Freikirchen in Österreich (FKÖ)

Anpassungen an die EU-Datenschutzgrundverordnung (DSGVO)

und das österreichische Datenschutz-Anpassungsgesetz 2018 (DSG)

Zur internen Verwendung in den Bünden und Gemeinden der FKÖ

Fragen und Antworten (FAQ)/Knowledge Base

V20200623, Stand 23.06.2020

Inhaltsverzeichnis

1 GIBT ES IN DEN FKÖ REGELUNGEN ZUM DATENSCHUTZ?

Ja. Die aktuelle Datenschutzordnung der FKÖ (DSO-FKÖ) wurde am 6. April d.J. beschlossen und tritt mit 25. Mai 2018 - dem Anwendungsdatum der EU-DSGVO - in Kraft. Die aktuelle Fassung ist vom 5. Juni 2018. In dieser Ordnung sind, im Rahmen der allgemeinen Gesetze und der Verfassung der FKÖ, jene Punkte geregelt, die den innerkirchlichen Angelegenheiten zuzurechnen sind. Wesentliches Ziel und Sinn dieser Ordnung ist es, Möglichkeiten in Synergien und Gemeinsamkeiten zu nutzen, um die Datenschutz-Aufgaben der Gemeinden zu vereinfachen und Kosten zu reduzieren.

2 GIBT ES IN DEN FKÖ UNTERSTÜTZUNG FÜR DIE GEMEINDEN BEI DER ANPASSUNG AN DIE NEUEN DATENSCHUTZGESETZE?

Ja. In der Datenschutzordnung der FKÖ (DSO-FKÖ) sind zwei Komponenten vorgesehen, die den Gemeinden die Anpassung vereinfachen und erleichtern sollen.

a) Informations- und Beratungsstruktur in drei Ebenen:

- Je Gemeinde eine Kontaktperson für Datenschutz. Für diese Kontaktperson wurde die Bezeichnung “Datenschutzzuständige(r)” (DSZ) der Gemeinde festgelegt. Die Datenschutzzuständigen der Gemeinden erhalten Information, Beratung und Schulung von einem Referenten des jeweiligen Gemeindebundes, und geben dies an die Personen in ihrer Gemein- de weiter, die mit Daten zu tun haben.

- Je Bund mindestens ein Datenschutzreferent (DSR). Dieser ist die Kontaktperson für die Datenschutzzuständigen der Gemeinden bei allen Datenschutzfragen und auch zuständig für deren Schulung, Beratung und Information. Die Datenschutzreferenten unterstützen den Datenschutzbeauftragen der FKÖ bei seiner Tätigkeit.

- Ein (gemeinsamer) Datenschutzbeauftragter (DSB) der FKÖ. Dieser unterrichtet und berät die Datenschutzreferenten der Bünde und den Rat der FKÖ hinsichtlich deren Pflichten nach der DSGVO und sonstigen Datenschutzvorschriften. Er überwacht die Einhaltung der

DSGVO und anderer Datenschutzvorschriften, berät im Zusammenhang mit der Datenschutzfolgeabschätzung und ist das Bindeglied zur Aufsichtsbehörde.

b) Bereitstellung einer technischen Lösung zur automatisierten Datenverarbeitung:
   - Je Bund wird eine geeignete, DSGVO-konforme Lösung (z.B. Office 365) zur automatisierten Datenverarbeitung eingerichtet und den ihm zugehörigen Gemeinden zur Nutzung angeboten.
   - Für die Datenschutzzuständigen wird ein Schulungs-Seminar zur Verwendung dieser Lösungen und zur Migration der Daten angeboten. Wenn die Kapazitäten es zulassen, können auch weitere Personen aus den Gemeinden, die im Gemeindeauftrag Daten verarbeiten, an diesen Seminaren teilnehmen.

3 Kann ein Datenschutzreferent (DSR) und ein Datenschutzzuständiger (DSZ) im selben Bund die ein und dieselbe Person sein?

Es ist möglich, aber es ist nicht anzuraten. Es soll nicht die gleiche Person als Datenschutzreferent die selbst durchgeführte Arbeit als Datenschutzzuständiger überprüfen.

Bei einem Audit der betroffenen Gemeinde ist dann diese Person der Datenschutzzuständige (DSZ) der Gemeinde und ein andere Datenschutzreferent (DSR), möglicherweise auch aus einem anderen Bund, führt dann das Audit durch.

