**Vereinbarung über die Auftragsdatenbearbeitung   
nach Art. 9 DSG**

# Parteien

**Auftraggeberin:** [*ausfüllen*]

**Auftragnehmerin**: [*ausfüllen*]

# Hauptvertrag

Diese Vereinbarung erweitert den zwischen den Parteien geschlossenen Hauptvertrag: [*einfügen:* Vertrag über XY vom Datum].

# Gegenstand dieser Vereinbarung

1. Gegenstand dieser Vereinbarung ist die Bearbeitung von Personendaten der Auftraggeberin im Rahmen der Erfüllung der Verpflichtungen aus dem Hauptvertrag durch die Auftragnehmerin.
2. Gegenstand der Datenbearbeitung sind folgende Datenkategorien: [*aufzählen:* bspw. Personenstammdaten, Kontaktdaten, Finanzdaten, Sozialversicherungsdaten, Gesundheitsdaten, Auftragsdaten, Aufnahmen, Lebenslaufdaten etc.]
3. Betroffen sind folgende Personenkategorien: [*aufzählen:* bspw. Mitarbeitende, Bewerber, Kunden, Lieferanten, Interessenten, Ansprechpartner etc.]
4. Die Datenbearbeitung findet an den folgenden Orten statt: [*aufzählen:* Schweiz, EU, EFTA-Staaten, *einzeln aufzählen:* Drittstaaten].
5. Folgende Unterauftragnehmer dürfen von der Auftragnehmerin eingesetzt werden:

|  |  |  |
| --- | --- | --- |
| **Name** | **Tätigkeit** | **Bearbeitungsort** |
| [*ausfüllen*] |  |  |
|  |  |  |

Die Auftragnehmerin gibt der Auftraggeberin den Wechsel oder den Beizug eines neuen Unterauftragnehmers mind. XX Wochen/Monate im Voraus in Textform (bspw. per E-Mail) bekannt.

# Grundsätzliche Pflichten der Auftragnehmerin

1. Die Auftragnehmerin verpflichtet sich, die bearbeiteten Personendaten zu keinen anderen als den vereinbarten Zwecken zu verwenden.
2. Die Auftragnehmerin setzt bei der Durchführung der Arbeiten nur Personen oder Unterauftragnehmer ein, die zur Geheimhaltung verpflichtet und mit den relevanten Bestimmungen des Datenschutzes vertraut gemacht wurden.
3. Die Auftragnehmerin bearbeitet die Personendaten nur im Rahmen von dokumentierten Weisungen der Auftraggeberin.
4. Die Auftragnehmerin ermöglicht es der Auftraggeberin, einem von ihr beauftragten Prüfer oder deren Aufsichtsbehörde, jederzeit Kontrollen betr. die Einhaltung dieser Vereinbarung auszuführen. Anstelle von Vorort-Kontrollen erbringt die Auftragnehmerin diesen Nachweis auf Verlangen schriftlich (bspw. mittels Offenlegung von Audit-, Zertifizierungs- oder sonstigen Prüfergebnissen wie Penetration Tests).
5. Die Auftragnehmerin stellt die Datensicherheit durch geeignete technische und organisatorische Massnahmen nach Anhang 1 sicher. Diese Massnahmen unterliegen dem technischen Fortschritt. Die Auftragnehmerin kann alternative adäquate Massnahmen umsetzen. Dabei darf das bisherige Sicherheitsniveau nicht unterschritten werden. Wesentliche Änderungen werden dokumentiert.
6. Die Auftragnehmerin verpflichtet sich ausserdem, die Auftraggeberin innert 48 Stunden seit Feststellung über einen Datensicherheitsvorfall zu informieren.
7. Die Auftragnehmerin unterstützt die Auftraggeberin im Rahmen von Behördenanfragen oder Kontrollen sowie zwecks Beantwortung von Betroffenengesuchen.
8. Kopien oder Duplikate der Daten werden ohne Wissen der Auftraggeberin nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemässen Datenbearbeitung erforderlich sind.
9. Auf Verlangen der Auftraggeberin, spätestens aber mit Beendigung des Hauptvertrags, löscht die Auftragnehmerin sämtliche Personendaten der Auftraggeberin, vorbehältlich anderweitiger Vereinbarungen (bspw. Backup-Aufbewahrung).

# Dauer der Auftragsbearbeitung

Diese Vereinbarung bleibt so lange in Kraft, wie die Auftragnehmerin Personendaten der Auftragnehmerin bearbeitet, d.h. ggf. über das Ende des Hauptvertrags hinaus, falls die Auftragnehmerin resp. deren Unterauftragnehmer noch Backups der Auftraggeberin aufbewahrt.

# Anhang 1 – Technische und organisatorische Massnahmen

Es handelt sich nachfolgend um Massnahmen der Datensicherheit und zur Gewährleistung eines angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei berücksichtigt die Auftragnehmerin den Stand der Technik, die Kosten und die Art, den Umfang und die Zwecke der Bearbeitung.

Die Auftragnehmerin ergreift die folgenden Massnahmen (bitte Zutreffendes ankreuzen):

Zugangskontrollen

Videoüberwachung

Sichere Aktenvernichtung

USV

Security-Checks des Personals

IAM

Datenzugriffe nur mit Authentifizierung

MFA für alle

MFA für externe Zugriffe

PAM

Admin nur temporär und  MFA

Passwortregeln

Least-Privilege-Prinzip

Need-to-know-Prinzip

Audit-Trails

Zero-Trust-Prinzip

Remote nur VDI

At-rest verschlüsselt

In-transit verschlüsselt

Endgeräte verschlüsselt

TLS enforced

Emails nur S/MIME

ASVS Level 2

Penetration Tests, ext. Security Audits

ISMS ASVS Level 2

Backups

BCM-Konzept

Firewalls

DLP

EDR/XDR

MDM

HW und SW alle inventarisiert

Malwareschutz

aktuelles Patchmanagement

Trennung produktive/andere Systeme

Installation von Software kontrolliert

Zertifizierung ISO 27001 (AVV im Scope)

SOC2 Typ II Bericht

SOC

SIEM

Weisung Informationssicherheit

Schulung Informationssicherheit

# Unterschriften

**Auftraggeberin: Unterschrift:**

Ort, Datum: ………………………………………. ………………………………………………..

Name

**Auftragnehmerin: Unterschrift:**

Ort, Datum: ………………………………………. ………………………………………………..

Name