

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 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**

## Neues zum Datenschutz: Gut zu wissen!

Der kirchliche Datenschutz hat **eine neue Rechtsgrundlage** bekommen:  
**Das neue Gesetz über den Kirchlichen Datenschutz (KDG)** wurde am 24. Mai 2018 durch Bischof Dr. Stephan Ackermann in Kraft gesetzt und löste unsere bisherige Anordnung über den kirchlichen Datenschutz (KDO) ab!

*Die Bekanntmachung hierzu finden Sie im Kirchlichen Amtsblatt (KA 2018 Nr. 65).*

**Neues Gesetz**  
seit 24. Mai 2018

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.

## Neue Durchführungsverordnung seit 1. März 2019

Am 1. März 2019 wurde die neue Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) in Kraft gesetzt.

*Die Bekanntmachung hierzu finden Sie im Kirchlichen Amtsblatt (KA 2019 Nr. 9).*

**Neue DVO**  
seit 1. März 2019

## 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 Mitarbeiterinnen und Mitarbeiter 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**  
Worum es geht!

## 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. In Zweifelsfällen fragen Sie bitte Ihre Betriebliche Datenschutzbeauftragte oder Ihren Betrieblichen Datenschutzbeauftragten (Kontaktdaten über die Stabsstelle).*

# 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 festgelegten Zwecke** erhoben werden!
3. **Datensparsam arbeiten:** so wenige Daten wie möglich, so viele Daten wie nötig!



Grundsätze



## **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!

## 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 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).
- ✘ 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).

## Neues zum Datenschutz: Gut zu wissen!

### Recht auf Auskunftserteilung (§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 transparente Information **innerhalb eines Monats nach Eingang des Antrags aus Auskunft**. Auf Verlangen informieren wir **schriftlich** darüber, welche personenbezogenen Daten des Antragstellers zu welchem Zweck verarbeitet werden.
- ✘ Achten Sie vor der Auskunftserteilung auf einen **Identitätsnachweis** der betroffenen Person. Falls erforderlich ist eine **Fristverlängerung** um weitere zwei Monate **möglich**. Die Gründe der Verzögerung sind darzulegen.

# Neues zum Datenschutz: Gut zu wissen!

## Informationspflicht vor der Datenerhebung (§§ 15 und 16 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).

### 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

## 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.

*Beachten Sie bitte die hierzu ergehenden Hinweise der Stabsstelle an die Einrichtungen und Dienststellenleitungen (§ 31 KDG i.V.m. § 1 KDG-DVO).*

# Neues zum Datenschutz: Gut zu wissen!

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

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

✘ **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.**

Beispiele für Auftragsverarbeitung sind: *Rechenzentren, externe Personalagenturen (Leiharbeit), externe Agenturen (Headhunter, Assessment-Center), externe Dienstleister mit „Remote-Zugriff“ (Server, Wartungsverträge, Softwarepflege), externe Dienstleister für Peripherie-Geräte (Fax, Drucker, Multifunktionsgeräte, Scanner, Kopierer), Entsorger (IT, TK, Aktenentsorgung), externe Berater mit Zugriff auf Software und personenbezogene Daten, externe Reinigungsdienste, Internet-Service-Provider (Fremdsoftware als Dienstleistung).*

*Auf Anfrage erhalten Sie Unterstützung durch die Stabsstelle Betrieblicher Datenschutz.*

## Neues zum Datenschutz: Gut zu wissen!

- ✘ Datenpannen (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 die Stabsstelle Betrieblicher Datenschutz gemeldet (§§ 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 Dienststellenleitung, deren/dessen Stellvertreter/in bzw. der/die verantwortliche Mitarbeiter/in. Im ehrenamtlichen Bereich ist der Verantwortliche der Pfarrer bzw. der/die 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 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.
- ✓ Ausdrücke 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 24.5.2018 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.

### Im Umgang mit der Technik:

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

- ✓ 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 aus seiner Sicht die Risiken 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 Person**

- eine Diskriminierung verursachen könnte;
- eine 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 seiner Daten zu kontrollieren;
- Persönlichkeitsprofile unter Verwendung besonderer Kategorien personenbezogener Daten erstellt;
- Daten schutzbedürftiger Personen, insbesondere Kinder verarbeitet;
- 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 Stabsstelle Betrieblicher 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 **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)?
- ✓ 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, welche 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 dann weiter, wenn es erlaubt ist, und geben Sie **keine Daten an unbefugte Dritte.**
- ✓ Achten Sie beim Versand darauf, dass Sie als Absender mit Adresse für den Zusteller erkennbar sind. So vermeiden Sie, dass die Postsendung im Falle von Unzustellbarkeit, geöffnet werden muss.

**Daten weitergeben**

## Datenschutz konkret: Tipps und Hinweise



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.



Beim Versand einer E-Mail an große Empfängerkreise außerhalb des gesicherten Netzwerkes gehören alle Empfängeradressen 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](mailto: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) 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.

### **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 die Sie betreffenden personenbezogenen Daten offengelegt wurden, diese Berichtigung oder Löschung der Daten 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)

Über Entscheidungen zu den von Ihnen geltend gemachten Rechten werden Sie regelmäßig schriftlich informiert. Von der Möglichkeit automatisierter Entscheidungen, die im Einzelfall zulässig wären, machen wir keinen Gebrauch.



## **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

Haus am Dom, Domplatz 3, 60311 Frankfurt

info@kdsz-ffm.de, Telefon (0 69) 8 00 87 18-800

**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 erfragen bei der

### **Stabsstelle Betrieblicher Datenschutz**

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

[datenschutz@bgv-trier.de](mailto:datenschutz@bgv-trier.de)

[datenschutz-pfarreien@bgv-trier.de](mailto:datenschutz-pfarreien@bgv-trier.de)

[datenschutz-lebensberatung@bgv-trier.de](mailto:datenschutz-lebensberatung@bgv-trier.de)

[datenschutz-telefonseelsorge@bgv-trier.de](mailto:datenschutz-telefonseelsorge@bgv-trier.de)



Weitere Informationen finden Sie auch unter:

**[www.bistum-trier.de/datenschutz](http://www.bistum-trier.de/datenschutz)**

**Kontakte**



# BISTUM TRIER

## Impressum

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

## 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 Mai 2019

*Diese Informationsschrift ist beispielhaft und erhebt keinen Anspruch auf Vollständigkeit.*