|  |  |  |  |
| --- | --- | --- | --- |
| **Auftraggeber** | **Auftragnehmer** | **Daten zum Auftragsverarbeitungsvertrags** | **Datum** |
|  |  | *Auftragsverarbeitungsvertrag (AVV) vom [\*\*\*]*  *ggf. Vertragsnummer* | *Datum der Beurteilung* |

**Anlage X**

**zum Auftragsverarbeitungsvertrag (AVV)**

**Technische und Organisatorische Maßnahmen gem. Art. 32 DSGVO**

[A. Vorwort 2](#_Toc43201065)

[A. Angaben zum Datenschutzbeauftragten des Auftragsverarbeiters 2](#_Toc43201066)

[B. Garantien für die datenschutzkonforme Verarbeitung personenbezogener Daten 3](#_Toc43201067)

[I. Nachweis der Garantien 3](#_Toc43201068)

[II. Technische und organisatorische Maßnahmen (TOM) 4](#_Toc43201069)

[1. Gewährleistung eines Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO) 4](#_Toc43201070)

[2. Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO) 7](#_Toc43201071)

[3. Gewährleistung der Integrität (Art. 32 Abs. 1 lit. b) DSGVO) 13](#_Toc43201072)

[4. Gewährleistung der Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO) 16](#_Toc43201073)

[5. Auftragskontrolle 18](#_Toc43201074)

[III. Auftragsspezifische Bemerkungen 20](#_Toc43201075)

# Vorwort

Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber, bei der Erfüllung der im Rahmen der Auftragsverarbeitung übernommenen Aufgaben die im vorliegenden Dokument beschriebenen technischen und organisatorischen Maßnahmen (im Folgenden „TOM“ genannt) einzuhalten, im Einklang mit Art. 32 DSGVO.

Das Dokument bildet Anlage X zur Auftragsverarbeitungsvertrag gemäß § XX Abs. X AVV.

Bei den TOM handelt es sich um Maßnahmen zur Sicherstellung der Vertraulichkeit (Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Trennungsgebots), der Integrität (Weitergabekontrolle und Eingabekontrolle), der Verfügbarkeit (Verfügbarkeitskontrolle, Gewährleistung zur raschen Wiederherstellung und Sicherstellung Belastbarkeit), der Auftragskontrolle sowie Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM.

# Angaben zum Datenschutzbeauftragten des Auftragsverarbeiters

|  |  |
| --- | --- |
| **Name** |  |
| Firma |  |
| Anschrift |  |
| Kontaktdaten |  |
| Ausbildung |  |
| Weiterbildung im Bereich Datenschutz |  |

# Garantien für die datenschutzkonforme Verarbeitung personenbezogener Daten

## Nachweis der Garantien

|  |  |
| --- | --- |
| **Fragestellungen** | **Dokumentation der Ergebnisse** |
| **Der Auftragsverarbeiter erbringt den Nachweis dafür, dass er eine datenschutzkonforme Verarbeitung personenbezogener Daten gewährleistet, durch** | ❑ die Einhaltung genehmigter Verhaltensregeln nach Art. 40 DSGVO,  nämlich |
|  | ❑ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. Art. 42 DSGVO, nämlich |
|  | ❑ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren),  nämlich |
|  | ❑ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz oder ISO 27001),  nämlich |
|  | ❑ Kontrolle durch den Auftraggeber |

