Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Vertragsparteien

Diese Vereinbarung wird zwischen dem **Auftraggeber/Vertragspartner** (nachfolgend „Auftraggeber“) und der BuchhaltungsButler GmbH als Auftragsverarbeiter mit Sitz in Spreestraße 5, 15913 Märkische Heide (nachfolgend „Auftragnehmer“) geschlossen.

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand des Auftrags

Der Gegenstand des Auftrags ergibt sich aus dem dazugehörigen mit dem Auftraggeber geschlossenen Vertrag über entsprechende Nutzungsrechte an der Software BuchhaltungsButler (im Folgenden Leistungsvereinbarung). Sofern der Auftraggeber zu einem späteren Zeitpunkt weitere Nutzungsrechte oder sonstige zusätzliche Leistungen beauftragt, so gilt diese Vereinbarung entsprechend auch für diese Leistungen.

Dieser Auftrag konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der in der Leistungsvereinbarung in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben.

Der Auftraggeber kann die Leistungsvereinbarung jederzeit unter Einhaltung einer Frist kündigen. Wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die Bestimmungen dieses Auftrags vorliegt, gilt diese Frist nicht.

(2) Dauer des Auftrags

Der Auftrag wird zur regelmäßigen Ausführung erteilt. Die Dauer richtet sich hierbei nach den Bestimmungen des Angebots sowie den AGB des Auftragnehmers. Sofern in bestimmten Fällen Individualvereinbarungen (Verträge) getroffen werden, so regeln diese die Wirksamkeit der AGB des Auftragnehmers.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Umfang, Art und Zweck der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet im Wesentlichen in Deutschland sowie in bestimmten Fällen (zeitlich befristet) in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den europäischen Wirtschaftsraum statt.

Insbesondere jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, sofern die besonderen Voraussetzungen der Artt. 44 ff DSGVO erfüllt sind. Falls ein Subunternehmer beauftragt werden soll, gelten diese Anforderungen zusätzlich zu den Bestimmungen in Art. 6 dieses Vertrags.

(2) Art der Daten

Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind folgende Datenarten/ -kategorien:

- Personendaten (im Rahmen der Nutzerverwaltung/-berechtigung sowie ggf. im Rahmen der Buchhaltung)
    - Vorname und Nachname
    - ggf. Position / Funktion
- Kommunikationsdaten (insb. Nutzerverwaltung,
    - Telefon
    - E-Mail
    - ggf. Fax
- Zahlungsdaten
    - Bankverbindungen (Kontoinhaber, Bankinstitut, IBAN, BIC)
    - Transaktionsdaten (u.a. Verwendungszweck , Betrag, Buchungsdatum/zeit, Transaktionsnummer)
    - ggf. Bankkonto Anbindung und Nutzung der Überweisungsfunktion
- Daten, die zur Buchhaltung erforderlich sind (abhängig von Umfang)
    - Rechnungsdaten
    - Angebotsdaten
    - Daten von Debitoren
    - Kreditoren & Interessenten

(3) Kategorien betroffener Personen

Die Kategorien betroffener Personen umfassen:

- Ansprechpartner / Nutzer (Mitarbeiter des Auftraggebers)
- Debitoren des Auftraggebers
- Kreditoren des Auftraggebers
- Interessenten des Auftraggebers
- Steuerberater des Auftraggebers
- Ggf. Geschäftspartner, Mitunternehmer, Gesellschafter u.ä.

Die tatsächlich betroffenen Kategorien betroffener Personen können je nach Auftraggeber und nach Umfang der Verarbeitungstätigkeiten, insbesondere je nach den auf Dokumenten/Belegen angegebenen Daten variieren. Die angegebenen Kategorien decken jedoch i.d.R. die betroffenen Kategorien ab.

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Dies gilt jedoch nur, insoweit dies für den Auftragnehmer wirtschaftlich und für das angestrebte bzw. tatsächlich erforderliche Schutzniveau angemessen sowie erforderlich ist.

