

Mustervereinbarung zur Auftragsverarbeitung

zwischen

JUGEND für Europa (nachfolgend JfE genannt), **Nationale Agentur die EU-Programme Erasmus+ Jugend, Erasmus+ Sport und Europäisches Solidaritätskorps** - vertreten durch Manfred von Hebel- (Rechtsträger: IJAB – Fachstelle für Internationale Jugendarbeit der Bundesrepublik Deutschland e.V.) Godesberger Allee 142-148, 53175 Bonn

- im Folgenden „Auftraggeber“ -

und

- im Folgenden „Auftragnehmer/in“ -

wird folgender Vertrag geschlossen.

(nachfolgend beide Parteien auch bezeichnet als „Partei“ oder „Parteien“)

§ 1 Allgemeine Bestimmungen und Auftragsgegenstand

- (1) Gegenstand des vorliegenden Vertrags ist die Verarbeitung personenbezogener Daten im Auftrag durch den Auftragsverarbeiter (Art. 28 DSGVO). Inhalt des Auftrags, Kategorien betroffener Personen und Datenarten sowie Zweck der Verarbeitung sind Anlage 1 zu entnehmen.
- (2) Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er allein ist für die Beurteilung der Zulässigkeit der Datenverarbeitungsvorgänge nach Art. 6 DSGVO und die Wahrung der Betroffenenrechte verantwortlich.
- (3) Die Verarbeitung der Daten durch den Auftragsverarbeiter findet ausschließlich auf dem Gebiet der Bundesrepublik Deutschland, einem Mitgliedsstaat der Europäischen Union oder einem Vertragsstaat des EWR-Abkommens statt. Eine Verarbeitung außerhalb dieser Staaten erfolgt nur unter den Voraussetzungen von Kapitel 5 der DSGVO (Art. 44 ff.) und mit vorheriger Zustimmung des Auftraggebers.
- (4) Die Vergütung wird außerhalb dieses Vertrags vereinbart.

§ 2 Vertragslaufzeit und Kündigung

Der vorliegende Vertrag wird auf unbestimmte Zeit geschlossen und kann von jeder Vertragspartei mit einer Frist von drei Monaten ordentlich gekündigt werden. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

§ 3 Weisungen des Auftraggebers

- (1) Dem Auftraggeber steht ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Modalitäten der Datenverarbeitung zu. Er kann insbesondere die unverzügliche Löschung, Berichtigung, Sperrung oder Herausgabe der Daten verlangen. Der Auftragsverarbeiter ist verpflichtet, den Weisungen zu folgen, sofern keine berechtigten vertraglichen oder gesetzlichen Interessen entgegenstehen.

- (2) Der Auftragsverarbeiter informiert den Auftraggeber unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen gesetzliche Vorschriften verstößt. Wird eine Weisung erteilt, deren Rechtmäßigkeit zweifelhaft ist, darf die Ausführung vorübergehend ausgesetzt werden, bis der Auftraggeber diese bestätigt oder ändert.
- (3) Weisungen sind schriftlich oder elektronisch (z. B. per E-Mail) zu erteilen. Mündliche Weisungen sind auf Verlangen schriftlich zu bestätigen. Person, Datum und Uhrzeit der Weisung sind zu protokollieren.
- (4) Der Auftraggeber benennt auf Verlangen des Auftragsverarbeiters eine oder mehrere weisungsberechtigte Personen. Änderungen sind unverzüglich mitzuteilen.

§ 4 Kontrollbefugnisse

- (1) Der Auftraggeber ist berechtigt, die Einhaltung der Datenschutzvorschriften regelmäßig zu kontrollieren oder durch Dritte kontrollieren zu lassen. Der Auftragsverarbeiter unterstützt diese Kontrollen umfassend.
- (2) Kontrollmaßnahmen müssen verhältnismäßig sein und den Betrieb nicht mehr als erforderlich beeinträchtigen. Vor-Ort-Kontrollen erfolgen nach Terminvereinbarung und üblicher Geschäftszeit.
- (3) Ergebnisse von Kontrollen und Weisungen sind von beiden Parteien zu protokollieren.

