reformierte
kirche weinland mitte

benken marthalen ossingen rheinau trüllikon truttikon

Datenschutzhandbuch
Reformierte Kirche Weinland Mitte

Dieses Datenschutzhandbuch ist durch die

Kirchenpflege der
Kirchgemeinde Weinland Mitte

an ihrer Sitzung vom 11. November 2024 in Kraft gesetzt worden.

Der entsprechende Beschluss lautet wie folgt:

Das Datenschutzhandbuch wird, wie unter dessen Ziffer 1.3. vorgeschlagen, als allgemeine Weisung verbindlich und an alle Mitarbeitenden und Kirchenpflege verteilt - mit Gegenzeichnung, dass das Dokument erhalten und der Inhalt gelesen und verstanden wurde (E-Mail-Bestätigung).
Zum Datenschutzbeauftragten der KG Weinland Mitte und Ansprechperson für Datenschutzfragen wird der amtierende Kirchenpflegepräsident Rolf Hans Elsener bestimmt.

Dieses Handbuch wird den Kirchgemeinden als Unterstützung bei der Umsetzung des Datenschutzes durch den Kirchenrat zur Verfügung gestellt. Es ist Sache der Kirchgemeinden, das Handbuch jeweils intern für die Kirchgemeinde mit Beschluss der Kirchenpflege für verbindlich zu erklären und das Datum des Beschlusses entsprechend zu integrieren. Es steht den Kirchgemeinden zudem frei, z.B. den Einband grafisch zu gestalten.

Version 1.0 / 04.07.2023

Inhaltsverzeichnis

1 Einleitung

1.1 Worum geht es?

Das vorliegende Handbuch hat zum Ziel, für den Arbeitsalltag in der Kirchgemeinde die wichtigsten Vorgaben des Datenschutzes zu erklären. Es soll als Nachschlagewerk dienen, wenn Datenschutzfragen auftauchen.

Mit der Digitalisierung nehmen die Risiken für die Privatsphäre derjenigen Personen zu, über die Personendaten bearbeitet werden: Daten werden in grossen Mengen und durch unzählige Akteure an verschiedensten Orten bearbeitet. Dieses Handbuch will die Kirchenpflegen sowie die Mitarbeiterinnen und Mitarbeiter in den Kirchgemeinden befähigen, selbst zum Datenschutz beizutragen, denn: Das Handeln der einzelnen Mitarbeiterinnen und Mitarbeiter im Alltag ist für den Datenschutz zentral. Jedes Gesetz, jede Richtlinie, jede Weisung ist unnütz, wenn sie nicht im Arbeitsalltag umgesetzt werden.

Guter Datenschutz – d.h. Datenschutz, den sich die Kirchgemeinden zu Herzen nehmen und im Alltag umsetzen – trägt bedeutend zum guten Ruf der Kirche bei. Im Fall der Kirchgemeinden kann Datenschutz als Ausdruck des wertschätzenden Umgangs mit Menschen einen Teil zur Verwirklichung des kirchlichen Auftrags leisten.

Dieses Handbuch richtet sich an die Kirchenpflegen und ihre Mitglieder sowie alle Mitarbeiterinnen und Mitarbeiter der Kirchgemeinden (Pfarrerinnen, Pfarrer und Angestellte sowie Freiwillige, die nachfolgend jeweils alle mitgemeint sind).

Jedes Mitglied der Kirchenpflege, jede Mitarbeiterin und jeder Mitarbeiter der Kirchgemeinde soll für die Arbeit im Alltag Folgendes wissen:

1	Wann man es im Arbeitsalltag mit Personendaten zu tun hat und welches die wichtigsten Datenschutzbegriffe sind (siehe dazu nachfolgend Ziffer 3.1).
2	Welche Grundsätze und Prinzipen im Umgang mit Personendaten zu beachten sind (siehe dazu nachfolgend Ziffer 3.2).
3	Welche Schritte die Kirchgemeinde unternehmen kann oder sogar muss, um den Datenschutz zu verbessern (siehe dazu bspw. die Prozesse in Ziffer 5).

1.2 Was will der Datenschutz?

Vereinfacht gesprochen sind Daten Informationsbestandteile. Beziehen sich solche Informationsbestandteile auf eine Person, handelt es sich um «Personendaten» (auch: «personenbezogene Daten»). Jede Person hat dabei ein Anrecht darauf, dass diese personenbezogenen Daten geschützt werden. Mit den Regeln des Datenschutzes soll folglich sichergestellt werden, dass die Privatsphäre bezüglich Datenbearbeitungen, d.h. im Umgang mit Personendaten, geschützt ist.

Der Schutz dieser Daten ist nicht nur ein «nice to have», sondern umfasst eine Reihe von gesetzlich verbindlichen Pflichten, die bei Nichteinhaltung bedeutende Reputationsschäden anrichten und zu Sanktionen führen können.

1.3 Benutzung und rechtliche Einordnung dieses Dokuments

Es wird empfohlen, dass die Kirchenpflege mit Beschluss das vorliegende Datenschutz-Handbuch als allgemeine Weisung innerhalb der Kirchgemeinde für verbindlich erklärt. Die im Handbuch enthaltenen Anweisungen und Regeln ergeben sich aber bereits aus den massgeblichen gesetzlichen Bestimmungen und sind daher schon deswegen verbindlich.

2 Verantwortlichkeiten innerhalb der Kirchgemeinde

Funktion	Verantwortlichkeiten
Kirchenpflege (Exekutive)	Die Kirchenpflege als Behörde trägt die Gesamtverantwortung für die Einhaltung der rechtlichen Vorgaben und damit auch für den Datenschutz. Sie sorgt für die Umsetzung der allgemeinen Vorgaben innerhalb der Organisation und stellt sicher, dass die notwendigen finanziellen und personellen Ressourcen vorhanden sind, damit die Kirchgemeinde datenschutzkonform handeln kann, und kontrolliert die Umsetzung des Datenschutzes kontinuierlich.
Ansprechperson für Datenschutzfragen	Innerhalb der Kirchgemeinde ist eine Person als Ansprechperson für Datenschutzfragen zu bestimmen und innerhalb der Kirchgemeinde bekannt zu geben. Es handelt sich um eine rein beratende Rolle. Dazu gibt es zwei Optionen: a) Ansprechperson für Datenschutzfragen Die Funktion wird in der Regel durch ein Mitglied der Kirchenpflege oder eine andere Person mit Affinität für Datenschutz-Fragen wahrgenommen. Diese Funktion kann innerhalb der Kirchgemeinde oder durch eine externe Person besetzt werden. Diese Person eignet sich ein minimales Datenschutzwissen an und dient, wie der Name sagt, als Ansprechperson für Datenschutzfragen. Nach § 10 des Kirchlichen Datenschutz-Reglements[1] ist diese Ansprechperson u.a. auch für Fragen regelmässiger Datenlieferanten wie beispielweise die Einwohnerkontrolle oder die Schulverwaltung zuständig. Die Funktion beinhaltet weniger aktive fachliche Tätigkeit als sie die/der Datenschutzbeauftragte (siehe nachstehend b)) wahrnimmt; es handelt sich um eine Triagefunktion, die die Umsetzung von Datenschutzprozessen in der Kirchgemeinde steuert und ggf. einfache Fragen selbst beantwortet. b) Datenschutzbeauftragte(r) Alternativ kann die Kirchgemeinde intern oder extern eine Person als Datenschutzbeauftragte oder Datenschutzbeauftragten ernennen (§ 33 IDG). Die oder der Datenschutzbeauftragte

[1] Kirchliches Datenschutz-Reglement vom 15./6. Dezember 1999 und 23. Mai 2000, LS 180.7.

	(nachfolgend jeweils «DSB» genannt) berät die Mitarbeiterinnen und Mitarbeiter der Kirchgemeinde in Datenschutzfragen, überwacht die Anwendung der Datenschutzvorschriften und sensibilisiert bzw. schult Mitarbeiterinnen und Mitarbeiter und Mitglieder der Kirchenpflege hinsichtlich des Datenschutzes. Es können auch mehrere Kirchgemeinden gemeinsam eine(n) DSB ernennen. Die oder der DSB verfügt über die nötigen fachlichen Voraussetzungen und übt Aufgaben und Befugnisse unabhängig aus. Sie oder er unterbreitet der Kirchenpflege Anträge auf Erlass verbindlicher Weisungen und Massnahmen und berichtet an diese. Basierend auf der aktuellen Rechtslage sind die Kirchgemeinden nicht verpflichtet, eine(n) DSB zu ernennen. Künftig könnte dies im Rahmen der pendenten Revision des IDG allerdings für grössere Gemeinden obligatorisch werden, weshalb es sich empfehlen kann, eine solche Position bereits einzuführen. **Wird eine oder ein DSB ernannt, nimmt er oder sie auch gleich die Funktion der Ansprechperson für Datenschutzfragen wahr.** Die Oberaufsicht behält stets die die kantonale Datenschutzbeauftragte (siehe dazu «kantonale Aufsichtsstelle» im Abkürzungsverzeichnis).
Mitarbeiterin oder Mitarbeiter	Jede Mitarbeiterin und jeder Mitarbeiter sorgt dafür, dass die Grundsätze des Datenschutzes sowie der Informationssicherheit und die definierten Prozesse im eigenen Tätigkeitsgebiet und im eigenen Arbeitsalltag umgesetzt werden; sie oder er hält die Pflichten gemäss dieser Weisung ein. Die Mitarbeiterin oder der Mitarbeiter wendet sich mit datenschutzrechtlichen Anliegen an die Ansprechperson für Datenschutzfragen. Wenn ein Verdacht besteht, dass ein Datenschutzvorfall gemäss Ziffer 5.4 vorliegen könnte, ist dies unverzüglich zu melden.

3 Einige Grundbegriffe und Prinzipien

3.1 Die wichtigsten Begriffe

3.1.1 Die drei Wichtigsten vorab

Begriff	Definition
Personendaten	Daten, die sich auf eine *bestimmte* oder *bestimmbare* Person beziehen. Auch *personenbezogene Daten* genannt. • Mit «Bestimmbarkeit» ist gemeint, dass die Daten in den Händen einer entsprechenden Person oder in Kombination mit weiteren Daten dazu führen können, dass eine Person identifiziert werden kann. • Mit der Angabe des Namens und einer Fotografie ist eine Person schon ohne Weiteres «bestimmt», d.h. identifiziert. Mit einer Telefonnummer und einem Zugang zu tel.search.ch oder einem Adressverwaltungssystem einer Kirchgemeinde kann eine Person ebenfalls oftmals im Arbeitsalltag identifiziert werden; die Telefonnummer bezieht sich in diesem Fall also auf eine «bestimmbare» Person und ist daher ein personenbezogenes Datum. • Der Begriff der Personendaten ist äusserst breit; auch Daten wie IP-Adressen, Kontonummern oder sogar Badge-Nummern stellen im Normalfall Personendaten dar. • Für den Arbeitsalltag in der Kirchgemeinde bedeutet dies, dass der Datenschutz immer einzuhalten ist.
⚠ *Besondere Personendaten*	Oftmals ist auch die Rede von *besonders schützenswerten* oder *sensitiven* Personendaten: Es geht um Daten, bei denen eine besondere Gefahr einer Persönlichkeitsverletzung besteht. Dies ist etwa dann der Fall, wenn Daten einen besonders tiefen Einblick in die Persönlichkeit und das Leben einer Person erlauben (Intimsphäre), weil sie in einer Art bearbeitet werden, die besondere Risiken birgt, oder weil viele verschiedene Daten miteinander kombiniert werden. Das Datenschutzgesetz[2] enthält strengere Anforderungen für die Bearbeitung besonderer Personendaten. Das Datenschutzgesetz nennt u.a. folgende Kategorien:

[2] Im Folgenden sind mit «Datenschutzgesetz» jeweils das kantonale Gesetz über die Information und den Datenschutz vom 12. Februar 2007 (IDG, LS 170.4) und die dazugehörige Verordnung über die Information und den Datenschutz vom 28. Mai 2008 (IDV, LS 170.41) gemeint. Relevant ist vorliegend § 3 Abs. 4 IDG.

