Checkliste für die Prüfung von Auftragnehmern im Rahmen der Auftragsverarbeitung

1 Angaben zum Datenschutzbeauftragten des Auftragnehmers

Name	
Firma	
Anschrift	
Kontaktdaten	
Ausbildung	
Weiterbildungen im Bereich Datenschutz	

2 Durch wen erfolgte die Prüfung des Auftragnehmers?

Name	
Firma	
Anschrift	
Kontaktdaten	
Ausbildung	
Weiterbildungen im Bereich Datenschutz und Technik	

3 Wer wurde beim Auftragnehmer beauftragt?

Name	
Firma	
Anschrift	
Kontaktdaten	
Ausbildung	
Weiterbildung im Bereich Datenschutz und Technik	
Funktion und Verantwortung im Unternehmen des Auftragnehmers	

4 Wie erfolgt die Auswahlprüfung?

Art der Prüfung	Datum/Zeitpunkt der Prüfung
Vor Ort / telefonisch / schriftlich	

5 Freigabe der Auftragsverarbeitung

Verantwortlicher	Name + ggf. Unterschrift
Datenschutzbeauftragter	
Anderer Verantwortlicher	
Freigabe erteilt?	Ja / Nein
Anmerkungen	
Datum	
Nächste Prüfung	

6 Erneute Prüfung

Prüfung	Wann?
Vor Ort / telefonisch /schriftlich	
Freigabe erteilt?	Ja / Nein
Anmerkungen	
Datum	
Nächste Prüfung	

7 Art. 28 Abs. 3 DSGVO – Vertrag zur Auftragsverarbeitung

Verantwortlicher und Auftragsverarbeiter müssen in einem Vertrag oder einem anderen Rechtsinstrument nach dem Unionsrechts die Rechte und Pflichten der Parteien zur Auftragsverarbeitung abschließen welches die Inhaltlichen Anforderungen gem. Art. 28 Abs. 3 DSGVO genügt.

Der Vertrag zur Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO berücksichtigt folgende Punkte:

- Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen;
- Verarbeitung auf dokumentierte Weisung des Verantwortlichen;
- Vertraulichkeitsverpflichtung;
- Ergreifen erforderlicher technischer und organisatorischer Maßnahmen;
- Inanspruchnahme von Unterauftragnehmern nach Art. Art. 28 Abs. 2 und Abs. 4 DSGVO;
- Unterstützung des Verantwortlichen bei der Beantwortung von Betroffenenanfragen;
- Unterstützung des Verantwortlichen bei den Pflichten nach Art. 32 – 36 DSGVO;
- Umgang mit personenbezogenen Daten nach Beendigung der Auftragsverarbeitung;
- Zurverfügungstellung von Informationen und Ermöglichung von Überprüfungen.
- Hinweispflicht

8 Art. 32 DSGVO – „Technische und organisatorische Maßnahmen“

Der Verantwortliche arbeitet gem. Art. 28 Abs. 1 DSGVO nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und der Schutz der Rechte der Betroffenen gewährleistet ist.

Die Prüfung der Sicherheit der Verarbeitung nach Art 32 DSGVO berücksichtigt risikoorientiert folgende Punkte:

- Pseudonymisierung;
- Verschlüsselung;
- Gewährleistung der Vertraulichkeit;
- Gewährleistung der Integrität;
- Gewährleistung der Verfügbarkeit;
- Gewährleistung der Belastbarkeit der Systeme;

- Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall;
- Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

8.1 Pseudonymisierung

Ziel ist es, Unbefugten eine Identifizierbarkeit von natürlichen Personen zu erschweren. Pseudonymisierung erfolgt dadurch, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen keine Identifizierung der betroffenen Person ermöglichen. Hierbei werden Identifikationsmerkmale einer Person durch ein Kennzeichen ersetzt. Diese zusätzlichen Informationen werden dabei gesondert und sicher aufbewahrt.

Maßnahmen

Datenminimierung **Prüfen, ob die Zwecke der Datenverarbeitung auch bei Pseudonymisierung erreicht werden können:** ☐ **Produktivsystem** ☐ **Testsystem**

8.2 Verschlüsselung

Verschlüsselung bietet Schutz vor Veränderungen und unbefugter Offenlegung oder unbefugtem Zugang zu den Daten. Das eingesetzte Verschlüsselungsverfahren muss dem Stand der Technik entsprechen.

