Graubünden reformiert
Grischun refurmà
Grigioni riformato

Merkblatt Datenschutz in der Kirchgemeinde

Dieses Merkblatt vermittelt die wichtigsten Grundprinzipien des Datenschutzes und die sich daraus ergebenden Pflichten der Kirchgemeinden für den Arbeitsalltag.

1. WAS IST DATENSCHUTZ?

1.1. Recht auf Privatsphäre

Der Schutz der eigenen Daten ist ein Grundrecht jedes Individuums und ist Ausfluss aus dem Recht auf Schutz der Privatsphäre gemäss Bundesverfassung. Es ist das Anrecht der Bürgerinnen und Bürger darauf, dass ihre Daten vor Missbrauch durch den Staat oder Private geschützt sind.

1.2. Wichtigste Begriffe

Personendaten	Der Begriff des Personendatums umfasst jede Information, die sich auf eine bestimmte (d.h. identifizierte) oder bestimmbare Person bezieht. Je nach Situation bedeutet dies: Namen, E-Mail, Geburtsdatum, Telefonnummer, AHV-Nummer, IP-Adresse des Computers, Badge- oder Kontonummer, usw.
Besondere Personendaten	Gewisse Kategorien von Daten, die besonders schützenswert sind – allen voran Daten über die Gesundheit, die Intimsphäre, die ethnische Herkunft und Kombinationen von Daten, die eine Beurteilung wesentlicher Persönlichkeitsaspekte erlauben.
Datenbearbeitung	Sobald man es mit Personendaten zu tun hat, ist alles eine Datenbearbeitung. So beispielsweise das Verändern, Löschen, Speichern oder Erfassen von Daten (digital oder auf einem Blatt Papier).
Verantwortliche/-r	Die Person oder Organisation, die über den Zweck einer Datenbearbeitung entscheidet und über die Mittel, die für die Bearbeitung verwendet werden.
Auftragsdatenbearbeiter/-in	Eine Person oder Firma, die im Auftrag einer anderen Personendaten bearbeitet.

1.3. Wichtigste Regeln

Kirchgemeinden dürfen Personendaten bearbeiten, so lange diese Bearbeitung für die Erfüllung der in der Kirchenordnung umschriebenen Aufgaben der Kirchgemeinde nötig ist (siehe dazu auch nachfolgend Ziff. 2.1). Eine Kirchgemeinde, die Daten zur Um-

setzung ihres Auftrags bearbeitet, ist dabei «Verantwortliche» im Sinne des Datenschutzes.

Das Datenschutzgesetz kennt sechs Grundprinzipien, die die Kirchgemeinde in dieser Rolle beachten muss:

Gesetzmässigkeitsprinzip	Die Bearbeitung von Personendaten ist nur im Rahmen der Erfüllung der kirchlichen Aufgaben erlaubt.
Datensparsamkeit	Es sollen jeweils so wenig Personendaten wie möglich bearbeitet werden. Mit Personendaten muss demnach sparsam umgegangen werden.
Zweckbindung	Eine Bearbeitung von Personendaten ist grundsätzlich nur im Zusammenhang mit dem Zweck der Erhebung erlaubt (Zweckänderungsverbot).
Datenrichtigkeit	Personendaten müssen korrekt sein.
Sicherheit	Die Personendaten sind vor Verlust, Verfälschung und unbefugtem Zugriff zu schützen (bspw. anhand von technischen und organisatorischen Massnahmen).
Rechenschaftsfähigkeit	Die Organisation muss nachweisen können, dass der Datenschutz umgesetzt wird.
Transparenz	Für die betroffene Person ist ersichtlich, dass Daten bearbeitet werden. In gewissen Fällen ist dabei eine proaktive Information über die Bearbeitung nötig.

Neben diesen Grundprinzipien gibt es zusätzlich verschiedene gesetzliche Pflichten, die im Detail im Rahmen der Datenschutzschulung (dazu auch nachfolgend Ziff. 3) erläutert werden. Es handelt sich dabei in aller Kürze um die Folgenden:

Datenschutz- Folgenabschätzung (DSFA)	Die Risiken und Schutzmassnahmen eines neuen Projekts werden jeweils vorab analysiert und dokumentiert.
Betroffenenrechte	Betroffene Personen haben gewisse Rechte im Zusammenhang mit der Bearbeitung der eigenen Personendaten durch eine öffentliche Behörde. Zu diesen Rechten gehören unter anderem die Berichtigung oder Vernichtung unrichtiger Daten sowie die Unterlassung sowie wo nötig Beseitigung widerrechtlicher Datenbearbeitung. Unter bestimmten Voraussetzungen kann eine Einschränkung der Bearbeitung verlangt werden sowie die Sperrung eigener Daten.
Informationszugang	Der Öffentlichkeit kommt unter gewissen Voraussetzungen das Recht zu, Zugang zu amtlichen Informationen der Kirchgemeinde zu erhalten. Zu diesem Recht gehört die Pflicht der Kirchgemeinde, diesen Zugang in den jeweiligen Fällen zu gewähren.
Datenschutzvorfall	Der Verlust oder die Verfälschung von Personendaten sowie unbefugte Zugriffe sind unter Umständen der kantonalen Datenschutzbeauftragten zu melden.
Auftragsdatenbearbeitungsvereinbarung (ADV)	Werden Daten im Auftrag bearbeitet, ist ein Vertrag zwischen der Verantwortlichen (Kirchgemeinde) und der Auftragsdatenbearbeiterin abzuschliessen. Dieser regelt die Datenbearbeitung im Auftrag der Kirchgemeinde.

2. PFLICHTEN DER KIRCHGEMEINDE

2.1. Rolle der Kirchgemeinde

Die Kirchgemeinden verantworten das kirchliche Leben vor Ort in der Gemeinde mit allen damit zusammenhängenden Rechten und Pflichten. Sie regeln ihre Angelegenheiten im Rahmen der Kirchenordnung und des übergeordneten Rechts selbständig. Zu ihren Aufgaben gehören beispielsweise die Durchführung von Gottesdiensten, von Trauungen und Abdankungen sowie die Wahrnehmung von diakonischen Aufgaben. In diesen Bereichen dürfen Daten unter Einhaltung der obigen Pflichten und Prinzipien bearbeitet werden.

2.2. Rolle der Kirchgemeindevorstände

Der Kirchgemeindevorstand ist das ausführende Organ der Kirchgemeinden und dementsprechend für die Einhaltung des Datenschutzes in der Kirchgemeinde verantwortlich.

Dies bedeutet, dass der Vorstand die datenschutzrechtlichen Pflichten umsetzen muss und dafür zu sorgen hat, dass die Mitarbeitenden der Kirchgemeinde die Regeln ihrerseits einhalten. Dies bedingt eine datenschutzrechtliche Sensibilisierung aller Mitarbeitenden.

Wichtig: Der Datenschutz stellt für den gesamten Kirchenvorstand ein wichtiges Thema dar und muss im Alltag ernst genommen und umgesetzt werden. Im Falle der Missachtung drohen verschiedenste Risiken und Sanktionen.

3. DATENABLAGE

Die Sicherstellung des Datenschutzes bei der Datenablage, sowohl elektronisch als auch in Papierform, erfordert unterschiedliche Ansätze, die jeweils auf die spezifischen Risiken und Anforderungen der beiden Formate abgestimmt sind. Hier sind einige Massnahmen, die helfen können, den Datenschutz in beiden Bereichen zu gewährleisten:

3.1. Elektronische Datenablage

1. **Zugriffskontrollen:** Implementieren Sie strenge Zugriffskontrollen, um sicherzustellen, dass nur autorisierte Personen auf die Daten zugreifen können. Nutzen Sie Passwörter, Zwei-Faktor-Authentifizierung und rollenbasierte Zugriffsrechte. Eine geprüfte Dokumentenverwaltungssoftware erleichtert Ihnen diese Anforderungen zu erfüllen.

2. **Verschlüsselung:** Verschlüsseln Sie sensible Daten sowohl bei der Übertragung als auch bei der Speicherung, um die Vertraulichkeit zu gewährleisten.

3. **Regelmässige Backups:** Erstellen Sie regelmässige Backups der Daten und speichern Sie diese an einem sicheren Ort, um Datenverluste zu vermeiden.

4. **Sicherheitssoftware:** Verwenden Sie aktuelle Sicherheitssoftware, einschliesslich Firewalls und Antivirenprogramme, um Ihre Systeme vor Malware und unbefugtem Zugriff zu schützen.

5. **Protokollierung und Überwachung**: Führen Sie Protokolle über den Zugriff auf Daten und überwachen Sie diese regelmässig, um verdächtige Aktivitäten zu

erkennen.

6. **Datenschutz durch Technikgestaltung**: Integrieren Sie Datenschutzaspekte in die Entwicklung und Implementierung von IT-Systemen (Privacy by Design).

