

LEITFADEN

zum Ausfüllen des

Verzeichnisses von Verarbeitungstätigkeiten (VVT)

gemäß Art. 30 DSGVO – für Gemeinden der Freikirchen in Österreich

Was ist dieses Dokument und wozu dient es?

Die Datenschutz-Grundverordnung (DSGVO) verpflichtet jede Organisation, die personenbezogene Daten verarbeitet, ein sogenanntes Verzeichnis von Verarbeitungstätigkeiten (VVT) zu führen. Das ist eine Art Bestandsaufnahme, in der dokumentiert wird:

- Welche Daten Ihre Gemeinde über Personen speichert,
- wofür diese Daten verwendet werden,
- wer Zugriff darauf hat und
- wie lange die Daten aufbewahrt werden.

Dieser Leitfaden erklärt Schritt für Schritt, was in jede Rubrik des Musterformulars einzutragen ist – auch ohne Vorkenntnisse im Datenschutz.

A. Stammdatenblatt

Das Stammdatenblatt ist der Deckblatt-Bereich Ihres VVT. Hier tragen Sie grundlegende Informationen über Ihre Gemeinde und die zuständigen Ansprechpersonen ein.

A.1 Name und Anschrift der Gemeinde

Was ist hier einzutragen?

Tragen Sie den offiziellen Namen Ihrer Gemeinde sowie die vollständige Postadresse ein (Straße, Hausnummer, Postleitzahl, Ort). Das ist die Anschrift, die auch auf offiziellen Schreiben Ihrer Gemeinde erscheint.

Beispiel:

Gemeinde Lebendige Hoffnung Rosengasse 12 4020 Linz

A.2 E-Mail und Telefonnummern

Was ist hier einzutragen?

Die offizielle E-Mail-Adresse und Telefonnummer, über die Ihre Gemeinde erreichbar ist. Diese Kontaktdaten müssen für Personen zugänglich sein, die Auskunft über ihre gespeicherten Daten verlangen möchten.

A.3 Datenschutzbeauftragter (DSB)

Was ist ein Datenschutzbeauftragter?

Der Datenschutzbeauftragte ist eine Person oder Stelle, die dafür zuständig ist, die Einhaltung der DSGVO zu überwachen. Für Gemeinden der Freikirchen in Österreich ist das der zentrale DSB der FKÖ. Sie müssen hier KEINE eigene Person benennen – tragen Sie einfach die bereits vorausgefüllten Daten des FKÖ-Datenschutzbeauftragten ein (Karl-Popper-Str. 16, 1100 Wien, datenschutz@freikirchen.at).

A.4 Datenschutzreferent des Bundes

Was ist einzutragen?

Tragen Sie hier den Namen, die E-Mail-Adresse und die Telefonnummer des Datenschutzreferenten Ihrer Freikirchen-Bundesorganisation ein. Diese Person ist Ansprechpartner auf Bundesebene. Falls Sie diese Information nicht kennen, wenden Sie sich an Ihr Bundesbüro der FKÖ.

A.5 Datenschutz-Zuständiger der Gemeinde

Was ist einzutragen?

Das ist die Person in Ihrer Gemeinde, die sich um Datenschutzfragen kümmert – oft ein Ältester, der Kassier, oder eine eigens beauftragte Person. Wenn Sie noch niemanden ernannt haben, sollten Sie das jetzt tun. Tragen Sie Namen, E-Mail und Telefonnummer dieser Person ein.

B. Datenverarbeitungen und Datenverarbeitungszwecke

In diesem Abschnitt listen Sie auf, WOFÜR Ihre Gemeinde überhaupt Daten verarbeitet. Das Musterformular enthält bereits drei typische Zwecke – Sie müssen diese nur überprüfen und ggf. ergänzen.

Einfache Erklärung: Was bedeutet Datenverarbeitungszweck?

Ein Zweck ist der Grund, warum Sie Daten über eine Person speichern oder nutzen. Beispiel: Sie speichern den Namen und die Adresse eines Gemeindeglieds, damit Sie Einladungen versenden können. Der Zweck ist hier: Mitgliederverwaltung.

B.1 Mitgliederverwaltung

Bereits vorausgefüllt im Muster. Dieser Zweck umfasst alles rund um die Verwaltung Ihrer Gemeindeglieder: Mitgliederlisten, Aufnahme neuer Mitglieder, Beitrittserklärungen, Korrespondenz mit Mitgliedern.