	• Informationen über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, • Informationen über die Gesundheit, die Intimsphäre, die ethnische Herkunft sowie genetische und biometrische Daten, • Informationen über Massnahmen der sozialen Hilfe, • Informationen über administrative oder strafrechtliche Verfolgungen oder Sanktionen, • Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit natürlicher Personen erlauben, • «Profiling», d.h. das automatisierte Auswerten von Informationen, «um wesentliche persönliche Merkmale zu analysieren oder persönliche Entwicklungen vorherzusagen». Beispiele besonderer Personendaten im Kontext der Kirchgemeinden sind etwa Daten aus der Seelsorge sowie je nachdem auch die umfangreichen Datensätze der Mitgliederdatenverwaltung. Die Konfession selbst («reformiert») ist im Kontext der Kirchgemeinde im Normalfall kein besonderes Personendatum, weil bei dieser Angabe im kirchlichen Kontext, im Gegensatz zu anderen Bereichen, keine besonderen Risiken bestehen (z.B. Diskriminierungsrisiko). Vorsicht ist jedoch bei der Weitergabe der Information an Dritte geboten: Denn die Konfession kann im nicht-internen Kontext als besonderes Personendatum gelten.
Datenbearbeitung *(auch: Bearbeitung, Datenverarbeitung)*	Jeder Umgang mit Personendaten: Erheben, Speichern, Versenden, Verändern, Veröffentlichen, Löschen, etc.

3.1.2 Ein Glossar in alphabetischer Reihenfolge für alles andere

Weitere wichtige Begriffe finden sich in der nachfolgenden Darstellung.

Begriff	Definition
ADV	Abkürzung für *Auftragsdatenbearbeitungsvertrag*, siehe dort.
Anonymisierung *(auch: anonyme Daten)*	Daten sind dann vollständig anonym, wenn keinerlei Personenbezug mehr hergestellt werden kann. Vollständige Anonymisierung ist sehr schwer zu erreichen; wenn man sie erzielt, liegen keine Personendaten mehr vor und die Pflichten des Datenschutzgesetzes gelten nicht mehr.
Attribut(e)	Ein Attribut ist ein Datentyp, also eine Kategorie von Daten, die bearbeitet werden.

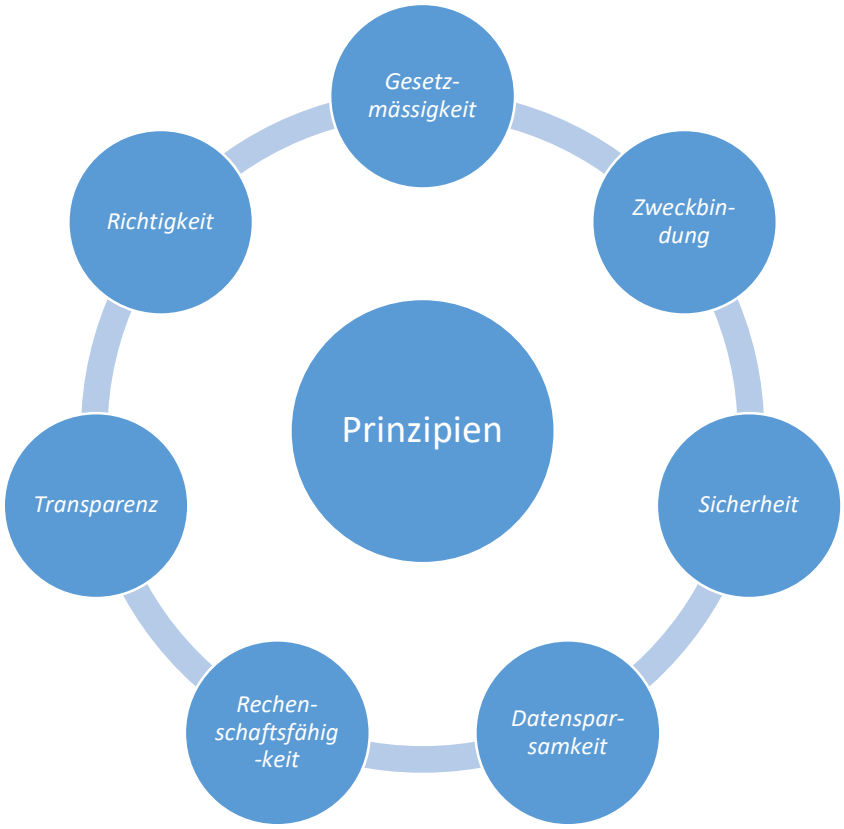
	Beispiele: «E-Mail-Adresse», «Nachname», «Postanschrift», «AHV-Nr.», «IP-Adresse», «Anzahl Kinder».
Auftragsdatenbearbeiterin oder Auftragsdatenbearbeiter	Diejenige Person oder Firma, die im Auftrag einer anderen Person Daten bearbeitet, wird als Auftragsdatenbearbeiterin oder Auftragsdatenbearbeiter bezeichnet. Sie darf nur nach den Weisungen der/des *Verantwortlichen* die Daten bearbeiten und die/der *Verantwortliche* muss vertraglich dafür sorgen, dass sich die Auftragsdatenbearbeiterin oder der Auftragsdatenbearbeiter an die Vorgaben des Datenschutzes hält. Beispiele: Hostingfirma, die im Auftrag der Kirchgemeinde einen Server oder eine Webseite betreibt; Softwarefirma, die der Kirchgemeinde eine Software zur Verfügung stellt, damit diese Podcasts produzieren kann. Wird oftmals auch – aus dem Englischen – *processor* genannt. Siehe dazu vorstehend Ziffer 4.3.
Betroffene Person	Eine Person, über die Daten bearbeitet werden. Bsp. *Kirchenpflegemitglied* Frau XY nimmt an einer Schulung teil und im Zuge der Anmeldung werden ihre Kontaktangaben (Name, E-Mail, Adresse, Kirchgemeinde) aufgenommen und bearbeitet. Frau XY ist die betroffene Person. Die betroffene Person wird oftmals auch als *Datensubjekt* bezeichnet.
Data breach notification	Englischer Begriff für die Meldung eines *Datenschutzvorfalls* (siehe dazu nachstehend *Datenschutzvorfall* sowie Ziffer 5.4).
Data processing agreement (DPA)	Englischer Begriff für den *Auftragsdatenbearbeitungsvereinbarung (ADV)*, siehe dort.
Daten (Einzahl: Datum)	Eine Ziffernfolge, bestehend aus Zahlen oder Buchstaben. Z.B.: Rechnungsnummer 5562-XY, Geburtsdatum 02.05.1963, E-Mail-Adresse vorname.name@zhref.ch.
Datenschutzbeauftragte oder *Datenschutzbeauftragter (DSB)*	Diejenige Person, die von der Kirchgemeinde ernannt ist, um innerhalb der Kirchgemeinde in Belangen des Datenschutzes zu beraten (aktuell ist die Ernennung fakultativ). Der bzw. die DSB wird vorliegend unter den Begriff «Absprechperson für Datenschutzfragen» gefasst (siehe vorstehend Ziffer 2). Für die/den *kantonale/-n Datenschutzbeauftragte/-n*: siehe dort.
Datenschutzgesetz	Ist in dieser Weisung vom «Datenschutzgesetz» die Rede, so ist damit das auf die Kirchgemeinde anwendbare kantonale Gesetz über die Information und den Datenschutz vom 12. Februar 2007 (IDG, LS 170.4) gemeint sowie der Einfachheit halber auch die dazugehörige Verordnung über die Information und den Datenschutz vom 28. Mai 2008 (IDV, LS 170.41).

	Es gibt zudem auf Bundesebene ein Datenschutzgesetz (Bundesgesetz über den Datenschutz, DSG), das auf Datenbearbeitungen durch Private sowie durch Bundesbehörden anwendbar ist. Es kommt vorliegend nicht zur Anwendung. Zum DSG Bund und zur EU-Datenschutz-Grundverordnung (EU-DSGVO bzw. DSGVO) siehe nachfolgend Ziffer 6.
Datenschutzvorfall *(auch: Datenschutzverstoss)*	Daten gehen verloren, werden verfälscht oder durch unbefugte Personen bearbeitet (z.B. ein Hackerangriff, jemand verliert einen geschäftlichen Laptop, etc.). Siehe dazu unten, Ziff. 5.4.1.
Datensparsamkeit	Siehe vorstehend Ziffer 3.2.
Datensubjekt	Siehe oben, *betroffene Person*.
DPA	Englische Bezeichnung für den *Auftragsdatenbearbeitungsvertrag (ADV)*, siehe dort.
Gesetzmässigkeit	Siehe unten, Rechtsgrundlage der Datenbearbeitung.
Information	Überbegriff, der alle Arten von Daten umfasst, aus denen eine Aussage oder ein Sinngehalt abgeleitet werden kann (sowohl personenbezogene als auch nicht personenbezogene Daten). Dies gilt ungeachtet der Form: Informationen können elektronisch oder mündlich, bzw. auf Papier festgehalten oder bearbeitet werden.
Kantonale Datenschutzbeauftragte bzw. kantonaler Datenschutzbeauftragter (kantonale Aufsichtsstelle)	Datenschutzbeauftragte/-r des Kantons Zürich, die kantonale Aufsichtsstelle über Datenbearbeitungen durch kantonale öffentliche Organe (www.datenschutz.ch). Ihr bzw. ihm sind Datenschutzvorfälle zu melden (siehe dazu vorstehend Ziffer 5.4). Kann Auskunft einholen, Aufsichtsverfahren führen und Sanktionen erlassen. Die bzw. der kantonale Datenschutzbeauftragte wird vom Kantonsrat gewählt und übt die Oberaufsicht über den Datenschutz aus (§ 30 ff. IDG). Sie wird in diesem Dokument als kantonale Aufsichtsstelle bezeichnet.
Privacy by default	Siehe vorstehend Ziffer 3.2.
Privacy by design	Siehe vorstehend Ziffer 3.2.
processor	Siehe oben, *Auftragsdatenbearbeiterin oder Auftragsdatenbearbeiter.*
Pseudonym (auch: pseudonyme Daten)	Ein Pseudonym ist eine Ziffernfolge, die an sich die Person nicht identifiziert und anstelle eines Personendatums verwendet wird. Beispiel: Ein Dienstleister erhält von der Kirchgemeinde eine Serie ausgefüllter Fragebogen zur Auswertung. Vor dem Versand an den Dienstleister werden die Namen der Personen, die den Fragebogen beantwortet haben, ersetzt durch Zahlen: Herr Meyer wird damit zu 0012, Frau Kostic zu 0013. Pseudonyme Daten sind weiterhin Personendaten, weil die zuständige Person

