Datenschutz

Vereinbarung über die Bearbeitung von Personendaten

(Auftragsdatenbearbeitungsvereinbarung ADV)

zwischen

**[Pfarrei]**

[Adresse]

[PLZ, Ort]

nachfolgend «Auftraggeberin»

und

**[Vertragspartei]**

[Adresse]

[PLZ, Ort]

nachfolgend «Auftragnehmer»

gemeinsam die «Parteien»

# Ausgangslage

Der Auftragnehmer erhält im Rahmen der Abwicklung eines Vertrags (Hauptvertrag) von der Auftraggeberin oder auf sonstige Weise Zugriff auf Daten, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (nachfolgend „Personendaten“ oder „personenbezogene Daten“ genannt).

Die vorliegende Vereinbarung konkretisiert die Verpflichtungen der Parteien in Bezug auf datenschutzrechtlich zwingende Vorgaben gemäss der Europäischen Datenschutz-Grundverordnung (DSGVO) sowie dem Schweizer Bundesgesetz über den Datenschutz (DSG) und gilt, sofern und soweit diese anwendbar sind.

Die Auftraggeberin unterliegt Schweizer Recht. Für die Beauftragung des Auftragnehmers durch die Auftraggeberin gilt das DSG.

Die vorliegende Vereinbarung ergänzt den Hauptvertrag zwischen der Auftraggeberin und dem Auftragnehmer.

# Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich dazu:

1. Personendaten nur für die gemäss Anhang A vereinbarten Zwecke und in jedem Falle gemäss allfälligen dokumentierten Weisungen der Auftraggeberin zu bearbeiten;
2. die nach dem jeweils aktuellen Stand der Technik angemessenen technischen und organisatorischen Massnahmen zu ergreifen und aufrecht zu erhalten, um eine unberechtigte Bearbeitung, den Verlust oder die Verfälschung von Informationen zu verhindern. Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Massnahmen entspricht den Angaben in Anhang C;
3. die Bearbeitung von Personendaten nur nach vorgängiger schriftlicher Einwilligung der Auftraggeberin weiter zu vergeben und nur, wenn der Auftragnehmer dem Dritten Pflichten überbunden hat, welche mit den Regelungen dieser Vereinbarung mindestens gleichwertig sind. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragnehmer im Anhang B zu dieser Vereinbarung angeben;
4. die Bearbeitung von Personendaten nur in der Schweiz, in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen. Eine Bearbeitung von Personendaten in einem Drittland bedarf der vorherigen Zustimmung der Auftraggeberin, die zumindest in Textform erfolgen muss (E-Mail genügt). Werden Personendaten im Rahmen einer gemäss dieser Vereinbarung zulässigen Datenbearbeitung in ein Drittland ohne angemessenes Datenschutzniveau übermittelt, kommt eine Zustimmung nur dann in Betracht, wenn gewährleistet ist, dass genügend Massnahmen der Datensicherheit umgesetzt werden, um einen dem Risiko angemessenen Schutz zu gewährleisten;
5. den mit der Bearbeitung der relevanten Daten der Auftraggeberin befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen zu untersagen, die relevanten Daten ausserhalb des Hauptvertrags und dieser Vereinbarung zu bearbeiten. Ferner stellt der Auftragnehmer sicher, dass sich die zur Bearbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
6. der Auftraggeberin ohne Verzug jegliche Datenschutzverletzung oder vermutete Datenschutzverletzung (einschliesslich Verletzungen dieser Vereinbarung) sowie behördliche Zugriffe und Aufforderungen zur Datenherausgabe mitzuteilen;
7. die Auftraggeberin auf entsprechende erste Aufforderung hin bei der Einhaltung der anwendbaren Datenschutzgesetze (z.B. Erfüllung der Rechte der betroffenen Personen, Meldung bei Datenschutzverletzungen und Datenschutz-Folgenabschätzungen) gemäss den dem Auftragnehmer vorliegenden Informationen und nach Möglichkeit zu unterstützen;
8. die Einhaltung dieser Klausel durch die Auftraggeberin kontrollieren zu lassen, ob durch die Auftraggeberin selbst oder einen Dritten im Namen und im Auftrag der Auftraggeberin:
9. vorbehältlich allfälliger gesetzlicher Aufbewahrungspflichten nach der Auflösung des Hauptvertrags oder nach entsprechender Aufforderung der Auftraggeberin die Personendaten zurückzugeben oder zu löschen, ohne davon eine Kopie zu behalten, und eine solche Löschung zu bestätigen.