4 Welches Risiko tragen die Datenschutzreferenten (DSR) und Datenschutzzuständigen (DSZ)

Es ist immer die Gemeinde als Rechtsträger haftbar. Wenn fahrlässig gehandelt wird, könnten im Innenverhältnis Regressforderungen gestellt werden. Diese sind nicht sehr aussichtsreich (Ehrenamt, …). Innerkirchlich wäre ohnehin zuerst das Schiedsgericht der FKÖ zu kontaktieren.

5 Darf eine Person ein Datenschutzzuständiger (DSZ) und gleichzeitig in der Gemeindeleitung in ein und derselben Gemeinde sein?

Der DSZ ist innerhalb der Gemeinde die erste Anlaufstelle für Anfragen über personenbezogene Daten der Gemeinde und überprüft, ob die personenbezogenen Daten nur durch die richtigen Personen verändert wer- den dürfen.

Eine Person die personenbezogenen Daten speichert, verändert oder bearbeitet sollte nicht der DSZ für diese personenbezogenen Daten sein, damit kein Interessenskonflikt entsteht.

Am besten hat der DSZ nur eine Leseberechtigung für die personenbezogenen Daten. Es ist nun möglich das eine Person aus der Gemeindeleitung ein DSZ ist, solange es die vorgenannte Voraussetzung erfüllt.

Folgende Möglichkeiten sind dadurch auch noch möglich:

- Eine Person ist ein Datenschutzzuständige in der Gemeinde X und Gemeinde Y
- Eine Person außerhalb der Gemeinde ist der Datenschutzzuständige der Gemeinde

Sollte es der Gemeinde nicht anders möglich sein, dann kann der DSZ auch personenbezogene Daten zB innerhalb

eines Dienstes verarbeiten, sollte aber nicht der Hauptverantwortliche für sämtliche Gemeindedaten sein.

6 Was muss eine Ortsgemeinde konkret tun, um am 25. Mai 2018 DSG-VO-konform zu sein?

Dies lässt sich konkret nur für Gemeinden beantworten, die die Regelungen der DSO-FKÖ mit ihren Synergieangeboten nutzen wollen. Für Gemeinden, die eigene Regelungen gemäß § 11 der DSO-FKÖ treffen wollen, können naturgemäß hier keine Schritte angegeben werden, das hängt fast ausschließlich von deren konkreten Regelungen ab. Für diese Gemeinden ist davon auszugehen, dass sie selbst wissen, was erforderlich ist, und ihre Regelungen und konkreten Lösungen den jeweiligen Bundesleitungen bis spätestens 25. Mai bekanntgeben werden.

Konkrete Schritte für jene Gemeinden, die die Regelungen der DSO-FKÖ und die damit verbundenen Angebote der Bünde wahrnehmen wollen, wären (alles Verwaltungsaufgaben in der Kompetenz der Gemeindeleitungen):

a) Benennung der Datenschutz-Kontaktperson der Gemeinde (“Datenschutzzuständige(r)” - DSZ).
b) Erhebung, wer aller in der Gemeinde personenbezogene Daten hat (speichert, verwaltet etc.)
c) Entscheidung, welche dieser Personen weiterhin Datenzugriff haben sollen, und mit welchen Aufträgen (wofür werden die Daten benötigt) und Verarbeitungsrechten (lesen- schreiben/ändern-löschen).
d) Information (Seminar, Schulung bundesweit oder durch DSZ nach dessen getrenntem Seminar vorher) dieser Personen zum Datengeheimnis und Unterzeichnen der Daten- Geheimhaltungserklärung durch die Personen, die Datenzugriff haben sollen.
e) Erstellung des Verzeichnisses der Verarbeitungstätigkeiten (VVT), auch genannt das Datenverarbeitungsverzeichnis (DVV), der Gemeinde (ein Muster wird als Formular zur Verfügung gestellt) und Übermittlung einer Kopie an die zuständige Bundesleitung.
f) Einrichtung von gesicherten Cloud-Zugängen (Max 3 pro Gemeinde, zumindest zu Anfang) für die Personen mit Auftrag zur Datenverarbeitung.
g) Auftrag zur Übergabe aller personenbezogenen Daten an die Personen mit Auftrag zur Datenverarbeitung.
h) Übertragung aller personenbezogenen Daten auf die Cloud.
i) Löschung aller personenbezogenen Daten auf allen persönlichen Geräten; Aktennotiz und Bestätigungen (Unterschriften), dass dies erfolgt ist.

