

Auftragsverarbeitungsvertrag (Anlage 2)

**Anlage 3 zum Auftragsverarbeitungsvertrag:
Beschreibung der technischen und organisatorischen Maßnahmen**

Die vorliegende Anlage 3 ist vom Auftragnehmer bei Bedarf (im abrufbezogenen Einzelfall) einzureichen. Alternativ ist die Nutzung eines bestehenden Dokuments mit einer Beschreibung der technischen und organisatorischen Maßnahmen des Auftragnehmers möglich (sofern alle relevanten Inhalte enthalten sind).

Bei Nutzung dieses Dokuments ist bei den nachfolgend aufgeführten Maßnahmen die jeweils zutreffende Antwort gemäß der tatsächlichen Umsetzung beim Bieter zu markieren und im Feld „Anmerkungen“ so weit wie möglich zu konkretisieren.

1.1. Zutrittskontrolle

Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

Frage	Antwort	Anmerkungen
Werden Zutrittsrechte dokumentiert?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Gibt es ein dokumentiertes Verfahren für die Vergabe / den Entzug von Zutrittsrechten bzw. Schlüsseln?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Gibt es Videoüberwachung in allen oder bestimmten Bereichen?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Verfügen externe Personen über Zutrittsberechtigungen?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier Personengruppen ergänzen
Sind die Eingangstüren und Nebentüren gesichert, sodass ein Schutz vor unbefugtem Betreten der Gebäude besteht?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier Art des Schließsystems / der Maßnahmen ergänzen
Werden Externe bzw. Besucher in den Gebäuden beaufsichtigt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden Besucher erfasst?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier Art der Dokumentation ergänzen
Werden Fenster und Türen verschlossen, wenn die Räume, in denen Daten verarbeitet werden, nicht besetzt sind?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	

Auftragsverarbeitungsvertrag (Anlage 2)

Frage	Antwort	Anmerkungen
Sind einstiegsgefährdete Fenster und Türen in Gebäuden, in denen Daten verarbeitet werden, gegen Einbruch abgesichert (z.B. durch Sicherheitsschlösser, Fenstergitter oder Sicherheitsglas)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier Maßnahmen auflisten
Gibt es eine Liste der Zutrittsberechtigungen zu den Serverräumen?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier Liste bzw. Personengruppen ergänzen
Sind die Serverräume vor dem Zutritt unberechtigter Personen – insbesondere auch außerhalb der Geschäftszeiten – geschützt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier Maßnahmen ergänzen
Gibt es weitere organisatorische/technische Maßnahmen (Alarmanlage, Wachdienst, Personenvereinzelungs-anlagen, etc.), die die Zutrittskontrolle unterstützen?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier Maßnahmen ergänzen

1.2. Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme (Netzwerk, Betriebssystem, Endgerät) von Unbefugten genutzt werden können.

Frage	Antwort	Anmerkungen
Existiert eine Passwortrichtlinie?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier technisch / organisatorisch sowie die Mindestanforderungen vermerken
Existiert eine andere technische Maßnahme, um den unbefugten Zugang zu IT-Systemen zu erschweren (z.B. Authentifizierung mittels Smart Cards / Token)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier beschreiben
Existieren weitere Vorgaben zum Umgang mit Passwörtern (Besonderheiten bei administrativen Passwörtern, Gruppenpasswörter, etc.)	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier Vorgaben ergänzen
Gibt es eine maximale Zahl Anmeldeversuche, bevor Nutzeraccounts gesperrt werden?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	

Auftragsverarbeitungsvertrag (Anlage 2)

Frage	Antwort	Anmerkungen
Sind Passwörter der Mitarbeitenden auch weiteren Personen bekannt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier Personenkreise grob beschreiben
Werden Anmeldungen an IT-Systemen automatisiert protokolliert?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Wird Mehr-Faktor-Authentifizierung oder eine andere Maßnahme genutzt, um den Zugang zu IT-Systemen zusätzlich abzusichern?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier Maßnahme beschreiben
Werden Maßnahmen zur Absicherung des Netzwerks ergriffen?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier beschreiben
Werden Mobilgeräte, sofern genutzt, über Mobile Device Management verwaltet?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Sind Laptop- und Desktop-Festplatten verschlüsselt (Verwendung eines „Pre-Boot-Passworts“)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Sind physische Schnittstellen von Endgeräten abgesichert (Sperrung von USB-Schnittstellen, Verhindern von Autostart, ...)	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier beschreiben

1.3. Zugriffskontrolle

Maßnahmen, 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.

Frage	Antwort	Anmerkungen
Existiert ein Berechtigungskonzept?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Wird die Vergabe von Berechtigungen dokumentiert?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier beschreiben
Sind Zugriffe auf Anwendungen und Dateien nur entsprechend berechtigten Nutzern möglich (Need-to-Know-Prinzip)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	

Auftragsverarbeitungsvertrag (Anlage 2)

Frage	Antwort	Anmerkungen
Werden besonders schützenswerte Daten verschlüsselt gespeichert (z.B. Dateiverschlüsselung, verschlüsselte Archivdateien)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier beschreiben
Ist die Ausführung von Programmen auf eine Liste erlaubter Programme eingeschränkt (Application Whitelisting)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden Benutzerrechte durch zentrale Administratoren verwaltet?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Besitzen Administratoren separate Administrations- und Standard-Zugänge für IT-Systeme?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden externe Datenträger zentral verwaltet (zentrale Ausgabe und Dokumentation)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier Prozesse beschreiben
Werden Datenträger nach Ende der Nutzungsdauer ordnungsgemäß vernichtet oder vor der Weitergabe nach Stand der Technik sicher gelöscht?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden Datenträger sicher aufbewahrt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier Maßnahmen zur Sicherung beschreiben
Gibt es weitere Zugriffsschutzmaßnahmen für Datenträger?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, Maßnahmen hier auflisten
Werden Aktenvernichter zur Entsorgung von Dokumenten verwendet?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden zur Vernichtung von Akten und Daten Dienstleister eingesetzt (vorzugsweise mit DIN 66399-Zertifikat)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden personenbezogene Daten in selbst betriebenen Webanwendungen verarbeitet, auf die von extern zugegriffen werden kann?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, Anwendungen hier auflisten
Falls ja, sind diese Anwendungen nach Stand der Technik gehärtet?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier Härtungsmaßnahmen beschreiben

Auftragsverarbeitungsvertrag (Anlage 2)**1.4. Trennungsgebot**

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Frage	Antwort	Anmerkungen
Sind Produktiv- und Testsysteme voneinander getrennt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, Maßnahmen hier auflisten
Werden zu unterschiedlichen Zwecken erhobene Daten auf separaten Systemen oder Datenträgern gespeichert?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Findet softwareseitig eine logische Mandantentrennung statt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Existiert ein Dateispeicherungs- und Ablagekonzept?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier grob beschreiben

1.5. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der (elektronischen) Übermittlung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Frage	Antwort	Anmerkungen
Werden beim mobilen Arbeiten, sofern zutreffend, VPN-Verbindungen genutzt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden E-Mails mit besonders schützenswerten Inhalten Ende-zu-Ende-verschlüsselt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Falls nein, werden besonders schützenswerte E-Mail-Anhänge verschlüsselt (Dateiverschlüsselung, verschlüsselte Archive)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden für den physischen Transport von Datenträgern besondere Schutzmaßnahmen ergriffen (z.B. Verschlüsselung, Auswahl von besonderem Personal)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier auflisten

Auftragsverarbeitungsvertrag (Anlage 2)

Frage	Antwort	Anmerkungen
Werden Daten vor der Weitergabe an Auftragsverarbeiter anonymisiert oder pseudonymisiert?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier spezifizieren

1.6. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen (Anwendungen / Software) eingegeben, verändert oder entfernt worden sind.

Frage	Antwort	Anmerkungen
Existiert ein Konzept zur Erfassung und Ablage von Protokolldaten auf IT-Systemen?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier grob beschreiben
Werden Zugriffe auf Anwendungen und Dateien protokolliert?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden Protokolldaten regelmäßig analysiert?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier Intervall und Art der Analyse beschreiben
Wird ein System Information und Event Management-System (SIEM) eingesetzt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden technische Integritätssicherungsmaßnahmen (digitale Signaturen, Abgleiche von Prüfsummen) eingesetzt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, Maßnahmen hier auflisten
Werden die Originale von Formularen aufbewahrt, die in automatisierte Verarbeitungen übernommen wurden?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Sind Änderungen an personenbezogenen Daten in der Software, mit der die Daten verarbeitet werden, nachvollziehbar (Wer hat wann welche Änderung vorgenommen)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	

1.7. Datenschutzmanagement

Gewährleisten, dass Datenschutz in der Organisation angemessene Beachtung findet.

Auftragsverarbeitungsvertrag (Anlage 2)

Frage	Antwort	Anmerkungen
Ist ein*e Datenschutzbeauftragte*r berufen?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden Mitarbeitende zum Thema Datenschutz geschult?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden Mitarbeitende zum Thema Informationssicherheit geschult?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden Mitarbeitende auf das Datengeheimnis verpflichtet?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	

1.8. Datensicherung

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Frage	Antwort	Anmerkungen
Werden regelmäßige Backups der personenbezogenen Daten durchgeführt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier Intervall und Anzahl der Backups angeben
Existiert ein Backup-Konzept?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden RAID-Systeme zur Speicherung personenbezogener Daten eingesetzt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier verwendete RAID-Level angeben
Sind die verwendeten IT-Systeme redundant aufgebaut?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier genauer ausführen
Wird bei Servern unterbrechungsfreie Stromversorgung (USV) genutzt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Wurden bei der Planung der Serverräume elementare physische Gefährdungen berücksichtigt und Maßnahmen ergriffen (z.B. Feuer, Hochwasser, Wasserrohrbrüche)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Existieren mit Dienstleistern Service Level Agreements (SLAs) für Verfügbarkeit?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	

1.9. Rasche Wiederherstellbarkeit der Verfügbarkeit

Gewährleisten, dass die Daten nach einer Verletzung der Verfügbarkeit möglichst schnell wieder zur Verfügung stehen.

Auftragsverarbeitungsvertrag (Anlage 2)

Frage	Antwort	Anmerkungen
Existiert ein Recovery-Konzept?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Wird die Datenwiederherstellung aus Backups regelmäßig getestet?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden Backups physisch getrennt von den Originaldaten aufbewahrt (z.B. in einem anderen Brandabschnitt, an einem anderen Standort)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, hier genauer ausführen
Werden Backups auf unterschiedlichen Medien gespeichert (z.B. Festplatte und Magnetband)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Existiert ein Business-Continuity-Managementsystem (BCMS)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Existieren Wiederanlaufpläne?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	

1.10. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Frage	Antwort	Anmerkungen
Werden (Unter-)Auftragnehmer unter Rücksichtnahme auf deren Sorgfalt hinsichtlich Datensicherheit ausgewählt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden Auftragnehmer vor Auftragsbeginn auf ihre Sicherheitsmaßnahmen hin überprüft?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden Auftragnehmer während der Vertragslaufzeit regelmäßig auf ihre Sicherheitsmaßnahmen hin überprüft?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden Mitarbeitende des Auftragnehmers auf das Datengeheimnis verpflichtet?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Wird sichergestellt, dass nach Ende des Auftrags alle Daten zurückgegeben oder gelöscht werden?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, Maßnahmen auflisten

1.11. Netzwerksicherheit

Gewährleisten, dass die IT-Infrastruktur netzwerkseitig gegen Angriffe geschützt ist.

Auftragsverarbeitungsvertrag (Anlage 2)

Frage	Antwort	Anmerkungen
Wird das interne Netz durch eine Firewall vom Internet getrennt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Wird Netzwerksegmentierung eingesetzt (z.B. Trennung von Clients und Servern, Trennung von Clients unterschiedlicher Abteilungen)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	Falls ja, Netzwerkplan grob skizzieren oder anhängen
Verwenden die eingesetzten Firewalls einen Whitelisting-Ansatz?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Befinden sich von außen erreichbare IT-Systeme in einer dedizierten Netzwerkzone (Demilitarisierte Zone, DMZ)?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Wird auf den Endgeräten eine Antimalware-Lösung eingesetzt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Wird auf den Endgeräten eine Endpoint-Security-Lösung eingesetzt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	

1.12. Incident-Response-Management

Maßnahmen, die gewährleisten, dass Sicherheitsvorfälle frühzeitig erkannt werden und hierauf unmittelbar reagiert werden kann, damit schwerwiegende Folgen möglichst begrenzt werden.

Frage	Antwort	Anmerkungen
Existieren Intrusion-Detection-Systeme, die Angriffe auf IT-Systeme erkennen und melden?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Ist geschultes Personal vorhanden oder existieren entsprechende Rahmenverträge mit Dienstleistern, um auf Vorfälle angemessen reagieren zu können?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Können kompromittierte Systeme netzwerktechnisch isoliert werden?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Sind die Abläufe im Fall eines Sicherheitsvorfalls dokumentiert und den Verantwortlichen bekannt?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	
Werden die Abläufe bei Sicherheitsvorfällen im Rahmen regelmäßiger Übungen getestet?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein	