Diözese ROTTENBURG-STUTTGART
Stabsstelle Datenschutz

Daten schützen? – Aber sicher!

Datenschutz in der Diözese Rottenburg-Stuttgart

Die haupt- und ehrenamtlichen Mitarbeiterinnen und Mitarbeiter in allen Einrichtungen und Dienststellen in der Diözese Rottenburg-Stuttgart 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!
„Niemand darf den guten Ruf, den jemand hat, rechtswidrig schädigen und das Recht einer jeden Person auf den Schutz der eigenen Intimsphäre verletzen."

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. Aus einer gesteigerten allgemeinen Sensibilität zur Verantwortung um den Datenschutz und den, von den verantwortlichen Stellen und Personen, getroffenen Maßnahmen, entsteht so ein 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) wurde zum 24. Mai 2018 durch Bischof Dr. Gebhard Fürst in Kraft gesetzt und löst unsere bisherige Anordnung über den kirchlichen Datenschutz (KDO) ab!

Achten Sie bitte auf die Bekanntmachung vom 5. März 2018 im Kirchlichen Amtsblatt (Sonderdruck KDG, KABl. Nr.4/2018).
Diese finden Sie auf www.drs.de/service/kirchliches-Amtsblatt.html

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. Dies ist jedoch zum Teil, beispielsweise bei der Veröffentlichung von Fotoaufnahmen, der Fall. Hier geht das KDG dem Kunsturhebergesetz vor. Dies bedeutet, dass die Zustimmung sowohl zur Aufnahme des Bildes, als auch zur Veröffentlichung des Bildes zuvor bei den betroffenen Personen eingeholt werden muss.

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 in der Diözese Rottenburg-Stuttgart.

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 nicht zur Datenschutzklasse 3.

Wie stark müssen wir schützen?

Daten werden in 3 Schutzklassen (je nach Risiko) eingeteilt:

Datenschutzklasse 1
Zur Datenschutzklasse 1 gehören z.B. Adressangaben, die so auch in Telefonbüchern oder anderen öffentlichen Quellen stehen, sowie z.B. dort auffindbare Berufs-, Branchen- oder Geschäftsbezeichnungen, etc.

Datenschutzklasse 2
Zur Datenschutzklasse 2 gehören z.B. Daten über Beschäftigungsverhältnis, Kontaktdaten von haupt- und ehrenamtlichen Mitarbeitenden, z. B. Handynummer, Vertragsdaten, Mietverhältnisse, etc.

Datenschutzklasse 3
Zur Datenschutzklasse 3 gehören 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. Die Abwägung, um welche schutzwürdigen Daten es sich bei der Bearbeitung eines Arbeitsvorgangs handelt, muss im Einzelfall getroffen werden. In Zweifelsfällen erkundigen Sie sich bitte bei der Stabsstelle Datenschutz (Betriebliche Datenschutzbeauftragte).

Um Arbeitsvorgänge kategorisieren zu können, sieht das KDG vor, dass **ein Verzeichnis der Verarbeitungstätigkeiten** erstellt wird. Die Stabsstelle Datenschutz wird Ihnen hierfür einen Vordruck „Verfahrensbeschreibung/ Beschreibung der Verarbeitungstätigkeit“ zukommen lassen, über den Sie die Prozesse zu den Arbeitsabläufen in Ihren Zuständigkeitsbereichen beschreiben müssen. Sie werden hierzu weiter informiert. Die Verzeichnisse von Verarbeitungstätigkeiten müssen bis zum **30.06.2019** erstellt werden. (§ 57 Abs. 4 KDG)

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, es sei denn, es liegt ein Fall des § 6 Abs.2 KDG vor (wenn insbesondere „der Auftrag der Kirche oder die Glaubwürdigkeit ihres Dienstes dies erfordern“).

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 dabei alle technischen und organisatorischen Maßnahmen, die die Einhaltung der datenschutzrechtlichen Vorgaben gewährleisten.

Schulungen und Informationsrechte zum Datenschutz

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.** Diese Online-Schulung wird ab Herbst 2018 stattfinden. Bitte achten Sie auf kommende Hinweise zur Online-Schulung und weitere Informationsveranstaltungen zum Thema Datenschutz.

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)

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

Verstöße gegen den Datenschutz – Datenpannen

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 Auftragsdatenverarbeiter. (§ 50 KDG)

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

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.

Datenschutz konkret: Tipps und Hinweise

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.

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

- ✓ 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; im Zweifelsfall keine personenbezogenen Daten am Telefon mitteilen.
- ✓ In Gesprächen Vertraulichkeit gewährleisten:
  ohne Einverständnis kein Mithören von Dritten ermöglichen.
- ✓ Personenbezogene Daten gehören nicht in öffentliche Foren!