7 Welche Personen sind auf Gemeindeebene zu schulen?

Jede Person mit potentiellem Zugang zu den personenbezogenen Daten und die eine Verarbeitung durchführt. Die Schulung sollte durch den Datenschutzzuständige durchgeführt werden. In regelmäßigen Abständen oder bei Änderungen (Gesetzeslage, Software, …) sollte die Schulung aufgefrischt werden.

8 Was genau ist mit „Verzeichnis der Verarbeitungstätigkeiten“ (VVT) bzw. „Datenverarbeitungsverzeichnis“ (DVV) gemeint? Was ist da einzutragen?

Musterverzeichnisse, die an den Bedarf unserer Gemeinden angepasst sind, werden bei den in 3.d) erwähnten Seminaren oder über den Datenschutzreferenten/Bundesbüro zur Verfügung gestellt. Ein allgemeines Verarbeitungsverzeichnis-Muster ist auf den Seiten der WKO zu finden.

Informationen, die dieses Verzeichnis enthalten muss, sind:

> Zweck der Verarbeitung, Kategorien der betroffenen Personen und Kategorien der personenbezogenen Daten dazu, Kategorien von Empfängern von Daten, ggf. Information zur Übermittlung von Daten in ein Drittland, vorgesehene Speicherdauer, und allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherheit der Datenverarbeitung.

9 Welche Sprache ist beim „Verzeichnis der Verarbeitungstätigkeiten“ (VVT) bzw. „Datenverarbeitungsverzeichnis“ (DVV) einzuhalten?

Alle Unterlagen, die der Verantwortliche/der Auftragsverarbeiter der Datenschutzbehörde im Rahmen eines (Prüf-)Verfahrens vorzulegen hat, müssen **in deutscher Sprache** (Amtssprache gemäß Art. 8 Abs. 1 Bundes-Verfassungsgesetz; siehe dazu auch die Erkenntnis des Verwaltungsgerichtshofes vom 17. Mai 2011, Zl. 2007/01/0389) abgefasst sein.

Das gilt **jedenfalls** für die **Datenschutz-Folgenabschätzung** gem. Art. 35 DSGVO, die der Datenschutzbehörde etwa im Rahmen der „Konsultation“ gem. Art 36 DSGVO vorgelegt werden muss, sowie für das **Verzeichnis von Verarbeitungstätigkeiten (VVT)** gem. Art. 30 DSGVO, dass in der Regel die Basis für die Datenschutz-Folgenabschätzung sein wird.

10 Wer ist der/die Verantwortliche für den Datenschutz in einer Ortsgemeinde? Vertretungsbefugte, Gemeindeleiter, Älteste, Pastor? Oder die Person, die in der Gemeinde für den Datenschutz zuständig ist?

Die Gemeinde selbst, in ihrer Eigenschaft als Körperschaft öffentlichen Rechts (KÖR). Ist die Organisation oder das Unternehmen eine juristische Person (GmbH, AG, KÖR), haftet diese in erster Linie.

In der DSGVO bezeichnet der Begriff Verantwortlicher (Auszug aus Art. 4 Abs. 7 DSGVO) *“… die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.”*

Damit löst der Begriff “Verantwortlicher” den Begriff “Auftraggeber” ab, der im DSG 2000 (noch bis 24. Mai 2018) gilt.

11 Wer ist in der Gemeinde für den Datenschutz zuständig?

In erster Linie die Gemeindeleitung (GL), weil es sich um eine Verwaltungsaufgabe handelt. Die GL kann jedoch auch operative Funktionen und Aufgaben an Personen außerhalb der GL übergeben, z.B. die Funktion des Datenschutzzuständigen (DSZ) der Gemeinde. Verantwortlicher im Sinne der DSGVO, vor allem auch hinsichtlich Haftung, bleibt aber immer die Gemeinde als juristische Person (KÖR).

12 Muss eine Körperschaft öffentlichen Rechts einen Datenschutzbeauftragten benennen (es geht nur um Daten in geringem Umfang)?