	innerhalb der Kirchgemeinde in ihrer Liste jederzeit nachschauen kann, welcher Person die Nummern 0012 und 0013 zugeteilt wurden.
Rechtsgrundlage der Datenbearbeitung	Jede Datenbearbeitung durch die Kirchgemeinde als öffentliches Organ braucht eine Rechtsgrundlage, d.h. einen im Recht festgehaltenen Grund, damit sie erlaubt ist. Das Datenschutzgesetz sieht vor, dass die Kirchgemeinde Personendaten bearbeiten darf, wenn dies *zur Erfüllung ihrer Aufgaben* notwendig ist. Geht es um besondere Personendaten, so ist sogar eine gesetzliche Grundlage, d.h. eine explizite Bestimmung in einem formellen Gesetz, nötig. Die Einwilligung, die im Wirtschaftsleben für Datenbearbeitungen zentral ist, wird von der Kirchgemeinde nur sehr selten als Rechtsgrundlage der Datenbearbeitung hinzugezogen werden können.
Technische und organisatorische Massnahmen (TOMs)	Überbegriff für alle Massnahmen, die innerhalb einer Organisation getroffen werden (müssen), um die Sicherheit von Personendaten zu gewährleisten. Technische Massnahmen sind etwa Verschlüsselung, Zugriffsbeschränkungen, Zutrittskontrolle, Datensicherung, etc. Organisatorische Massnahmen sind interne Prozesse, Schulungen des Personals, Sensibilisierung der Mitarbeitenden im Bereich des Datenschutzes und der Informationssicherheit, Geheimhaltungserklärungen in Verträgen (sogenannte «NDAs», *Non-Disclosure Agreements*), etc.
TOMs	Siehe oben, *technische und organisatorische Massnahmen.*
Transparenz	Siehe vorstehend Ziffer 3.2.
Verantwortliche oder Verantwortlicher	Diejenige Person oder Organisation, die über den Zweck einer Datenbearbeitung entscheidet und über die Mittel, die dazu benutzt werden. Sie hat dafür zu sorgen, dass alle Pflichten des Datenschutzgesetzes eingehalten werden. Beispiel: Die Kirchgemeinde entscheidet sich, zur Mitgliederverwaltung (= Zweck) alle relevanten Daten in einer zentralen Datenbank zu vereinen und mithilfe einer Software zu verwalten (= Mittel). Sie (die Kirchgemeinde, nicht die projektverantwortliche Person!) ist entsprechend «Verantwortliche» im Sinne des Datenschutzes. Ebenfalls verbreitet: der englische Begriff *controller*. Siehe dazu vorstehend Ziffer 4.2.
Verhältnismässigkeit	Siehe dazu vorstehend Ziffer 3.2.
Vermeidung des Personenbezugs	Siehe dazu vorstehend Ziffer 3.2.
Zweckbindung	Siehe dazu vorstehend Ziffer 3.2.

3.2 Datenschutz-Prinzipien

Das Datenschutzgesetz enthält eine Serie von Grundprinzipien des Datenschutzes. Es sind Regeln, die bei der Datenbearbeitung immer einzuhalten sind.



Im Folgenden soll kurz darauf eingegangen werden, was die einzelnen Prinzipien genau bedeuten.

Prinzip	Bedeutung
Gesetzmässigkeit	Die Kirchgemeinde bearbeitet Personendaten *zur Erfüllung ihrer kirchlichen Aufgaben* im Rahmen der geltenden gesetzlichen Vorgaben. Achtung: Für die Bearbeitung *besonderer Personendaten* verlangt das Datenschutzgesetz nicht nur, dass die Bearbeitung zur Erfüllung kirchlicher Aufgaben nötig ist, sondern dass eine *Bestimmung in einem Gesetz* diese Art der Datenbearbeitung vorsieht (§ 8 Abs. 2 IDG).
Zweckbindung	Personendaten dürfen nur zu dem Zweck bearbeitet werden, zu dem sie erhoben wurden oder zu dem die Kirchgemeinde auf andere Weise ermächtigt wird. Auf andere Weise ermächtigt wird die Kirchgemeinde z.B.:

	• durch ein Gesetz, das die Datenbearbeitung zu einem anderen Zweck vorsieht, • durch die Einwilligung der betroffenen Person zur neuen Datenbearbeitung im Einzelfall oder • wenn Daten zu nicht personenbezogenen Zwecken ausgewertet werden.
Sicherheit	Personendaten sind vor *Verlust*, vor *Verfälschung* und vor *unbefugtem Zugriff* zu schützen. Dazu werden Massnahmen umgesetzt, die sowohl technische als auch organisatorische Aspekte beinhalten (entsprechend wird der Begriff «TOMs», also «technische und organisatorische Massnahmen», verwendet; s. dazu auch die Vorlage ADV [insb. Ziff. 2.2] sowie die Vorlage TOMs).
Datensparsamkeit	Dies kann man zusammenfassen als: «so wenig Personendaten wie möglich!» Hier gibt es verschiedenste Begriffe und Prinzipien, die alle darauf abzielen, dass immer nur so viele Daten bearbeitet werden wie absolut nötig, um die entsprechende Aufgabe zu erfüllen. Auch: • *Verhältnismässigkeit* • *Vermeidung des Personenbezugs* • *Datenminimierung* • *Privacy by design* – Arbeitsprozesse und technische Systeme werden so ausgestaltet, dass so wenige Personendaten wie möglich bearbeitet und dabei die Persönlichkeitsrechte der betroffenen Personen gewahrt werden. • *Privacy by default* – als Grundregel wird jeweils die maximal schützende Ausgestaltung eines Prozesses, eines Formulars, etc. gewählt. Zur Datensparsamkeit gehört auch die *Speicherbegrenzung*, d.h. die Löschung von Daten, sobald sie nicht mehr benötigt werden.
Transparenz	Betroffene Personen werden über Datenbearbeitungen im Rahmen der gesetzlichen Vorgaben informiert; es wird darauf geachtet, dass die betroffenen Personen ihre Rechte geltend machen können (vgl. dazu nachstehend Ziffer 5.3 unten). Stichwort: Datenschutzerklärung!
Richtigkeit	Es muss sichergestellt werden, dass die bearbeiteten Daten richtig sind. Dazu müssen angemessene Massnahmen getroffen werden, um unrichtige Daten berichtigen oder löschen zu können.
Rechenschaftsfähigkeit	Die Kirchgemeinde sorgt organisationsintern für die notwendigen *Prozesse* und *Verfahren*, um den Datenschutz kontinuierlich umzusetzen, die getroffenen Massnahmen zu dokumentieren

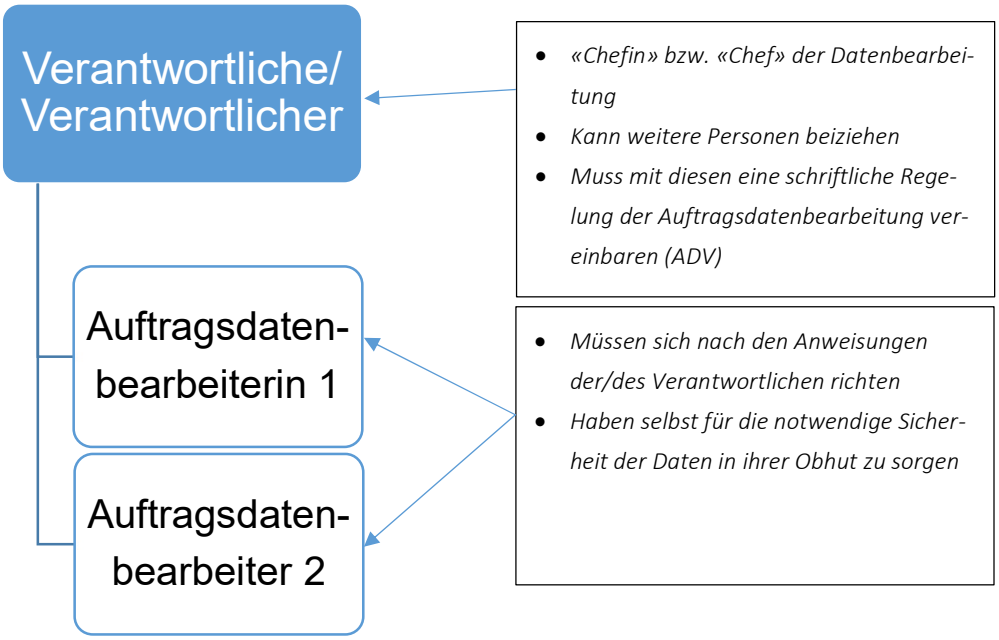
	und damit nachzuweisen, dass der Datenschutz gelebt wird. Es ist im Datenschutzgesetz von *Prozessen* oder *Nachvollziehbarkeit* die Rede.

4 Datenbearbeitung im Auftrag und Besonderheiten der Datenübermittlung ins Ausland

4.1 Einleitung

Im Datenschutz gilt es zwischen den nachfolgenden beiden Rollen zu unterscheiden. An erster Stelle steht dabei die oder der *Verantwortliche*. Die oder der Verantwortliche ist, wie es der Wortlaut besagt, verantwortlich dafür, dass alle Pflichten des Datenschutzgesetzes eingehalten werden. Er oder sie muss den Schutz der ihr oder ihm zur Kenntnis gelangten Personendaten gewähren.

Als weitere Rolle gilt es die *Auftragsdatenbearbeiterin* oder den *Auftragsdatenbearbeiter* zu kennen. Als Auftragsdatenbearbeiterin oder Auftragsdatenbearbeiter wird diejenige Organisation (bzw. Firma) oder natürliche Person bezeichnet, die im Auftrag der oder des Verantwortlichen gewisse Tätigkeiten übernimmt.



Nutzt die oder der Verantwortliche solche Dienstleistungen und erhalten Auftragsdatenbearbeiterinnen oder Auftragsdatenbearbeiter dadurch Kenntnis von Personendaten (bspw. Auslagerung IT-Funktionen oder Werbeversand), ist es wichtig, dass die oder der Verantwortliche mit den jeweiligen Organisationen oder natürlichen Personen einen schriftlichen Vertrag betreffend den Schutz dieser Personendaten abschliesst (siehe dazu nachstehend Ziffer 4.4).

Ein Spezialfall stellt dabei die sogenannte Auslandsübermittlung dar, bei welcher es zusätzliche Regeln zu beachten gilt (siehe dazu nachstehend Ziffer 4.5).

4.2 Verantwortliche oder Verantwortlicher

Im Datenschutz ist Verantwortliche oder Verantwortlicher (Englisch: *controller*), wer den *Zweck* einer Datenbearbeitung festlegt und darüber entscheidet, welche *Mittel* zur Bearbeitung der Daten eingesetzt werden. Geht es um einen geschäftlichen Kontext, ist die oder der Verantwortliche immer eine *Organisation* (d.h. hier die Kirchgemeinde), nie eine einzelne Person innerhalb dieser Organisation: Wenn eine Mitarbeiterin oder ein Mitarbeiter im Rahmen des Arbeitsverhältnisses mit

einer Kirchgemeinde eine Aufgabe ausführt, so ist immer die Kirchgemeinde als Arbeitgeberin *Verantwortliche* im Sinne des Datenschutzgesetzes.

Es kann auch vorkommen, dass in einer bestimmten Situation mehrere Organisationen Verantwortliche im Sinne des Datenschutzgesetzes sind, weil sie gemeinsam ein Projekt durchführen und gemeinsam über Zwecke und Mittel der Datenbearbeitung entscheiden. Denkbar ist dies z.B. bei einem ökumenischen Projekt, bei dem verschiedene Institutionen gemeinsam entscheiden. In diesem Falle sind beide *Verantwortliche* im Sinne des Datenschutzgesetzes (Englisch: *joint controllers*). Sie müssen entsprechend gemeinsam (vertraglich) festlegen, wer welchen Pflichten nachkommt.

Zieht die oder der Verantwortliche weitere Unternehmen oder Private bei, die im Auftrag an der Datenbearbeitung mitwirken, so bleibt gegen aussen immer die oder der Verantwortliche für die Daten verantwortlich, auch hinsichtlich des Handelns der Auftragsdatenbearbeiterin oder des Auftragsdatenbearbeiters. Es ist also die Pflicht der oder des Verantwortlichen:

- Auftragsdatenbearbeiterinnen und Auftragsdatenbearbeiter *sorgfältig auszuwählen*,
- ihnen schriftliche *Anweisungen* zu geben (in einem Vertrag, siehe dazu nachstehend Ziffer 4.4), an die sie sich halten müssen, und
- sie zu *beaufsichtigen* (d.h. prüfen, ob die Leistung auch so erbracht wird, wie sie vereinbart wurde, ggf. ein Audit der Tätigkeiten des Unternehmens durchführen lassen).

