

Informationen zum Datenschutz für KAB-Bezirke und Ortsgruppen



Um Ihnen – den KAB-Verantwortlichen in den Bezirken und Ortsgruppen – den Umgang mit den Bestimmungen des Datenschutzes zu erleichtern und gleichzeitig der Verantwortung für den (kirchlichen) Datenschutz Rechnung zu tragen, haben wir im Folgenden wichtige Informationen und Regeln zusammengefasst.

Grundsätzliches

Bei allen Änderungen und Neuerungen ist uns wichtig hervorzuheben: Sie sind in Ihrer täglichen Praxis bereits verantwortungsvoll, sensibel und sorgsam mit personenbezogenen Daten umgegangen. Die bislang gültige Kirchliche Datenschutzordnung (KDO) ist durch das Kirchliche Datenschutzgesetz (KDG) am 24. Mai 2018 abgelöst worden. Das KDG hat einige Regeln verschärft und ist eng an die Europäische Datenschutzgrundverordnung (EU-DSGVO) angelehnt. Sie sind streng – aber machbar.

Datenschutz – worum 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. Dazu gehören die typischen Daten der Mitglieder (Name, Geburtsdatum, Beruf, Familienstand, Adresse, E-Mail, Kontoverbindung). Aber auch Daten von TeilnehmerInnen an Veranstaltungen, Referenten oder sonstiger Personen. Ebenso zählen Fotos zu den personenbezogenen Daten.

Guter Datenschutz schützt nicht nur die betroffenen Personen, deren Daten Ihnen anvertraut sind, sondern auch uns alle, die Ehren- und/oder Hauptamtlich in der KAB tätig sind.

Datenschutz konkret: Tipps und Hinweise

Grundsatz der Datensicherheit - Personenbezogene Daten müssen besonders geschützt werden!

- Verwenden Sie nur verschlüsselte Laufwerke – bewahren Sie das Notebook an einem sicheren Ort auf.
- Benutzen Sie keine Sticks zum Speichern oder Weitergeben von Daten – ist die Nutzung von Sticks nicht vermeidbar, dann verwenden Sie Sticks mit Verschlüsselung (Empfehlung: SanDisk Extreme 500).
- Die Personengruppe, die personengebundene Daten bearbeiten oder verwalten, sollte so klein wie möglich sein (z.B. Vorsitzender, Stellvertreter und Kassier).
- Es dürfen nur die Daten erhoben werden, deren Kenntnis zur Aufgabenerfüllung notwendig sind. Hierzu gehören im Besonderen: Name und Anschrift zur Identifikation des Mitglieds; Kontoverbindung, soweit sie für Zahlungsvorgänge benötigt werden.

Am Arbeitsplatz zu Hause, am Telefon, in offenen Räumen...

- Wer Umgang pflegt mit personenbezogenen Daten hat eine Verschwiegenheitspflicht! Keine sensiblen Unterlagen bei eigener Abwesenheit offen auf dem Schreibtisch liegen lassen und diese 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.

E-Mail-Kommunikation...

- ... ist nicht datensicher. Daher dürfen keine personenbezogenen Daten per Mail versandt werden.
- Prüfen Sie kritisch, ob die Inhalte in einer E-Mail versendet werden können. Eine ungesicherte E-Mail ist offener als eine Postkarte.
- Senden Sie nur die Daten und Informationen, die die Empfängerin oder der Empfänger für die Weiterverarbeitung benötigt.
- Das Versenden von Mails an mehrere Personen gleichzeitig immer als „Blindkopie“ („bcc“) – der Empfänger darf nicht sehen, wer sonst noch die Mail bekommen hat (es sei denn, eine schriftliche Zustimmung liegt vor).

Wesentliches im Umgang mit Teilnehmerlisten und Fotos

- Wenn Sie bei Ihren Veranstaltungen Teilnehmerlisten auslegen, dann gilt auch hier der Grundsatz „so wenig wie möglich“. Wichtig ist, dass die Namen zuordenbar sind. Auf TN-Listen sollten lediglich der Familienname und ggf. mit der erste Buchstabe des Vornamens vermerkt sein – keine Adresse, kein Geburtsdatum.
- Sobald jemand auf Fotos erkennbar abgebildet ist, muss vor Veröffentlichung des Fotos die Zustimmung eingeholt werden. Vor einer Veranstaltung muss auf eventuelles Fotografieren hingewiesen werden.

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!).
- Sperren Sie bei Abwesenheit Ihren Bildschirm/PC.
- Wer eine eigene Homepage pflegt, muss Hinweise zum Datenschutz hinterlegen.

Auskunft an Mitglieder und „Beteiligte“

- Jedes Mitglied, aber auch Referenten oder Beteiligte an z.B. einzelner Aktionen können jederzeit nachfragen, welche Daten gespeichert werden.
- Wünsche auf Löschung und Sperrung müssen zeitnah bearbeitet werden – einen solchen Vorgang unbedingt dokumentieren. Zudem erhält der Antragsteller eine Mitteilung auf dem Postweg (nicht per Mail!).

Löschen, Sperren und Entsorgen von Daten

- Entsorgen Sie keine sensiblen Unterlagen ungeschreddert im Papierkorb – prüfen Sie die Aufbewahrungsfristen.
- Das Löschen von sensiblen Daten (z.B. Kontoverbindung) soll zeitnah bei Austritt eine Mitglieds erfolgen; ebenso wenn ein Mitglied verstirbt – jedoch spätestens nach einem Jahr.
- Der Name und das Geburtsdatum dürfen erhalten bleiben, um sie im Rahmen des Datenschutzes für das Vereinsarchiv, Vereinsjubiläen oder sonstige interne Anlässe zu nutzen.
- Jede Löschung von personenbezogenen Daten soll dokumentiert werden

Hilfreiche Internetseiten

www.sensus.drs.de	//	www.katholisches-datenschutzzentrum.de
www.datenschutz-kirche.de	//	www.baden-wuerttemberg.datenschutz.de

Diese Informationsschrift ist beispielhaft und erhebt keinen Anspruch auf Vollständigkeit. Bei Fragen oder Unsicherheiten wenden Sie sich bitte gerne an das KAB-Diözesansekretariat.