Aktion erforderlich:

Prüfen Sie, ob dieser Punkt auf Ihre Gemeinde zutrifft (er trifft auf nahezu alle Gemeinden zu). Falls ja, behalten Sie ihn bei.

B.2 Personalverwaltung

Dieser Zweck gilt, wenn Ihre Gemeinde bezahlte Mitarbeiter oder Personen mit vertraglichen Vereinbarungen beschäftigt (z.B. Pastoren, Buchhalter, Reinigungspersonal). Auch freiwillige Mitarbeiter fallen darunter, sofern schriftliche Vereinbarungen bestehen.

Aktion erforderlich:

Falls Ihre Gemeinde KEINE Angestellten hat, können Sie diesen Punkt streichen oder mit dem Hinweis "nicht zutreffend" versehen.

B.3 Standortaufgaben und Objektverwaltung

Dieser Zweck gilt, wenn Ihre Gemeinde Verträge mit Vermietern, Lieferanten (z.B. Strom, Heizung, Reinigung) oder Dienstleistern (z.B. IT-Firma) hat und dabei Kontaktdaten dieser Personen/Firmen verwaltet.

B.4 Weitere Zwecke (ggf. ergänzen)

Typische weitere Zwecke, die Sie ergänzen könnten:

- Verwaltung von Kinderbetreuungsangeboten (Jungschar, Kindergottesdienst) •
- Veranstaltungsorganisation (Konzerte, Seminare) • Newsletter-Versand • Verwaltung von Spendern und Unterstützern • Buchhaltung und Finanzverwaltung

Fügen Sie nur Punkte hinzu, die auf Ihre Gemeinde tatsächlich zutreffen.

C. Detailangaben zu den einzelnen Datenverarbeitungen

Dieser Abschnitt ist der ausführlichste Teil des VVT. Hier werden die in Abschnitt B aufgelisteten Verarbeitungszwecke im Detail beschrieben. Gehen Sie die fünf Unterabschnitte (C.1 bis C.5) nacheinander durch.

C.1 Kategorien betroffener Personengruppen und Rechtsgrundlagen

Personengruppen (Tabelle a bis f)

Im Muster sind sechs Personengruppen vordefiniert. Prüfen Sie, welche davon auf Ihre Gemeinde zutreffen:

Gruppe	Bezeichnung im Formular	Bedeutung in der Praxis
a)	Gemeindemitglieder	Alle eingetragenen Mitglieder Ihrer Gemeinde
b)	Mitarbeiter im Ehrenamt	Freiwillige Helfer (z.B. Musiker, Jungscharmitarbeiter, Küchendienst)
c)	Mitarbeiter mit Anstellung	Bezahlte Angestellte der Gemeinde (Pastor, Sekretariat, etc.)
d)	Vertretungsorgane	Ältestenrat, Gemeindeleitung, Vorstand
e)	Lieferanten, Vertragspartner	Firmen oder Personen, mit denen Verträge bestehen
f)	Sponsoren und Unterstützer	Personen, die die Gemeinde finanziell unterstützen (ohne Mitglied zu sein)

Rechtsgrundlagen – Was bedeutet das?

Einfache Erklärung: Rechtsgrundlage

Eine Rechtsgrundlage ist der rechtliche Grund, warum Sie Daten einer Person speichern dürfen. Die DSGVO verlangt, dass es immer einen solchen Grund geben muss. Die häufigsten Gründe sind: • Einwilligung: Die Person hat ausdrücklich zugestimmt (z.B. durch Unterzeichnung einer Beitrittserklärung). • Vertragserfüllung: Die Daten sind notwendig, um einen Vertrag zu erfüllen (z.B. Arbeitsvertrag). • Gesetzliche Verpflichtung: Ein Gesetz schreibt vor, dass Sie die Daten haben müssen (z.B. Buchhaltung).

Das Musterformular enthält bereits die passenden Rechtsgrundlagen für jede Gruppe. Sie müssen diese in der Regel nicht ändern, außer Sie haben besondere Verarbeitungen.

C.2 Zugriffsrechte

Diese Tabelle zeigt, wer in Ihrer Gemeinde auf welche Daten zugreifen darf. Sie verwendet folgende Abkürzungen:

X = Kein Zugriff	Diese Person darf diese Daten weder sehen noch bearbeiten.
L = Lesezugriff	Diese Person darf die Daten NUR lesen, aber nicht verändern oder löschen.
S = Schreib-	Diese Person darf die Daten lesen UND verändern (z.B. neue Einträge machen oder bestehende Daten korrigieren).

und
Lesezugriff

Aktion erforderlich:

Prüfen Sie die Tabelle im Muster und passen Sie sie an Ihre Gemeindestruktur an. Überlegen Sie: Wer in Ihrer Gemeinde hat welche Funktion? Welche Daten benötigt diese Person für ihre Aufgaben? Das Prinzip lautet: So wenig Zugriff wie möglich, so viel wie nötig.