# Pflichten der Auftraggeberin

Die Auftraggeberin verpflichtet sich:

1. dem Auftragnehmer die im Vertrag und der Vereinbarung genannten personenbezogenen Daten in der vereinbarten Form zur Verfügung zu stellen;
2. zu gewährleisten, dass die Bearbeitung der übermittelten Personendaten durch die Auftraggeberin und deren Übermittlung an den Auftragnehmer rechtmässig und unter Einhaltung der massgeblichen gesetzlichen Bestimmungen erfolgt; dass diese namentlich nicht durch Gesetz oder aufgrund einer Geheimhaltungspflicht verboten sind;
3. alle Anweisungen bezüglich der Bearbeitung personenbezogener Daten durch den Auftragnehmer schriftlich zu dokumentieren (E-Mail gilt ebenfalls als schriftlich);
4. die Bearbeitung regelmässig zu überprüfen und wo nötig zu kontrollieren.

# Schlussbestimmungen

## Vertragsdauer

Die Vertragsdauer richtet sich nach der Laufzeit des Hauptvertrags, sofern sich aus den Bestimmungen dieser Vereinbarung nicht länger dauernde Verpflichtungen ergeben. Diese Vereinbarung kann nicht separat gekündigt werden.

## Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder unvollständig sein oder sollte die Erfüllung unmöglich werden, so wird hierdurch die Wirksamkeit der übrigen Teile des Vertrages nicht beeinträchtigt.

## Elektronische Unterschrift

Jede Partei stimmt zu, dass diese Vereinbarung bzw. jede Änderung oder Ergänzung elektronisch signiert werden kann, und dass alle elektronischen Signaturen, die auf diesem Vertrag erscheinen, hinsichtlich Gültigkeit, Durchsetzbarkeit und Zulässigkeit den handschriftlichen Unterschriften bzw. der Schriftform gleichwertig sind.

## Änderungen des Vertrages

Ergänzungen, Abänderungen oder die Aufhebung der vorliegenden Vereinbarung bedürfen zu ihrer Rechtswirksamkeit der Schriftform und müssen von jeder Partei handschriftlich oder elektronisch signiert werden.

## Anwendbares Recht und Gerichtsstand

Auf diese Vereinbarung ist schweizerisches Recht anwendbar. Für allfällige Streitigkeiten aus dieser Vereinbarung werden die Gerichte in [Ort] als zuständig erklärt.

|  |  |  |
| --- | --- | --- |
| **Pfarrei** |  |  |
|  |  |  |
| Datum |  | Datum |
|  |  |  |
| [Vorname Name] [Funktion] |  | [Vorname Name] [Funktion] |
|  |  |  |
| [**Auftragnehmer**] |  |  |
|  |  |  |
| Datum |  | Datum |
| [Vorname Name] [Funktion] |  | [Vorname Name] [Funktion] |

Anhang A: Spezifikation der Bearbeitung von Personendaten und Kontaktdaten

|  |
| --- |
| **Art und Zweck der Bearbeitung** |
| […] |

|  |
| --- |
| **Kategorien betroffener Personen** |
| […] |

|  |
| --- |
| **Art(en)** **der bearbeiteten Personendaten** |
| […] |

|  |  |  |  |
| --- | --- | --- | --- |
| **Allgemeine Kontaktinformationen** | **Name** | **E-Mailadresse** | **Telefonnummer** |
| Auftraggeberin | […] | […] | […] |
| Auftragnehmer | […] | […] | […] |

|  |  |  |  |
| --- | --- | --- | --- |
| **Kontaktinformationen für Verletzung der Datensicherheit** | **Name** | **E-Mailadresse** | **Telefonnummer** |
| Auftraggeberin | […] | […] | […] |
| Auftragnehmer | […] | […] | […] |

Anhang B: Liste der beigezogenen Unterauftragnehmer

Der Auftragnehmer nimmt für die Bearbeitung von Daten im Auftrag der Auftraggeberin Leistungen folgender Dritter in Anspruch, die in dem Auftrag des Auftragnehmers Daten bearbeiten („Unterauftragnehmer“):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Unterauftragnehmer (Name, Rechtsform, Sitz der Gesellschaft)** | **Kategorien von Personendaten die vom Unterauftragnehmer bearbeitet werden** | **Art und Zweck der Bearbeitung** | **Bearbeitungsort** | **Transfermechanismus**  (Wie werden Daten übermittelt?) | **Zusätzliche Garantien für die Übermittlung von Daten ausserhalb des EWR und der Schweiz** |
| […] | […] | […] | […] | […] | […] |
| […] | […] | […] | […] | […] | […] |