Datenschutz gilt immer und gleichermaßen für haupt- und ehrenamtlich 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 in der Diözese Rottenburg-Stuttgart ist uns nicht erst seit dem 24.5. wichtig! => Passwort: #DidDRSiunesd24.5.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 Datenschutz.

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 Zentrale Benutzerservice der IT-Abteilung bzw. das Intranet-Technik-Team (Service-Hotline) der richtige Ansprechpartner für Sie:

für das Bischöfliche Ordinariat:
hotline@bo.drs.de
Telefon (07472) 169-777

für Kirchengemeinden und diözesane Einrichtungen:
service@drs.de
Telefon: (07472) 169-961

Der Umgang mit Daten gehört zu sämtlichen Arbeitsprozessen, die wir in unserem Arbeitsalltag erfüllen. Machen Sie sich bewusst, wo Sie mit Daten arbeiten, was Sie beim Umgang mit diesen Daten beachten müssen und für was bzw. wie Sie diese Daten verwenden dürfen. Folgende Hinweise können Ihnen beider Prüfung hilfreich sein:

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)

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.
- ✓ Prüfen Sie kritisch, ob die Inhalte in einer E-Mail versendet werden können. Eine ungesicherte E-Mail ist offener als eine Postkarte. Nutzen Sie hier den sicheren Versand über das Secure-Mail-Gateway, sofern Ihre E-Mail schützenswerte Daten enthält. (Weitere Informationen finden Sie unter https://sensus.drs.de/smg)
- ✓ Beim Versand einer E-Mail an große Empfängerkreise gehören die Empfängeradressen alle in das „BCC“-Feld (Blindkopie) 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 Diözesanarchiv hinzu und bieten Sie diese Unterlagen vor einer Vernichtung/Löschung dem Diözesanarchiv an. Gemäß § 6 der Kirchlichen Archivordnung (KABl. Nr 4/2014, S. 123) besteht eine Anbietungspflicht für alle Unterlagen.
  Kontakt: Diözesanarchiv, dar@bo.drs.de, Telefon (07472) 169-254
- ✓ 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/Personalkatalog etc.) gehören in die „silbernen Tonnen“ oder in einen abgeschlossenen Container und werden einer professionellen Löschung zugeführt.

Hilfe? Hilfe!

Die Stabsstelle Datenschutz im Bischöflichen Ordinariat befindet sich derzeit noch im Aufbau. Die Betrieblichen Datenschutzbeauftragten stehen Ihnen gerne beratend und unterstützend bei allen datenschutzrechtlichen Fragen und Anregungen zur Seite. Sie wirken auf die Einhaltung der Vorschriften über den Datenschutz im verfassten Bereich der Diözese Rottenburg-Stuttgart hin. Zu diesem Zweck beraten sie die Einrichtungsleitung und die Beschäftigten, informieren über und kontrollieren die Einhaltung der datenschutzrechtlichen Vorgaben und stehen als Ansprechpartner bei datenschutzrechtlichen Fragestellungen zur Verfügung.

Stabsstelle Datenschutz

Bischöfliches Ordinariat
Stabsstelle Datenschutz
Postfach 9
72101 Rottenburg
Tel: 07472 169-890
Fax: 07472 169-83890
E-Mail: datenschutz@bo.drs.de

Überdiözesane Aufsicht

Um die Einhaltung der datenschutzrechtlichen Bestimmungen nach dem Gesetz über den Kirchlichen Datenschutz (KDG, veröffentlicht im KABl. Nr. 4/2018) zu gewährleisten, wurde zum 1. Januar 2018 die gemeinsame Diözesandatenschutzbeauftragte der Diözesen Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier bestellt. Die Überdiözesane Aufsicht überwacht die Einhaltung der datenschutzrechtlichen Bestimmungen.

Katholisches Datenschutzzentrum Frankfurt/M
Frau Ursula Becker-Rathmair
Haus am Dom
Domplatz 3
60311 Frankfurt
Tel.: 069 800871-8800
Fax: 069 800871-8815
E-Mail: info@kdsz-ffm.de
Internet: http://kdsz-ffm.de oder http://kdsz-ffm.bistumlimburg.de

Weitere Informationen erhalten Sie unter:
www.katholisches-Datenschutzzentrum.de
www.datenschutz-kirche.de

Impressum

Bischöfliches Ordinariat der Diözese Rottenburg-Stuttgart
Stabsstelle Datenschutz

Diese Information wurde in Anlehnung an eine Informationsschrift der Betrieblichen Datenschutzbeauftragten für den Bereich des Bischöflichen Generalvikariates Trier erstellt (Stand April 2018). Wir danken Frau Ursula Eiden für die freundliche Genehmigung der Nutzung ihrer Vorlage.

Stand Mai 2018

Diese Informationsschrift ist beispielhaft und erhebt keinen Anspruch auf Vollständigkeit.