§ 5 Allgemeine Pflichten des Auftragsverarbeiters

- (1) Die Verarbeitung der Daten erfolgt ausschließlich auf Grundlage des Vertrags und der Weisungen des Auftraggebers. Abweichungen nur bei gesetzlicher Verpflichtung, wobei der Auftraggeber unverzüglich informiert wird.
- (2) Der Auftragsverarbeiter hat alle gesetzlichen Vorschriften einzuhalten, insbesondere die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen.
- (3) Besteht eine Pflicht zur Benennung eines Datenschutzbeauftragten, bestätigt der Auftragsverarbeiter, diesen bestellt zu haben und benennt seine Kontaktdaten. Änderungen sind unverzüglich mitzuteilen.
- (4) Datenverarbeitung außerhalb der Betriebsstätten oder in Privatwohnungen (z. B. Homeoffice) nur mit ausdrücklicher Zustimmung des Auftraggebers.
- (5) Personen, die Daten verarbeiten, müssen zur Vertraulichkeit verpflichtet sein oder einer gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO).
- (6) Der Auftragsverarbeiter kontrolliert und dokumentiert regelmäßig die Einhaltung seiner Pflichten.

§ 6 Technische und organisatorische Maßnahmen

- (1) Der Auftragsverarbeiter setzt geeignete technische und organisatorische Maßnahmen (Anlage 2) um, abgestimmt auf Art. 32 DSGVO.
- (2) Anpassungen und Änderungen werden dokumentiert und dem Auftraggeber auf Nachfrage mitgeteilt. Wesentliche Änderungen werden vorab abgestimmt.

§ 7 Unterstützungspflichten des Auftragsverarbeiters

- (1) Unterstützung des Auftraggebers bei Wahrung der Betroffenenrechte (Art. 28 Abs. 3 lit. e DSGVO).
- (2) Unterstützung bei Pflichten nach Art. 32–36 DSGVO (z. B. Meldepflichten), unter Berücksichtigung der verfügbaren Informationen.

§ 8 Einsatz von Unterauftragsverarbeitung (Subunternehmer)

- (1) Einsatz von Subunternehmern nur mit Zustimmung des Auftraggebers. Bereits bestätigte Subunternehmer in Anlage 3.
- (2) Subunternehmer müssen gesetzliche und vertragliche Vorgaben einhalten; Nebentätigkeiten stellen keine Unterauftragsverhältnisse dar.
- (3) Verträge mit Subunternehmern müssen Art. 32 DSGVO erfüllen und Kontroll- sowie Weisungsrechte des Auftraggebers gewährleisten.
- (4) Subunternehmerpflichten sind vertraglich festzulegen.
- (5) Datenweiterleitung an Subunternehmer nur, wenn Pflichten erfüllt sind.
- (6) Auftragsverarbeiter haftet für Einhaltung der Datenschutzbestimmungen durch Subunternehmer.
- (7) Subunternehmer benennen, soweit gesetzlich vorgeschrieben, einen Datenschutzbeauftragten.
- (8) Beauftragung von Subunternehmern in Drittstaaten nur mit Einhaltung der Art. 44 ff. DSGVO und Zustimmung des Auftraggebers.

§ 9 Mitteilungspflichten des Auftragsverarbeiters

- (1) Verstöße gegen Vertrag, Weisungen oder Datenschutzgesetze unverzüglich melden.
- (2) Unterstützung des Auftraggebers bei Meldungen nach Art. 33 und 34 DSGVO; eigenständige Meldungen nur nach Weisung.
- (3) Anfragen von Betroffenen, Behörden oder Dritten unverzüglich weiterleiten.
- (4) Information des Auftraggebers über bevorstehende Aufsichtshandlungen oder Gefährdung der Daten.

§ 10 Vertragsbeendigung, Löschung und Rückgabe der Daten

Nach Abschluss oder Beendigung der Verarbeitung: Löschung oder Rückgabe der personenbezogenen Daten gemäß Weisung des Auftraggebers. Der Auftraggeber kann dies überprüfen.

§ 11 Datengeheimnis und Vertraulichkeit

- (1) Auftragsverarbeiter verpflichtet sich zur unbefristeten Vertraulichkeit der Daten über Vertragsende hinaus.
- (2) Mitarbeiter werden vor Tätigkeitsaufnahme zur Verschwiegenheit verpflichtet.
- (3) Einhaltung der Maßnahmen wird dokumentiert und auf Anfrage vorgelegt.

§ 12 Schlussbestimmungen

- (1) Änderungen und Nebenabreden bedürfen der schriftlichen oder elektronischen Form.
- (2) Gesetzesänderungen gelten auch für die Verweise in diesem Vertrag.
- (3) Unwirksamkeit einzelner Bestimmungen berührt die übrigen nicht.
- (4) Sämtliche Anlagen sind Vertragsbestandteil.

Manfred von Hebel
(acting director/ Geschäftsleitung)

Auftragnehmer/-in

Anlagen

Anlage 1 – Auftragsdetails

- (1) Der vorliegende Vertrag umfasst (ggf. im Zusammenhang mit dem Hauptvertrag) folgende Leistungen:

[Hier müssen sämtliche Leistungen im Rahmen der Verarbeitung personenbezogener Daten benannt werden.]