## Technische und organisatorische Maßnahmen (TOM)

## Gewährleistung eines Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d) DSGVO; Art. 25 Abs. 1 DSGVO)

1. **Datenschutz-Management**

| **Nr.** | **Prüfungspunkt** | **Antwort** | **Dokumentation der Ergebnisse** | **Beurteilung der TOM**  (wird vom Auftraggeber ausgefüllt) |
| --- | --- | --- | --- | --- |
| **0.** | **Organisationskontrolle** | | | |
| 0.1 | Wie ist die Umsetzung des Datenschutzes organisiert?  (interner/externer Datenschutzbeauftragter, freiwillige Bestellung ohne gesetzlichen Zwang, hauptamtliche/nebenamtliche Bestellung, Einbindung des Datenschutzbeauftragten in die Unternehmensstruktur, Unterstützung des Datenschutzbeauftragten durch ihm zugeordnete Mitarbeiter „Abteilung Datenschutz“/Datenschutzkoordinatoren in den jeweiligen Unternehmensbereichen etc.) |  |  |  |
| 0.2 | Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt?  (Verpflichtung der Mitarbeiter auf das Daten- und Fernmeldegeheimnis, Datenschutzordnung, interne Arbeitsanweisungen, unternehmensinterne Richtlinie, Implementierung von unternehmensinternen Gremien unter Mitarbeit des Datenschutzbeauftragten, Implementierung von Prozessen, die die Mitarbeit des Datenschutzbeauftragten sicherstellt etc.) |  |  |  |
| 0.3 | Wie wird sichergestellt, dass die internen Prozesse bzw. Arbeitsabläufe gemäß der jeweils aktuell, gültigen Datenschutzbestimmungen und nur auf Anweisung des Auftraggebers ablaufen und wird dies regelmäßig einer Qualitätsprüfung unterzogen?  (Auditierung der internen Prozesse, Schulung der Mitarbeiter, vertragliche Regelungen, regelmäßige Optimierung von Prozessen, Zertifizierung des Datenschutzmanagementsystems etc.) |  |  |  |
| 0.4 | In welcher Form werden die Mitarbeiter in Bezug auf die Umsetzung der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO geschult?  (Einweisungen, Präsenzschulungen, Arbeitsanweisungen, Handbücher in speziellen Aufgabengebieten etc.) |  |  |  |
| 0.5 | Wie sind die einschlägigen Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit (z.B. Vorabkontrolle) dokumentiert?  (Verfahrensverzeichnis, Verarbeitungsübersicht, Dokumentation Vorabkontrolle/Folgeabschätzung, Stellungnahmen Datenschutzbeauftragter etc.) |  |  |  |
| 0.6 | Werden – und wenn ja, wie werden – die Privacy-/Data Protection-by-Design- und -by-Default-Prinzipien unternehmensintern umgesetzt?   * Ist per Voreinstellung der Empfängerkreis sowie das Maß der Datenerhebung auf das erforderliche Mindestmaß beschränkt? * Sonstiges |  |  |  |
| 0.7 | Welche Überwachungsmaßnahmen hat der Auftragnehmer installiert?   * Existiert ein Verzeichnis der Verarbeitungstätigkeiten? * Existieren Richtlinien und Dokumentationen zum Datenschutz? * Welche Risikobewertungsmethoden und -werkzeuge verwendet der Auftragnehmer? * Werden die Mitarbeiter zum Datenschutz geschult? * Existiert ein Prozess zur Bewertung und Verbesserung? |  |  |  |
| 0.8 | Werden Subunternehmer des Auftragnehmers eingesetzt?  (Sind die Regelungen mindestens so restriktiv, wie die des Auftraggebers?) |  |  |  |
| 0.9 | Bestehen Kontrollrechte des Auftraggebers beim Subunternehmer des Auftragnehmers?  (Sind diese Kontrollrechte in den Vertrag zwischen Auftragnehmer und dessen Subunternehmer aufgenommen?) |  |  |  |
| 0.10 | Sonstiges |  |  |  |

1. **Incident-Response-Management**

| **Nr.** | **Prüfungspunkt** | **Antwort** | **Dokumentation der Ergebnisse** | **Beurteilung der TOM**  (wird vom Auftraggeber ausgefüllt) |
| --- | --- | --- | --- | --- |
| **0.** | **Incident-Response-Management** | | | |
| 0.11 | Der Auftragnehmer hat einen Prozess zur Meldung von Datenschutzvorfällen in seinem Unternehmen installiert.   * Es existieren Vorgaben zum Vorgehen bei Datenschutzverstößen. * Existieren Formblätter zur Meldung von Verstößen? |  |  |  |
| 0.12 | Sonstiges |  |  |  |

## Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)

