Anlagen zum Auftragsverarbeitungsvertrag

Anlage 1 – Gegenstand des Auftrags
Anlage 2 – Weitere Auftragsverarbeiter
Anlage 3 - Technische und organisatorische Maßnahmen (TOM) des Auftragnehmers

Aktenzeichen:

Anlage 1 - Gegenstand des Auftrags

1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen, bei denen personenbezogene Daten verarbeitet werden:

Zur Digitalisierung der Personalverwaltung werden die bestehenden papierbasierten Personalakten der Beschäftigten durch einen externen Dienstleister erfasst (gescannt) und in ein elektronisches Dokumentenmanagementsystem überführt.

Näheres ergibt sich aus dem Hauptvertrag/Werkvertrag/Honorarvertrag/Auftrag vom:

Vom Bedarfsträger des DJI auszufüllen.

2. Art(en) der personenbezogenen Daten

Kategorien der personenbezogenen Daten, die zur Erbringung der Leistung verarbeitet werden.

Im Auftrag des Auftraggebers werden folgende personenbezogenen Daten verarbeitet:

☐	**Aufnahmen**	*(z. B. Fotos, Ton, Video)*
☐	**Benutzerkonten**	*(z. B. Benutzername, Profilbild)*
☒	**Bewerbungsdaten**	*(z. B. Zeugnis, Lebenslauf)*
☐	**Forschungsdaten/ wiss. Rohdaten**	*(z. B. Fragebögen, Transkripte)*
☒	**Inhaltsdaten**	*(z. B. Schriftwechsel, E-Mails)*
☐	**Nutzungsdaten**	*(z. B. Verweildauer, Zugriffszeit)*
☐	**Protokolle/ Logdaten**	*(z. B. Zeitstempel, Browserversion)*
☐	**Projektdaten**	*(z. B. Projektbericht, Publikationen)*
☒	**Sensible Daten**	*(z. B. Gesundheit, Straffälligkeit)*
☒	**Stammdaten/ Kontaktdaten**	*(z. B. Name, E-Mail-Adresse)*
☐	**Verkehrs-/ Metadaten**	*(z. B. IP-Adresse, Datenmenge)*
☒	**Vertrags-/ Abrechnungsdaten**	*(z. B. Verträge, Rechnungen)*
☒	**Verwaltungs-/ Personalverwaltungsdaten**	*(z. B. Personalnummer, Gehalt)*
☐	**Zugangsdaten**	*(z. B. Benutzerkennung, Passwort)*
☐	**Sonstiges (bitte erläutern)**	

Erläuterungen:

Daten, die im Rahmen der Personalakte verwaltet werden.

Anlagen zum Auftragsverarbeitungsvertrag
Anlage 1 – Gegenstand des Auftrags
Anlage 2 – Weitere Auftragsverarbeiter
Anlage 3 - Technische und organisatorische Maßnahmen (TOM) des Auftragnehmers

3. Kategorien betroffener Person

Kreis der Personen, auf die sich die Daten beziehen.

- ☐ **Bewerber:innen**
- ☐ **Interessent:innen**
- ☐ **Kooperationspartner:innen**
- ☒ **Mitarbeiter:innen**
- ☐ **Nutzer:innen**
- ☐ **Studienteilnehmer:innen**
- ☐ **Veranstaltungsteilnehmer:innen**
- ☐ **Vertragspartner:innen**
- ☐ **Vulnerable Personengruppen** *(z. B. Minderjährige, Missbrauchsopfer, Flüchtlinge)*
- ☐ **Sonstige (bitte erläutern)**

Erläuterungen:

Personaldaten von Mitarbeitenden und Hilfskräften des DJI

4. Weisungsberechtigte Personen des Auftraggebers

Hier ggf. Personen benennen, Passage streichen oder z.B. „trifft nicht zu" eintragen.

Mitarbeitende des Sachgebiets Personal

5. Weisungsempfangsberechtigte Personen des Auftragnehmers

Hier ggf. Personen benennen, Passage streichen oder z.B. „trifft nicht zu" eintragen.