- (2) Im Rahmen der vertraglichen Leistungserbringung werden regelmäßig folgende Datenarten verarbeitet:

[Hier muss eine detaillierte Aufstellung der verarbeiteten Datenarten erfolgen (z.B.: Daten von Teilnehmenden, Name, Vorname, Anschrift Geburtsdatum, Beruf, etc.)]

- (3) Bei dem Kreis der von der Datenverarbeitung betroffenen Personen handelt es sich um:

[Auflistung der betroffenen Personengruppen; vorliegend z.B. Mitarbeiter, Kunden, etc.]

Anlage 2 – Liste der bestehenden technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach Art. 32 DSGVO (TOM-Liste)

Der Auftragsverarbeiter setzt folgende technische und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DSGVO festgelegt und mit dem Auftraggeber abgestimmt.

I. Zweckbindung und Trennbarkeit

Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

Beispiele:

- *physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern*
- *Logische Mandantentrennung (softwareseitig)*
- *Berechtigungskonzept*
- *Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden*
- *Versehen der Datensätze mit Zweckattributen / Datenfeldern / Signaturen*
- *Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten und abgesicherten IT-System*
- *Trennung von Produktiv- und Testsystem*
- *Sonstige:*

(Bitte Maßnahmen konkret beschreiben)

II. Vertraulichkeit und Integrität

Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme des Auftragsverarbeiters:

(1) Verschlüsselung

Die im Auftrag verarbeiteten Daten bzw. Datenträger werden in folgender Weise verschlüsselt:

(Bitte Verschlüsselungsmaßnahmen konkret beschreiben)

(2) Pseudonymisierung

„Pseudonymisierung“ bedeutet, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine Identifizierung der betroffenen Person ohne Hinzuziehung weiterer Informationen ausschließt (z.B. Verwendung von Fantasienamen, die ohne zusätzliche Informationen keiner bestimmten Person zugeordnet werden können).

() Nein.

() Ja, und zwar in folgender Art und Weise: *(Bitte Maßnahmen zur Pseudonymisierung konkret beschreiben)*

(3) Es wurden folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern (Zutrittskontrolle):

Beispiele:

- *Alarmanlage*
- *Absicherung von Gebäudeschächten*
- *Automatisches Zugangskontrollsystem*
- *Chipkarten-/Transponder-Schließsystem*
- *Schließsystem mit Codesperre*
- *Manuelles Schließsystem*
- *Biometrische Zugangssperren*
- *Videoüberwachung der Zugänge*
- *Lichtschraken / Bewegungsmelder*
- *Sicherheitsschlosser*
- *Schlüsselregelung (Schlüsselausgabe etc.)*

- *Personenkontrolle beim Pförtner / Empfang*
 - *Protokollierung der Besucher*
 - *Sorgfältige Auswahl von Reinigungspersonal*
 - *Sorgfältige Auswahl von Wachpersonal*
 - *Tragepflicht von Berechtigungsausweisen*
 - *Zutrittskonzept / Besucherregelung*
 - *Sonstige:*
- (Bitte Maßnahmen konkret beschreiben)*

(4) Es wurden folgende Maßnahmen getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern (Zugangskontrolle):

Beispiele:

- *Zuordnung von Benutzerrechten*
 - *Erstellen von Benutzerprofilen*
 - *Passwortvergabe*
 - *Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)*
 - *Authentifikation mit biometrischen Verfahren*
 - *Authentifikation mit Benutzername / Passwort*
 - *Zuordnung von Benutzerprofilen zu IT-Systemen*
 - *Gehäuseverriegelungen*
 - *Einsatz von VPN-Technologie bei der Übertragung von Daten*
 - *Verschlüsselung mobiler IT-Systeme*
 - *Verschlüsselung mobiler Datenträger*
 - *Verschlüsselung der Datensicherungssysteme*
 - *Sperren externer Schnittstellen (USB etc.)*
 - *Sicherheitsschlosser*
 - *Schlüsselregelung (Schlüsselausgabe etc.)*
 - *Personenkontrolle beim Pförtner / Empfang*
 - *Protokollierung der Besucher*
 - *Sorgfältige Auswahl von Reinigungspersonal*
 - *Sorgfältige Auswahl von Wachpersonal*
 - *Tragepflicht von Berechtigungsausweisen*
 - *Einsatz von Intrusion-Detection-Systemen*
 - *Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)*
 - *Einsatz von Anti-Viren-Software*
 - *Verschlüsselung von Datenträgern in Laptops / Notebooks*
 - *Einsatz einer Hardware-Firewall*
 - *Einsatz einer Software-Firewall*
 - *Sonstige:*
- (Bitte Maßnahmen konkret beschreiben)*