7. **Datenminimierung:** Erheben und verarbeiten Sie nur die Daten, die unbedingt notwendig sind. Vermeiden Sie die Speicherung unnötiger personenbezogener Informationen.

8. **Verträge mit Drittanbietern:** Stellen Sie sicher, dass Verträge mit Drittanbietern, die Zugang zu personenbezogenen Daten haben, klare Datenschutzanforderungen enthalten und die Einhaltung dieser Anforderungen überwacht wird.

3.2. Papierbasierte Datenablage

1. **Physische Sicherheit:** Bewahren Sie Papierdokumente in abschliessbaren Schränken oder Räumen auf, zu denen nur autorisierte Personen Zugang haben.

2. **Zugriffskontrollen:** Stellen Sie sicher, dass der Zugang zu sensiblen Dokumenten auf diejenigen beschränkt ist, die sie für ihre Arbeit benötigen.

3. **Dokumentenmanagement:** Implementieren Sie ein System zur Nachverfolgung von Dokumenten, um zu wissen, wer wann auf welche Informationen zugegriffen hat.

4. **Sichere Entsorgung:** Vernichten Sie nicht mehr benötigte Dokumente sicher, z.B. durch Schreddern, um unbefugten Zugriff auf vertrauliche Informationen zu verhindern.

5. **Schulung und Sensibilisierung:** Schulen Sie Mitarbeiter im Umgang mit sensiblen Informationen und sensibilisieren Sie sie für die Bedeutung des Datenschutzes.

6. **Regelmässige Überprüfungen:** Führen Sie regelmässige Überprüfungen der physischen Sicherheitsmassnahmen durch, um sicherzustellen, dass sie wirksam sind.

Durch die Kombination dieser Massnahmen können Organisationen den Datenschutz sowohl bei der elektronischen als auch bei der papierbasierten Datenablage effektiv sicherstellen und das Risiko von Datenschutzverletzungen minimieren.

4. SANKTIONEN BEI NICHTEINHALTUNG DES DATENSCHUTZES

In der Schweiz kann die Nichteinhaltung von Datenschutzbestimmungen verschiedene Auswirkungen haben, sowohl rechtlicher als auch praktischer Natur. Hier sind einige der wichtigsten Konsequenzen:

1. **Rechtliche Sanktionen:** Bei Verstössen gegen das Datenschutzgesetz (DSG) können rechtliche Massnahmen ergriffen werden. Dazu gehören Bussgelder, die gegen verantwortliche Personen verhängt werden können. Die Höhe der Bussgelder kann je nach Schwere des Verstosses variieren.

2. **Zivilrechtliche Ansprüche:** Betroffene Personen können zivilrechtliche An-

sprüche geltend machen, wenn sie durch die Verletzung ihrer Datenschutzrechte Schaden erlitten haben. Dies kann zu Schadensersatzforderungen führen.

3. **Reputationsschäden:** Datenschutzverletzungen können das Vertrauen der Mitglieder und der Öffentlichkeit in die Organisation erheblich beeinträchtigen. Ein Verlust an Vertrauen kann langfristige negative Auswirkungen auf das Ansehen und die Glaubwürdigkeit der Kirchgemeinde haben.

4. **Erhöhte Überwachung:** Organisationen, die gegen Datenschutzbestimmungen verstossen haben, können unter verstärkte Beobachtung durch die Datenschutzbehörden geraten, was zu häufigeren Kontrollen und Audits führen kann.

5. **Interne Konsequenzen:** Innerhalb der Organisation kann es zu internen Disziplinarmassnahmen gegen Mitarbeiter kommen, die für den Verstoss verantwortlich sind. Dies kann auch zu einer Überprüfung und Anpassung interner Prozesse und Richtlinien führen.

5. UNTERSTÜTZUNG DER KIRCHGEMEINDEN

Ab Herbst 2025 wird die Landeskirche eine Behördenschulung zum Datenschutz in Kooperation mit Partnern für die Kirchgemeinden zur Verfügung stellen. Ziel der Schulung wird es sein, die Mitglieder der Kirch in das Thema Datenschutz einzuführen und zu sensibilisieren.

Als Datenschutzbeauftragte stehen den Kirchgemeinden bei Fragen folgende Personen zur Verfügung:

- rechtliche Fragen: Kirchenrätin, Dr. Raphaela Holliger, raphaela.holliger@gr-ref.ch, 081252 26 82
- technische Fragen: Finanzverwalter, Marcel Schädler, marcel.schaedler@gr-ref.ch, 081 257 11 00