In Bezug auf die Kirchgemeinden liegt diese Verantwortung in letzter Instanz bei der Kirchenpflege.

4.3 Auftragsdatenbearbeiterin oder -bearbeiter

Wenn die oder der Verantwortliche ein weiteres Unternehmen bzw. eine Dienstleisterin oder einen Dienstleister in Anspruch nimmt, um eine Aufgabe zu erfüllen (und dann entsprechend Daten zu bearbeiten), so sind diese *Auftragsdatenbearbeiterin oder Auftragsdatenbearbeiter* im Sinne des Datenschutzgesetzes. Dieses Unternehmen (oder die Einzelperson) hat dafür zu sorgen, dass die Vorgaben der oder des Verantwortlichen genau eingehalten und namentlich Daten für keine anderen Zwecke bearbeitet werden, als dies von der oder dem Verantwortlichen vorgegeben wird. Sie oder er muss ferner sicherstellen, dass die Sicherheit derjenigen Personendaten, die in ihrer/seiner Obhut sind, gewährleistet wird (durch *technische und organisatorische Massnahmen [TOMs]*).

Typische Auftragsdatenbearbeiterinnen oder Auftragsdatenbearbeiter sind etwa:

- Hosting-Firmen, die Daten einer Organisation für diese speichern,
- Anbieterinnen und Anbieter von Softwarelösungen, die die Kirchgemeinde für ihre Zwecke einsetzt, oder
- eine Marketingagentur, die im Auftrag einer Kirchgemeinde ein Kommunikationskonzept umsetzt.

Auch hier ist wichtig: Wenn die Datenbearbeitung durch ein Unternehmen vorgenommen wird, nimmt das Unternehmen die Rolle der Auftragsdatenbearbeiterin wahr, nicht die einzelnen Mitarbeitenden.

4.4 Vertrag über die Auftragsdatenbearbeitung (oder: Auftragsdatenbearbeitungsvereinbarung, «ADV»)

Wie vorstehend ausgeführt, bleibt die oder der Verantwortliche auch bei der Beauftragung eines Dritten (Auftragsdatenbearbeiterin oder Auftragsdatenbearbeiter) verantwortlich für die Einhaltung der gesetzlichen Datenschutzpflichten. Bei jedem geplanten oder bestehenden Projekt, bei

dem Personendaten durch Dritte bearbeitet werden (physische Weitergabe oder Fernzugriff), braucht es deshalb immer einen Vertrag, der die Einhaltung der datenschutzrechtlichen Pflichten durch die oder den Dritten sicherstellt (§ 6 IDG).

Eine solche Auftragsdatenbearbeitungsvereinbarung (kurz ADV) regelt unter anderem Folgendes (§ 25 IDV):

- Umschreibung des Projekts/der Dienstleistung und Angabe des Zwecks der Datenbearbeitung sowie Nennung der betroffenen Personendaten Gruppen;
- Geheimhaltungsverpflichtungen;
- Den Umgang mit Informationszugangsgesuchen;
- Pflicht zur Umsetzung geeigneter TOMs (technischer und organisatorischer Schutzmassnahmen) und Beschreibung der implementierten Massnahmen;
- Die Kontrolle der Auftragserfüllung und damit einhergehend die Vereinbarung von Auditrechten und die Pflichten bei Vertragsauflösung (bspw. Löschung der Daten);
- Sanktionen bei Pflichtverletzung durch die Auftragsdatenbearbeiterin oder den Auftragsdatenbearbeiter;
- Die Vertragsdauer und die Kündigungsbedingungen.

► *Eine Vorlage für eine ADV inklusive TOMs und Erläuterungen dazu stehen den Kirchgemeinden in den Schulungsunterlagen auf OpenOLAT zur Verfügung.*

4.5 Datenübermittlung ins Ausland

4.5.1 Übermittlung von Personendaten

Im Zusammenhang mit der Auftragsdatenbearbeitung kann es sein, dass eine der folgenden Situationen auftritt:

- Bei der Auftragsdatenbearbeiterin handelt es sich um ein Unternehmen mit Sitz im Ausland; oder
- die Auftragsdatenbearbeiterin ist zwar eine lokale Firma, hostet Daten aber im Ausland (d.h. die Daten werden auf einem Server im Ausland gespeichert).

Hierbei gilt es eine äusserst wichtige Unterscheidung zu beachten: Es gibt unter dem Gesichtspunkt des Datenschutzes sichere und unsichere Drittländer. Tritt eine der aufgelisteten Situationen ein, ist immer zu prüfen, welche Länder ausser der Schweiz betroffen sind (dies kann aufwändige Recherchen mit sich bringen!).

Gelten die betroffenen Länder als sichere Drittländer (d.h. Länder mit einem adäquaten Datenschutzrecht), ist es mit einer geeigneten ADV und genügenden TOMs zulässig, die Auftragsdatenbearbeiterin beizuziehen. Als sichere Drittländer gelten die Länder der EU, Andorra, Argentinien, Kanada (teilweise, d.h. für Datenbearbeitungen im Rahmen kommerzieller Tätigkeiten), Guernsey, Isle of Man, Island, Israel, Jersey, Liechtenstein, Monaco, Norwegen, Neuseeland, UK (inkl. Gibraltar) und Uruguay.

Gelten die betroffenen Länder als unsichere Drittländer (die USA gelten u.a. als unsicheres Drittland), ist die Nutzung der Dienstleistung grundsätzlich zu vermeiden, und es müssen primär Alter-

nativlösungen aus Europa, d.h. EWR/Schweiz oder sonstigen sicheren Drittländern, gesucht werden.[3] Alternativ müssen die Personen- und anderen schützenswerten Daten rechtlich genügend verschlüsselt werden (oder vollständig anonymisiert, was in der Praxis jedoch nur schwer erreichbar ist).

Falls man sich für einen Auftragsdatenbearbeiter mit Datenbearbeitungen in unsicheren Drittstaaten entscheiden will, so ist folgendes Vorgehen zu wählen:

- Es ist genügend Zeit für die rechtliche Klärung und Vertragsverhandlung einzuplanen;
- Beim Entscheid, ob das Projekt umgesetzt werden soll, muss der zusätzliche zeitliche und finanzielle Aufwand für umfangreiche Risikoeinschätzungen und diverse Vertragskonstrukte einberechnet und berücksichtigt werden;
- Sind strafrechtlich geschützte Daten (Amts- oder Berufsgeheimnisse) involviert, erhöht sich der zeitliche und finanzielle Aufwand zusätzlich;
- Die allfälligen Restrisiken sind durch die Verantwortlichen zu tragen und dies ist entsprechend zu dokumentieren.

4.5.2 Übermittlung von Amtsgeheimnissen

a) Sinn, Zweck und Inhalt des Amtsgeheimnisses

Bei der Übermittlung von Daten ins Ausland sind neben den Personendaten die Daten unter dem Amtsgeheimnis zusätzlich zu berücksichtigen. Denn als öffentliche Institutionen unterliegen die Kirchgemeinden bzw. deren Mitarbeitenden der Pflicht zur Geheimhaltung solcher Amtsgeheimnisse. Das Amtsgeheimnis schützt nicht nur Personendaten, sondern Informationen, die Im Zuge der öffentlichen Tätigkeit erlangt werden und die aufgrund öffentlicher oder privater Interessen geheimzuhalten sind.

Sinn und Zweck des Amtsgeheimnisschutzes ist das Interesse des Staates an der Diskretion seiner Angestellten, damit die Preisgabe sensibler Informationen durch die Bürgerinnen und Bürger an die Behörden und deren Angestellten zumutbar ist. Weiter dient das Amtsgeheimnis dem Schutz der Privatsphäre als Individualinteresse der Bürgerin und des Bürgers.

Ein Amtsgeheimnis ist gegeben, wenn

- nach dem für die Ausübung des Amtes massgebenden Gesetz eine Geheimhaltepflicht besteht und
- es sich materiell um ein Geheimnis (öffentliches oder privates Geheimhaltungsinteresse) handelt und
- das Geheimnis im Rahmen der Tätigkeit als Amtsträgerin oder Amtsträger in Erfahrung gebracht wurde.

Was genau unter das Amtsgeheimnis fällt, muss durch die jeweilige Kirchgemeinde individuell definiert werden unter Betrachtung möglicher anwendbarer gesetzlicher Bestimmungen, geltender verbindlicher Vorschriften (Reglemente, Weisungen, Verträge etc.) sowie generell bestehender öffentlicher und privater Geheimhaltungsinteressen.

[3] Eine aktuelle und vollständige Liste aller sicheren und unsicheren Drittstaaten findet sich in Anhang 1 der Datenschutzverordnung des Bundes (DSV), die am 1. September 2023 in Kraft tritt und die sinngemäss beigezogen werden kann.

b) Konsequenzen bei der Übermittlung

Enthält ein Informationsbestand (voraussichtlich) Amtsgeheimnisse, so sind diese nicht an Dritte im Ausland bekannt zu geben.

Von der obigen Regel können Ausnahmen vorliegen, z.B. wenn eine genügende Verschlüsselung oder Anonymisierung gegeben ist (in der Praxis ist dies nur schwierig zu erreichen), eine gesetzliche Grundlage die Übermittlung erlaubt oder wenn eine Entbindung von der Geheimhaltung vorliegt.

Für die Beurteilung, ob ein solcher Ausnahmetatbestand vorliegt, sind stets die Ansprechperson für Datenschutzfragen sowie ggf. externe Expertinnen und Experten beizuziehen. Denn das Thema Amtsgeheimnis wird sehr kontrovers diskutiert, es fehlt eine klare Rechtspraxis, und die rechtlichen Konsequenzen für eine Institution bzw. deren Mitarbeitende können erheblich sein.

5 Die wichtigsten Datenschutzprozesse innerhalb einer Kirchgemeinde

5.1 Datenschutz-Folgenabschätzung (sowie ggf. Vorabkontrolle)

⇒ Vgl. grafische Übersicht im Anhang 1

Das Datenschutzgesetz sieht vor, dass die Auswirkungen einer Datenbearbeitung auf die betroffenen Personen immer vorab zu prüfen sind, und zwar bei jedem neuen Projekt, das die Bearbeitung von Personendaten mit sich bringt, sowie dann, wenn eine bestehende Datenbearbeitung angepasst wird.

Das heisst: Bei jeder neuen Software, die eingeführt wird, bei einem neuen Newsletter oder einer Veränderung eines Prozesses, muss man sich die Frage stellen: Welche Auswirkungen hat dies für die Privatsphäre der betroffenen Personen?

Die Datenschutz-Folgenabschätzung ist ein zusätzlicher Schritt im Arbeitsablauf: Die Mitarbeiterinnen und Mitarbeiter sollen jeweils innehalten und darüber nachdenken, was die neue oder veränderte Datenbearbeitung bewirkt, und dies dokumentieren. Eine Datenschutz-Folgenabschätzung ist immer dann notwendig, *wenn eine Bearbeitung von Personendaten beabsichtigt ist*. Es gehört also als Grundregel dazu, dass die datenschutzrechtlichen Auswirkungen geprüft werden, bevor die Kirchgemeinde beginnt, Daten zu bearbeiten, oder bevor eine bestehende Datenbearbeitung umgestellt wird (§ 10 Abs. 1 IDG). Je nachdem, wie umfangreich und sensitiv die Datenbearbeitung ist, wird diese Prüfung wenig oder mehr Zeit in Anspruch nehmen. Wichtig ist aber, dass sie durchgeführt wird.