Maßnahmen

Schriftliche Regelungen für die Verschlüsselung	
Verschlüsselung von Datenträgern ☐ **Vertrauliche Datenträger** ☐ **Laptopfestplatten** ☐ **Mobile Datenträger**	
Verschlüsselte Speicherung von Daten ☐ **Verwendete Schlüsselalgorithmen** ☐ **Verwendete Hash-Funktionen**	
Verschlüsselung bei der Übermittlung ☐ **Citrix-Verbindung (128 Bit verschlüsselt)** ☐ **VPN-Verbindung (IP-Sec)** ☐ **E-Mail Versand mit verschlüsselten ZIP-Dateien** ☐ **Datenaustausch über https-Verbindung**	

☐ Verschlüsselung von Netzwerken	
Zentrale Schlüsselverwaltung	
Sonstiges	

8.3 Vertraulichkeit

Ziel ist es, einen sicheren Schutz vor Zugriffen unbefugter Personen auf Datenverarbeitungsanlagen und Verfahren zu gewährleisten.

Maßnahmen

Zutrittskontrolle
z. B.:

- ☐ Berechtigungsausweise
- ☐ Elektronische Zutrittscodekarten/Zutrittstransponder
- ☐ Zutrittsberechtigungskonzept
- ☐ Videoüberwachung
- ☐ Alarmanlage
- ☐ Schlüsselregelung
- ☐ Begleitung von Besucherzutritten durch eigene Mitarbeiter
- ☐ Anwesenheitsaufzeichnungen von Besucherzutritten
- ☐ Abgestufte Sicherheitsbereiche und kontrollierter Zutritt
- ☐ Gesondert gesicherter Zutritt zum Rechenzentrum
- ☐ Aufbewahrung der Server in verschlossenen Räumen
- ☐ Aufbewahrung der Datenträger unter Verschluss bzw. abgeschlossenen Räumen

Zugangskontrolle
z.B.:

- ☐ Verschluss von Datenverarbeitungsanlagen
- ☐ Passwortsicherung von Bildschirmarbeitsplätzen
- ☐ Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen
- ☐ Verwendung von individuellen Passwörtern
- ☐ Automatisierte Sperrung von Accounts nach mehrfacher Fehleingabe von Passwörtern
- ☐ Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner)
- ☐ Passwortpolicy mit Mindestvorgaben zur Passwortkomplexität
- ☐ Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern
- ☐ Prozess zum Rechteentzug bei Abteilungswechsel von Mitarbeitern
- ☐ Prozess zum Rechteentzug bei Austritt von Mitarbeitern
- ☐ Verpflichtung zur Vertraulichkeit
- ☐ Protokollierung und Auswertung der Systembenutzung

Zugriffskontrolle z.B.: ☐ Festlegung der Zugriffsberechtigung, Berechtigungskonzept ☐ Regelung zur Wiederherstellung von Daten aus Backups ☐ Regelmäßige Überprüfung von Berechtigungen ☐ Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken ☐ Regelmäßige Auswertung von Protokollen (Logfiles) ☐ Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen (Read, Write, Execute) ☐ Protokollierung von Dateizugriffen und -löschungen ☐ Sicherheitssysteme (z.B. Virenscanner, Firewalls, SPAM-Filter)
Trennungskontrolle z.B: ☐ Trennung von Kunden (Mandantenfähigkeit des verwendeten Systems) ☐ Dateiseparierung bei Datenbanken ☐ Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern) ☐ Datensicherungen der Auftraggeber-Daten auf separaten Datenträgern (ohne Daten anderer Kunden) ☐ Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt ☐ Funktionstrennung ☐ Trennung von Entwicklungs-, Test und Produktivsystem

Sonstiges	

8.4 Integrität

Ziel ist es, die Manipulation und Veränderung von Daten zu verhindern.

Maßnahmen

Weitergabekontrolle ☐ Sichere Versandart der Daten zwischen Auftraggeber und Dritten ☐ Gesicherter Eingang für An- und Ablieferung ☐ Dokumentierte Verwaltung von Datenträgern, Bestandskontrolle ☐ Festlegung der Bereiche, in dem sich Datenträger befinden müssen ☐ Kontrollierte Vernichtung von Datenträgern (Physikalische Zerstörung oder überschreiben) ☐ Kontrollierte Zerstörung von Papierdokumenten (Verschlossene Behältnisse aus Metall (sog. Datenschutztonnen), Entsorgung durch Dienstleiter ☐ Sicherungskopien von Datenträgern, die transportiert werden müssen ☐ Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege ☐ Verpackungs- und Versandvorschriften ☐ Vollständigkeits- und Richtigkeitsprüfung

Eingabekontrolle	
☐ Kennzeichnung erfasster Daten ☐ Festlegung von Benutzerprofilen ☐ Differenzierte Benutzerberechtigungen: Lesen/Ändern/Löschen ☐ Teilzugriff bei Datenbanken ☐ Organisatorische Festlegung von Eingabezuständigkeiten ☐ Protokollierung von Eingaben/Löschungen ☐ Protokollauswertungssystem ☐ Verpflichtung auf das Datengeheimnis ☐ Über OS-Standard hinausgehende Log-Konzept ☐ Dezidierter Logserver ☐ Regelung der Zugriffsberechtigungen für Logserver (LogAdmin) ☐ Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke	
Sonstiges	

8.5 Verfügbarkeit und Belastbarkeit

Ziel ist es, die Daten gegen zufällige Zerstörung oder Verlust zu schützen sowie zu gewährleisten, dass die Systeme mit risikobedingten Veränderungen umgehen können und eine Toleranz mit Ausgleichsfähigkeit gegenüber Störungen aufweisen.

