

Verzeichnis von Verarbeitungstätigkeiten

nach Art 30 Abs 1 EU-Datenschutz-Grundverordnung (DSGVO)
(Verantwortlicher - Gemeinde als KÖR in den FreiKirchen in Österreich)

Aktualisierungsverlauf:

Versionsbezeichnung	V-Nr.	Datum	Bearbeitet von:
<i>Aktuelle Version:</i>	V01.33	24.06.2020	Philipp Marsak
Vorversionen:	V01.32	19.01.2020	Philipp Marsak
	V01.31	03.05.2019	Philipp Marsak
	V01.3	23.04.2019	Philipp Marsak
	V01.2	10.01.2019	Philipp Marsak
	V01.1	02.10.2018	Philipp Marsak
	V01	11.07.2018	Philipp Marsak

INHALT

- A Stammdatenblatt**
- B Datenverarbeitungen und Datenverarbeitungszwecke**
- C Detailangaben zu den einzelnen Datenverarbeitungszwecken**
- D Allgemeine Beschreibung organisatorisch-technischer Maßnahmen**

A Stammdatenblatt

A.1 Namen und Kontaktdaten des für die Datenverarbeitung Verantwortlichen

A.1.a Name und Anschrift:

Grace Church Vienna – Internationale Evangelikale Freikirche
Kenyongasse 15
1070 Wien

A.1.b E-Mail:

gracechurch.vie@gmail.com

A.1.c Vertreten durch:

Philipp Marsak
gracechurch.vie@gmail.com
+43 676 355 84 51

A.2 Name und Kontaktdaten der Datenschutzbeauftragten, Referenten und Zuständigen

A.2.a Datenschutzbeauftragter (FKÖ)

Michael Punz
datenschutz@freikirchen.at

A.2.b Datenschutzreferent des Bundes (gemäß DSO-FKÖ)

Wolfgang Luttenberger
datenschutz@beg.or.at
+43 660 316 06 99

A.2.c Datenschutz-Zuständiger der Gemeinde (gemäß DSO-FKÖ)

Philipp Marsak
gracechurch.vie@gmail.com
+43 676 355 84 51

B Datenverarbeitungen und Datenverarbeitungszwecke

- B.1 Mitgliederverwaltung:** Verarbeitung und Übermittlung von Daten im Rahmen der Führung gesetzlich vorgeschriebener Mitgliederverzeichnisse einschließlich automationsunterstützt erstellter und archivierter Beitragstabellen und Textdokumente (wie z.B. Korrespondenzen oder Vereinbarungen) in diesen Angelegenheiten.
- B.2 Personalverwaltung:** Verarbeitung und Übermittlung der Daten von Angestellten und ehrenamtlichen Mitarbeitern einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenzen oder Verträge) in diesen Angelegenheiten.
- B.3 Standortaufgaben und Objektverwaltung:** Verarbeitung und Übermittlung von Daten im Rahmen von Geschäftsbeziehungen mit Vermietern, Lieferanten und Dienstleistern, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenzen oder Verträge) in diesen Angelegenheiten.
- B.4 Kommunikation nach außen** für Informationen, Newsletter, etc.

C Detailangaben zu den in B. angegebenen Datenverarbeitungen

C.1 Personenkategorien und Rechtsgrundlagen zu den Datenverarbeitungen

C.1.a Kategorien der betroffenen Personengruppen

Beschreibung der Kategorien betroffener Personen und Einteilung in Gruppen a bis g

a)	Gemeindemitglieder
b)	Mitarbeiter im Ehrenamt
c)	Mitarbeiter mit Anstellung oder anderem Vertrag
d)	Vertretungsorgane des verantwortlichen Rechtsträgers
e)	Lieferanten, Vertragspartner
f)	Freunde und Interessenten der Gemeinde
g)	Sponsoren und Unterstützer

C.1.b Rechtsgrundlagen

a und b	Beitrittserklärung, Einwilligung zur Mitarbeit; <i>(Art 6 Abs. 1 lit a - Einwilligung der Betroffenen; gesetzliche Verpflichtungen (Stw. Sokrates, E-Government); zur Vertragserfüllung erforderlich)</i>
c und d	Dienstvertrag, Bestellung in eine Funktion; <i>(gesetzliche Verpflichtungen nach der BAO; zur Vertragserfüllung erforderlich)</i>
e	Bestellung, Vertrag; ein berechtigtes Interesse des Betroffenen; zur Vertragserfüllung erforderlich
f	Eintragung in einer Datenliste zum Erhalt von Information
g	Berechtigte Interessen des Betroffenen

C.2 Zugriffsrechte

Datenart	Funktionen in der Gemeinde									
	Personenstandsverwalter/in	Gemeindefeiler	Älteste	Diakone	Pastor	Gruppenleiter/innen	Kassier	Mitglieder	Ehrenamtliche Mitarbeiter/innen	Registrierte Planningcenter-Nutzer
Name	S	L	L	L	L	L	L	L	L	L
Vorname	S	L	L	L	L	L	L	L	L	L
Geburtsdatum	S	L	L	L	L	X	L	X	X	L
Adresse	S	L	L	L	L	L	L	X	X	X
Aufnahmedatum und Aufnahmeart (Taufe/Überweisung/anderes)	S	L	L	L	L	L	L	X	X	X
Taufdatum	S	L	L	L	L	X	X	X	X	X
Weitere erhobene Daten im Zuge der Mitgliedschaft (Studentenstatus, Ehepartner, Kinder,...)	S	L	L	L	L	X	X	X	X	X
Austrittsdatum und Austrittsart	S	L	L	L	L	L	L	X	X	X
Beitragsdaten	X	X	X	X	X	X	S	X	X	X
Funktion in der Gemeinde	S	L	L	L	L	L	L	L	L	L
Gemeindeguppen Mitgliedschaft	S	S	S	S	S	S	L	L	L	X
Anstellungsverträge	S	S	S	L	S	X	L	X	X	X

***Legende:** X = Kein Zugriff / L = Lesezugriff / S = Schreib- und Lesezugriff

(Wenn Personen mehreren Funktionen belegen für die unterschiedliche Zugriffsrechte gelten, kommt automatisch die höherrangigen Klasse in der jeweiligen Kategorie zu tragen)

C.3 Kategorien der verarbeiteten Daten und ob sie an Empfänger übermittelt werden

Kategorien der betroffenen Personengruppen aus Kapitel B)	Lfd.Nr.	Art	Datenkategorien	BDK	Empfänger, Übermittlung J/N												
					Gemeindeleitung	BEG-Büro	FKÖ-Büro	Schulamt FKÖ	Andere Gemeinden	Finanzamt GKK, SV	Steuerberater	Office-365-Cloud	Archiv	Webseite (Wix)	Planningcenter	Gmail Adressbuch	Mailchimp
a) Gemeinde-Mitglieder	1	N	Namen	N	J	J	N	B	B	Z	N	J	J	B	J	J	J
	2	N	Geb. Datum	N	J	J	N	B	B	Z	N	J	J	N	J	N	J
	3	N	Adresse	N	J	J	N	B	B	Z	N	J	J	N	J	N	N
	4	N	Telefonnummer, E-Mail (Korrespondenz)	N	J	J	N	B	B	N	N	J	J	B	J	J	J
	5	N	Soz. Vers.Nr.	N	B	N	N	B	N	Z	N	J	J	N	N	N	N
	6	N	Status (z.B. Student, Familienstand, Kinder etc.)	N	J	J	N	B	B	N	N	J	J	N	J	N	N
	7	N	Taufdaten	N	J	J	N	B	B	N	N	J	J	N	J	N	N
	8	S	Religionszugehörigkeit	N	J	J	B	B	B	N	N	J	J	N	N	N	N
	9	S	Beitragsdaten	N	B	N	N	N	B	Z	N	J	J	N	N	N	N
	10	S	Fotos	N	N	N	N	N	B	N	N	Z	J	Z	B	N	N
b) Mitarbeiter im Ehrenamt	11	N	Namen	N	J	J	N	N	B	Z	N	J	J	B	J	J	J
	12	N	Geb. Datum	N	J	J	N	B	B	Z	N	J	J	N	J	N	J
	13	N	Adresse	N	J	J	N	B	B	Z	N	J	J	N	J	N	N
	14	N	Telefonnummer, E-Mail (Korrespondenz)	N	J	J	N	B	B	N	N	J	J	B	J	J	J
	15	N	Soz. Vers.Nr.	N	B	N	N	B	N	Z	N	J	J	N	N	N	N
	16	N	Status (z.B. Student, Familienstand, Kinder etc.)	N	J	J	N	B	B	N	N	J	J	N	J	N	N
	17	N	Taufdaten	N	J	J	N	B	B	N	N	J	J	N	J	N	N
	18	S	Religionszugehörigkeit	N	B	B	B	B	B	N	N	J	J	N	N	N	N
	19	S	Beitragsdaten	N	B	N	N	N	B	Z	N	J	J	N	N	N	N
	20	S	Fotos	N	N	N	N	N	Z	N	N	Z	J	Z	B	N	N
c) d) Mitarbeiter und Organe des Rechtsträgers	21	N	Namen	N	J	B	J	B	B	Z	J	J	J	B	B	J	J
	22	N	Geb. Datum	N	J	B	J	B	B	Z	J	J	J	N	B	N	J
	23	N	Adresse	N	J	B	J	B	B	Z	J	J	J	N	B	N	N
	24	N	Telefonnummer, E-Mail (Korrespondenz)	N	J	B	J	B	B	N	J	J	J	B	B	J	J
	25	N	Soz. Vers.Nr.	N	B	B	B	B	Z	Z	J	J	J	N	B	N	N
	26	N	Funktion im Betrieb	N	J	B	J	B	B	Z	J	J	J	B	B	N	N
	27	N	IBAN, Einstellungsdatum, Beschäftigungsverhältnis, Wochenstunden, Familienstand, Anzahl der Kinder,	N	J	B	J	B	Z	Z	J	J	J	N	B	N	N
	28	N	Taufdaten	N	J	B	B	B	B	N	N	J	J	N	B	N	N
	29	S	Religionszugehörigkeit	N	J	J	J	B	B	N	N	J	J	N	B	N	N
e) Lieferanten und Vertragspartner	30	N	Name, Adresse, E-Mail, Tel-Nr., Branche	N	J	N	N	N	B	N	B	J	J	B	N	J	B
f) Freunde und Interessenten	31	N	Name, Adresse, (Geb. Datum), E-Mail, Tel-Nr.	N	J	N	N	N	B	N	N	J	J	B	N	Z	Z
g) Sponsoren, und Unterstützer	32	N	Namen, Adresse, Telefonnummer, E-Mail,	N	J	N	N	N	Z	N	N	J	J	B	N	J	B

*Art = N = nicht sensibel, S = sensibel, BDK = Besondere Datenkategorien iSd Art 9 DSGVO, strafrechtlich relevant iSd Art 10 DSGVO -
J = Ja / N = Nein / B = unterliegt spezifischen Bedingungen / Z = nur mit dokumentierter Zustimmung

C.4 Löschungs- und Aufbewahrungsfristen

Daten aus Kapitel C3 (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
10, 20, 21, 24, 26, 31, 32	Nach Aufforderung werden Daten in Messenger Diensten, Soz. Medien (sofern von der Gemeinde genutzt) und der Webseite sofort gelöscht, ansonsten Aufbewahrung so lange es für Dokumentationszwecke oder repräsentative Zwecke der Gemeinde notwendig ist.
1-8, 11-18, 21-30, 32	Aufgrund der gesetzlichen Aufbewahrungsfristen, auf jeden Fall 7 Jahre; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefrieten.
10, 20 (nur Gruppenfotos von Ereignissen)	Permanent nur für Archivzwecke
9, 10, 19, 20, 32	Bis zur Beendigung der Geschäftsbeziehungen, bzw. der Mitgliedschaft oder Unterstützung