(2) Der Auftragnehmer stellt die Sicherheit gem. Artt. 28 Abs. 3 lit. c sowie 32 DSGVO insbesondere i.V.m. Art. 5 Abs. 1, Abs. 2 DSGVO her. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32. Abs. 1 DSGVO zu berücksichtigen. Einzelheiten der durch den Auftragnehmer getroffenen technisch-organisatorischen Maßnahmen sind der Anlage zu entnehmen

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gem. Artt. 28 bis 32 DSGVO. Insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten insbesondere sofern der Auftragnehmer hierzu nach § 38 BDSG verpflichtet ist, der seine Tätigkeit gem. Artt. 38 und 39 DSGVO ausübt. Die aktuellen Kontaktdaten sind auf der Website des Auftragnehmers leicht zugänglich hinterlegt.
b) Die Wahrung der Vertraulichkeit gem. Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt 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. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag notwendigen technischen und organisatorischen Maßnahmen gem. Artt. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (Einzelheiten siehe Anlage).
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) Die unverzügliche Information des Auftraggebers 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 Auftragnehmer ermittelt.
f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
g) Der Auftragnehmer 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 Personen gewährleistet wird.
h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Art. 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer 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 Auftragnehmers nach diesem Vertrag erbracht werden. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Der Auftraggeber stimmt der Beauftragung der in Abs. 3 benannten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu.

Die Auslagerung auf Unterauftragnehmer oder der Wechsel der gemäß Abs. 3 bestehenden Unterauftragnehmer sind zulässig, soweit:

a. der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab in Textform anzeigt und

b. der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer in Textform oder schriftlich Einspruch gegen die geplante Auslagerung erhebt und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

(3) Der Auftraggeber stimmt der Beauftragung des nachfolgenden Unterauftragnehmers unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu:

Nr.	**Firma Unterauftragnehmer / Anschrift**	**Leistung** (ggf. weitere Angaben)	**Bei Daten-übermittlungen in ein Drittland: Angaben zu geeigneten Garantien**
1	ABBYY Europe GmbH Landsberger Str. 300 80687 München	Bild und Texterkennung	-
2	Bayerische Landesamt für Steuern Dienststelle München 80284 München	ELSTER-Schnittstelle, Übermittlung u.a. der USt.-Voranmeldung	-
3	Amazon Web Services EMEA SARL	Webhosting der BuchhaltungsButler (SaaS) am	-

	38 Avenue John F. Kennedy L-1855 Luxemburg	Serverstandort Frankfurt a. M.	
4	ZOHO CORPORATION B. V. Hoogoorddreef 15, 1101BA Amsterdam, Niederlande und ZOHO CORPORATION PVT. LTD., Estancia IT Park, Plot No. 140 & 151, GST Road, Vallancherry Village, Chengalpattu Taluk, Kanchipuram District 603 202, Indien	CRM/ERP auf europäischen Servern von zoho.eu	technischer Support: erfolgt durch ZOHO CORPORATION PVT. LTD.: Standdartvertrags-klauseln vereinbart
5	Google Ireland Limited Gordon House, Barrow Street Dublin 4 Irland	Google G Suite, CRM	Standartvertrags-klauseln vereinbart

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterauftragung gestattet.

(4) Eine weitere Auslagerung durch den Unterauftragnehmer ist insoweit nicht gestattet.

(5) Gem. Abs. 2 hat der Auftragnehmer das Recht, bereits bestehende Unterauftragnehmer zu ersetzen oder neue Unterauftragnehmer zu beauftragen. Dieses Recht besteht insbesondere dann, sofern dies im Einzelfall notwendig ist. Jede Beauftragung eines neuen Unterauftragnehmers ist dem Auftraggeber im Voraus mitzuteilen, woraufhin dem Auftraggeber ein Widerspruchsrecht zusteht. Sofern der Auftraggeber sein Widerspruchsrecht ausübt, steht dem Auftragnehmer zur Wahrung insbesondere seiner wirtschaftlichen Interessen das Recht zu, den Hauptvertrag mit dem Auftragnehmer zu kündigen. Dies gilt insbesondere, sofern dem Auftragnehmer infolge des Widerspruchs ein Verzicht auf dieses/diese Unterauftragsverhältnis/e aufgrund von Mehrkosten oder sonstigen Mehraufwand nicht zumutbar ist.

(6) Sofern Unterauftragnehmer personenbezogene Daten in ein Drittland übermittelt, stellt der Auftragnehmer sicher, dass dies auf Grundlage von geeigneten Schutzvorschriften, wie einem Angemessenheitsbeschluss der EU-Kommission gem. Art 45 Abs. 3 DSGVO, Standarddatenschutzklauseln sowie auf Grundlage von Art. 49 Abs. 1 lit. b DSGVO stattfindet.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem

Auftraggeber auf Aufforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, erfolgt durch die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DSGVO sowie unter Umständen aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen.