1. **Zutritts-, Zugangs-, Zugriffs und Trennungskontrolle**

| **Nr.** | **Prüfungspunkt** | **Antwort** | **Dokumentation der Ergebnisse** | **Beurteilung der TOM**  (wird vom Auftraggeber ausgefüllt) | |
| --- | --- | --- | --- | --- | --- |
| **1.** | **Maßnahmen zur Zutrittskontrolle**  Ziel ist es, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren. Hiermit ist der räumliche Zugang zu den Anlagen gemeint. | | | | |
| 1.1 | Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?  (Schließverfahren, elektronische Zutrittskontrolle, Videoüberwachung, Einbruchssicherung, Wachpersonal, Alarmanlage, Bewegungsmelder etc.) |  |  |  | |
| 1.2 | Wie werden die Räume/Büros, in denen die personenbezogenen Daten verarbeitet werden, vor unbefugtem Zutritt gesichert?  (Schließverfahren, elektronische Zutrittskontrolle, Alarmanlage, Rollläden mit Hochschiebesicherung etc.) |  |  |  | |
| 1.3 | Wie werden die Hardwarekomponenten selbst vor Missbrauch geschützt?  (Diebstahlschutz z.B. durch Kensington-Lock für Notebooks, PC-Schutzschrank, Wegschließen nach Arbeitsende etc.) |  |  |  | |
| 1.4 | Wie werden die umgesetzten Zutrittskontrollmaßnahmen auf Tauglichkeit geprüft?  (Dokumentierte Testverfahren etc.) |  |  |  | |
| 1.5 | Besteht eine Zutrittskontrolle des Gebäudes Tag/Nacht?   * z.B. Ausweise ohne/mit Foto, Codeschloss, neutrale Karten / Schlüssel * Dokumentation der Vergabe von Schlüsseln oder Karten?? |  |  |  | |
| 1.6 | Erfolgt eine Besucherkontrolle?  •z.B. durch Besucherbuch, Besucherausweis  •Begleitung durch Mitarbeiter? |  |  |  | |
| 1.7 | Besteht eine Zutrittskontrolle für den Serverraum?  (Erfolgt eine Protokollierung?) |  |  |  | |
| 1.7 | Sonstiges |  |  |  | |
| **2.** | **Maßnahmen zur Zugangskontrolle**  Maßnahmen, die sicherstellen, dass Unbefugte an der Benutzung der Datenverarbeitungsanlagen und -verfahren gehindert werden. Diese beziehen sich – im Gegensatz zur Zutrittskontrolle – auf das Eindringen unbefugter Personen in das EDV-System selbst. | | | | |
| 2.1 | Benutzerverwaltung |  |  |  | |
| 2.1.1 | Wie erfolgt die Vergabe von Benutzerzugängen (-accounts)?  (Standardisierter Prozess zur Antragstellung, Genehmigung, Einrichtung, Änderung, Löschung etc.) |  |  |  | |
| 2.1.2 | Wie wird die Gültigkeit von Benutzerzugängen (-accounts) überprüft?  (bei geänderter Aufgabenstellung, Versetzungen, Austritten; regelmäßige Prüfung etc.) |  |  |  | |
| 2.1.3 | Wie werden Benutzerzugänge (-accounts) (inkl. Antrags- und Genehmigungsverfahren, Änderungsverfahren) dokumentiert?  (Systemprotokollierung, Workflow-Management etc.) |  |  |  | |
| 2.1.4 | Wie stellen Sie sicher, dass   1. die Vergabe von Administrationszugängen auf die notwendige Anzahl beschränkt ist? 2. diese Administratoren die fachlich und persönlich geeignet sind? 3. externe Administratoren, Service oder Wartungstechniker persönlich geeignet sind? |  |  |  | |
| 2.1.5 | Bestehen schriftliche Regelungen für die Nutzung von Datenträgern und Notebooks?   * Wird die Einhaltung der Regelungen überprüft? * Werden Daten des Auftraggebers auf mobilen Datenträgern verarbeitet? |  |  |  | |
| 2.2 | Passwortsicherheit |  |  | |  |
| 2.2.1 | Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind und keinem Unbefugten?  (Verschlüsselte Speicherung, sichere Übermittlung, Verbot der Weitergabe von Passwörtern, Anweisung zur Geheimhaltung etc.) |  |  | |  |