- (5) Es wurden folgende Maßnahmen getroffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle):

Beispiele:

- *Berechtigungskonzept*
- *Verwaltung der Rechte durch Systemadministrator*
- *regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern)*
- *Anzahl der Administratoren ist das „Notwendigste“ reduziert*
- *Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel*
- *Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten*
- *Sichere Aufbewahrung von Datenträgern*
- *physische Löschung von Datenträgern vor Wiederverwendung*
- *ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)*
- *Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)*
- *Protokollierung der Vernichtung*
- *Verschlüsselung von Datenträgern*
- *Sonstige:*

(Bitte Maßnahmen konkret beschreiben)

- (6) Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle).

Beispiele:

- *Protokollierung der Eingabe, Änderung und Löschung von Daten*
- *Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.*
- *Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)*
- *Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind*
- *Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts*
- *Sonstige:*

(Bitte Maßnahmen konkret beschreiben)

- (7) Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die von Unterauftragnehmern / Subunternehmern des Auftragnehmers verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers und des Auftragnehmers verarbeitet werden können (Auftragskontrolle).

Beispiele:

- *Auswahl des Subunternehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)*

- vorherige Prüfung der und Dokumentation der beim Subunternehmer getroffenen Sicherheitsmaßnahmen
 - schriftliche Weisungen an den Subunternehmer (z.B. durch Auftragsverarbeitungsvertrag)
 - Verpflichtung der Mitarbeiter des Subunternehmers auf das Datengeheimnis
 - Subunternehmer hat Datenschutzbeauftragten bestellt
 - Sicherstellung der Vernichtung von Daten von den Systemen des Subunternehmers nach Beendigung des Auftrags
 - Wirksame Kontrollrechte gegenüber dem Subunternehmer vereinbart
 - laufende Überprüfung des Subunternehmers und seiner Tätigkeiten
 - Vertragsstrafen bei Verstößen
 - Sonstige:
- (Bitte Maßnahmen konkret beschreiben)

(8) Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können (Transport- bzw. Weitergabekontrolle):

Beispiele:

- Einsatz von VPN-Tunneln
- Verschlüsselung der Kommunikationswege (z.B. Verschlüsselung des E-Mail-Verkehrs)
- Verschlüsselung physischer Datenträger bei Transport
- Sonstige:

(Bitte Maßnahmen konkret beschreiben)

III. Verfügbarkeit, Wiederherstellbarkeit und Belastbarkeit der Systeme

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

Beispiele:

- Unterbrechungsfreie Stromversorgung (USV)
- Klimatisierung der Serverräume
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Backup- & Recovery-Konzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen
- In Hochwassergebieten: Serverräume über der Wassergrenze
- belastbares Datensicherungs- und Wiederherstellungskonzept vorhanden
- Sonstige:

(Bitte Maßnahmen konkret beschreiben)

IV. Besondere Datenschutzmaßnahmen

Es liegen schriftlich vor:

Beispiele:

- interne Verhaltensregeln
- Risikoanalyse
- Datenschutz-Folgenabschätzung
- Datensicherheitskonzept
- Wiederanlaufkonzept
- Zertifikat
- Sonstige

(Bitte konkrete Maßnahmen auflisten)

V. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen

Der Auftragsverarbeiter wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand vonMonaten / Jahren und anlassbezogen, prüfen, evaluieren und bei Bedarf anpassen.

Anlage 3 – Liste der bestehenden Subunternehmer zum Zeitpunkt des Vertragsschlusses

[Diese Tabelle kann bei einer längeren Liste von aufzuführenden Subunternehmen beliebig oft kopiert und ausgefüllt werden.] Änderungen bedürfen der Zustimmung der Auftraggeber*in.

Name des*der Unterauftragnehmenden	Adresse des*der Unterauftragnehmenden	Beschreibung der Leistungen	Geplanter Leistungszeitraum und Ort
[Name 1]	[Adresse 1]	[Leistungsbeschreibung 1]	[Zeitraum 1] [Ort 1]
[Name 2]	[Adresse 2]	[Leistungsbeschreibung 2]	[Zeitraum 2] [Ort 1]
[Name 3]	[Adresse 3]	[Leistungsbeschreibung 3]	[Zeitraum 3] [Ort 1]

Ort, Datum

Unterschrift Unterauftragnehmer*in

(Name des*der Unterzeichnenden zu 1/2/3)

Unterschrift Hauptauftragnehmer*in

(Name des*der Unterzeichnenden, falls erforderlich)