Verantwortlich für die Initiierung der Datenschutz-Folgenabschätzung (sowie ggf. Vorabkontrolle) ist die bzw. der für eine Datenbearbeitung zuständige Mitarbeiterin bzw. Mitarbeiter. Sie bzw. er zieht für die Durchführung die Ansprechperson für Datenschutzfragen bei. Über allfällige Restrisiken entscheidet die Kirchenpflege als Gesamtgremium.

►*Die kt. Datenschutzbeauftragte stellt zurzeit auf ihrer Webseite ein Formular und ein Merkblatt zur Datenschutz-Folgenabschätzung zur Verfügung. Es wird empfohlen, dieses Formular zu benützen. Zurzeit sind die entsprechenden Informationen an folgender Stelle auffindbar: https://www.datenschutz.ch/datenschutz-in-oeffentlichen-organen/datenschutz-folgenabschaetzung.*

Nachfolgend wird erläutert, wann und wie eine Datenschutz-Folgenabschätzung durchzuführen ist.

5.1.1 Planungsphase

⇒ Vgl. grafische Übersicht: Schritt 1

Bevor man beginnt, Personendaten zu bearbeiten, bevor man Datenbearbeitungen anpasst, sogar *bevor man einen Vertrag über eine neue Software unterzeichnet* (sehr wichtig!), muss man sich über die Umsetzung des Datenschutzes Gedanken machen.

Das Datenschutzgesetz verlangt dazu die Durchführung einer Datenschutz-Folgenabschätzung.

5.1.2 Durchführung der Datenschutz-Folgenabschätzung

⇒ Vgl. grafische Übersicht: Schritt 2

Bei einer Datenschutz-Folgenabschätzung geht es inhaltlich darum, die nachfolgend aufgelisteten Schritte durchzuführen:

1. Beschreibung der Tätigkeit (z.B. «Einführung eines neuen Tools für den Versand eines Newsletters durch die Kirchgemeinde zum Thema 'Angebote für Jugendliche'»)
2. Zu welchem möglichst genauen Zweck (bzw. zu welchen Zwecken) sollen die Daten bearbeitet werden? (z.B. «Beziehungspflege zu Familien und Jugendlichen der Kirchgemeinde, die an Angeboten der Kirchgemeinde für Jugendliche von 12-17 Jahren interessiert sind)»
3. Welche Datenattribute werden bearbeitet? (z.B. E-Mail-Adresse, Vor- und Nachname)
4. Welche Kategorie(n) von Personen sind davon betroffen? (z.B. Behördenmitglieder, Interessierte, Personal, hier z.B.: «Mitglieder, teilweise minderjährig»)
5. Woher stammen die Daten? (z.B. aus einem Anmeldeformular auf einer Homepage)
6. Werden diese Daten danach für weitere Tätigkeiten genutzt?
7. Werden diese Daten mit einer anderen Organisation geteilt bzw. einer anderen Organisation weitergereicht?
8. Wer wird innerhalb der Kirchgemeinde Zugriff zu den Daten haben?
9. Angaben zum Unternehmen, dem Daten weitergegeben werden oder Fernzugriff gewährt wird (bspw. von dem eine allfällige Software lizenziert wird):
    - vollständiger Name und Rechtsform
    - Ort und Land des Sitzes
    - Vertragsentwürfe und/oder AGBs
10. Beschreibung von allfälligen Risiken, die im Zusammenhang mit dem Projekt erkennbar sind (z.B. «Aufgrund eines Sicherheitsproblems bei der Anbieterin oder dem Anbieter des Newsletters könnten E-Mail-Adressen im Internet frei zugänglich werden.»).
11. Falls bereits vorhanden: Massnahmen, wie man die unter Punkt 10. beschriebenen Risiken reduzieren könnte (z.B. Verweis auf den Teil des Vertrags, der detaillierte Sicherheitsmassnahmen auflistet, oder: Abschluss eines Vertrags über die Auftragsdatenbearbeitung [ADV]).

Wichtig: Bei den aufgezählten Punkten handelt es sich lediglich um eine Auswahl von wichtigen Aspekten. Es empfiehlt sich, das auf der Website der kantonalen Aufsichtsstelle zur Verfügung gestellte Formular auszufüllen sowie das dazugehörende Merkblatt zu lesen.

5.1.3 Evaluation: Besteht nach wie vor ein grosses Risiko oder nicht?

⇒ Vgl. grafische Übersicht: Schritt 3

Bei der Datenschutz-Folgenabschätzung geht es nicht nur darum, die Datenbearbeitung zu beschreiben und darüber nachzudenken, welche Risiken sie für die betroffenen Personen mit sich bringen könnte. Die Datenschutz-Folgenabschätzung ist zugleich der Moment, in dem Massnahmen ergriffen oder geplant werden, welche die erkannten Risiken verringern oder vollständig vermeiden sollen.

Entsprechend ist die Mitarbeiterin oder der Mitarbeiter in der Pflicht, zum Schluss der Datenschutz-Folgenabschätzung zusammen mit der Ansprechperson für Datenschutzfragen eine Einschätzung vorzunehmen: Bestehen auch nach Umsetzung der Massnahmen besondere Risiken für die Grundrechte der betroffenen Personen oder nicht?

Als besondere Risiken gelten unter anderem folgende Situationen (vgl. § 24 IDV):

- Es wird eine neue Technologie eingesetzt, z.B. eine Videoüberwachung mit softwaregestützten Analysefunktionen oder ein Zutrittssystem mit Erfassung von Fingerabdrücken.
- Es werden Personendaten im Abrufverfahren über eine Webseite zur Verfügung gestellt.
- Drei oder mehr öffentliche Organe bearbeiten Daten gemeinsam (bei der Kirchgemeinde dürfte dieser Sachverhalt bei ökumenischen Projekten zum Tragen kommen).
- Es werden eine Vielzahl besonderer Personendaten oder Personendaten sehr vieler Personen bearbeitet.

5.1.4 Schlussfolgerung dokumentieren oder Vorabkontrolle

⇒ Vgl. grafische Übersicht: Schritt 4

Bestehen auch mit den getroffenen Massnahmen besondere Risiken gemäss der vorstehenden Liste, so ist die Datenbearbeitung bzw. das neue Projekt der kantonalen Aufsichtsstelle zur Vorabkontrolle zu unterbreiten.

Die dokumentierte Datenschutz-Folgenabschätzung ist hierfür der Kirchenpflege vorzulegen. Sie entscheidet über die Vorlage der Datenschutz-Folgenabschätzung an die kantonale Aufsichtsstelle (Vorabkontrolle) bzw. die allfällige Inkaufnahme von Restrisiken.

Achtung: Wenn sich dieser Schritt als nötig erweist, muss die Zeit, welche die kantonale Aufsichtsstelle zur Prüfung des Projekts benötigt, mit eingerechnet werden. *Bis eine positive Rückmeldung vorliegt, dürfen keine Verträge abgeschlossen oder Umsetzungsarbeiten gestartet werden.* Ansonsten wird das Risiko eingegangen, dass getroffene Massnahmen wieder rückgängig gemacht werden müssen oder dass die kantonale Aufsichtsstelle Anpassungen verlangt, die nachträglich nur schwer vorgenommen werden können.

5.2 Informationszugangsgesuche (Gesuche um Zugang zu amtlichen Informationen)

⇒ Vgl. grafische Übersicht im Anhang 2

Als Körperschaft des öffentlichen Rechts hat eine Kirchgemeinde im Grundsatz amtliche Informationen der Öffentlichkeit zur Verfügung zu stellen (Öffentlichkeitsprinzip). Entsprechend sieht das Datenschutzgesetz vor, dass jede Person Anspruch auf «Zugang zu den bei einem öffentlichen Organ vorhandenen Informationen» hat (§ 20 Abs. 1 IDG). Im Einzelfall kann es aber durchaus auch entgegenstehende Interessen geben, die der Bekanntgabe eines Dokuments oder einer Information entgegenstehen, weshalb Gesuche immer im Einzelfall zu prüfen sind.

Das Datenschutzgesetz schreibt vor, dass ein Informationszugangsgesuch *innert 30 Tagen* zu beantworten ist. Ist dies nicht möglich, ist die gesuchstellende Person rechtzeitig zu informieren. Sie

muss über die Gründe für die Verzögerung sowie den Zeitpunkt, wann sie einen Entscheid erhalten wird, informiert werden (§ 28 IDG).

Für die inhaltliche Bearbeitung eines Informationszugangsgesuchs ist die Ansprechperson für Datenschutzfragen zuständig, die von den Mitarbeitenden über den Gesucheingang informiert werden muss (siehe dazu nachstehend Ziffer 5.2.1).

Die Gesamtverantwortung für die korrekte und fristgerechte Beantwortung von Informationszugangsgesuchen obliegt jedoch der Kirchenpflege; diese entscheidet letztendlich über die Gewährung bzw. Einschränkung des Informationszugangs.

5.2.1 Gesuchseingang

⇒ Vgl. grafische Übersicht: Schritt 1

5.2.1.1 Zuständigkeit

Geht ein Gesuch bei einer Mitarbeiterin oder einem Mitarbeiter ein, so ist es unverzüglich (Frist: 1 Arbeitstag!) an die Ansprechperson für Datenschutzfragen weiterzuleiten.

5.2.1.2 Form des Gesuchs

Zwar spricht das Datenschutzgesetz davon, dass es für den Zugang zu amtlichen Informationen ein «Gesuch» braucht (§ 24 IDG). Es ist aber zu differenzieren:

- Formlose Anfrage:
    - Allgemeine Auskünfte zur Tätigkeit der Kirchgemeinde und zu als öffentlich klassifizierten Informationen können durch formlose Anfrage, also per E-Mail, per Telefon oder sogar mündlich vor Ort eingeholt werden (§ 7 Abs. 1 IDV). Solche Auskünfte können auf demselben Weg erteilt werden, wie sie erfragt wurden (§ 24 Abs. 2 IDG, § 10 Abs. 1 IDV).
- Schriftliches Gesuch:
    - Sobald eine Anfrage *über eine allgemeine Auskunft hinausgeht* und konkrete Dokumente betrifft, die nicht als öffentlich klassifiziert sind, muss die interessierte Person ein schriftliches Gesuch stellen (§ 8 Abs. 1 IDV). Schriftlich bedeutet, dass das Gesuch eigenhändig und im Original unterzeichnet ist oder eine rechtsgültige digitale Signatur enthält.
    - Betrifft das Gesuch Informationen einer Kirchgemeinde, *die Personendaten Dritter enthalten* oder *Informationen, die als vertraulich klassifiziert sind*, so kann keine Herausgabe auf formlose Anfrage hin erfolgen. In einem solchen Fall ist der gesuchstellenden Person mitzuteilen, dass sie ihr Gesuch schriftlich zu stellen hat, und dass dieses Kostenfolgen haben kann (§ 7 Abs. 2 lit. a IDV i.V.m. § 26 IDG).
    - Dasselbe gilt, wenn die ersuchten Informationen nicht ohne Weiteres herausgegeben werden können, weil eine *Interessenabwägung* vorgenommen werden muss, die vertiefter Abklärungen bedarf – so etwa, wenn das Gesuch Informationen aus einem laufenden Verfahren oder die Position einer Kirchgemeinde in Vertragsverhandlungen betrifft (die vollständige Liste der Gründe ist in § 23 IDG aufgeführt).
    - Dasselbe gilt ferner, wenn die Bearbeitung des Gesuchs *mit besonderem Aufwand verbunden* ist (z.B., weil eine grosse Anzahl Dokumente verlangt werden).

Das schriftliche Gesuch muss möglichst genau bezeichnen, worauf es sich bezieht (Inhalt, Dokumente, Datum der Entstehung, wer die Informationen verfasst hat [§ 8 Abs. 2 IDV]).

Ist das eingehende Gesuch nicht genügend klar formuliert, so ist eine Präzisierung von der gesuchstellenden Person einzufordern. Wenn diese Präzisierung nicht innert *zehn Tagen* erfolgt, darf die Kirchgemeinde das Gesuch als zurückgezogen betrachten (§ 8 Abs. 3 und 4 IDV).

Im Zweifelsfall wird empfohlen, dass von der gesuchstellenden Person ein schriftliches Gesuch verlangt und der Prozess dokumentiert wird.

5.2.2 Prüfung: Sind die gewünschten Informationen herauszugeben?

⇒ Vgl. grafische Übersicht: Schritt 2

Betrifft ein Gesuch öffentlich verfügbare Informationen, reicht es, die Quelle der Informationen anzugeben (z.B. Webseite der Kirchgemeinde; vgl. § 25 Abs. 1 IDG).

Eine vertiefte Prüfung ist namentlich in denjenigen Fällen nötig, in denen es ein schriftliches Gesuch braucht (siehe oben Ziff. 5.2.1.2), nämlich:

- Das Gesuch betrifft Personendaten Dritter oder vertrauliche Informationen.
- Es sind entgegenstehende Interessen abzuwägen.
- Die Bearbeitung des Gesuchs erscheint als sehr aufwändig.

Achtung: Wenn das Gesuch Informationen aus einem laufenden Verwaltungsverfahren betrifft, richtet sich das Recht auf Zugang nach dem entsprechenden Verfahrensrecht (§ 20 Abs. 3 IDG).

Geht es um Informationen, die eine Kirchgemeinde von einer anderen öffentlichen Behörde erhalten hat, so ist das Gesuch an die betreffende Behörde zur Behandlung zu überweisen (§ 9 Abs. 2 IDG). Wenn Informationen mehrerer Organisationen betroffen sind, so spricht sich die Kirchgemeinde mit den anderen Organisationen über die Behandlung und Beurteilung des Gesuchs ab (§ 9 Abs. 3 IDV).

5.2.3 Stellungnahme durch Dritte, Entscheid betreffend Informationszugang

⇒ Vgl. grafische Übersicht: Schritte 2-3

Die Ansprechperson für Datenschutzfragen prüft das Informationszugangsgesuch auf Hinweis der Mitarbeiterin bzw. dem Mitarbeiter, bei denen das Gesuch eingegangen ist. Die Beurteilung des Gesuchs wird sodann der Kirchenpflege vorgelegt. Gelangt sie zum Schluss, dass die Information herauszugeben ist, so erfolgt die Herausgabe gemäss Ziffer 5.2.4 nachstehend.

Betrifft das Zugangsgesuch Personendaten oder besondere Personendaten Dritter, so ist diesen betroffenen Dritten eine Frist einzuräumen, um dazu Stellung zu nehmen, ob aus ihrer Sicht die sie betreffenden Informationen herauszugeben sind oder nicht. *Besondere Personendaten dürfen ohne ausdrückliche Zustimmung der betroffenen Personen nicht herausgegeben werden* (§ 26 IDG).

Achtung: Die Frist zur Stellungnahme ist mit der Gesamtfrist zur Beantwortung des Zugangsgesuchs zu koordinieren. Zeichnet sich ab, dass mit der Frist zur Stellungnahme durch die betroffenen Personen die 30 Tage nicht eingehalten werden können, so ist eine Fristverlängerung zu definieren und der gesuchstellenden Person mit Begründung zu kommunizieren (vgl. zur Frist zur Stellungnahme § 26 IDG).

Stellt sich heraus, dass die Information nicht herauszugeben ist oder dass es sich um einen komplexen Fall handelt (namentlich weil als vertraulich klassifizierte Informationen betroffen sind), so hat die Kirchenpflege auf Vorlage der Ansprechperson für Datenschutzfragen über das Gesuch zu beraten und beschliessen. Eine Antwort auf das Gesuch, in welcher der Zugang verweigert oder nur teilweise gewährt wird, wird in Form eines Kirchenpflegebeschlusses an die betreffende Person kommuniziert. Der Beschluss ist mit einer Rechtsmittelbelehrung an den Bezirksrat zu versehen. Ein

Beschluss ist ebenfalls derjenigen Drittpersonen zuzustellen, deren Personendaten in den Unterlagen oder Informationen enthalten sind und die sich gegen die Veröffentlichung ausgesprochen hatten (vgl. zum Ganzen (§ 27 IDG).

5.2.4 Kommunikation an die gesuchstellende Person und Gewährung des Zugangs

⇒ Vgl. grafische Übersicht: Schritt 4

Der Entscheid der Kirchenpflege über die Gewährung, Einschränkung oder Nichtgewährung des Zugangs ist zu dokumentieren.

Wird der Informationszugang der gesuchstellenden Person auf formlose Anfrage gewährt, so kann das Gesuch ebenfalls formlos, d.h. mündlich, telefonisch oder auf elektronischem Wege beantwortet werden.

Wurde das Gesuch schriftlich gestellt (zu den Fällen, in denen ein schriftliches Gesuch nötig ist, siehe Ziff. 5.2.1.2), kann der Zugang in folgender Form gewährt werden:

- Zustellung von Kopien,
- Einsichtnahme vor Ort bei der Kirchgemeinde,
- auf elektronischem Wege (nur soweit keine Personendaten enthalten sind oder ein genügender Schutz bei der Übermittlung gegeben ist; § 10 Abs. 3 IDV).

Wenn die Einsichtnahme vor Ort gewährt wird, kann die gesuchstellende Person um die Erstellung von Kopien bitten. Die Kirchenpflege bzw. auf deren Anweisung die Ansprechperson für Datenschutzfragen kann die Identität der Person beim Zutritt zu den Räumlichkeiten kontrollieren. Diejenigen Informationen, die aufgrund überwiegender Interessen von Drittpersonen oder Interessen der Kirchgemeinde nicht zur Einsicht freigegeben werden, sind abzudecken bzw. zu schwärzen. Ist dies nicht sinnvoll möglich, kann stattdessen eine Zusammenfassung eines Dokuments erstellt und zugänglich gemacht werden (vgl. zum Ganzen § 11 und 13 Abs. 2 IDV).

Erhält die Kirchgemeinde viele Gesuche, die sich alle auf dieselben Informationen beziehen, kann der Einfachheit halber auch ein anderer Weg gewählt werden, um Zugang zu gewähren (z.B. Online-Einsicht mit Zustellung eines Passworts). Bei sehr aufwändigen Gesuchen, die derart viel Arbeit verursachen, dass darunter die Erfüllung der eigentlichen Aufgaben der Kirchgemeinde leidet, kann die gesuchstellende Person zuerst gebeten werden, schriftlich darzulegen, welches schutzwürdige Interesse sie daran hat, Zugang zu den entsprechenden amtlichen Unterlagen oder Informationen der Kirchgemeinde zu erhalten. Wird der Nachweis erbracht, kann die 30-tägige Frist für die Gewährung des Zugangs entsprechend («angemessen») verlängert werden (vgl. zum Ganzen § 25 Abs. 2 IDG, § 14 und 15 Abs. 2 IDV).

5.2.5 Gebühren

Im Normalfall werden Informationszugangsgesuche gebührenfrei bearbeitet. Gebühren können dann erhoben werden, wenn der Aufwand für den Informationszugang erheblich ist und in keinem Verhältnis zum öffentlichen Interesse steht (§ 29 Abs. 2 IDG). Falls der Informationszugang Kosten verursacht, ist die gesuchstellende Person darauf hinzuweisen, und das öffentliche Organ kann eine angemessene Vorauszahlung verlangen.

5.3 Rechte der betroffenen Person

⇒ Vgl. grafische Übersicht im Anhang 3

5.3.1 Allgemeines für alle Betroffenenrechte

Das Datenschutzgesetz sieht verschiedene Ansprüche vor, die eine von einer Datenbearbeitung betroffene Person im Zusammenhang mit ihren eigenen Personendaten bei der Kirchgemeinde geltend machen kann. Im Folgenden wird der Prozess anhand des Rechts auf *Zugang* zu den eigenen Personendaten erläutert. Daneben sind weitere Rechte vorgesehen, die nachstehend unter Ziffern 5.3.6-5.3.9 beschrieben werden.

Der Prozess bei Geltendmachung von Betroffenenrechten wird durch diejenige Mitarbeiterin bzw. denjenigen Mitarbeiter initiiert, bei welcher bzw. welchem ein Gesuch eingeht. Inhaltlich wird das Gesuch durch die Ansprechperson für Datenschutzfragen bearbeitet. Bei komplexen oder heiklen Fällen entscheidet die Kirchenpflege als Gesamtverantwortliche.

Wichtig: Die Auskunft ist in der Regel innert 30 Tagen ab erfolgter Identifikation der gesuchstellenden Person zu erteilen. In komplexen Fällen kann diese Frist verlängert werden. Die gesuchstellende Person ist über diese Verlängerung zu informieren.

5.3.2 Eingang des Gesuchs/Nachweis der Identität

⇒ Vgl. grafische Übersicht: Schritte 1-2

Das Gesetz sieht vor, dass ein Gesuch schriftlich oder telefonisch gestellt werden kann. Geht eine Anfrage per Telefon ein, wird jedoch empfohlen, die gesuchstellende Person darauf hinzuweisen, dass sie ihre Anfrage bei der Kirchgemeinde schriftlich einreichen muss.

Gesuche, die bei einer Mitarbeiterin oder einem Mitarbeiter eingehen, sind unverzüglich (Frist: 1 Arbeitstag!) an die Ansprechperson für Datenschutzfragen weiterzuleiten.

Die gesuchstellende Person muss ihre Identität nachweisen. Wird aus dem Gesuch klar, um wen es sich handelt (z.B. geht ein unterzeichnetes Schreiben einer Pfarrperson ein, die von einer Kirchgemeinde angestellt war und entsprechend bekannt ist), steht die Identität bereits fest. Es muss kein weiterer Nachweis verlangt werden. Wenn die Identität nicht zweifelsfrei feststeht, ist durch geeignetes Nachfragen oder allenfalls durch eine Ausweiskopie die Identität zu eruieren. Bei Vorlage von Ausweiskopien ist die gesuchstellende Person darauf hinzuweisen, dass sie nicht erforderliche Informationen schwärzen kann.

Weist sich die gesuchstellende Person innerhalb der gesetzten Frist aus, so ist die Anfrage inhaltlich zu prüfen. Unterlässt sie dies, so muss die Anfrage nicht beantwortet werden.

5.3.3 Suche nach den Personendaten der gesuchstellenden Person

⇒ Vgl. grafische Übersicht: Schritte 3-4

Der in der Praxis wichtigste Anspruch ist der *Zugang* zu den eigenen Personendaten. Eine Person kann verlangen, dass ihr die vollständige Liste aller Daten gezeigt wird, welche die Kirchgemeinde über sie bearbeitet (§ 20 Abs. 2 IDG; § 18 Abs. 3 lit. a IDV).

Dabei gibt es zwei Herausforderungen:

- Es sind alle Datensammlungen und Orte zu identifizieren, an denen sich Daten der betreffenden Person befinden könnten. Dieselben Daten können sich u.U. in mehreren Systemen, Dokumenten oder Applikationen befinden.