Eine Körperschaft öffentlichen Rechts ist eine öffentliche Stelle und muss daher zwingend einen Datenschutz- beauftragten (DSB) bestellen (Art. 37 Abs. 1 DSGVO). Dies gilt unabhängig davon, welche Daten verarbeitet werden und in welchem Umfang. Die Regelungen erlauben aber, dass für mehrere öffentliche Einrichtungen und Stellen ein gemeinsamer Datenschutzbeauftragter benannt und ggf. durch ein Team unterstützt wird. Für alle Gemeinden, die ihre Datenschutzaufgaben im Rahmen der Strukturen wahrnehmen wollen, die in den §§ 5-6 der DSO-FKÖ festgelegt sind, ist dies der Datenschutzbeauftragte der FKÖ, der durch das Team aus Datenschutzreferenten (DSR) und Datenschutzzuständigen (DSZ) der Gemeinden unterstützt wird. Weitere Regelungen bzgl. des Datenschutzbeauftragten (DSB) in der FKÖ steht in der DSO-FKÖ.

13 Für Gemeinden in den FKÖ gilt die Autonomie der Ortsgemeinde. Was bedeutet das im Zusammenhang mit der FKÖ-Datenschutzordnung? Kann eine Gemeinde auch eigene Regelungen festlegen?

Eine Gemeinde kann im Rahmen ihrer Autonomie auch eigene Regelungen zum Datenschutz treffen, in denen aber natürlich die allgemeinen staatlichen Gesetze, die Verfassung der FKÖ und die Ordnungen des jeweiligen Gemeindebundes eingehalten sein müssen. Diese Möglichkeit ist in § 11 der DSO-FKÖ vorgesehen. Wenn in einer (größeren) Gemeinde die erforderlichen Kompetenzen und Kapazitäten für die Erstellung gesetzeskonformer Regelungen und die Ausführung aller dazu nötigen Aufgaben vorhanden sind, kann das eine sinnvolle Lösung sein. Die eigenen Regelungen bedeuten in diesem Fall auch die Verpflichtung zur Bestellung eines eigenen Datenschutzbeauftragen (DSB) gemäß DSGVO. Dies kann auch der von den FKÖ bestellte DSB sein, wenn dieser zustimmt. In diesem Fall muss die betreffende Gemeinde selbst mit dem DSB eine entsprechende Vereinbarung treffen, und der (Mehr)Aufwand, der dem DSB aus den eigenen Regelungen der Gemeinde entsteht, muss jeden- falls von der betreffenden Gemeinde selbst getragen werden. Ebenfalls einzuhalten ist die Verpflichtung zur Information gemäß FKÖ-Verfassung, d.h. die Gemeinde muss Kopien aller ihrer Regelungen und ihres DSGVO-konformen „Verzeichnis der Verarbeitungstätigkeiten“ sowie die Kontaktdaten ihres DSB der jeweiligen Bundesleitung in der jeweils aktuellen Form zur Prüfung und Freigabe vorlegen.

14 Wenn wir als Gemeinde eine eigene Lösung wollen:

14.1 Was ist die Funktion und vor allem die Haftung des Datenschutzbeauftragten?

- Der Datenschutzbeauftragte (DSB) unterrichtet und berät den Verantwortlichen hinsichtlich dessen

Pflichten nach der DSGVO und sonstigen Datenschutzvorschriften. Er überwacht die Einhaltung der DSGVO und anderer Datenschutzvorschriften, berät im Zusammenhang mit der Datenschutz- Folgenabschätzung und ist das Bindeglied zur Aufsichtsbehörde. Wenn ein „interner" Datenschutzbeauftragter benannt wird, dann darf er in der Organisation (=Gemeinde) keine Funktion haben, die mit seinen Aufgaben im Widerspruch steht.

- Der Datenschutzbeauftragte haftet lediglich dem Auftraggeber nach den allgemeinen Regeln (Sorgfaltspflicht, Informationspflicht etc.), nicht aber gegenüber der Behörde für die Strafen.

14.2 Welche fachliche Qualifikation wird von einem Datenschutzbeauftragen erwartet? Ist das eine geschützte berufliche Bezeichnung?

- Der Datenschutzbeauftragte muss über die notwendigen Qualifikationen und das Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis zu verfügen. Er muss in der Lage sein, den Verantwortlichen hinsichtlich seiner Pflichten nach der DSGVO und sonstigen Datenschutzvorschriften zu unterrichten und zu beraten, die Einhaltung der DSGVO und sonstiger Datenschutzvorschriften zu überwachen, in Bezug auf eine Datenschutz-Folgenabschätzung zu beraten und als Bindeglied zur Aufsichtsbehörde zu fungieren.
- Datenschutzbeauftragter selbst ist keine geschützte berufliche Bezeichnung. Es sind aber alle Rechte und Pflichten eines Datenschutzbeauftragen nach der DSGVO einzuhalten, wenn man jemanden in einer Gemeinde so benennt.