C.5 Kategorien von Empfängern, an die personenbezogene Daten offengelegt werden (inkl. Auftragsverarbeitung), speziell bei Empfängern in Drittländern außerhalb der EU

- **Offenlegung von personenbezogenen Daten in internationalen Social Media Diensten ausschließlich mit ausdrücklicher nachweislicher Zustimmung der jeweils Betroffenen.**
- **Finanzamt, Weiterleitung von Beitragsdaten nur mit ausdrücklicher Genehmigung der Betroffenen**
 - Name, Adresse, Soz.Vers.Nr., Geb. Datum, Beitragszahlungen
- **Bund Evangelikaler Gemeinden Österreichs:**
 - Name, Adresse, Geb. Datum, Kinder-Daten, E-Mail Adresse,
 - Soz.Vers.Nr und Beitragszahlungen (zur Weiterleitung an das FA)
- **Unterkunftgeber bei Gemeindeveranstaltungen**
 - Name, Geb. Datum

C.6 Datenschutz-Folgenabschätzung

Gem. Art 35, Abs 1

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

Pos	Impact Frage gem. Art 35, Abs 3	Trifft zu J/N	Begründung/Maßnahme
a	Wird eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen (Profiling) durchgeführt, die in weiterer Folge als Grundlage für Entscheidungen herangezogen werden soll, die für natürliche Personen Rechtswirkungen entfalten könnte (z.B. zur Frage der Kreditvergabe)?	N	Wird nicht durchgeführt
b	Werden in umfangreicher Art und Weise sensible Daten oder Daten über strafrechtliche Verurteilungen und Straftaten selbst verarbeitet?	N	Es gibt sensible Daten, wie Religionszugehörigkeit, die Verarbeitung erfolgt jedoch nur im beschränkten Umfang im Rahmen der Mitgliederverwaltung.
c	Erfolgt bei der Datenverarbeitung eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (z.B. Videoüberwachungen)?	N	Wird nicht gemacht.
Und gem. Abs. (4)	Gibt es Listen der Datenschutzbehörde, die Fälle aufzählen, in denen eine Datenschutz-Folgenabschätzung zwingend durchzuführen ist?	N	Noch nichts bekannt

Ergebnis:

Keine der vier Fragen ergaben ein JA, somit kann auf eine Datenschutz-Folgenabschätzung verzichtet werden.

D Allgemeine Beschreibung der technisch-organisatorischen Maßnahmen

Vertraulichkeit:

- **Zutrittskontrolle:** Derzeit wird kein eigener Server verwendet. Sämtliche elektronischen Daten werden im Cloud Dienst von Microsoft Office 365 verwaltet. Zwecks Kommunikation und Planung werden ausgesuchte personenbezogene Daten auch über die Dienste Mailchimp und Planningcenter verwendet (Art der Daten siehe Punkt C3). Sämtliche der verwendete Dienste entsprechen der DSGVO (siehe Microsoft Office 365 Cloud: <https://privacy.microsoft.com/de-de/privacystatement>, Planningcenter: <https://planning.center/gdpr/>, Mailchimp: <https://mailchimp.com/legal/privacy/>). Mit letzteren beiden Diensten wurden auch eigene Verträge zur DSGVO-konformen Datenverarbeitung abgeschlossen. Einige wenige personenbezogene Daten werden auch über den DSGVO-konformen Webseitenbetreiber WIX übermittelt. Hierbei insbesondere Daten die Nutzer über ein Kontaktformular oder den Beitritt in den geschützten Mitglieder-Bereich selbst bekannt geben. Mehr zur Datenverarbeitung bei WIX unter diesem Link: <https://de.wix.com/about/privacy>. Daten in Papierform werden zur Erhöhung der Sicherheit, da die Räumlichkeiten der Gemeinde vielen Personen zugänglich sind, im Wohnsitz des Datenschutzzuständigen der Gemeinde, versperrt, unter Wahrung der Datenschutzaufgaben, von selbigem verwahrt.
- **Zugangskontrolle:** Sämtliche Geräte in Besitz der Grace Church, die Zugriff auf Daten ermöglichen können, sind vor unbefugter Systembenutzung durch Kennwörter geschützt. Alle Personen, die Zugang zu den Daten haben sind durch den Datenschutzzuständigen dahingehend geschult worden auch auf ihren Geräten den unbefugten Zugang durch Aktivierung von Passwörtern und automatischen Sperrmechanismen auf allen Endgeräten (Smart Phone, Tablets, PC) zu verhindern. Weiters haben sämtliche Personen, die Zugang zu personenbezogenen Daten haben, eine Geheimhaltungserklärung unterschrieben und sind über die Vorgangsweisen (z.B. keine unverschlüsselte Speicherung oder Übertragung,...) und Konsequenzen bei Nichteinhaltung aufgeklärt.
- **Zugriffskontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch Rechteverwaltung und Protokollierung von Zugriffen in der Microsoft Office 365 Cloud und in Planningcenter.

Integrität

- **Weitergabekontrolle:** Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch SSL Verschlüsselung durch 7zip.
- **Eingabekontrolle:** Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind: durch Protokollierungsmodule in der verwendeten Software von Microsoft Office 365 und Planningcenter, und durch Einschränkung und Schulung des Personenkreises.

Verfügbarkeit und Belastbarkeit:

- **Verfügbarkeitskontrolle:** Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch Backup-Strategie, Virenschutz und Firewall auf den verwendeten Computern und in der Microsoft Office 365 Cloud und Planningcenter.

Pseudonymisierung und Verschlüsselung:

- **Pseudonymisierung:** Wird auf Grund der geringen Anzahl von Datensätzen nicht angewandt.
- **Verschlüsselung:** Es werden in der Office 356 Cloud verschiedene Technologien eingesetzt, siehe: <https://www.microsoft.com/de-DE/trustcenter/security/encryption>. Technologien der Datenverarbeitung bei Planningcenter siehe: <https://planning.center/security/>. Technologien der Datenverarbeitung bei Mailchimp siehe: <https://mailchimp.com/about/security/>.

- **Alle PC Endgeräte von Nutzern** die auf personenbezogene Datenverzeichnisse zugreifen und diese lokal speichern (Offline verfügbar), weisen für die betroffenen Datenbereiche eine Verschlüsselung nach aktuellem Stand der Technik auf (z.B. Bitlocker oder VeraCrypt). Prinzipiell werden aber alle personenbezogenen Daten über die unter Punkt „Zutrittskontrolle“ beschriebene Cloud-Lösung verwaltet und nur in anlassbezogenen Ausnahmefällen direkt auf einem Gerät unter den oben beschriebenen Voraussetzungen gespeichert.

Evaluierungsmaßnahmen:

- **Datenschutz-Management** durch zyklisches Überarbeiten dieses Dokumentes, einschließlich regelmäßiger Mitarbeiter-Schulungen;

Protokollierung Datenschutzrelevanter Vorgänge:

- **20.10.2020: Datenübermittlung an BEG-Administration** per Onedrive-Cloud: Mitgliederverzeichnis, Eckdatenerhebung, Registerblatt
- **03.10.2019: Datenübermittlung an BEG-Administration** per Onedrive-Link: Mitgliederverzeichnis, Eckdatenerhebung, Registerblatt
- **26.09.2018: Datenübermittlung an BEG-Administration** per Onedrive-Link: Mitgliederverzeichnis, Eckdatenerhebung, Registerblatt