- Es ist daran zu denken, dass nicht nur solche Daten herauszugeben sind, die eine Person eindeutig identifizieren (d.h. Name und Vorname, Adresse, E-Mail-Adresse, etc.) sondern auch Daten, die indirekt Auskunft über die betroffene Person geben können. So z.B.:
    - Daten der Arbeitszeiterfassung oder Badge-Daten, wenn solche genutzt werden, um Zugang zu Arbeitsräumlichkeiten zu erlangen. Wenn die Listen mit den Uhrzeiten innerhalb einer Kirchgemeinde der betroffenen Person zugeordnet werden können, so handelt es sich um Personendaten, die je nach Anfrage (z.B. von einer ehemaligen Mitarbeiterin oder einem ehemaligen Mitarbeiter) herauszugeben sind.
    - Logdaten, die über die Nutzung von Arbeitsgeräten Auskunft geben. Wenn von einer Kirchgemeinde zur Verfügung gestellte Laptops mit der Gerätenummer (MAC-Adresse) oder auf sonstige Weise (IP-Adresse o.ä.) der entsprechenden Person zugeordnet werden können, so sind u.U. auch Serverlog-Daten, die diese Ziffernfolgen enthalten, herauszugeben. Je nachdem ist also für die Beantwortung eines Zugangsgesuchs auch die Hilfe externer IT-Anbieter einzuholen, und es ist ihnen das Zugangsgesuch weiterzuleiten.

Zuständig für die Suche und Herausgabe der Daten ist die oder der für einen Prozess oder Infrastruktur verantwortliche Mitarbeiterin oder Mitarbeiter. Die Ansprechperson für Datenschutzfragen unterstützt dabei.

Werden für die Suche nach den entsprechenden Daten weitere Personen (intern oder extern) um Unterstützung gebeten, so ist ihnen eine *Frist von 5 Arbeitstagen* zu geben, um die gewünschten Daten zusammenzustellen.

5.3.4 Prüfung des Gesuchs

⇒ Vgl. grafische Übersicht: Schritt 5

Sobald die nachgesuchten Personendaten bei der Ansprechperson für Datenschutzfragen eingegangen sind, prüft diese, ob vor Gewährung des Zugangs Daten zu schwärzen oder zu entfernen sind (Daten von Dritten in Dokumenten, Informationen, die dem Amtsgeheimnis unterliegen, o.ä.). In komplexen oder heiklen Fällen zieht sie die Kirchenpflege zur Beurteilung bei.

5.3.5 Beantwortung des Gesuchs

⇒ Vgl. grafische Übersicht: Schritt 6

Sind alle Daten definiert, zu denen Zugang zu gewähren ist, so können sie auf folgendem Weg zur Verfügung gestellt werden:

- schriftlich (Ausdruck oder Fotokopie),
- je nachdem auf andere geeignete Weise (Einsicht vor Ort, elektronisch [bspw. E-Mail], mündlich), wobei elektronisch und mündlich nur mit Zustimmung der gesuchstellenden Person zulässig sind.

Bei elektronischer Übermittlung ist zudem sicherzustellen, dass die Daten genügend geschützt sind (Verschlüsselung der Dokumente mit einem Passwort, das der gesuchstellenden Person auf anderem Kanal, z.B. per Telefon, mitzuteilen ist – kein ungesicherter Versand als E-Mail-Beilage).

Zudem ist der gesuchstellenden Person über Folgendes Auskunft zu geben (§ 18 Abs. 3 lit. b IDV):

- Zweck(e) der Datenbearbeitung,

- Rechtsgrundlage(n) der Datenbearbeitung,
- die an der Datenbearbeitung beteiligten Stellen,
- allfällige Dritte, die regelmässig von der Kirchgemeinde die Personendaten der gesuchstellenden Person erhalten (z.B. Projektpartner in der ökumenischen Zusammenarbeit, kantonale/kommunale Ämter oder Bundesämter, etc.).

5.3.6 Berichtigung/Löschung unrichtiger Personendaten

Nebst dem Zugang zu den eigenen Personendaten kann auch eine *Berichtigung oder Löschung von Personendaten* verlangt werden (§ 21 Abs. 1 li. a IDG). In beiden Fällen ist Voraussetzung dieses Anspruchs, dass es sich um *unrichtige* Personendaten handeln muss. *Weil eine Kirchgemeinde als öffentliches Organ des kantonalen Rechts im Vollzug gesetzlicher Aufgaben Personendaten bearbeitet, dürfen korrekte Personendaten in den meisten Fällen nicht auf Gesuch der betroffenen Person hin gelöscht werden.* Dies ist ein wichtiger Unterschied zur Privatwirtschaft, wo die Datenlöschung breiter zugelassen wird.

Gesuche auf Löschung von Personendaten sind somit sorgfältig durch die Ansprechperson für Datenschutzfragen und bei Bedarf unter Beizug der Kirchenpflege zu prüfen.

5.3.7 Ansprüche im Zusammenhang mit unrechtmässiger Datenbearbeitung

Werden Personendaten «widerrechtlich» bearbeitet, so kann die betroffene Person verlangen, dass die Kirchgemeinde dieses unrechtmässige Bearbeiten einstellt («unterlässt»), die Folgen davon beseitigt und/oder feststellt, dass die Bearbeitung unrechtmässig war (§ 21 Abs. 1 lit. b-d IDG).

Eine Datenbearbeitung durch eine Kirchgemeinde ist etwa dann unrechtmässig, wenn die Datenbearbeitung nicht durch eine Rechtsgrundlage gedeckt ist. Dies ist dann der Fall, wenn die Datenbearbeitung nicht zur Erfüllung der Aufgaben einer Kirchgemeinde erfolgt.

5.3.8 Datensperre

Darüber hinaus kann eine betroffene Person unter gewissen – einschränkenden – Bedingungen verlangen, dass die Kirchgemeinde ihre Personendaten sperrt, d.h. nicht an Private bekannt gibt (§ 22 IDG). Voraussetzung dafür ist, dass die Kirchgemeinde aufgrund einer Bestimmung in einem Spezialgesetz Personendaten voraussetzungslos bekannt geben kann. Das Kirchliche Datenschutz-Reglement[4] sieht vor, dass Daten gesperrt werden können. Die Weitergabe an andere öffentliche Behörden ist auch mit einer Datensperre nicht ausgeschlossen.

Wichtig: Nur die *Bekanntgabe* an Dritte kann verhindert werden. Gemeint ist damit, dass Personendaten der Drittperson zur Verfügung gestellt werden, damit diese sie zu eigenen Zwecken bearbeitet. Anders behandelt wird bspw. der Fall, wenn eine Druckerei als privates Unternehmen für die Kirchgemeinde einen Flyer erstellt und verschickt. Die Druckerei handelt dabei *im Auftrag* der Kirchgemeinde und wird dieser als Lieferantin rechtlich zugerechnet (sie ist *Auftragsdatenbearbeiterin*, siehe dazu vorstehend Ziffer 4.3). Eine solche Weitergabe ist keine «Bekanntgabe» und fällt deshalb nicht unter die hier diskutierte Datensperre.

5.3.9 Sonderfall: Auskunft über verstorbene Personen

Es kann vorkommen, dass eine Person Auskunft über Personendaten verlangt, die nicht sie selbst betreffen, sondern eine verstorbene Person. In einem solchen Fall kann Auskunft erteilt werden, wenn folgende Voraussetzungen *kumulativ* erfüllt sind (§ 19 IDV):

---

[4] § 6 des Kirchlichen Datenschutz-Reglements vom 15./6. Dezember 1999 und 23. Mai 2000 (LS 180.7).

- Die gesuchstellende Person weist ein *Interesse* an der Auskunft nach.
- Der Auskunft stehen *keine überwiegenden Interessen* von *Angehörigen* der verstorbenen Person oder von *Dritten* entgegen.

Das Interesse der gesuchstellenden Person an der Auskunft ist von Gesetzes wegen dann gegeben, wenn diese in naher Verwandtschaft oder im Todeszeitpunkt in einer Lebensgemeinschaft zur bzw. mit der verstorbenen Person stand (Ehe, eingetragene Partnerschaft oder eheähnliche Lebensgemeinschaft).

5.4 Meldepflicht Datenschutzvorfall

⇒ Vgl. grafische Übersicht im Anhang 4

Das Datenschutzgesetz verlangt, dass die «unbefugte Bearbeitung» und der «Verlust» von Personendaten unverzüglich der kantonalen Aufsichtsstelle zu melden sind (§ 12a IDG). Die kantonale Aufsichtsstelle nennt dies auch einen «Datenschutzvorfall».

Verantwortlich für die Initiierung des Prozesses ist die Mitarbeiterin bzw. der Mitarbeiter, die bzw. der von einem (mutmasslichen) Datenschutzvorfall Kenntnis erhält. Sie bzw. er meldet dies unverzüglich (!) der Ansprechperson für Datenschutzfragen. Diese bearbeitet den Vorfall inhaltlich. Wenn eine IT-Fachperson oder sogar eine Sicherheitsbeauftragte oder ein Sicherheitsbeauftragter vorhanden ist, sollte diese Person für die Beurteilung der technischen Aspekte des Vorfalls unbedingt beigezogen werden. Bei komplexen oder heiklen Fällen wird auch die Kirchenpflege rechtzeitig informiert.

In jedem Fall sind der Kirchenpflege die nötigen Massnahmen zur Behebung des Vorfalls zum Beschluss zu unterbreiten. Ebenfalls zum Beschluss unterbreitet wird die Meldung an die kantonale Aufsichtsstelle, wofür die Kirchenpflege die finale Verantwortung trägt.

5.4.1 Was ist ein Datenschutzvorfall?

⇒ Vgl. grafische Übersicht: Schritt 1

Unter Datenschutzvorfall versteht man alle Verletzungen der Sicherheit von Personendaten; die «unbefugte Bearbeitung» und der «Verlust» sind dafür lediglich zwei Beispiele. Laut Gesetz gelten die Pflichten zu Datenschutzvorfällen nur bei Personendaten. In der Praxis dürfte es bei den Kirchgemeinden aber so sein, dass bei jedem Datenschutzvorfall unweigerlich auch Personendaten im Datensatz vorhanden und somit betroffen sind. Daher ist *jeder* Datenverlust oder *jeder* unbefugte Zugang zu Daten einer Kirchgemeinde vorsorglich als Datenschutzvorfall zu behandeln.

U.a. stellen folgende Sachverhalte Datenschutzvorfälle dar:

- Ein USB-Stick, eine CD-ROM, ein Laptop oder ein Mobiltelefon mit dienstlichen Daten geht verloren.
- Daten sind plötzlich nicht mehr vorhanden oder sind inhaltlich unrichtig.
- Eine nicht berechtigte Person hatte Zugriff auf Daten einer Kirchgemeinde (z.B. Logins wurden geteilt).
- Daten wurden von Mitarbeiterinnen und Mitarbeitern auf nicht zugelassenen Cloud-Lösungen gespeichert.
- Daten wurden von Mitarbeiterinnen und Mitarbeitern an ihre privaten E-Mail-Adressen oder an unbefugte Dritte weitergeleitet.

- Es besteht die Vermutung, dass eine Cyberattacke ausgeübt wurde oder Schadsoftware (Ransomware, Viren, etc.) auf ein Gerät gelangt ist.

5.4.2 Interne Meldepflicht

⇒ Vgl. grafische Übersicht: Schritt 2

Sobald eine Mitarbeiterin oder ein Mitarbeiter vermutet, dass ein Datenschutzvorfall eingetreten sein könnte, ist dies intern sofort der Ansprechperson für Datenschutzfragen zu melden (per E-Mail oder Telefon). Bei komplexen oder heiklen Fällen wird auch direkt das Kirchenpflegepräsidium informiert.

Es ist so viel Information und Kontext wie möglich zu geben, damit die benachrichtigten Stellen den Vorfall abklären können.

Wichtig: Die Meldung muss *sofort* erfolgen; sie geht dem Tagesgeschäft immer vor! Nur mit einer sofortigen Benachrichtigung ist es der Kirchgemeinde möglich, den Sachverhalt im Rahmen der gesetzlichen Frist abzuklären und ggf. die kantonale Aufsichtsstelle zu informieren. Erfolgt eine Meldung nicht rechtzeitig, können sich daraus für die betroffene Kirchgemeinde rechtliche Konsequenzen ergeben.