Maßnahmen

Verfügbarkeitskontrolle
☐ Datensicherungs- und Backupkonzepte ☐ Durchführung der Datensicherungs- und Backupkonzepte ☐ Zutrittsbegrenzung in Serverräumlichkeiten auf notwendiges Personal ☐ Brandmeldeanlagen in Serverräumlichkeiten ☐ Rauchmelder in Serverräumlichkeiten ☐ Wasserlose Brandbekämpfungssysteme in separaten Räumlichkeiten und Brandabschnitt ☐ Klimatisierte Serverräumlichkeiten ☐ Serverräumlichkeiten in separaten Brandabschnitt ☐ Unterbringung von Backupsystemen in separaten Räumlichkeiten und Brandabschnitt ☐ Gewährleistung der technischen Lesbarkeit von Backupspeichermedien für die Zukunft ☐ Lagerung von Archiv-Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.) ☐ CO2 Feuerlöscher in unmittelbarer Nähe der Serverräumlichkeiten ☐ Vereinbarung bzgl. Übergabe der (Daten-) Sicherungen ☐ Katastrophen- oder Notfallplan (z.B. Wasser, Feuer, Explosion, Androhung von Anschlägen, Absturz, Erdbeben) ☐ Einbeziehung des Einflusses angrenzender baulicher Einrichtungen ☐ Schwachstellenanalyse (Geländeschutz, Gebäudeschutz, Eindringen in Rechner, Rechnernetze)

- ☐ USV-Anlage (Unterbrechungsfreie Stromversorgung)
- ☐ Stromgenerator

Widerstandsfähigkeits- und Ausfallsicherheitskontrolle
z.B.:

- ☐ Ausweich-Rechenzentren
- ☐ Redundante Stromversorgung / USV-Anlage / Stromgeneratoren / Klimatisierung / Brandbekämpfung
- ☐ Datenspeicherung auf RAID-Systemen
- ☐ Durchführung von Penetrationstests
- ☐ Unverzügliche und regelmäßige Aktivierung von verfügbaren Soft- und Firmware-updates
- ☐ Periodische Sicherheitstrainings und Sensibilisierungskampagnen innerhalb der Organisation.

Sonstiges	

8.6 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM

Ziel ist es, durch regelmäßige Prüfungen und Evaluierungen die Risikoangemessenheit zu bewerten um entsprechende Anpassungsmaßnahmen vorzunehmen. Insbesondere können sich neue Risiken durch die stetige Entwicklung der Technik ergeben.

Maßnahmen

Kontrollverfahren

- ☐ Interne Verfahrensverzeichnisse werden mind. jährlich aktualisiert
- ☐ Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten
- ☐ Meldung neuer/veränderter Datenverarbeitungsverfahren an den IT-Sicherheitsbeauftragten
- ☐ Prozesse zur Meldung neuer/veränderter Verfahren sind dokumentiert
- ☐ Es werden datenschutzfreundliche Voreinstellungen gewählt
- ☐ Getroffene Sicherheitsmaßnahmen werden einer regelmäßigen internen Kontrolle unterzogen
- ☐ Bei negativem Verlauf der zuvor genannten Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst, erneuert und umgesetzt
- ☐ Es besteht ein Prozess zur Vorbereitung auf Sicherheitsverletzungen (Angriffen) und Systemstörungen sowie zur Identifizierung, Eingrenzung, Beseitigung und Erholung von selbigen (Incident-Response-Prozess).

Auftragskontrolle • Vertragsgestaltung gem. gesetzlichen Vorgaben (Art. 28 DSGVO) • Zentrale Erfassung vorhandener Auftragsverarbeiter (einheitliches Vertragsmanagement) • Regelmäßige Kontrollen beim Auftragnehmer nach Vertragsbeginn (Während Vertragsdauer) • Vor-Ort-Kontrollen beim Auftragnehmer • Überprüfung des Datensicherheitskonzepts beim Auftragnehmer • Sichtung vorhandener IT-Sicherheitszertifikate der Auftragnehmer • Externe Auftragnehmer und Wartungspersonal erhalten einen spezifischen Zugang, der nur während des Eingriffs aktiv und den Rest der Zeit deaktiviert ist.	
Sonstiges	

8.7 Auftragsspezifische Zusatzmaßnahmen

Ziel ist es, die besonderen Risiken, die sich aus dem spezifischen Auftrag ergeben können, zu minimieren.

Maßnahmen