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.:

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung.
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich schriftlich oder alternativ in Textform.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung von Daten und Rückgabe von Datenträgern

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers 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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber, spätestens mit Beendigung der Leistungsvereinbarung, hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber

auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Anlage

Technische und organisatorische Maßnahmen (TOM)

Nachfolgend stellt der Auftragnehmer die technischen und organisatorischen Maßnahmen dar, die jeweils in unserem Verantwortungsbereich oder im Rechenzentrum des unter Art. 6 Abs. 2 genannten Unterauftragnehmers getroffen worden sind.

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

A) Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen (geeignete Maßnahmen, um Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet, zu verwehren):

- ⇨ Schließsystem mit Codesperre
- ⇨ Chipkarten / Transpondersysteme

- ⇨ Besucher: Anmeldung und Protokoll am Empfang
- ⇨ Besucher nur in Begleitung durch Mitarbeiter
- ⇨ Empfang, 24/7 Security im Eingangs und Außenbereich

Die eigenen Büro- und Geschäftsräume des Auftragnehmers sind mit verschlossenen Türen und Schließsystemen versehen, so dass ein unbefugter Zutritt von Dritten wirksam unterbunden werden kann. Während der Geschäftszeiten gibt es eine Besucherregelung, die unter anderem vorsieht, dass jeder Besucher sich nicht ohne Begleitung durch die Büroräume bewegen kann.

Im Rechenzentrum sind folgende Maßnahmen getroffen:

- ⇨ Zutritt zum Gebäude nur durch Legitimation über eine persönliche Code-Karte (RFID)
- ⇨ Besucher können nur nach vorheriger Anmeldung das Gebäude betreten. Während des gesamten Aufenthalts begleitet mindestens ein Mitarbeiter die Gäste, welche einen gesonderten Ausweis erhalten, der jedoch keinen Zutritt zu geschützten Bereichen ermöglicht
- ⇨ Wachschutz 24h/Tag, 365 Tage im Jahr, Kontrollgänge werden durchgeführt
- ⇨ Alarmanlagensystem mit Aufschaltung auf örtliche Polizeidienststellen
- ⇨ abgesichertes Rechenzentrum mit eigenem Eingang, geschützt durch speziell codierte Zugangskarten (personenbezogen, RFID)
- ⇨ Schleusensystem, Kameraüberwachung und Protokollierung von Zugängen sichern den Aufenthalt ab
- ⇨ Serverracks sind verschlossen und werden nur im Bedarfsfall geöffnet. Die Schlüssel zu den Racks liegen in einem verschlossenen Safe, zu dem nur autorisierte Personen Zugang haben

B) Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- ⇨ Login mit Benutzername sowie geeignetem Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, bedarfsorientierter Wechsel des Kennworts)
- ⇨ Einsatz aktueller Antivirus-Client (Endpoint-Security)
- ⇨ Einsatz aktueller Antivirus-Software für mobile Endgeräte (insbesondere Notebooks)
- ⇨ Einsatz von VPN-Verbindungen bei Remotezugriffen
- ⇨ Sperre von externen Schnittstellen (insb. USB)
- ⇨ Automatische Bildschirm- bzw. Desktopsperre
- ⇨ Verschlüsselung von Datenträgern (insb. Festplatten)
- ⇨ Verschlüsselung von Datenträgern in mobilen Endgeraten (u.a. Notebooks, Tablets, Smartphones)
- ⇨ Einsatz moderner Firewall Technologien (Bsp. Application Layer Firewall, Intrusion Detection System, Intrusion Prevention System etc.)
- ⇨ Verwalten von Benutzerberechtigungen durch Systemadministratoren
- ⇨ Erstellen von Benutzerprofilen (insbesondere Einrichtung eines Benutzerstammsatzes pro User)
- ⇨ Richtlinie für die Erstellung und Verwendung sicherer Passwörter sowie Logindaten
- ⇨ Richtlinie für einen aufgeräumten Schreibtisch (Clean-Desk-Policy

Alle vorstehenden Punkte werden durch den Auftragnehmer erfüllt.
Alle IT-Systeme und Applikationen des Auftragnehmers sind erst nach vorheriger Authentifizierung zugänglich.

Die Mindestpasswortlänge beträgt derzeit 20 Zeichen. Passwörter müssen zudem komplex sein (Groß-/Kleinbuchstaben, Ziffern, Sonderzeichen).

Alle Server-Systeme sind mit Firewall-Technologie (Hardware) gesichert. Auf allen Systemen ist moderne Antiviren-Software installiert, bei der eine regelmäßige Aktualisierung gewährleistet ist.

C) 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.