5.4.3 Prüfung und ggf. Meldung an kantonale/-n Datenschutzbeauftragte/-n

⇒ Vgl. grafische Übersicht: Schritte 3, 4, 5

Sobald die gemäss Ziffer 5.4.2 zuständigen Stellen die Meldung erhalten haben, klärt die Ansprechperson für Datenschutzfragen ggf. unter Beizug weiterer Mitarbeitenden den Sachverhalt ab oder lässt ihn abklären (unverzüglich!). Es muss dabei eine Einschätzung vorgenommen werden, ob es sich um einen Datenschutzvorfall im Sinne des Datenschutzgesetzes handelt. Wenn ja, erlässt die Ansprechperson für Datenschutzfragen jeweils nach Rücksprache mit der Kirchenpflege Handlungsanweisungen zur Behebung oder Risikoverringerung. Gleichzeitig ist die Meldung an die kantonale Aufsichtsstelle vorzubereiten und einzureichen. Das Gesetz sieht eine «unverzügliche» Meldung vor, ohne eine Zeitangabe vorzunehmen. Zum Vergleich: Die EU-Datenschutz-Grundverordnung (die im Datenschutz zurzeit den Standard setzt) sieht verbindlich vor, dass Datenschutzverstösse innert 72 Stunden zu melden sind, also lediglich drei Kalendertage ab dem Zeitpunkt, in dem eine solide Vermutung besteht.

Die Verantwortung für die Meldung obliegt dem obersten geschäftsführenden Organ. Für die Kirchgemeinden ist es damit die Kirchenpflege bzw. aufgrund der Dringlichkeit das Kirchenpflegepräsidium, die oder das die vorbereitete Meldung genehmigen muss. Aufgrund der grossen Reputationsrisiken, die mit einem Datenschutzverstoss und der Meldung desselben verbunden sind, ist die Meldung besonders vorsichtig zu verfassen.

Wichtig ist, dass die Meldung an die kantonale Aufsichtsstelle so rasch wie möglich zu erfolgen hat.

Zum Vollzug der Meldepflicht kann das von der kantonalen Aufsichtsstelle zur Verfügung gestellte Formular verwendet werden (https://datenschutz.ch/datenschutz-in-oeffentlichen-organen/datenschutzvorfall-melden).

5.4.4 Information an die betroffenen Personen

⇒ Vgl. grafische Übersicht: Schritt 6

In gewissen Fällen ist nebst der Meldung an die kantonale Aufsichtsstelle auch eine Information der betroffenen Personen erforderlich (§ 12a IDG). Dies ist dann der Fall, wenn sich die Meldung zum Schutz der betroffenen Personen aufdrängt, z.B. wenn sich aus dem Datenschutzvorfall für diese

ein grosses Risiko ergibt oder sie Massnahmen zu ihrem eigenen Schutz ergreifen können müssen. Zudem kann die kantonale Aufsichtsstelle die Information an die betroffenen Personen anordnen.

Im Einzelfall ist zu prüfen, in welcher Form die betroffenen Personen zu informieren sind. Das anwendbare Recht erlaubt u.U. auch eine allgemeine Information, z.B. via eine Meldung auf der Webseite. Soweit möglich und verhältnismässig, sind die betroffenen Personen aber direkt zu informieren.

Es muss vorab stets geprüft werden, ob überwiegende öffentliche oder private Interessen einer Information der betroffenen Personen entgegenstehen (§ 12a IDG).

6 Sonderfrage: Welche gesetzlichen Bestimmungen sind überhaupt anwendbar?

Seit ihrem Inkrafttreten ist die EU-Datenschutz-Grundverordnung (EU-DSGVO oder DSGVO, oder mit dem englischen Akronym GDPR) in aller Munde und prägt das Datenschutzrecht auch in der Schweiz. Aber ist sie auch für die Kirchgemeinden anwendbar?

Die Besonderheit der DSGVO liegt darin, dass sie in gewissen Fällen auch für Unternehmen oder Organisationen in der Schweiz anwendbar ist. Dies ist dann der Fall, a), wenn diese Organisationen natürlichen Personen in der EU Waren oder Dienstleistungen anbieten oder b) wenn das Verhalten von natürlichen Personen in der EU beobachtet wird, etwa durch weitgehendes Tracking des Surfverhaltens dieser Personen im Internet.

Gemäss aktueller Einschätzung ist die DSGVO für die Aktivitäten der Kirchgemeinden nicht anwendbar. Dies kann sich mit der Einführung neuer Angebote oder neuer Software aber ändern.

Für die Kirchgemeinden als Körperschaften des öffentlichen Rechts des Kantons Zürich gelten wie bereits erwähnt das kantonale Gesetz über die Information und den Datenschutz (IDG, LS 170.4) sowie weitere Vorgaben aus dem kantonalen und landeskirchlichen Recht sowie allenfalls aus Erlassen der jeweiligen Kirchgemeinde.

Das Bundesgesetz über den Datenschutz (DSG, SR 235.1) kann zur Anwendung kommen, wenn eine Kirchgemeinde «am wirtschaftlichen Wettbewerb teilnimmt» (§ 2 IDG). Dies wird vermutlich selten der Fall sein, weil sich die Kirchgemeindein im Normalfall ausschliesslich der Erfüllung kirchlicher Aufgaben widmen.

7 Spezialthemen

7.1 Klassifizierung von Dokumenten und Informationen

Als Ausfluss der Anforderungen an die Informations- und Datensicherheit sind sämtliche Dokumente und Informationsbestände, die im Rahmen der amtlichen Tätigkeiten der Kirchgemeinde erstellt oder genutzt werden, durch die Mitarbeiterinnen und Mitarbeiter mit einer Schutzstufe (Klassifizierung) zu versehen.

Die verschiedenen Schutzklassen werden in der ICT-Nutzungsweisung erläutert (siehe Ziffer 4.3 Datenklassifizierung der ICT-Nutzungsweisung).

7.2 Nutzung von ICT-Mitteln

Datenschutz zeigt sich auch ganz konkret darin, wie geschäftliche Informationen (die immer auch Personendaten enthalten) im Alltag geschützt werden. In dieser Hinsicht trägt jede noch so kleine Massnahme, die durch die Mitarbeiterinnen und Mitarbeiter umgesetzt wird, zu einer Verbesserung bei. Den Bildschirm des Arbeitscomputers sperren, wenn man das Büro verlässt, Passwörter mit hoher Komplexität benutzen und diese regelmässig ändern, keine Login-Daten mit anderen Personen teilen. Ziel muss es sein, sich datenschutzfreundliches, sicheres Arbeiten im Alltag zur Gewohnheit zu machen.

Weitere Informationen und Pflichten in diesem Kontext sind in der ICT-Nutzungsweisung enthalten.

►*Eine Vorlage für eine ICT-Nutzungsweisung steht den Kirchgemeinden in den Schulungsunterlagen auf OpenOLAT zur Verfügung.*

8 Datenschutz-Checkliste

Für die Arbeit mit Personendaten im Alltag werden nachfolgend die wichtigsten Schritte und Fragen aufgeführt, mit denen sich alle Mitarbeiterinnen und Mitarbeiter auseinanderzusetzen haben. Diese Prüfschritte müssen bei neuen Projekten *immer in die Planung integriert* und *vor Beginn der Umsetzung thematisiert* werden.

	Prüfschritt
Zweck	Zu welchem *Zweck* sollen Personendaten bearbeitet werden? Dies sollte zu Beginn klar definiert werden; es sind auch mehrere Zwecke möglich. Zur Beschreibung des Zwecks kann auch auf die kirchlichen Aufgaben oder auch andere Dokumente, wie beispielsweise ein Organigramm, Bezug genommen werden.
Arten von Daten (Attributen)	Welche Arten von Daten sollen bearbeitet werden? Werden *besondere Personendaten* bearbeitet (siehe Definition vorstehend Ziffer 3.1)? Wenn ja, empfiehlt sich eine Information an die Kirchenpflege oder an die für den Datenschutz zuständige Person, damit geklärt werden kann, ob aus gesetzlicher Sicht die nötigen Voraussetzungen erfüllt sind.
Rolle der Kirchgemeinde	Welche Rolle spielt die Kirchgemeinde in dieser Datenbearbeitung? Ist sie *Verantwortliche* oder *Auftragsdatenbearbeiterin*? Sie wird in der Regel Verantwortliche sein, womit sie auch alle Datenschutzprinzipien einhalten muss (siehe dazu vorstehend Ziffer 4.2).
Datenschutzprinzipien	Werden in einem konkreten Projekt die *Datenschutzprinzipien* (siehe dazu vorstehend Ziffer 3.2) eingehalten? Z.B. Kann ich weniger Datenattribute bearbeiten, um die Privatsphäre der betroffenen Personen zu schonen? Muss ich mit einer Datenschutzerklärung oder einer sonstigen Information darauf hinweisen, dass ich Daten bearbeite?
Konsultation der Ansprechperson für Datenschutzfragen	Habe ich offene Fragen mit der Ansprechperson für Datenschutzfragen geklärt?
Datenschutz-Folgenabschätzung (DSFA)	Habe ich die Auswirkungen der Datenbearbeitung auf die Rechte der betroffenen Personen geprüft? Vgl. Prozess DSFA und Vorabklärung, vorstehend Ziffer 5.1. Dazu ist die Kirchenpflege oder die Ansprechperson für Datenschutzfragen zu kontaktieren und die Datenschutz-Folgenabschätzung dokumentieren.
Auftragnehmerin oder Auftragnehmer	Ist eine Auftragnehmerin oder ein Auftragnehmer involviert, die als *Auftragsdatenbearbeiterin* oder *Auftragsdatenbearbeiter* zu qualifizieren ist? Wird z.B. eine Software genutzt, um den Datenbearbeitungsvorgang durchzuführen? Wenn ja: • Wer ist Vertragspartnerin oder Vertragspartner?

	• Wo hat das Unternehmen seinen Sitz? Wo findet die Datenbearbeitung statt? • Habe ich den Vertrag genau geprüft? Ist die Kirchgemeinde vertraglich genügend geschützt? Achtung: Es kann sich auch nur um AGBs handeln (AGBs sind auch Verträge). • Weist der Vertrag einen Bestandteil auf, der als *Auftragsdatenbearbeitungsvereinbarung, ADV, Data Processing Agreement, DPA* oder eine Variante davon bezeichnet wird und die Bearbeitung der Daten im Detail regelt? *Vor Vertragsschluss* muss die für den Datenschutz zuständige Person und falls vorhanden die/der DSB beigezogen werden, um diese Fragen im Detail zu klären. Achtung: Bei Anbieterinnen und Anbietern aus den USA oder Datenhaltung in den USA ist möglichst nach einer europäischen Alternative zu suchen. Die USA gelten datenschutzrechtlich nicht als sicheres Land, und entsprechend ist die Nutzung solcher Angebote datenschutzrechtlich heikel und im Einzelfall mit aufwändigen Risikoprüfungen und zusätzlichen vertraglichen Regeln verbunden.

9 Kontaktpersonen für Fragen

Bei Fragen im Zusammenhang mit dem Datenschutz oder der Benutzung des vorliegenden Handbuchs steht der Rechtsdienst der Landeskirche zur Verfügung:

RA Dr. iur. Martin Röhl	Leiter Rechtsdienst martin.roehl@zhref.ch Tel. 044 258 92 21
RAin lic. iur. Franziska Kramer-Schwob	Mitarbeiterin Rechtsdienst franziska.kramer@zhref.ch Tel. 044 258 92 40

Anhang 1-4: grafische Übersichten der Datenschutzprozesse

- Anhang 1: Datenschutz-Folgenabschätzung (DSFA) (Ziff. 5.1)
- Anhang 2: Informationszugang (Ziff. 5.2)
- Anhang 3: Rechte der betroffenen Personen (Ziff. 5.3)
- Anhang 4: Meldung Datenschutzvorfall (Ziff. 5.4)