Anhang C: Technische und organisatorische Massnahmen der Datensicherheit

Detaillierte Angaben zu den vom Auftragnehmer getroffenen technischen und organisatorischen Massnahmen:

|  |
| --- |
| **Vertraulichkeit** |
| Zutrittskontrolle: Der Auftragnehmer trägt Sorge dafür, dass seine Büro- und Geschäftsräume grundsätzlich ausserhalb der Büro- und Geschäftszeiten geschlossen sind.  Während der Büro- und Geschäftszeiten ist sichergestellt, dass Besucher oder sonstige Dritte sich nicht alleine in Räumen bewegen können, in denen sie Zugang zu personenbezogenen Daten erhalten könnten.  Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt. |
| Zugangskontrolle: Um Zugang zu IT-Systemen zu erhalten, müssen der Auftragnehmer und seine Beschäftigten über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von einem oder mehreren Administratoren vergeben.  Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 12 Zeichen, wobei das Passwort auf Gross-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss.  Ein Passwortwechsel wird nicht erzwungen.  Eine Passworthistorie ist hinterlegt. So wird sichergestellt, dass die vergangenen 10 Passwörter nicht noch einmal verwendet werden können.  Fehlerhafte Anmeldeversuche werden protokolliert. Bei 3-maliger Fehleingabe erfolgt eine Sperrung des jeweiligen Benutzer-Accounts.  Remote-Zugriffe auf IT-Systeme des Auftragnehmers erfolgen stets über verschlüsselte Verbindungen.  Alle Server und Client-Systeme, die bei der Erbringung von Leistungen für die Auftraggeberin im Einsatz sind, sind durch Firewalls geschützt, die gewartet und mit aktuellen Updates und Patches versorgt werden.  Alle Mitarbeitenden sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen. Die IT-Systeme werden nach einer gewissen Zeit der Inaktivität automatisch gesperrt und sind passwortgeschützt.  Passwörter, die der Auftragnehmer von der Auftraggeberin erhält oder für dessen IT-Systeme verwendet, werden grundsätzlich verschlüsselt gespeichert und sind nur den Beschäftigten zugänglich zu machen, die konkret mit der Erbringung von Leistungen für die Auftraggeberin betraut sind. |
| Zugriffskontrolle: Berechtigungen für IT-Systeme und Applikationen des Auftragnehmers werden nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind.  Die Vernichtung von Datenträgern und Papier erfolgt durch einen Dienstleister, der eine Vernichtung nach DIN 66399 gewährleistet. |
| Trennung: Soweit der Auftragnehmer personenbezogene Daten von der Auftraggeberin im Zusammenhang mit der Auftragsbearbeitung erhält, wird er diese getrennt von Daten anderer Kunden bearbeiten. |
| Pseudonymisierung & Verschlüsselung: Ein administrativer Zugriff auf IT-Systeme der Auftraggeberin erfolgt über verschlüsselte Verbindungen. |
| **Integrität** |
| Eingabekontrolle: Der Auftragnehmer wird Eingaben, Änderungen oder Löschungen von personenbezogenen Daten, die er im Auftrag der Auftraggeberin durchführt, in geeigneter Weise dokumentieren, sofern nicht sichergestellt ist, dass das jeweilige IT-System selbst eine Protokollierung entsprechender Aktivitäten durchführt. |
| Weitergabekontrolle: Eine Weitergabe von personenbezogenen Daten, die im Auftrag der Auftraggeberin erfolgt, darf jeweils nur in dem Umfang erfolgen, wie und soweit dies mit der Auftraggeberin abgestimmt ist. Die Nutzung von privaten Datenträgern ist dem Auftragnehmer im Zusammenhang mit der Auftragsbearbeitung für die Auftraggeberin untersagt. |
| **Verfügbarkeit und Belastbarkeit** |
| Soweit der Auftragnehmer personenbezogene Daten oder Zugangsdaten für die Auftraggeberin speichert oder verwaltet, trägt er Sorge dafür, dass diese Daten mindestens täglich inkrementell und wöchentlich „voll“ gesichert werden. Es gibt ein Datensicherungskonzept, dass auch das erfolgreiche Testen der Wiederherstellung von Daten beinhaltet. |
| **Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung** |
| Der Auftragnehmer trägt durch Richtlinien und/oder Anweisungen an die Beschäftigten dazu bei, dass eine Bearbeitung personenbezogener Daten in einer Weise gewährleistet ist, welche den gesetzlichen Anforderungen entspricht.  Dies beinhaltet insbesondere eine regelmässige Überprüfung der Wirksamkeit der getroffenen Maßnahmen zum Schutz personenbezogener Daten und ggf. der Anpassung.  Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Beschäftigten erkannt und unverzüglich der Auftraggeberin gemeldet werden, wenn dies Daten betrifft, die im Rahmen der Auftragsbearbeitung für die Auftraggeberin bearbeitet werden. |
| **Auftragskontrolle** |
| Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben des jeweils anzuwendenden Datenschutzrechts ein Auftragsdatenbearbeitungs-Vertrag abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmässig kontrolliert. |

Zertifizierungen des Auftragnehmers:

|  |  |  |
| --- | --- | --- |
| **Zertifikat** | **Organisatorische Einheit, auf die sich die Zertifizierung bezieht** | **Gültigkeitsdauer des Zertifikats** |
|  |  |  |