Vom Bedarfsträger des DJI oder Auftragnehmer auszufüllen, falls weisungsempfangs-berechtigte Personen benannt.

ENTWURF

Anlage 2 – Weitere Auftragsverarbeiter

Nimmt der *Auftragnehmer* zur Erbringung der Leistung und zum Zeitpunkt der Vertragsunterzeichnung weitere Auftragsverarbeiter in Anspruch, die in seinem Auftrag personenbezogene Daten verarbeiten (sog. „Unterauftragsverarbeiter")?

- ☐ **Nein**
- ☐ **Ja**, weitere Auftragsverarbeiter werden in separatem Dokument beigefügt
- ☐ **Ja**, weitere Auftragsverarbeiter werden nachfolgend genannt:

Name, Anschrift	Aufgabe / Leistung	Leistungsort(e)

ENTWURF

Anlage 3 - Technische und organisatorische Maßnahmen (TOM) des Auftragnehmers

Der Auftragnehmer trifft technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

☐	**Ja**, die technisch-organisatorischen Maßnahmen werden in einem separaten Dokument beigefügt
☐	**Ja**, die technisch-organisatorischen Maßnahmen werden nachfolgend angekreuzt und/oder erläutert:

1. Vertraulichkeit

Zutrittskontrolle

Die „Zutrittskontrolle" umfasst jene Maßnahmen, die den unbefugten physischen Zutritt zu Anlagen verhindern sollen, mit denen personenbezogene Daten verarbeitet werden.

☐	**Alarmanlage**
☐	**Protokollierung des Zutritts von Besucherinnen und Besuchern**
☐	**Regeln zum Umgang mit Besucherinnen und Besuchern**
☐	**Regeln zum Umgang mit Fremdpersonal**
☐	**Rezeption, Empfang oder Pforte mit Personenkontrolle**
☐	**Schließsystem (automatisch), z.B. Chip-/Transpondersystem**
☐	**Schließsystem (manuell), z.B. Schließanlage**
☐	**Schlüsselregelung mit dokumentierter Schlüsselvergabe**
☐	**Verschließen von Büroräumen**
☐	**Verschließen von Gebäudeeingängen**
☐	**Verschließen von Serverräumen und Datenverarbeitungsanlagen**
☐	**Videoüberwachung**

Erläuterungen / weitere Maßnahmen:

Ggf. vom Auftragnehmer auszufüllen.

Anlagen zum Auftragsverarbeitungsvertrag

Anlage 1 – Gegenstand des Auftrags
Anlage 2 – Weitere Auftragsverarbeiter
Anlage 3 - Technische und organisatorische Maßnahmen (TOM) des Auftragnehmers

Zugangskontrolle

Die „Zugangskontrolle" umfasst jene Maßnahmen, die eine unbefugte Nutzung von Systemen zur Datenverarbeitung verhindern sollen.

- ☐ **Anti-Virus-Software auf aktuellem Stand**
- ☐ **Authentifizierung mit individuellem Login oder Passwort**
- ☐ **Authentifizierung mit 2-Faktor-Authentisierung**
- ☐ **Automatische Desktop-Sperre**
- ☐ **Firewall auf aktuellem Stand**
- ☐ **Intrusion-Detection-System, Intrusion-Prevention-System**
- ☐ **Passwortrichtlinie, Vorgaben zu Komplexität und Länge von Passwörtern**
- ☐ **Protokollierung des Zugangs zu Datenverarbeitungssystemen**
- ☐ **Sperre externer Geräteschnittstellen, z.B. USB-Anschlüsse**
- ☐ **Wartung/Support durch externe Dienstleister ausschließlich unter Aufsicht**
- ☐ **Zentrale und dokumentierte Geräteausgabe und -rückgabe**
- ☐ **Zentrale Administration von Hardware und/oder Software**

Erläuterungen / weitere Maßnahmen:

Ggf. vom Auftragnehmer auszufüllen.