- ⇨ Aktenvernichter (Sicherheitsstufe 5 nach DIN 66399)
- ⇨ Einsatz externer Datenvernichter zur Löschung / Vernichtung von Daten und Datenträgern wie Festplatten, PCs, Notebooks und sonstiger Speichermedien (zertifiziert, AVV erforderlich)
- ⇨ Protokollierung der Zugriffe auf Anwendungen, insbesondere von Eingabe, Änderung und Löschung von Daten
- ⇨ Einsatz eines Berechtigungskonzepts inkl. Rollendefinition
- ⇨ Richtlinie zur Verwendung von Datenverarbeitungsanlagen bzw. Datenträgern (u.a. Verbot zur Nutzung privater Geräte)
- ⇨ Kontrolle der ordnungsgemäßen Löschung von Daten und Vernichtung von Datenträgern anhand von Stichproben
- ⇨ minimale Anzahl an Administratoren (Begrenzung auf die unbedingt erforderliche Anzahl)

Alle vorstehenden Punkte werden vom Auftragnehmer erfüllt. Die Protokollierung erfolgt im jeweiligen System oder, sofern technisch nicht möglich, an separater Stelle.

Ein Berechtigungskonzept ist im Einsatz. Alle Applikationen und Datenbanken sehen eine differenzierte Einräumung von Berechtigungen vor (Profile, Rollen, Transaktionen und Objekte). Im Verantwortungsbereich des Auftragnehmers werden Berechtigungen ausschließlich nach dem „Need-to-know-Prinzip“ vergeben.

Bei ausscheidenden Mitarbeitenden wird dafür Sorge getragen, dass die Berechtigungen rechtzeitig wieder entzogen werden.
Die Zugriffsrechte von Datenbanknutzern sind auf das Notwendigste reduziert, um die Integrität der Daten bestmöglich zu gewährleisten.

D) Trennungskontrolle

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

Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken:

- ⇨ Trennung von Produktiv- und Testumgebung
- ⇨ Physikalische Trennung von Systemen, Datenbanken und Datenträgern
- ⇨ Strikte räumliche Trennung von Arbeitsplätzen und Servern
- ⇨ Mandantenfähigkeit relevanter Anwendungen
- ⇨ Steuerung über Berechtigungskonzept
- ⇨ Festlegung/Zuweisung von Datenbankrechten
- ⇨ Datensätze sind mit Zweckattributen versehen (so dass eine zweckgebundene Verarbeitung jederzeit gewährleistet ist)

Eine Trennung der Daten ist so jederzeit gewährleistet.

E) Pseudonymisierung (Art. 32 Abs. 1 lit. DSGVO, Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten erfolgt 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:

- ⇨ Soweit Pseudonymisierung verwendet wird: Trennung der jeweiligen Zuordnungsdaten und Aufbewahrung in getrennten und abgesicherten Systemen (unter Verwendung einer geeigneten Verschlüsselung

Eine Pseudonymisierung wird je nach Schutzbedarf der personenbezogenen Daten angewendet.

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

A) Weitergabekontrolle

Maßnahmen, die gewährleisten, 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, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- ⇨ Einsatz von VPN geschützten Verbindungen (Virtual Private Network)
- ⇨ E-Mail-Verschlüsselung (i.d.R. SSL/TLS)
- ⇨ Bereitstellung von Daten mittels verschlüsselter Verbindungen wie sftp, https etc.
- ⇨ https verschlüsselte Datenübertragung über Website und Webapp
- ⇨ Einsatz von aktueller Firewall

Alle vorstehenden Punkte werden vom Auftragnehmer erfüllt.
Der Auftragnehmer gibt grundsätzlich keine Daten an Dritte weiter, sofern dies nicht zu den Vertragspflichten gegenüber dem Auftraggeber gehört.

Es werden verschlüsselte Verbindungen zur Nutzung der Applikation verwendet.

B) Eingabekontrolle

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

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:

- ⇨ Stichproben und Anlass basierte Kontrolle von Protokollen
- ⇨ Sicherstellung durch Übersicht mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
- ⇨ Die Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten wird durch individuelle Benutzernamen mit einem Benutzer gewährleistet
- ⇨ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ⇨ Klare Zuständigkeiten für Vornahme/Kontrolle/Protokollierung von Löschungen
- ⇨ Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten (durch Logfiles). Der Zugriff auf Datenbestände erfolgt anhand von Berechtigungen. Das

Verfahren gewährleistet, dass keine Datenveränderungen unbemerkt vorgenommen werden können

Die Eingabe, Änderung und Löschung von Daten werden, soweit technisch und unter angemessenem Aufwand möglich, protokolliert. Vornahmen von Eingaben oder Datenveränderungen können Nutzern zugeordnet werden.