| 2.2.2 | Welche Anforderungen werden an die Komplexität von Passwörtern gestellt?  (Mindestlänge, Aufbau, Historie, Vermeidung von Trivialpasswörtern etc.) |  |  | |  |
| 2.2.3 | Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann bzw. muss?  (Erzwungener Passwortwechsel bei Erstanmeldung bzw. in regelmäßigen Abständen, jederzeitige Möglichkeit des Benutzers, das Passwort zu ändern) |  |  | |  |
| 2.2.4 | Wie erfolgt die Administration von Passwörtern?  (Standardisierter Prozess zur Passwort-Vergabe, Rücksetzung von gesperrten Benutzerkonten, sichere Authentifizierung etc.) |  |  | |  |
| 2.2.5 | Welche Maßnahmen werden bei gescheiterten Anmeldeversuchen zur Abwehr unberechtigter Zugriffe ergriffen?  (Art und Weise der Sperrung des Benutzerkontos (z.B. nach n-Fehlversuchen, temporäre Sperrung), automatische Information an Systemadministrator etc.) |  |  | |  |
| 2.2.6 | Welche organisatorischen Vorkehrungen werden zur Verhinderung unberechtigter Zugriffe auf personenbezogene Daten am Arbeitsplatz getroffen?  (regelmäßige Unterweisungen zum Umgang mit PCs, Kopierern und Fax-Geräten, Handhabung von Dokumenten etc.) |  |  | |  |
| 2.3 | Erfolgt eine Verschlüsselung von Notebooks, USB Sticks und von sonstigen Datenträgern?  Erfolgt eine zentrale Schlüsselverwaltung für verschlüsselte Systeme? |  |  |  | |
| 2.4 | Erfolgt eine kontrollierte Vernichtung von Datenträgern und elektronischen Daten des Auftraggebers?   * Externer Dienstleister? * Existiert datenschutzkonformer Vertrag? * Sichere Löschprogramme? Welche? |  |  |  | |
| 2.5 | Wann erfolgt die Reinigung der Geschäftsräume durch den Reinigungsdienst?   * Ist der Dienstleister entsprechend verpflichtet? * Werden die Daten des Auftraggebers bei Arbeitsende weggesperrt? |  |  |  | |
| 2.6 | Sonstiges |  |  |  | |
| **3.** | **Maßnahmen zur Zugriffskontrolle**  Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und dass die bei der Bearbeitung verwendeten personenbezogenen Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. | | | | |
| 3.1 | Wie wird sichergestellt, dass Rollen / Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden?  (Standardisierter Vergabeprozess, 4-Augen-Prinzip, Genehmigung etc.) |  |  | |  |
| 3.2 | Wie erfolgt die Dokumentation der Zugriffsberechtigungen?  (Berechtigungskonzept, Rollenvergabe, Anträge etc.) |  |  | |  |
| 3.3 | Wie wird sichergestellt, dass Benutzer ihre Zugriffsberechtigung nicht missbräuchlich verwenden?  (Monitoring, Protokollierung etc.) |  |  | |  |
| 3.4 | Sonstiges  (Protokollierung Dateizugriff; Protokollierung Datenbankzugriff, etc.) |  |  | |  |
| **4.** | **Maßnahmen zur Trennungskontrolle**  Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. | | | | |
| 4.1 | Welche Maßnahmen werden getroffen, um das Trennungsgebot, insbesondere in Bezug auf die Zweckgebundenheit der personenbezogenen Daten, zu gewährleisten?  (Nutzung von unterschiedlichen, kundenspezifischen bzw. mandantenfähigen Systemen, detaillierte Zugriffskonzepte, Verschlüsselung der Datensätze etc.) |  |  |  | |
| 4.2 | Erfolgt eine Trennung der Daten des Auftraggebers von eigenen Daten / anderen Auftragsdaten   * physikalische Trennung? * Trennung im Rahmen des Berechtigungskonzepts? * Mandantenfähigkeit des Systems, Sandboxing |  |  |  | |
| 4.3 | Besteht eine Trennung von Entwicklungs-, Test- und Produktivsystem?  (Sind die Systeme in einem anderen Netzsegment?) |  |  |  | |
| 4.4 | Sonstiges |  |  |  | |

1. **Verschlüsselung und Pseudonymisierung**

| **Nr.** | **Prüfungspunkt** | **Antwort** | **Dokumentation der Ergebnisse** | **Beurteilung der TOM**  (wird vom Auftraggeber ausgefüllt) |
| --- | --- | --- | --- | --- |
| **5.** | **Verschlüsselung und Pseudonymisierung**  Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen. | | | |
| 5.1 | Setzt der Auftragnehmer Verschlüsselungsverfahren ein?   * Liegt eine ausreichende Verschlüsselungstiefe vor? * Name des Verfahrens. |  |  |  |
| 5.2 | Pseudonymisiert der Auftragnehmer die personenbezogenen Daten? |  |  |  |
| 5.2 | Sonstiges |  |  |  |

## Gewährleistung der Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

| **Nr.** | **Prüfungspunkt** | **Antwort** | **Dokumentation der Ergebnisse** | **Beurteilung der TOM**  (wird vom Auftraggeber ausgefüllt) | |
| --- | --- | --- | --- | --- | --- |
| **6.** | **Maßnahmen zur Weitergabekontrolle**  Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. | | | | |
| 6.1 | Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten?  (vertragliche Abreden, technische Maßnahmen (z.B. elektronische Signaturen, Verschlüsselungen) etc.) |  |  | |  |
| 6.2 | Welche Verschlüsselungssysteme werden bei der Weitergabe von personenbezogenen Daten eingesetzt?  (Ipsec-Verfahren, SSH-Verfahren, verschlüsselte Plattformen zum Datenaustausch, E-Mail-Verschlüsselung etc.) |  |  | |  |
| 6.3 | Wie wird die Weitergabe personenbezogener Daten dokumentiert?  (Konzept zur Weitergabe von Daten, Protokollierung von Datenabrufen, Empfängerliste etc.) |  |  | |  |
| 6.4 | Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?  (Berechtigungen für Download, Ausdruck, Speichern beschränken etc.) |  |  | |  |
| 6.5 | Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann?  (Systemseitige Protokollierung und regelmäßiger Auswerteprozess etc.) |  |  | |  |
| 6.6 | Wie werden physikalische Datenträger mit Daten des Auftraggebers aufbewahrt?   * Bestehen Regelungen? * Wo erfolgt die Aufbewahrung |  |  | |  |
| 6.7 | Welche Regelungen bestehen zur Vernichtung / Rückgabe von Datenträgern des Auftraggebers   * Schriftliche im Auftrag * Zusage durch Auftragnehmer? |  |  | |  |
| 6.8 | Wer darf auf Daten des Auftraggebers durch Fernzugriff zugreifen und wie erfolgt der Schutz?   * Administratoren? * Externe Dienstleister? * Schutz durch IP SEC VPN oder ähnliches |  |  | |  |
| 6.9 | Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?  (Berechtigungen für Download, Ausdruck, Speichern beschränken etc.) |  |  | |  |
| 6.10 | Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann?  (Systemseitige Protokollierung und regelmäßiger Auswerteprozess etc.) |  |  | |  |
| 6.11 | Sonstiges |  |  | |  |
| **7.** | **Maßnahmen zur Eingabekontrolle**  Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind. | | | | |
| 7.1 | Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie lange auf die Applikationen zugegriffen hat?  (Login-, Logout-Protokollierung etc.) |  |  | |  |
| 7.2 | Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?  (Protokollierung von Eingabe, Änderungs- bzw. Löschzugriffen, Starten von Reports etc.) |  |  | |  |
| 7.3 | Besteht eine Dokumentation der Verfahren, bei denen Daten des Auftraggebers verarbeitet werden?  (Wird die Einhaltung der Verfahren regelmäßig geprüft?) |  |  | |  |
| 7.4 | Besteht eine regelmäßige Protokollkontrolle und -auswertungen bei Änderungen an Daten des Auftraggebers?  (Erfolgt eine automatische Eskalation bei Sicherheitsmeldungen?) |  |  | |  |
| 7.5 | Sonstiges |  |  | |  |

