichtung zu einer Datenschutz-Folgenabschätzung durch die verantwortliche Stelle. Im Zweifelsfall kontaktieren Sie bitte die Stabsstelle Betrieblicher Datenschutz.

Technik

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. Leisten Sie keiner Aufforderung „bitte klicken“ Folge.

In Zweifelsfällen im Umgang mit Technik, Software und E-Mail-Verkehr ist der **ZB 2.7 Abteilung Informationssysteme** der richtige Ansprechpartner für Sie:

helpdesk@bgv-trier.de
Telefon (06 51) 7105-123

Vor der Erhebung von Daten:

- ✓ Klären Sie die Rechtsgrundlage: Gibt es eine Rechtsvorschrift und/oder eine Einwilligung der Betroffenen? *(§§ 6 – 8 KDG)*
- ✓ Legen Sie die Zweckbestimmung fest: Welche Daten brauche ich wofür? *(§§ 6 – 8 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)*
- ✓ 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.
- ✓ Senden Sie nur die Daten und Informationen, die die Empfängerin oder der Empfänger 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 Mitarbeiterin und Mitarbeiter in Ihrem Tun.
- ✓ Geben Sie Unterlagen und Daten nur weiter, wenn es erlaubt ist, und geben Sie keine Daten an unbefugte Dritte.

Daten weitergeben

✓ 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.
- Keine Kommunikation per E-Mail wenn besondere personenbezogene Daten (Datenschutzklasse 3) enthalten sind.

✓ Beim Versand einer E-Mail an große Empfängerkreise gehören die Empfängeradressen alle in das bcc-Feld und die eigene E-Mail-Adresse ins Empfängerfeld. Geben Sie eine aufschlussreiche Betreffzeile an.

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 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 etc.) gehören in die „silbernen Tonnen" oder in einen abgeschlossenen Container und werden einer professionellen Löschung zugeführt.

Daten löschen

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 erfragen bei der

Stabsstelle Betrieblicher Datenschutz
Mustorstraße 2, 54290 Trier
datenschutz@bgv-trier.de, Telefon (06 51) 7105-468

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

Überdiözesane Aufsichtsstelle im Datenschutz der (Erz-)Diözesen Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier:
Gemeinsame Datenschutzstelle
Diözesandatenschutzbeauftragte: Ursula Becker-Rathmair
Haus am Dom, Domplatz 3, 60311 Frankfurt
info@kdsz-ffm.de, Telefon (0 69) 8 00 87 18-0

Kontakte

BISTUM
TRIER

Impressum

Bischöfliches Generalvikariat Trier
Stabsstelle Betrieblicher Datenschutz
Mustorstraße 2, 54290 Trier
datenschutz@bgv-trier.de
Telefon (06 51) 7105-468

Redaktion
Ursula Eiden (Betriebliche Datenschutzbeauftragte für den Bereich des Bischöflichen Generalvikariates und die folgenden Dienststellen: Bischöfliches Offizialat, Diözesanstelle Weltkirche, Geschäftsstelle der diözesanen Arbeitsgemeinschaften der Mitarbeitervertretungen, das Büro des Bischofs, die Büros der Weihbischöfe, die Katholischen Büros in Mainz und Saarbrücken, sowie die Schulen in Trägerschaft des Bistums Trier)

Stand April 2018
Diese Informationsschrift ist beispielhaft und erhebt keinen Anspruch auf Vollständigkeit.