

Datenschutz-Vereinbarung zur Verarbeitung von Daten im Auftrag gem. Art. 28 DSGVO

zwischen

- Auftraggeber, nachstehend „Verantwortlicher“ genannt -

und

...

- Auftragnehmer, nachstehend „Auftragsverarbeiter“ genannt –

1. Gegenstand und Dauer des Auftrags

1.1 Der Gegenstand des Auftrags zur Verarbeitung personenbezogener Daten

- ☐ ergibt sich aus dem Vertrag ... vom ... (im Folgenden: Hauptvertrag).
- ☐ ist die Durchführung folgender Aufgaben durch den Auftragsverarbeiter: ...

1.2 Die Dauer der Datenverarbeitung

- ☐ ergibt sich aus dem oben genannten Hauptvertrag.
- ☐ beginnt mit Vertragsunterzeichnung und wird unbefristet durchgeführt.
- ☐ beginnt am ... und endet am ...
- ☐ beginnt mit Vertragsunterzeichnung und wird nur einmalig durchgeführt.

1.3 Die Vorgaben dieser Vereinbarung wirken nach, so lange der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen verarbeitet (einschließlich Backups).

2. Konkretisierung des Auftragsinhalts

2.1 Umfang, Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter für den Verantwortlichen

- ☐ sind konkret im Hauptvertrag beschrieben.
- ☐ lassen sich folgendermaßen beschreiben:

2.2 Die Arten der verwendeten personenbezogenen Daten

- ☐ sind im Hauptvertrag konkret beschrieben unter Nr.
- ☐ sind folgende: ...

2.3 Die Kategorien der durch die Verarbeitung betroffenen Personen

- ☐ sind im Hauptvertrag konkret beschrieben unter Nr.
- ☐ sind folgende: ...

3. Technische und organisatorische Maßnahmen

- 3.1 Der Auftragsverarbeiter ergreift in seinem Verantwortungsbereich alle erforderlichen technischen und organisatorischen Maßnahmen gem. Art. 32 DSGVO zum Schutz der personenbezogenen Daten und übergibt dem Verantwortlichen die Dokumentation zur Prüfung (Anlage 1). Bei Akzeptanz durch den Verantwortlichen werden die dokumentierten Maßnahmen Grundlage der Vereinbarung.
- 3.2 Soweit eine Prüfung oder ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- 3.3 Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten

werden. Über wesentliche Änderungen, die durch den Auftragsverarbeiter zu dokumentieren sind, ist der Verantwortliche in Kenntnis zu setzen.

4. Rechte von betroffenen Personen

- 4.1 Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von betroffenen Personen erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.
- 4.2 Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß Nr. 4 befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

5. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter hat (zusätzlich zu den Pflichten nach dieser Vereinbarung) eigene gesetzliche Pflichten gemäß der DSGVO. Hierzu zählen insbesondere, aber nicht nur:

- 5.1. Der Auftragsverarbeiter bestellt – soweit gesetzlich erforderlich – schriftlich einen Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und Art. 39 DSGVO ausübt.
- 5.2. Der Auftragsverarbeiter wahrt die Vertraulichkeit gemäß Art. 28 Abs. 3 Buchst. b, Art. 29, Art. 32 Abs. 4 DSGVO. Deshalb setzt er bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Er und jede ihm unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, es besteht eine gesetzliche Verpflichtung zur Datenverarbeitung.
- 5.3. Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- 5.4. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt.
- 5.5. Soweit der Verantwortliche seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen.
- 5.6. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der Pflichten, die sich aus den Artikeln 32 bis 36 DSGVO ergeben.
- 5.7. Der Auftragsverarbeiter kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- 5.8. Der Auftragsverarbeiter kann die getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollbefugnisse nach Nr. 8 dieser Vereinbarung nachweisen.
- 5.9. Der Auftragsverarbeiter meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Verantwortlichen in der Weise, dass der Verantwortliche seinen gesetzlichen Pflichten, insbesondere nach Artt. 33, 34 DSGVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Verantwortlichen für weitere Maßnahmen zur Verfügung stellt.

- 5.10. Der Auftragsverarbeiter unterstützt den Verantwortlichen in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung.
- 5.11. Soweit der Verantwortliche zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragsverarbeiter unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

6. Unterauftragsverhältnisse

- 6.1 Als Unterauftragsverhältnisse sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/ Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragsverarbeiter nach diesem Vertrag stehen. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Sicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
- 6.2 Der Auftragsverarbeiter darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Verantwortlichen beauftragen.
 - ☐ Eine Unterbeauftragung ist unzulässig.
 - ☐ Der Verantwortliche stimmt der Beauftragung der in Anlage 2 bezeichneten Unterauftragnehmer zu.

Die Auslagerung auf Unterauftragnehmer und der Wechsel von bestehenden Unterauftragnehmern sind nur zulässig, soweit

 - a) der Auftragsverarbeiter eine solche Auslagerung auf Unterauftragnehmer dem Verantwortlichen eine angemessene Zeit vorab (mindestens 14 Tage) schriftlich oder in Textform anzeigt und
 - b) der Verantwortliche bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragsverarbeiter nicht schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
 - c) eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO sowie die Vorgaben dieser Vereinbarung zugrunde gelegt werden. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend dieser Vereinbarung und gemäß der Datenschutz-Grundverordnung unterliegt.
- 6.3 Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter die betreffenden Passagen der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.
- 6.4 Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter

benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

- 6.5 Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – falls der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7. Internationale Datenübermittlungen

- 7.1 Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Datenschutz-Grundverordnung im Einklang stehen.
- 7.2 Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Nr. 6 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten in Drittländer beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Datenschutz-Grundverordnung sicherstellen.

8. Kontrollrechte des Verantwortlichen

- 8.1 Der Verantwortliche hat das Recht, im Benehmen mit dem Auftragsverarbeiter Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich selbst oder durch einen beauftragten Dritten durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.
- 8.2 Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DSGVO überzeugen kann. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
- 8.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO
 - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO
 - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
 - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

9. Weisungsbefugnis des Verantwortlichen

- 9.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer

der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

- 9.2 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Datenschutz-Grundverordnung oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen. In diesem Fall ist der Auftragsverarbeiter berechtigt, die Ausführung der Weisung auszusetzen, bis der Verantwortliche die Weisung geändert hat oder diese bestätigt.

10. Löschung und Rückgabe von personenbezogenen Daten

- 10.1 Kopien oder Duplikate der Daten werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- 10.2 Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung des Hauptvertrags – löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung dieser personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

11. Weitere Regelung

Im Fall eines Widerspruchs zwischen dieser Vereinbarung zur Verarbeitung von Daten im Auftrag und von damit zusammenhängenden Vereinbarungen zwischen den Parteien hat diese Vereinbarung Vorrang.

Anlage 1: Technische und organisatorische Maßnahmen des Auftragsverarbeiters

Anlage 2: Genehmigte Unterauftragsverhältnisse

Für den Verantwortlichen (Auftraggeber):

Für den Auftragsverarbeiter (Auftragnehmer):

Ort, Datum

Ort, Datum

Name und Funktion des Unterzeichnenden

Name und Funktion des Unterzeichnenden

Unterschrift

Unterschrift

Anlage 1: Technische und organisatorische Maßnahmen des Auftragsverarbeiters

nach Art. 32 DSGVO
(zu Nr. 3 der Datenschutz-Vereinbarung)

Konkrete Beschreibung der technisch-organisatorischen Maßnahmen des Auftragsverarbeiters unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener Personen (eine allgemeine Beschreibung ist nicht ausreichend):

1. Vertraulichkeit (Art. 32 Abs. 1 Buchst. b DSGVO)

1.1 Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

- Zutrittskontrollsystem durch Schlüssel, Ausweisleser, Magnetkarte, Chipkarte
- Schlüsselvergabe und Schlüsselmanagement erfolgt nach einem definierten Prozess
- Zutrittsberechtigung nur für berechtigte Personen
- Türsicherung (Sicherheitsschlösser, elektrische Türöffner usw.)
- Abschließen von Räumen nach Arbeitsschluss
- Protokollierung von Besuchern
- Gäste werden innerhalb des Betriebsgeländes stets begleitet
- Gäste müssen sich registrieren (Besucherbuch)
- Tragepflicht von Berechtigungsausweisen
- Zutrittskontrolle durch Werkschutz, Pförtner
- sorgfältige Auswahl des Wach- und Reinigungspersonals
- Videoüberwachung
- Alarmanlage für Eingänge und Fenster
- Bewegungsmelder
- Server in abschließbaren Serverschränken

1.2 Zugangskontrolle

Das Eindringen Unbefugter in die IT-Systeme ist zu verhindern.

- Server sind nur nach einem individuellen Login nutzbar
- Clients sind nur nach einem individuellen Login nutzbar
- Login mit Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- fehlerhafte Anmeldeversuche werden protokolliert
- Anweisung zum Sperren des IT-Systems bei Verlassen des Arbeitsplatzes
- Automatische Sperrung bei Pausen und Fehlanmeldungen (z.B. Kennwort oder Pausenschaltung)
- Einrichtung eines Benutzerstammsatzes pro User
- automatisierte Standardroutinen für regelmäßige Aktualisierung von Schutzsoftware
- Verschlüsselung von Datenträgern
- Sperren von externen Schnittstellen (USB etc.)
- mobile IT-Systeme sind verschlüsselt
- mobile Datenträger sind verschlüsselt
- Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum Löschen von Daten aus der Ferne)

1.3 Zugriffskontrolle

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

- es gibt ein schriftliches Berechtigungskonzept mit differenzierten Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
- Verfahren zur Vergabe und periodischen Überprüfung der Berechtigungen ist definiert
- Berechtigungen werden ausschließlich von Administratoren eingerichtet
- Anzahl der Administratoren ist weitgehend reduziert
- ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen
- Zugriffe auf Anwendungen und/oder Daten werden protokolliert und können ausgewertet werden
- nicht mehr verwendete Datenträger werden sicher gelöscht / vernichtet
- Papierunterlagen mit personenbezogenen Daten werden sicher vernichtet
- Daten-Löschungen/-Vernichtungen werden protokolliert

1.4 Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

- interne Mandantenfähigkeit (z.B.: Daten von unterschiedlichen Auftraggebern sind logisch/physikalisch voneinander getrennt)
- Funktionstrennung (Produktion/Test)
- Zuständigkeiten und Verantwortlichkeiten sind eindeutig festgelegt

1.5 Pseudonymisierung (Art. 32 Abs. 1 Buchst. a DSGVO; Art. 25 Abs. 1 DSGVO)

Ein Personenbezug ist nur möglich, wenn zusätzliche Informationen hinzugezogen werden können.

