Merkblatt Datenschutz

I. Für ehrenamtlich Mitarbeitende, die mit personenbezogene Daten zu tun haben

Im Rahmen Ihrer Tätigkeit arbeiten Sie mit personenbezogenen Daten z. B. unserer Mitglieder, Mitarbeitenden und Geschäftspartnerinnen und -partner oder es gibt für Sie die Möglichkeit des Zugriffs auf solche Daten. Deshalb müssen Sie sich mit den wichtigsten Grundsätzen des Datenschutzes vertraut machen.

(1) Die wichtigste Grundlage für den Datenschutz bei uns ist das KDG. Das kirchliche Datenschutzgesetz schützt **personenbezogene Daten**. Das sind alle Informationen, die sich auf einen identifizierten oder identifizierbaren Menschen („natürliche Person“) beziehen, wie z.B. Geburtsdatum, Anschrift. Anonyme Daten fallen nicht unter das Datenschutzgesetz.
„Sensible“ Daten, z.B. Gesundheitsdaten, Straftaten u.a., sind besonders schützenswert.

(2) **Geschützt wird das informationelle Selbstbestimmungsrechts jedes Einzelnen**: Jeder soll grundsätzlich selbst darüber bestimmen dürfen, wer welche Daten über ihn kennt und verarbeitet. Deshalb dürfen personenbezogene Daten nur verarbeitet werden, wenn hierfür eine „Erlaubnis“, eine sogenannte Rechtsgrundlage, vorliegt. Personenbezogene Daten dürfen nur zweckbezogen verarbeitet werden.

(3) Häufig verwendete **Rechtsgrundlagen für die Datenverarbeitung** sind:
- zur Erfüllung eines Gesetzes, z.B. 10-jährige Aufbewahrungsfrist von Rechnungen gemäß AO.
- zur Erfüllung eines Vertrags, z. B. Mietvertrag des Gemeindesaals;
- zur Erfüllung einer Aufgabe, die im kirchlichen Interesse liegt, z.B. Einladung zur Gebetswache oder
- die **Einwilligung** der betroffenen Person, z.B. Einwilligung zum Erhalt eines Newsletters. Die Erteilung der Einwilligung ist immer freiwillig. Der Betroffene darf nicht benachteiligt werden und kann die Einwilligung jederzeit widerrufen.

(4) Die Transparenz der Datenverarbeitung ist eine wichtige Voraussetzung für das informationelle Selbstbestimmungsrecht. Es besteht eine Informationspflicht gegenüber der betroffenen Person. Bei Erhebung der Daten oder beim erstmaligen Kontakt muss die Person umfassend mit einem **Datenschutzhinweis** informiert werden.

(5) Bei Vorliegen der gesetzlichen Voraussetzungen stehen jeder betroffenen Person die **Betroffenenrechte** zu. Diese sind die Rechte auf Auskunft, Berichtigung, Löschung, Beschränkung der Verarbeitung, Widerspruch gegen die Verarbeitung und Datenübertragbarkeit, sowie ein Recht auf Beschwerde bei der Datenschutzaufsichtsbehörde.

(6) Verarbeitete Daten, wie z.B. Adresslisten, Email-Verteiler, sind zu **löschen**, sobald der Zweck erfüllt ist. Längere Aufbewahrungsfristen aufgrund von gesetzlichen Regelungen sind zu beachten.

(7) Schließlich müssen die Personen, von welchen wir Daten verarbeiten, darauf vertrauen können, dass ihre personenbezogenen Daten bei uns sicher sind. Datenschutz und Datensicherheit haben zwei wichtige Grundlagen: eine persönliche und eine technische.

Persönlich müssen Sie als ehrenamtliche/r Mitarbeitende/r die Vertraulichkeit der Verarbeitung beachten, zu der Sie sich umseitig verpflichtet haben.

Bitte beachten Sie, dass ein **Verstoß gegen die datenschutzrechtlichen Bestimmungen** ein Verstoß gegen rechtliche Pflichten darstellt, der entsprechend geahndet werden kann. Dies kann bei vorsätzlichem oder grob fahrlässigem Handeln zu Geldbußen, Geldstrafen oder gar Freiheitsstrafen führen. Entsteht der betroffenen Person durch die unbefugte Verarbeitung ein Schaden, kann ebenfalls ein Schadensersatzanspruch entstehen.

Technisch und organisatorisch muss die Datensicherheit durch geeignete und angemessene Maßnahmen (**TOM**) sichergestellt werden. Personenbezogenen Daten sind gegen zufällige oder vorsätzliche Manipulationen, Verlust, Zerstörung oder gegen den Zugriff unberechtigter Personen zu schützen. Ebenso ist der Schutz der Rechte der betroffenen Personen und die Einhaltung der anwendbaren datenschutzrechtlichen Bestimmungen zu gewährleisten.

(8) Helfen Sie dabei, die Ihnen anvertrauten personenbezogenen Daten zu schützen. Gehen Sie weisungsgemäß und sorgfältig damit um. **Melden Sie verdächtige Beobachtungen und Datenschutz- oder Datensicherheitsverletzungen** Ihrem/r Verantwortlichen.

(9) **Schulungsangebote**, gesetzliche Grundlagen (KDG, KDG-DVO), Mustervorlagen und weiterführende Informationen finden Sie unter www.ebfr.de/datenschutz oder wenden Sie sich an Ihre/n betriebliche/n Datenschutzbeauftragte/n.

II. Für ehrenamtlich Mitarbeitende, die personenbezogene Daten zusätzlich digital verarbeiten:

(1) Die Nutzung von Telefax, E-Mail, Internet/Intranet sowie sonstiger im Rahmen meines Auftrages zur Verfügung gestellter dienstlicher Hard- und Software für private Zwecke ist nicht zulässig.

(2) Die Verarbeitung personenbezogener Daten auf privaten IT-Systemen zu Aufgaben i.Z. mit dem Ehrenamt ist grundsätzlich unzulässig. Sie kann gem. § 20 der Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) als Ausnahme von dem Verantwortlichen unter Beachtung der jeweils geltenden gesetzlichen Regelungen zugelassen werden.

III. Praktische Hinweise im Umgang mit der Verarbeitung von personenbezogenen Daten im Alltag:

Diese praktischen Hinweise dienen der allgemeinen Unterstützung im Umgang mit der Verarbeitung von personenbezogenen Daten im Alltag für ehrenamtlich Mitarbeitende. Die Hinweise können nicht vollständig sein, geben jedoch einen grundlegenden Rahmen.

Bei allen Fragen rund um IT-Sicherheit wenden Sie sich bitte an Ihren zuständigen IT-Ansprechpartner.

(1) Zweckbindung
- Die Datenverarbeitung ist zweckgebunden. Eine Zweckänderung bedarf im Einzelfall einer neuen Rechtsgrundlage.
- Personenbezogene Daten dürfen nur in besonderen Fällen für andere Zwecke verarbeitet werden (§ 6 Abs. 2 KDG), z.B. dürfen Kommunionkinder-Adressen nicht an die Ferienlagerleitung weitergegeben werden; Helferlisten dürfen nicht für eine Tupperparty-Einladung verwendet werden etc.

(2) Zugang zu PC/ Laptop
- Der Zugang zu den PCs oder Laptops muss über ein Passwort geschützt sein. Bitte beachten Sie die jeweils aktuelle Empfehlung der Diözesanen IT.
- Speichern Sie keine Passwörter in Ihrem Browser ab.
- Passwörter dürfen nicht auf Notizzetteln oder ähnlichem aufgeschrieben werden.
- Wird der PC von mehreren Personen oder Gruppen benutzt, ist darauf zu achten, dass jeder nur die Programme und Daten benutzen kann, die für seine Arbeit erforderlich sind.
- Nach Möglichkeit sollten sich Monitore nach einer bestimmten voreingestellten Zeit abschalten (Bildschirmschoner).

(3) E-Mail
- Vor dem Versenden Adressat prüfen.
- Bcc nutzen, wo immer möglich.
- E-Mails mit Daten der Datenschutzklassen II (z.B. Daten über Mietverhältnisse und Geburts- und Jubiläumsdaten) und III dürfen nur mit einer Ende-zu–Ende-Verschlüsselung übertragen werden.

(4) Telefon
- Schutz vor Mithören sicherstellen.

(5) Datenverwaltung
- Akten und Datenträger (USB-Sticks, CD's, externe Festplatten und andere Speichermedien), die personenbezogene Daten beinhalten, sind in verschließbaren Räumen, Schränken, Behältern aufzubewahren.
- Unbefugte dürfen keine Einsicht in Akten und Datenträger nehmen.
- Mobile Datenträger sind zu verschlüsseln.

(6) Schriftgutverwaltung
- Papierakten mit personenbezogenen Daten nie im normalen Müll entsorgen.
- Geheimhaltungsbedürftige Dokumente verschlüsseln oder per Post senden.