C.3 Kategorien der verarbeiteten Daten und Weitergabe

Diese große Tabelle ist auf den ersten Blick etwas unübersichtlich. Sie zeigt, welche Datenkategorien Sie für jede Personengruppe verarbeiten, und ob diese Daten an externe Stellen weitergegeben werden.

Was bedeuten die Spalten?

BDK	Besondere Datenkategorien (z.B. Gesundheitsdaten, religiöse Überzeugungen) – diese genießen besonderen Schutz.
Gemeindeleitung	Wird die Information intern an die Gemeindeleitung weitergegeben?
BBGÖ-Bundesbüro	Wird sie an das Bundesbüro der Baptistengemeinden Österreich weitergegeben?
FKÖ-Büro	Wird sie an das Büro der Freikirchen in Österreich weitergegeben?
Finanzamt / GKK / SV	Werden die Daten an Behörden weitergeleitet? (z.B. für die Lohnverrechnung)
O-365-Cloud	Werden die Daten in Microsoft Office 365 (OneDrive, SharePoint) gespeichert?
Webseite	Erscheinen die Daten auf der Gemeindef Webseite?

Bedeutung der Kürzel J, N, B, Z:

J	Ja – diese Daten werden an diese Stelle weitergegeben / dort gespeichert.
N	Nein – keine Weitergabe.
B	Nur unter bestimmten Bedingungen (z.B. nur wenn gesetzlich erlaubt oder vertraglich geregelt).
Z	Nur mit ausdrücklicher, dokumentierter Zustimmung der betroffenen Person.

Wichtiger Hinweis zu Fotos und sozialen Medien:

Wenn Sie Fotos von Personen auf der Gemeindef Webseite oder in sozialen Medien (Facebook, Instagram etc.) veröffentlichen, brauchen Sie IMMER die ausdrückliche und schriftliche Zustimmung der abgebildeten Personen. Bei Minderjährigen müssen die Eltern zustimmen.
Kürzel: Z.

C.4 Lösungs- und Aufbewahrungsfristen

Daten dürfen nicht ewig gespeichert werden. In diesem Abschnitt legen Sie fest, wie lange Sie welche Daten aufbewahren müssen oder dürfen.

Warum ist das wichtig?

Die DSGVO verlangt, dass personenbezogene Daten nur so lange gespeichert werden, wie es notwendig ist. Danach müssen sie gelöscht werden – es sei denn, ein Gesetz schreibt eine längere Aufbewahrung vor.

Die wichtigsten Fristen im Überblick:

Datenart	Aufbewahrungsfrist
Buchhaltungsdaten, Verträge, allgemeine Mitgliederdaten	Mindestens 7 Jahre (gesetzliche Aufbewahrungspflicht aus der BAO – Bundesabgabenordnung)
Fotos in sozialen Medien oder auf der Webseite	Sofortige Löschung auf Verlangen der betroffenen Person
Gruppenfotos von Gemeindeevents (nur für Archivzwecke)	Dauerhaft, aber nur im internen Archiv
Daten von ausgetretenen Mitgliedern	Bis Ende der Mitgliedschaft, dann gemäß Aufbewahrungspflicht

C.5 Empfänger personenbezogener Daten

Hier beschreiben Sie, an wen Daten außerhalb Ihrer Gemeinde weitergegeben werden – insbesondere wenn dies Stellen außerhalb der EU betrifft.

Wichtige Regel für Social Media:

Wenn Sie Daten von Gemeindemitgliedern in sozialen Netzwerken (Facebook, WhatsApp, Instagram etc.) teilen, darf das NUR mit ausdrücklicher, nachweisbarer Zustimmung der betroffenen Person geschehen. Eine mündliche Erlaubnis reicht nicht – es sollte eine schriftliche Zustimmung vorliegen.

D. Datenschutz-Folgenabschätzung

Dieser Abschnitt klingt kompliziert, ist aber für die meisten Gemeinden schnell zu erledigen.

Was ist eine Datenschutz-Folgenabschätzung (DSFA)?

Eine DSFA ist eine vertiefte Risikoanalyse, die nur bei besonders riskanten Datenverarbeitungen notwendig ist – z.B. wenn eine Organisation Tausende von Personen überwacht oder medizinische Daten in großem Stil verarbeitet. Für eine normale Gemeinde ist diese tiefgehende Analyse in der Regel NICHT erforderlich.

Das Formular enthält vier Fragen. Beantworten Sie jede mit Ja oder Nein:

#	Frage	Typisch für Gemeinden	Hinweis
a	Führen Sie automatische Persönlichkeitsprofile durch, die für wichtige Entscheidungen (z.B. Kreditvergabe) genutzt werden?	NEIN	Gemeinden erstellen keine solchen Profile.
b	Verarbeiten Sie in großem Umfang sensible Daten wie Gesundheitsdaten oder Strafregisterauszüge?	NEIN	Die Religionszugehörigkeit gilt als sensibel, wird aber nur im begrenzten Rahmen verarbeitet.
c	Überwachen Sie systematisch öffentliche Bereiche (z.B. Videoüberwachung in großem Stil)?	NEIN	Normale Gemeinden haben keine flächendeckende Videoüberwachung.
d	Stehen Ihre Verarbeitungen auf einer Risikoliste der Datenschutzbehörde?	NEIN	Nein oder Ja.

Ergebnis für die meisten Gemeinden:

Wenn alle vier Fragen mit NEIN beantwortet werden können – was für normale Gemeinden der Regelfall ist – ist KEINE vertiefte Datenschutz-Folgenabschätzung erforderlich. Tragen Sie dies entsprechend in das Formular ein.

Umgang mit Strafregisterbescheinigungen:

Personen im Kinder- und Jugenddienst haben als Diensterfordernis eine Strafregisterbescheinigung (früher: Leumunds-, Führungs- oder Sittenzeugnis oder sogenanntes polizeiliches Führungszeugnis) vorzulegen. Da diese Daten über strafrechtliche Verurteilungen und Straftaten enthalten kann und damit unter Art. 10 DSGVO fällt, wird empfohlen, die Bescheinigung lediglich einzusehen, die Unbedenklichkeit zu dokumentieren und das Dokument anschließend an den Mitarbeiter zurückzugeben. Andernfalls wäre eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen.

E. Technisch-organisatorische Maßnahmen (TOM)

Im letzten Abschnitt beschreiben Sie, wie Sie die Daten technisch und organisatorisch schützen. Das Musterformular enthält bereits konkrete Vorlagen – Sie müssen diese nur mit Ihren spezifischen Systemen ergänzen.

Einfache Erklärung:

TOMs sind alle Maßnahmen, die Sie ergreifen, damit Daten nicht in falsche Hände geraten, verloren gehen oder manipuliert werden. Das umfasst sowohl technische Dinge (Passwörter, Verschlüsselung) als auch organisatorische (wer darf was, Schulungen).

E.1 Zutrittskontrolle – Wer kommt physisch an die Daten heran?

Beschreiben Sie, wo Ihr Server oder Ihre Ablagesysteme stehen und wie der physische Zugang gesichert ist.

Beispiele zum Eintragen:

- "Der PC mit den Mitgliederdaten steht im Büro des Pastors, das immer versperrt ist, wenn keine Person anwesend ist." • "Alle Daten sind in der Microsoft Office 365 Cloud gespeichert (kein lokaler Server)." • "Der Server befindet sich in einem abgesperrten Kellerraum; Schlüssel haben nur Gemeindeleiter und Kassier."

E.2 Zugangskontrolle – Wer kann sich in die Systeme einloggen?

Beschreiben Sie, wie Ihre Computer und Programme durch Passwörter und Sperrmechanismen geschützt sind.

Was muss umgesetzt sein:

- Alle PCs, Tablets und Smartphones mit Gemeinddaten haben ein Passwort oder eine PIN. • Automatische Bildschirmsperre ist aktiviert (z.B. nach 5 Minuten ohne Eingabe). • Passwörter werden nicht auf Zetteln notiert oder mit anderen geteilt.

E.3 Zugriffskontrolle – Wer kann innerhalb des Systems was tun?

Das entspricht der Zugriffsrechte-Tabelle aus Abschnitt C.2. Beschreiben Sie, wo Ihre Daten gespeichert sind.

Beispiele zum Eintragen:

- "Daten werden in SharePoint/OneDrive gespeichert; Zugriffsrechte werden über Microsoft-Benutzergruppen verwaltet." • "Daten werden auf einem lokalen PC verwaltet; nur Pastorin und Personenstandsverwalterin haben Zugang."

E.4 Weitergabekontrolle – Schutz bei der Übertragung

Beschreiben Sie, wie Daten beim Versenden (E-Mail, Upload) geschützt sind.

Was ist einzutragen:

Geben Sie an, welchen E-Mail-Dienst Sie nutzen. Wenn Sie z.B. Gmail oder Outlook 365 nutzen, bieten diese standardmäßig SSL-Verschlüsselung. Beispiel: "E-Mails werden über Microsoft Outlook 365 gesendet, das SSL-Verschlüsselung verwendet."

E.5 Verfügbarkeitskontrolle – Datensicherung (Backup)

Beschreiben Sie, wie Sie sicherstellen, dass Daten nicht verloren gehen.

Beispiele:

- "Alle Daten werden täglich automatisch in der Microsoft 365 Cloud gesichert." • "Wöchentliches manuelles Backup auf eine externe Festplatte, die sicher aufbewahrt wird." • Wichtig: Nennen Sie auch Ihren Virenschutz (z.B. Windows Defender, Avast) und ob eine Firewall aktiv ist.

E.6 Verschlüsselung

Die DSGVO empfiehlt, dass alle Geräte, auf denen personenbezogene Daten gespeichert sind, verschlüsselt sein sollen.

Was ist zu tun:

- Windows-Nutzer: Aktivieren Sie BitLocker (in den Windows-Einstellungen unter "Geräteverschlüsselung" oder "BitLocker-Laufwerkverschlüsselung"). • Wenn Sie ausschließlich Cloud-Dienste wie Microsoft 365 nutzen, ist die Verschlüsselung durch Microsoft bereits sichergestellt – geben Sie das im Formular an. • Tragen Sie ein, welche Technologie Sie verwenden.

E.7 Datenschutz-Management

Was ist einzutragen?

Beschreiben Sie, wie Sie sicherstellen, dass das VVT regelmäßig aktualisiert wird und wie Mitarbeitende in Datenschutzfragen geschult werden. Empfehlung: Legen Sie fest, dass das VVT einmal jährlich überprüft wird (z.B. immer im Januar). Halten Sie Schulungen oder Informationsveranstaltungen für Mitarbeitende fest.

Abschluss-Checkliste: Ist mein VVT vollständig?

Gehen Sie diese Punkte durch, bevor Sie das VVT als fertig betrachten:

✓	Zu erledigen
<input type="checkbox"/>	Abschnitt A: Name, Adresse, E-Mail, Telefon der Gemeinde eingetragen
<input type="checkbox"/>	Abschnitt A: Kontaktdaten des DSB, des Datenschutzreferenten und des gemeindeeigenen Zuständigen eingetragen
<input type="checkbox"/>	Abschnitt B: Alle zutreffenden Verarbeitungszwecke gelistet (ggf. ergänzt)
<input type="checkbox"/>	Abschnitt C.1: Personengruppen und Rechtsgrundlagen überprüft
<input type="checkbox"/>	Abschnitt C.2: Zugriffsrechte-Tabelle an die eigene Gemeindestruktur angepasst
<input type="checkbox"/>	Abschnitt C.3: Datenkategorien und Weitergabe-Tabelle überprüft und ggf. angepasst
<input type="checkbox"/>	Abschnitt C.4: Löschfristen überprüft
<input type="checkbox"/>	Abschnitt C.5: Hinweis zur Social-Media-Zustimmung beachtet
<input type="checkbox"/>	Abschnitt D: Alle vier Fragen zur Folgenabschätzung beantwortet (für Gemeinden typischerweise alle NEIN)
<input type="checkbox"/>	Abschnitt E: Alle TOMs mit konkreten Angaben zu Ihren Systemen ausgefüllt (Serverstandort, Backup-System, Cloud-Dienst, Verschlüsselung)
<input type="checkbox"/>	Versionsnummer und Datum der aktuellen Version eingetragen
<input type="checkbox"/>	Name des Bearbeiters eingetragen
<input type="checkbox"/>	Dokument gespeichert und sicher aufbewahrt (digital verschlüsselt und/oder als Ausdruck in verschlossenem Ordner)

Haben Sie noch Fragen?

Wenden Sie sich an den Datenschutzbeauftragten der Freikirchen in Österreich: E-Mail: datenschutz@freikirchen.at | Tel: +43 1 943 67 14 Karl-Popper-Str. 16, 1100 Wien

Dieser Leitfaden bezieht sich auf das VVT-Muster V04 (Stand: 22.06.2020) der Freikirchen in Österreich.