- personenbezogene Daten werden, soweit möglich, nur unter einem Pseudonym gespeichert
- die zusätzlichen Informationen, die einen Personenbezug herstellen können, werden unter Verschluss aufbewahrt

2. Integrität (Art. 32 Abs. 1 Buchst. b DSGVO)

2.1. Weitergabekontrolle

Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, Übermittlungskontrolle, ...

- Mitarbeiter in Kundenprojekten werden belehrt über die zulässige Nutzung und Weitergabe von Daten
- Verschlüsselte Leitungen
- Zugriff von extern nur über verschlüsselte VPN-Tunnelverbindung
- Elektronische Signatur
- Protokollierung von Datenübermittlungen
- Sicherung von Datenträgertransporten (verschießbarer Transportbehälter), auch für Papier
- sorgfältige Auswahl von Transportpersonal und Fahrzeugen
- Versand von passwortgeschützten Dateien per E-Mail
- Versand von Daten nur in anonymisierter bzw. pseudonymisierter Form
- E-Mail-Verschlüsselung

2.2. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

- Protokollierungs- und Protokollauswertungssysteme (wer hat was eingegeben, geändert, gelöscht?)
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Mitarbeiter sind verpflichtet, nur unter ihren eigenen Benutzerkonten zu arbeiten
- Kontrolldaten werden aufbewahrt
- Zugriff auf die Protokolle ist nur Berechtigten möglich

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 Buchst. b DSGVO)

3.1. Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

- Verfahren zur regelmäßigen Sicherung der Daten (Backup)
- getrennte und katastrophensichere Aufbewahrung von Backups
- Backups sind verschlüsselt
- Einspielen von Backups wird regelmäßig getestet (Recovery)
- Spiegeln von Festplatten, z.B. RAID-Verfahren
- Einsatz von Unterbrechungsfreier Stromversorgung (USV)
- Serverraum ist klimatisiert
- Einsatz von Schutzprogrammen (Virens Scanner, Firewalls, Verschlüsselungsprogramme, Spam-Filter)
- IT-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert
- Feuer- und Rauchmeldeanlagen sind vorhanden
- feuerfeste Türen zum Serverraum
- Notfallplan liegt vor

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 Buchst. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1 Datenschutz-Management

Der Auftragsverarbeiter hat ein Verfahren im Einsatz, das die Beachtung des Datenschutzes sicherstellt.

- ein Datenschutz-Management-System (DSMS) ist implementiert
- Handbuch / Richtlinie zum Datenschutz ist für die Mitarbeiter vorhanden
- Datenschutzbeauftragter ist benannt
- regelmäßige Kontrolle durch den Datenschutzbeauftragten
- Beschäftigte werden im Datenschutz geschult
- Beschäftigten sind zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet
- Vorgaben zum Umgang mit Datenpannen sind für Mitarbeiter vorhanden
- interne Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst
- Verzeichnis von Verarbeitungstätigkeiten im Sinn des Art. 30 DSGVO wird geführt
- es finden verfahrensunabhängige Plausibilitäts- und Sicherheitsprüfungen statt

4.2 Incident-Response-Management

Der Auftragsverarbeiter hat ein Verfahren im Einsatz, das den Umgang mit datenschutzrechtlichen Vorfällen beschreibt.

- Vorgaben vorhanden, was als Datenpanne anzusehen ist
- Vorgaben vorhanden, wie mit Datenpannen umzugehen ist
- Notfallplan vorhanden

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Der Auftragsverarbeiter hat ggf. ein Verfahren im Einsatz, mit dem datenschutzfreundliche Voreinstellungen gewährleistet werden.

- Rechte- und Rollenkonzept nach dem „Need to know“-Prinzip
- externe Ressourcen werden, soweit möglich, vermieden

4.4 Auftragskontrolle

Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

- Eindeutige Vertragsgestaltung
- formalisierte Auftragserteilung (Auftragsformular)
- Kriterien zur Auswahl von Auftragsverarbeitern
- Kontrolle der Vertragsausführung
- weitere Auftragsverarbeiter werden schriftlich beauftragt

Anlage 2: Genehmigte Unterauftragsverhältnisse

Unterauftragsverarbeiter (Firmenname mit Rechtsform)	Anschrift / Land	Beschreibung der Datenverarbeitung (einschließlich einer klaren Abgrenzung der Verantwortlichkeiten, falls mehrere Unterauftragsverarbeiter genehmigt werden)