Zugriffskontrolle

Die „Zugriffskontrolle" umfasst jene Maßnahmen, die sicherstellen, dass nur diejenigen Personen auf personenbezogene Daten zugreifen können, die dazu berechtigt sind. Ferner sind damit Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- ☐ **Aktenschredder (mind. Sicherheitsstufe 3)**
- ☐ **Akten- und Datenvernichtung durch spezialisierten Dienstleister**
- ☐ **Berechtigungskonzept, Vergabe von differenzierten Berechtigungen**
- ☐ **Datenverarbeitung ausschließlich innerhalb der EU/EWG**
- ☐ **Datenschutztresor, gesicherte Aufbewahrung von Datenträgern**
- ☐ **Einsatz von Kopierschutzmaßnahmen, Data-Loss-Prevention**
- ☐ **Regelmäßige Kontrolle von Berechtigungen, z.B. bei Mitarbeiterwechsel**
- ☐ **Vergabe von Berechtigungen nach dem Minimalprinzip**
- ☐ **Verschlüsselung von Cloud-Daten**
- ☐ **Verschlüsselung von Datenträgern**
- ☐ **Verschlüsselung von mobilen Geräten**
- ☐ **Verzicht auf Cloud-Dienste**
- ☐ **Zentrale Administration von Berechtigungen**

Erläuterungen / weitere Maßnahmen:

Ggf. vom Auftragnehmer auszufüllen.

Anlagen zum Auftragsverarbeitungsvertrag
Anlage 1 – Gegenstand des Auftrags
Anlage 2 – Weitere Auftragsverarbeiter
Anlage 3 - Technische und organisatorische Maßnahmen (TOM) des Auftragnehmers

Trennungskontrolle

Mit „Trennungskontrolle" sind jene Maßnahmen gemeint, die gewährleisten, dass zu unterschiedlichen Zwecken verarbeitete Daten getrennt voneinander verarbeitet werden können.

- ☐ **Mandantenfähigkeit der verwendeten Systeme**
- ☐ **Datentrennung durch mandantenspezifische Verschlüsselung**
- ☐ **Logische Datentrennung, z.B. in Applikationen, virtuellen Systemen**
- ☐ **Physische Datentrennung, z.B. Separierung von Datenträgern**
- ☐ **Trennung von Entwicklungs-, Test- und Produktivumgebungen**
- ☐ **Zweckgebundene Datentrennung und/oder Zweckattribute für Daten**

Erläuterungen / weitere Maßnahmen:

Ggf. vom Auftragnehmer auszufüllen.

Pseudonymisierung, Anonymisierung & Verschlüsselung

Unter „Pseudonymisierung, Anonymisierung und Verschlüsselung" werden datenverändernde Maßnahmen zusammengefasst, die im Ergebnis zu einer Aufhebung oder Verschleierung des Personenbezugs führen. Der Bezug der Daten auf bestimmte oder bestimmbare Einzelpersonen ist danach nicht mehr bzw. nur noch durch Hinzuziehen zusätzlicher Informationen möglich.

- ☐ **Anonymisierungskonzept**
- ☐ **Pseudonymisierungskonzept**
- ☐ **Verschlüsselte Speicherung von Pseudonymen oder Zuordnungsdaten**
- ☐ **Verschlüsselungskonzept**

Erläuterungen / weitere Maßnahmen:

Ggf. vom Auftragnehmer auszufüllen.

2. Integrität

Eingabekontrolle

Die „Eingabekontrolle" umfasst Maßnahmen, die dazu dienen, nachträglich zu überprüfen, ob und von wem Daten in ein Verarbeitungssystem eingegeben, verändert oder entfernt wurden.

- ☐ **Vergabe von differenzierten Berechtigungen, z.B. Lesen, Schreiben, Ändern**
- ☐ **Dokumenten-Management-System (DMS) mit Änderungshistorie**
- ☐ **Nachvollziehbarkeit anhand individueller Benutzerkennungen**
- ☐ **Organisatorische Festlegung von Zuständigkeiten, z.B. Eingabe, Löschen**
- ☐ **Protokollierung bei Eingabe, Ändern, Löschen von Daten**

Erläuterungen / weitere Maßnahmen:

Ggf. vom Auftragnehmer auszufüllen.

Weitergabekontrolle

Die „Weitergabekontrolle" umfasst Maßnahmen, die eine sicherstellen, dass Datenträger bei der elektronischen Übertragung oder bei Transport und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Ferner werden darunter Maßnahmen zusammengefasst, mit denen überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten vorgesehen ist.

- ☐ **Anonymisierung, Pseudonymisierung der Daten vor Weitergabe**
- ☐ **Dokumentation der Empfänger und Überlassungsfristen**
- ☐ **E-Mail-Verschlüsselung**
- ☐ **E-Mail-Signaturverfahren**
- ☐ **Persönliche Übergabe mit Protokoll**
- ☐ **Sichere Transportbehälter**
- ☐ **Verschlüsselte Datenübermittlung, z.B. Transportverschlüsselung, E2E-Verschlüsselung**
- ☐ **Verschlüsselte Kommunikationswege, z.B. Videokonferenz, Messenger**
- ☐ **Verschlüsselte Datenfernverbindung, VPN-Verbindung**

Erläuterungen / weitere Maßnahmen:

Ggf. vom Auftragnehmer auszufüllen.

3. Verfügbarkeit und Belastbarkeit

Die „Verfügbarkeitskontrolle" bezieht sich auf Maßnahmen zum Schutz der Daten gegen unbeabsichtigte Zerstörung oder Verlust.

- ☐ **Backup- und Recoverykonzept**
- ☐ **Feuerlöscher für Serverräume**
- ☐ **Feuer- oder Rauchmelder**
- ☐ **Klimatisierte Serverräume**
- ☐ **Notfallplan zum Ausfall von IT-Systemen**
- ☐ **Überspannungsschutz für kritische IT-Systeme**
- ☐ **Redundante Datenhaltung, z.B. RAID**
- ☐ **Regelmäßige Tests zur Wiederherstellung von Backups**
- ☐ **Sichere Aufbewahrung von Backups, z.B. Off-Site-Lagerung**
- ☐ **Unterbrechungsfreie Stromversorgung (USV)**
- ☐ **Überwachung von IT-Systemen und Speicherkapazität**
- ☐ **Verfahren zur raschen Wiederherstellung von Backups**

Erläuterungen / weitere Maßnahmen:

Ggf. vom Auftragnehmer auszufüllen.

Anlagen zum Auftragsverarbeitungsvertrag

Anlage 1 – Gegenstand des Auftrags
Anlage 2 – Weitere Auftragsverarbeiter
Anlage 3 - Technische und organisatorische Maßnahmen (TOM) des Auftragnehmers

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Darunter werden die Maßnahmen zusammengefasst, die vom Auftragnehmer zur Überprüfung, Bewertung und Evaluation von Datenschutz- und Datensicherheitsmaßnahmen ergriffen werden.

☐	**Auswahl von Auftragnehmern nach Gesichtspunkten des Datenschutzes**
☐	**Datenschutzbeauftragter vorhanden**
☐	**Datenschutzleitbild, Datenschutzrichtlinie vorhanden**
☐	**IT-Sicherheitsbeauftragter vorhanden**
☐	**IT-Sicherheitskonzept vorhanden**
☐	**Prozess zur Bearbeitung von Betroffenenanfragen**
☐	**Prozess zur Bearbeitung von Sicherheitsvorfällen, Datenpannen**
☐	**Regelungen zum Datenschutz durch Technikgestaltung, Voreinstellungen**
☐	**Regelmäßige Kontrolle von Datenschutz- und Sicherheitsmaßnahmen**
☐	**Regelung zum Einsatz von Auftragnehmern**
☐	**Regelmäßige Schulung der Mitarbeitenden zu Datenschutz, IT-Sicherheit**
☐	**Verpflichtung der Mitarbeitenden auf Vertraulichkeit**
☐	**Weisungen an Auftragnehmer werden schriftlich erteilt**
☐	**Zertifizierung der IT-Sicherheit, z.B. ISO 27001, BSI-Grundschutz**

Erläuterungen / weitere Maßnahmen:

Ggf. vom Auftragnehmer auszufüllen.

ENTWURF