14.3 Braucht ein Datenschutzbeauftragter eine spezielle Ausbildung und/oder ein Zertifikat, oder kann man sich das Wissen dazu auch selbstständig aneignen?

- Ein Datenschutzbeauftragter muss ein gewisses Maß an Erfahrung in datenschutzrechtlichen Dingen aufweisen. Konkrete Ausbildungen sind zwar nicht verpflichtend, aber empfehlenswert.

14.4 Soll ein Datenschutzbeauftragter eher aus dem juristischen Bereich kommen oder eher ein IT-Fachmann sein?

- Ein Datenschutzbeauftragter benötigt Kompetenzen aus beiden Bereichen. IT-Fachleute benötigen auch Verständnis/Fachwissen in juristisch relevanten Gebieten und Juristen müssen ein ausrechendes technisches Verständnis haben, dass sie auch die technischen Komponenten von Datenverarbeitungen beurteilen können.

15 Ich habe die Daten bisher auf meinem Notebook (PC, Smartphone, externem Datenträger …) gespeichert und bearbeitet. Ist das weiter möglich?

Im Prinzip ja, aber nur unter einer Reihe von Voraussetzungen, deren Einhaltung nicht nur am Beginn, sondern auch dauerhaft nachweisbar sein muss und regelmäßig überprüft wird. Die Voraussetzungen enthalten Verpflichtungen zum Schutz der Daten durch Zugriffsbeschränkung und Verschlüsselung mit geeigneten Passwörtern, zur Protokollierung von Datenzugriffen und Verarbeitungsvorgängen und zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit. Eine bessere Lösung wäre es, wenn das individuelle Gerät (Notebook etc.) nur mehr für den Zugriff auf einen Server verwendet würde, auf dem dies alles eingerichtet ist, und die Daten nicht mehr auf individuellen Gerä-

ten gespeichert werden. Auch dabei ist noch zu beachten, dass diese Geräte keinen ungeschützten Zugriff auf den Server haben dürfen. D.h., auf den Geräten selbst muss Passwortschutz eingerichtet sein und es sollen keine Server-Passwörter für automatischen Zugriff auf dem Gerät gespeichert werden.

Detail-Auszüge aus den Vorschriften:

> *Aus DSG (2018) § 50 – Protokollierung:*
>
> *(1) Jeder Verarbeitungsvorgang ist in geeigneter Weise so zu protokollieren, dass die Zulässigkeit der Verarbeitung nachvollzogen und überprüft werden kann.*
>
> *(2) In automatisierten Verarbeitungssystemen sind alle Verarbeitungsvorgänge in automatisierter Form zu protokollieren. Aus diesen Protokolldaten müssen zumindest der Zweck, die verarbeiteten Daten, das Datum und die Uhrzeit der Verarbeitung, die Identifizierung der Person, die die personenbezogenen Daten verarbeitet hat, sowie die Identität eines allfälligen Empfängers solcher personenbezogenen Daten hervorgehen.*
>
> *(3) In nicht automatisierten Verarbeitungssystemen sind zumindest Abfragen und Offenlegungen einschließlich Übermittlungen, Veränderungen sowie Löschungen zu protokollieren. Für diese Protokolldaten gilt Abs.2 zweiter Satz.*
>
> *(4) Die Protokolle dürfen ausschließlich zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung einschließlich der Eigenüberwachung, der Gewährleistung von Integrität und Sicherheit der personenbezogenen Daten sowie in gerichtlichen Strafverfahren verwendet werden.*
>
> *(5) Der Verantwortliche und der Auftragsverarbeiter haben der Datenschutzbehörde auf deren Verlangen die Protokolle zur Verfügung zu stellen*
>
> *Aus DSGVO Art. 32 (1) – zu regelmäßiger Datenschutz-Evaluierung*
>
> *(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:*
>
> *…. (d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.*
>
> *Aus DSGVO Art. 33 (5) – zu Dokumentation von Datenschutzverletzungen*
>
> *Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.*

16 Wir verschicken öfters Kontakt-Daten per E-Mail an Gemeinde-Gruppen oder an alle Mitglieder. Ist das auch weiterhin möglich?