## Gewährleistung der Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO)

| **Nr.** | **Prüfungspunkt** | **Antwort** | **Dokumentation der Ergebnisse** | | **Beurteilung der TOM**  (wird vom Auftraggeber ausgefüllt) |
| --- | --- | --- | --- | --- | --- |
| **8.** | **Maßnahmen zur Verfügbarkeitskontrolle**  Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. | | | | |
| 8.1 | Werden organisatorische und technische Maßnahmen getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten?  (Backup und Disaster-Recovery mit Notfallplänen, Spiegeln von Festplatten an getrennten Data-Center-Lokationen mit adäquaten Betriebsszenarien (unabhängige Stromversorgung) etc.) |  |  | |  |
| 8.2 | Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlungen etc.) geschützt sind?  (Rauch- & Brandmelder, Sprinkleranlage, Brandschutztüren, Wasserschutzeinrichtungen, Schirmdämpfung etc.) |  |  | |  |
| 8.3 | Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet?  (Virenscanner, Firewalls, Anti-Spy-Programme, Spam-Filter, IDS-/IPS-Systeme, Vorgehensweise zur Aktualisierung etc.) |  |  |  | |
| 8.4 | Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?  (Beauftragung von speziellen Entsorgungsunternehmen und deren Überprüfung etc.) |  |  |  | |
| 8.5 | Besteht ein Datensicherungskonzept und eine Dokumentation der Datensicherung?  (Sind die Daten des Auftraggebers durch die Datensicherung erfasst?) |  |  |  | |
| 8.6 | Wie viele Datensicherungsgenerationen werden in welchem zeitlichen Abstand erstellt?   * Sicherung per Band? * Sicherung per Snapshot? |  |  |  | |
| 8.7 | Werden regelmäßig Rücksicherungen getestet?  (Wird dies dokumentiert?) |  |  |  | |
| 8.8 | Wo werden die Datenträger der Datensicherung gelagert?   * Dokumentation Datenträger? * Sichere Aufbewahrung in anderem Brandabschnitt? * Sichere Entsorgung? |  |  |  | |
| 8.9 | Wo werden die Datenträger der Datensicherung gelagert?   * Dokumentation Datenträger? * Sichere Aufbewahrung in anderem Brandabschnitt? * Sichere Entsorgung? |  |  |  | |
| 8.10 | Würde ein Feuer in Serverraum bemerkt werden und besteht hierfür eine Gegenmaßnahme?  (Erfolgen dokumentierte Tests?) |  |  |  | |
| 8.11 | Werden die Systeme des Auftragnehmers regelmäßig mit Sicherheitsupdates versehen?  (Eingesetztes Tool?) |  |  |  | |
| 8.12 | Besteht ein Notfallplan?  (Erfolgen dokumentierte Notfalltests?) |  |  |  | |
| 8.13 | Werden die Systeme regelmäßige auf ihre Belastbarkeit geprüft? Mangelnde Belastbarkeit wirkt sich auf die Verfügbarkeit aus, da Server die unter Last stehen nicht performen können.  (Pentests, Performance Teste etc.) |  |  |  | |
| 8.14 | Sonstiges |  |  |  | |

## Auftragskontrolle

| **Nr.** | **Prüfungspunkt** | **Antwort** | **Dokumentation der Ergebnisse** | **Beurteilung der TOM**  (wird vom Auftraggeber ausgefüllt) |
| --- | --- | --- | --- | --- |
| **9.** | **Maßnahmen zur Auftragskontrolle**  Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. | | | |
| 9.1 | Welche Maßnahmen werden ergriffen, damit die Verarbeitung der personenbezogenen Daten durch die damit betrauten Mitarbeiter nur gemäß den Weisungen des Auftraggebers erfolgen kann?  (Richtlinien, Arbeitsanweisungen, Zugriffssteuerung, Verpflichtung auf das Datengeheimnis etc.) |  |  |  |
| 9.2 | Welche Maßnahmen werden getroffen, damit auch ggf. Unterauftragnehmer keine unbefugten Aktivitäten mit den zur Verfügung gestellten Daten durchführt?  (sorgfältige Auswahl der Unterauftragnehmer, vertragliche Verpflichtung der Unterauftragnehmer etc.) |  |  |  |
| 9.3 | Werden Maßnahmen getroffen, die am Ende des Aufbewahrungszwecks der personenbezogenen Daten deren Löschung/ Sperrung sicherstellen und sind diese technisch implementiert?  (sorgfältige Auswahl der Unterauftragnehmer, vertragliche Verpflichtung der Unterauftragnehmer etc.) |  |  |  |
| 9.4 | Existieren datenschutzgerechte Verträge nach Art. 28 DS-GVO zwischen Auftraggeber und Auftragnehmer?  (Wurden diese Verträge auf den Vertragsgegenstand, Art der Daten und Datenkategorien angepasst?) |  |  |  |
| 9.5 | Wie erfolgt die Authentisierung bei Aufträgen des Auftraggebers?   * Nur schriftlich? * Nur wenn persönlich bekannt? |  |  |  |
| 9.6 | Werden Subunternehmer des Auftragnehmers eingesetzt?  (Sind die Regelungen mindestens so restriktiv, wie die des Auftraggebers?) |  |  |  |
| 9.7 | Bestehen Kontrollrechte des Auftraggebers beim Subunternehmer des Auftragnehmers?  (Sind diese Kontrollrechte in den Vertrag zwischen Auftragnehmer und dessen Subunternehmer aufgenommen) |  |  |  |
| 9.8 | Sonstiges |  |  |  |

## Auftragsspezifische Bemerkungen

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |