C. Allgemeines Muster einer Auftragsverarbeitervereinbarung (deutsche Version)

Auftragsverarbeitervereinbarung
(nachfolgend „**Vereinbarung**")

zwischen

[Firmenwortlaut des Verantwortlichen]
[Anschrift des Verantwortlichen]
(nachfolgend „**Verantwortlicher**")

und

[Firmenwortlaut des Auftragsverarbeiters]

[Anschrift des Auftragsverarbeiters]

(nachfolgend „**Auftragsverarbeiter**")

1. Ziel der Vereinbarung

Der Auftragsverarbeiter hat sich verpflichtet, die in Anhang 1 beschriebenen Datenverarbeitungen gegenüber dem Verantwortlichen zu erbringen. Für die Zwecke dieser Vereinbarung gelten die Begriffsdefinitionen der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, nachfolgend „**DSGVO**").

2. Weisungsrecht

2.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation –, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist.

2.2 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der EU oder der Mitgliedstaaten verstößt.

2.3 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, falls er nach dem Recht der Union oder der Mitgliedstaaten dazu verpflichtet ist, entgegen den Weisungen des Verantwortlichen oder

ohne Weisung des Verantwortlichen eine Datenverarbeitung vorzunehmen (sofern eine solche Mitteilung zulässig ist).

3. Vertraulichkeit

Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

4. Datensicherheit

4.1 Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er ausreichende Sicherheitsmaßnahmen ergriffen hat, um zu verhindern, dass Daten ordnungswidrig verwendet oder Dritten unbefugt zugänglich werden.

4.2 Der Auftragsverarbeiter hat insbesondere die in Anhang 2 angeführten Maßnahmen zu implementieren.

4.3 Außerdem erklärt der Auftragsverarbeiter, dass er alle gemäß Artikel 32 DSGVO erforderlichen Maßnahmen ergreift.

5. Sub-Auftragsverarbeitung

5.1. Der Auftragsverarbeiter ist befugt, folgende Unternehmen als Sub-Auftragsverarbeiter heranzuziehen (im Folgenden zusammen **„Sub-Auftragsverarbeiter“**):

a. *[Firmenwortlaut des Sub-Auftragsverarbeiters]*
[Anschrift des Sub-Auftragsverarbeiters]

5.2. Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Sub-Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben und die Hinzuziehung oder die Ersetzung zu untersagen. Erhebt der Verantwortliche innerhalb von zwei Wochen keinen Einspruch, so gilt die Hinzuziehung oder Ersetzung als genehmigt.

5.3 Nimmt der Auftragsverarbeiter einen anderen Sub-Auftragsverarbeiter in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem Sub-Auftragsverarbeiter im Wege eines Vertrags dieselben Datenschutzpflichten auferlegt, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entspre-

chend den Anforderungen des anwendbaren Datenschutzrechts erfolgt.

5.4 Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

6. Unterstützung

6.1 Soweit dies möglich ist, unterstützt der Auftragsverarbeiter den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Pflichten des Verantwortlichen bei Anträgen auf Wahrnehmung der Betroffenenrechte gemäß dem anwendbaren Datenschutzrecht, einschließlich Kapitel III der DSGVO.

6.2 Darüber hinaus unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Einhaltung seiner Pflichten gemäß dem anwendbaren Datenschutzrecht, einschließlich Artikel 32–36 DSGVO.

7. Rückgabe von personenbezogenen Daten

Nach Wahl des Verantwortlichen löscht der Verantwortliche nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten oder gibt diese zurück, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

8. Überprüfung

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen, einschließlich Inspektionen, die von dem Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden.

9. Haftung

Beide Parteien haften nach den Grundsätzen des österreichischen Zivilrechts.

10. Sonstiges

10.1 Änderungen dieser Vereinbarung sind ausschließlich in schriftlicher Form vorzunehmen. Dies gilt auch für dieses Schriftlichkeitsgebot.

10.2 Sollte eine Bestimmung dieser Vereinbarung ungültig oder unwirksam sein, wird sie, soweit gesetzlich zulässig, durch jene Bestimmung ersetzt, die wirtschaftlich der ungültigen oder unwirksamen Bestimmung am nächsten kommt.

Im Namen des Verantwortlichen:	Im Namen des Auftragsverarbeiters:
.....	.....
Ort und Datum:	Ort und Datum:
.....	.....

Anhang 1: Details der erbrachten Datenverarbeitungen

Anhang 2: Technische und organisatorische Maßnahmen zum Schutz von personenbezogenen Daten

Anhang 1: Details der erbrachten Datenverarbeitungen

Betroffene Personen

Die übermittelten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen:

.....

.....

Kategorien von Daten

Die übermittelten personenbezogenen Daten gehören zu folgenden Datenkategorien (bitte genau angeben):

.....

.....

Kategorien von sensiblen Daten (falls zutreffend)

Die übermittelten personenbezogenen Daten umfassen folgende sensible Daten:

.....

.....

Gegenstand der Verarbeitung und Verarbeitungsmaßnahmen

Die übermittelten personenbezogenen Daten werden folgenden grundlegenden Verarbeitungsmaßnahmen unterzogen:

.....

.....

Verarbeitungszwecke

Die übermittelten personenbezogenen Daten werden zu folgenden Zwecken des Verantwortlichen verarbeitet:

.....

.....

Anhang 2: Technische und organisatorische Maßnahmen zum Schutz von personenbezogenen Daten

Präventive Sicherheitsmaßnahmen – Maßnahmen zur Verhinderung eines erfolgreichen Angriffs

- Technische Maßnahmen
  - **Logische Zugriffskontrolle**: Die Vergabe von Zugriffsberechtigungen erfolgt nach dem „Need-to-Know"-Prinzip.
  - **Authentifizierung**: Jeglicher Zugriff auf personenbezogene Daten erfolgt ausschließlich nach einer erfolgreichen Authentifizierung.
  - **Passwortsicherheit**: Soweit Passwörter zur Authentifizierung eingesetzt werden, sollten diese mindestens acht Zeichen lang sein und aus Klein- und Großbuchstaben, Zahlen und Sonderzeichen bestehen. Passwörter werden ausschließlich verschlüsselt gespeichert.
  - **Verschlüsselung auf dem Übertragungsweg**: Personenbezogene Daten werden auf dem Übertragungsweg über das Internet verschlüsselt, zumindest soweit es sich um Daten der Lohnverrechnung oder sensible Daten handelt.
  - **Verschlüsselung mobiler Geräte**: Mobile Endgeräte und mobile Datenträger werden verschlüsselt, zumindest soweit auf diesen Geräten Daten der Lohnverrechnung oder sensible Daten gespeichert werden.
  - **Netzwerksicherheit**: Es wird eine Firewall eingesetzt, welche das interne Netzwerk vom Internet trennt und – soweit möglich – eingehenden Netzwerkverkehr blockiert.
  - **Maßnahmen gegen Schadsoftware**: Es wird nach Möglichkeit auf allen Systemen Anti-Viren Software eingesetzt. Alle eingehenden E-Mails werden automatisch auf Schadsoftware gescannt.
  - **Management von Sicherheitslücken**: Soweit möglich, wird auf allen Geräten die automatische Installation von Sicherheitsupdates aktiviert. Ansonsten erfolgt die Installation kritischer Sicherheitsupdates binnen drei Arbeitstagen, die Installation von Sicherheitsupdates mittlerer Kritikalität binnen 25 Arbeitstagen und die Installation von Sicherheitsupdates geringer Kritikalität binnen 40 Arbeitstagen.
- Organisatorische Maßnahmen
  - **Klare Zuständigkeiten**: Interne Zuständigkeiten für Fragen der Datensicherheit werden definiert.
  - **Verschwiegenheitspflicht der Dienstnehmer**: Die Dienstnehmer werden über die Dauer ihres Dienstverhältnisses hinaus zur Ver-