Mustervertrag über die Auftragsverarbeitung   
gemäß Artikel 28 Absatz 3 DSGVO[[1]](#footnote-1)

zwischen

dem **Verein ##**, ZVR ##, Anschrift ##, vertreten durch den Obmann/Obfrau ##, als Verantwortlicher im Sinn von Artikel 4 Ziffer 7 DSGVO (im Folgenden: „Auftraggeber“ genannt)

und

dem Unternehmen ##, Anschrift, als Auftragsverarbeiter im Sinn von Artikel 4 Ziffer 8 DSGVO (im Folgenden: „Auftragnehmer“ genannt).

**Präambel**

Zwischen dem Auftraggeber und dem Auftragnehmer besteht ein zivilrechtliches Auftragsverhältnis gemäß Vereinbarung vom ## (im Folgenden: „zivilrechtlicher Auftrag“). Mit dem gegenständlichen Vertrag über die Auftragsverarbeitung werden datenschutzrechtliche Aspekte dieses zivilrechtlichen Auftrages geregelt.

**§ 1 Gegenstand und Dauer des Vertrages**

(1) Nach dem zivilrechtlichen Auftrag übernimmt der Auftragnehmer zB Aufgaben eines Systemadministrators sowie die Betreuung / Wartung der Applikationen ## sowie...).

(2) Im Rahmen der Erfüllung des zivilrechtlichen Auftrages hat der Auftragnehmer Zugriff auf alle Kategorien personenbezogener Daten, die in den in Absatz 1 angeführten Applikationen verarbeitet werden (Datenverarbeitung). Ausdrücklich festgehalten wird, dass davon auch besondere Kategorien personenbezogener Daten (insbesondere Gesundheitsdaten) und strafrelevante Daten betroffen sind. Kategorien betroffener Personen sind Jugendliche, die Unterstützungsleistungen des Auftraggebers in Anspruch nehmen und Mitarbeiter\*innen des Auftraggebers.

**§ 2 Dauer des Vertrages**

(1) Die Dauer (Laufzeit) dieses Vertrages entspricht der Dauer (Laufzeit) des zivilrechtlichen Auftrages.

(2) Wird der zivilrechtliche Auftrag vorzeitig beendet oder aufgelöst, so gilt dies auch für den gegenständlichen Vertrag.

**§ 3 Pflichten des Auftragnehmers**

(1) Die Datenverarbeitung durch den Auftragnehmer findet ausschließlich in einem Mitgliedstaat der Europäischen Union (EU) oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Jede Verlagerung der Datenübertragung in ein Drittland, wenn auch nur teilweise, bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artikel 44 folgende DSGVO nachweislich erfüllt sind.

(2) Der Auftragnehmer verpflichtet sich, alle gemäß Artikel 32 DSGVO erforderlichen Maßnahmen zu ergreifen. Bei der Auswahl geeigneter technischer und organisatorischer Maßnahmen, die ein angemessenes Schutzniveau gewährleisten, ist vom Auftragnehmer zu berücksichtigen, dass von der Verarbeitung auch besondere Kategorien personenbezogener Daten (insbesondere Gesundheitsdaten) und strafrelevante Daten betroffen sind.

(3) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

(4) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich in diesem Zusammenhang unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer das entsprechende Ersuchen unverzüglich an den Auftraggeber weiterleiten.

**§ 4 Qualitätssicherung und sonstige Pflichten des Auftragnehmers**

(1) Der Auftragnehmer hat nach Maßgabe von Artikel 37 DSGVO einen Datenschutzbeauftragten zu benennen und dem Auftraggeber die Kontaktdaten dieses Datenschutzbeauftragten zum Zweck der direkten Kontaktaufnahme mitzuteilen. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.

(2) Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten schriftlich auf das Datengeheimnis verpflichtet und zuvor über die für sie relevanten Bestimmungen zum Datenschutz belehrt wurden. Der Auftraggeber behält sich ausdrücklich vor, das Vorliegen schriftlicher Verpflichtungen auf das Datengeheimnis zu kontrollieren. Auf Verlangen sind dem Auftraggeber schriftliche Verpflichtungen auf das Datengeheimnis einzelner Mitarbeiter vorzulegen.

(3) Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, dass eine Weisung gegen Datenschutzvorschriften verstößt. Der Auftragnehmer ist in diesem Fall berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(4) Der Auftragnehmer hat den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde zu informieren, soweit sich diese Kontrollen und Maßnahmen auf den gegenständlichen Auftrag beziehen. Dies gilt auch dann, wenn eine zuständige Behörde im Rahmen eines Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(5) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

(6) Der Auftragnehmer hat interne Prozesse sowie technische und organisatorische Maßnahmen regelmäßig zu kontrollieren, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(7) Der Auftragnehmer hat den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten zu unterstützen (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

(8) Der Auftragnehmer hat den Auftraggeber über Verstöße gegen die DSGVO oder gegen jede andere datenschutzrelevante Vorschrift, unverzüglich nach Bekanntwerden zu informieren.

(9) Der Auftragnehmer nimmt zur Kenntnis, dass er für die gegenständliche Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Artikel 30 DSGVO zu errichten hat.

**§ 5 Subauftragsverhältnisse**

(1) Als Subauftragsverhältnisse sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nebenleistungen, die der Auftragnehmer in Anspruch nimmt (z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice, Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen) fallen nicht darunter. Zur Gewährleistung des Datenschutzes und der Datensicherheit in Bezug auf die Daten des Auftraggebers verpflichtet sich der Auftragnehmer jedoch, über ausgelagerte Nebenleistungen angemessene Vereinbarungen über den Datenschutz und die Datensicherheit abzuschließen und entsprechende Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Subauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

(3) Der Auftragnehmer schließt mit dem Subauftragnehmer erforderliche Vereinbarungen gemäß Artikel 28 Absatz 4 DSGVO ab. Dabei ist sicherzustellen, dass der Subauftragnehmer dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund der gegenständlichen Vereinbarung obliegen. Kommt der Subaufragnehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Subauftragnehmers.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für ein Subauftragsverhältnis gestattet.

**§ 6 Kontrollrechte des Auftraggebers**

(1) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch ihn beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind. Der Auftragnehmer verpflichtet sich weiters, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. Der Nachweis solcher Maßnahmen, die nicht nur den gegenständlichen Auftrag betreffen, kann durch die Zertifizierung nach einem genehmigten Zertifizierungsverfahren, aktuelle Testate, Berichte oder Berichtsauszüge (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) erfolgen.

**§ 7 Löschung und Rückgabe personenbezogener Daten**

(1) Ohne Genehmigung des Auftraggebers dürfen keine Kopien oder Duplikate der Daten erstellt werden. Davon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung von gesetzlichen Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss des gegenständlichen Auftrages oder früher nach Aufforderung durch den Auftraggeber, spätestens jedoch mit Beendigung des gegenständlichen Vertrages, hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung ordnungsgemäß zu vernichten. Auf Verlangen ist dem Auftraggeber das Protokoll der Löschung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

Ort, Datum

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Für den Auftraggeber

Name, Vorname

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Für den Auftragnehmer

Name, Vorname

**Anlage**

Geeignete technische und organisatorische Maßnahmen im Sinn dieses Vertrages können insbesondere sein:

**Vertraulichkeit**

* Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B. durch Schlüssel, Magnet- oder Chipkarten, elektronische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;
* Zugangskontrolle: Schutz vor unbefugter Systembenutzung, z.B. durch eindeutige Authentifikation (einschließlich einer entsprechenden Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
* Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B. durch Standard-Berechtigungsprofile auf „need to know-Basis“, Standardprozesse für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten;
* Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt und gesondert aufbewahrt.
* Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

**Integrität**

* Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
* Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

**Verfügbarkeit und Belastbarkeit**

* Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;
* Rasche Wiederherstellbarkeit;
* Löschungsfristen: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.

**Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

* Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen;
* Incident-Response-Management;
* Datenschutzfreundliche Voreinstellungen;
* Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Artikel 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS), Vorabüberzeugungspflicht;

1. Dieser Mustervertrag wird trotz sorgfältiger Bearbeitung ohne Gewähr zur Verfügung gestellt. Eine Anpassung dieses Musters ist im Einzelfall unerlässlich. Eine Haftung der Verfasser wird ebenso ausgeschlossen wie eine Haftung des Herstellers. [↑](#footnote-ref-1)