Die Voraussetzung dafür war auch bisher schon, dass alle Betroffenen, deren Daten verschickt werden, ausnahmslos damit einverstanden sind (nachweislich), und dass beim Versand Verschlüsselung nach aktuellem Stand der Technik verwendet wird. Bei Versand per E-Mail ist auch zu beachten, dass Adressen in den An (To)- oder CC-Feldern personenbezogene Daten sind, die für alle lesbar und offen zugänglich gemacht werden. Bei Versandlisten soll deshalb immer das BCC-Feld verwendet werden.

Nach den neuen Regelungen sind für eine solche Datenübermittlung auch ein Auftrag des Vorgesetzten (z.B. Gemeindeleitung) und entsprechende Geheimhaltungserklärungen (nachweislich) der Empfänger nötig. Ob, und inwieweit, die Geräte der Empfänger dann auch von der DSGVO erfasst sind, werden wohl erst die allgemeine Praxis und allenfalls eine Feinabstimmung der Regelungen in Zukunft zeigen.

17 Ich verwende „WhatsApp“ auf meinen dienstlichen Handy. Ist das Problematisch?

WhatsApp versendet automatisch die im Adressbuch gespeicherten Kontakte (Telefonnummern, …) an dritte. Diese Datenweitergabe kann momentan weder gestoppt noch können die übermittelten Kontakte nachträglich gelöscht werden.

Die gespeicherten Kontakte stellen personenbezogene Daten dar. Es ist anzunehmen das die Personen hinter den Kontakten keine Erlaubnis zur Weitergabe der eigenen Telefonnummer genehmigt haben (Verstoß gegen DSGVO Art. 6). Dadurch ist die Verwendung von WhatsApp für dienstliche Handys problematisch und ist nicht gestattet.

Alternativen zu WhatsApp gibt es viele. Als Alternative kann genannt werden:

a) Threema
   - Kostenpflichtig

b) Telegram
   - Kontakte müssen am Anfang synchronisiert werden
   - Danach „Kontakte synchronisieren“ ausschalten in den Einstellungen
   - Danach „Synchronisierte Kontakte löschen“
   - Keinen "Benutzernamen" vergeben, da der Benutzer dann öffentlich gefunden werden kann

c) Signal

18 In den Adressbüchern auf meinem Handy und Notebook sind (natürlich) auch Daten von Freunden, die in meiner Gemeinde sind. Bin ich damit auch von diesen Regelungen betroffen?

Nein. Wenn Privatpersonen personenbezogene Daten nur zur Ausübung persönlicher und familiärer Tätigkeiten verarbeiten, gilt die DSGVO dafür nicht. Eine vollständige Gemeindeliste auf dem persönlichen Gerät wäre allerdings kaum damit argumentierbar.

19 Wir verwenden OPTIGEM als Buchhaltungsprogramm. Ist das von den neuen Regelungen betroffen?

Von OPTIGEM gibt es dazu die Auskunft, dass es noch im Mai eine neue Version 6.2 geben wird, in der Protokollierungs- und Sicherheitsmodule DSGVO-konform enthalten sind. Sobald diese Version verfügbar ist, soll es eine Informationsmail an alle bestehenden Kunden geben. Empfehlenswert ist dabei, wie in den meisten Fällen, die Web-basierte Lösung (Link hier), weil diese auch die Bereiche

Zugangskontrolle, Sicherung gegen Datenverlust bei Geräteschäden, Virenschutz, Softwareaktualisierungen etc. mit abdeckt.

Inwieweit oder in welcher Form dies in die Struktur mit einem gemeinsamen DSB einzubinden ist bleibt noch zu klären. Diese Frage betrifft mehrere Gemeinden in den FKÖ, damit sind Synergien beim Aufwand in der Struktur zu erwarten. Die lokalen Datenschutz-Überwachungsaufgaben wären in jedem Fall durch den DSZ der Gemeinde wahrzunehmen.

20 Wir möchten ChurchTools verwenden. Ist das mit der DSGVO möglich, und wenn ja, was ist dabei zu beachten?

ChurchTools wird als Webhosting-Lösung mit einem Rechenzentrum in Deutschland angeboten. Dabei übernimmt der Anbieter die Rolle eine Auftragsverarbeiters im Sinne der DSGVO und ist damit für die Sicherheit der Daten zuständig, die bei ihm gespeichert sind. Wie auch bei Optigem betrifft diese Frage mehrere Gemeinden in den FKÖ, damit sind auch hier Synergien beim Aufwand in der Struktur zu erwarten. Die lokalen Datenschutz-Überwachungsaufgaben wären auch dabei jedenfalls vom DSZ der Gemeinde wahrzunehmen.

ChurchTools wird auch in einer Version angeboten, die auf einem eigenen Server direkt durch die Gemeinde selbst gehostet werden kann. Davon ist abzuraten. Die Gemeinde wäre dann selbst für alle Fragen der Sicherheit ihres Webservers verantwortlich, und es würde jedenfalls die Beauftragung eines eigenen kompetenten Datenschutzbeauftragen bedeuten.

21 Warum sind wir so spät dran mit dieser Datenschutzanpassung?

Dazu gibt es Antworten auf mehreren Ebenen. Einerseits muss sich diese Frage jeder selbst stellen die Autonomie der Ortsgemeinde bedeutet hier auch Eigenverantwortung. Dazu kommt: wer sich an die bisherigen in Österreich geltenden Gesetze zum Datenschutz gehalten hat, muss nur sehr wenig ändern. Neu ist vor allem eine Verlagerung der Verantwortung für die Dokumentation und Gewährleistung der Nachvollziehbarkeit von der Behörde hin zur verantwortlichen Organisation. Die DVR-Meldung entfällt in Zukunft, die Vorgaben für Dokumentation und interne Qualitätssicherung beim Datenschutz sind dann von der verantwortlichen Stelle in Eigenverantwortung zu erfüllen. Andererseits: Seitens der Freikirchen kann lediglich Unterstützung angeboten werden, in Form von Vereinfachungen bei Aufgaben, die für alle ähnlich oder gleich sind, z.B. beim gemeinsamen Datenschutzbeauftragten. Generell ist die Anpassung aber noch immer ein dynamischer Prozess, weil etliches an Details in den gesetzlichen Vorschriften und bei den Softwareangeboten noch immer im Fluss ist.

22 Wann wird die Zustimmung der Eltern zur Datenverarbeitung von Minderjährigen benötigt?

Gem. österr. DSG § 4 Abs 4 kann der Jugendliche, wenn er das 14. Lebensjahr vollendet hat, seine Einwilligung selbst erteilen.

Links zu Seiten mit weiterführender Information:

DSGVO: Kurzüberblick und Zeitplan (WKO)

DSGVO-Übersicht (WKO)

DSGVO-FAQ (WKO)

Office 365 DSGVO Compliance Seite

Leitfaden der Datenschutzbehörde zur DSGVO

Text der "Verordnung (EU) 2016/679" (EU-DSGVO)

FAQ auf der Webseite der Datenschutzbehörde

Link zur Datenschutzbehörde

Buchempfehlungen:

- **Datenschutz-Grundverordnung (EU-DSGVO) und Datenschutz-Anpassungsgesetz 2018 (** 18. Jan. 2018, Rosenmayr-Klemenz, Broschüre der WKO, Bestellung über den WKO-Webshop)
- **Umsetzung der DSGVO in der Praxis: Fragen, Antworten, Muster (**Taschenbuch – 1. Februar 2018, Lukas Feiler und Bernhard Horn, ISBN-10: 3704678597, ISBN-13: 978-3704678591)

Hinweise und Haftungsausschluss:

Diese Zusammenstellung dient ausschließlich dem internen Gebrauch in den Freikirchen in Österreich. Die Information ist nach aktuellem Wissensstand des Verfassers erstellt und enthält keinerlei Gewähr für Richtigkeit oder Vollständigkeit. Jede Haftung ist damit explizit ausgeschlossen. Ebenso kann für den Inhalt von Web-Seiten, die über Hyperlinks in diesem Dokument erreichbar sind, keinerlei Verantwortung übernommen werden, die Haftung dazu liegt ausschließlich bei den Betreibern dieser Seiten.

Die in dieser Zusammenstellung verwendeten männlichen oder weiblichen Bezeichnungen dienen ausschließlich der besseren Lesbarkeit und der Vergleichbarkeit mit den Texten externer Dokumente und gelten für beide Geschlechter.