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

Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zur Datensicherung (physikalisch/logisch):

- ⇨ Moderne Feuer- und Rauchmeldeanlage (Büros / Rechenzentrum)
- ⇨ Inertgas-Löschanlage (Rechenzentrum)
- ⇨ Klimatisierter Serverraum (Rechenzentrum)
- ⇨ USV (Unterbrechungsfreie Stromversorgung, insbesondere Rechenzentrum)
- ⇨ RAID System (gespiegelte Festplatten, Rechenzentrum)
- ⇨ Serverräume sind hochwassergeschützt errichtet (Rechenzentrum)
- ⇨ Videoüberwachung Serverraum (Rechenzentrum)
- ⇨ Alarmmeldung bei unberechtigtem Zutritt zu Serveräumen (Rechenzentrum)
- ⇨ Sprinkleranlage (Rechenzentrum)
- ⇨ Brandklasseneinteilung (Kennzeichnung besonders gefährdeter Räume, Rechenzentrum)
- ⇨ Feuerlöscher an/in den PC-Arbeitsräumen (Rechenzentrum / Büros)
- ⇨ Einsatz eines geeigneten Antivieren Programms
- ⇨ Bestehendes Backup & Recovery-Konzept
- ⇨ Regelmäßige Test zur Datenwiederherstellung und Protokollierung der Ergebnisse
- ⇨ Backups und Sicherungsmedien werden örtlich getrennt aufbewahrt
- ⇨ Keine sanitären Anschlüsse im oder oberhalb der Serverräume
- ⇨ Vorliegen eines geeigneten Notfallplans
- ⇨ Getrennte Partitionen für Betriebssysteme und Daten

Alle eingesetzten Serversysteme arbeiten mit gespiegelten Festplattensystemen (RAID). Das Backup-Konzept sieht mindestens eine tägliche inkrementelle und eine wöchentliche Vollsicherung vor. Die Backups werden örtlich getrennt aufbewahrt. Ausgelagerte Backups werden zudem verschlüsselt.

Alle Serversysteme im Rechenzentrum verfügen über eine unterbrechungsfreie Stromversorgung (Akkus und Dieselgeneratoren).

Ein Inergen-Gas basierendes Feuerlöschsystem mit Aufschaltung auf örtliche Feuerleitstellen ist im Einsatz.

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

A) Datenschutz-Management

- ⇨ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Intranet, Collaboration-Software etc.)

- ⇨ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt
- ⇨ Bestehende Sicherheitszertifizierung nach ISO 27001, BSI-Grundschutz, ggf. weitere oder sonstige Zertifizierungen, u.a. VdS-Zertifikat)
- ⇨ Externer Datenschutzbeauftragter bestellt – dessen Kontaktdaten sind auf der Website des Verantwortlichen jederzeit einsehbar
- ⇨ Regelmäßige und dem individuellen Bedarf angepasste Schulung der Mitarbeiter zum Datenschutz
- ⇨ Durchführung Datenschutz-Folgenabschätzung soweit erforderlich
- ⇨ Erfüllung sämtlicher Informationspflichten nach Artt. 13 und 14 DSGVO
- ⇨ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen durch Betroffene

Alle vorgenannten Maßnahmen werden umgesetzt und regelmäßig überprüft und bei Änderungsbedarf entsprechend angepasst. Die getroffenen Maßnahmen werden entsprechend protokolliert.

B) Incident-Response-Management

- ⇨ Einsatz von Firewall und regelmäßige Aktualisierung (s. auch Zugriffskontrolle)
- ⇨ Einsatz von Spamfilter und regelmäßige Aktualisierung
- ⇨ Einsatz geeigneter sowie regelmäßig aktualisierter Antivirus-Software (mit Virenscanner)
- ⇨ Einsatz eines Intrusion Detection Systems (IDS) zur Aufdeckung von Sicherheitsvorfällen (Netzwerk)
- ⇨ Einsatz eines Intrusion Prevention Systems (IPS) zur Behebung und Einleitung von Gegenmaßnamen bei Sicherheitsvorfällen
- ⇨ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (dieser berücksichtigt ebenfalls Meldepflicht gegenüber Aufsichtsbehörde und Betroffenen)
- ⇨ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- ⇨ Einbindung von DSB und der IT-Sicherheit in Sicherheitsvorfälle und Datenpannen
- ⇨ Dokumentation von Sicherheitsvorfällen und Datenpannen (u.a. Ticketsystem)
- ⇨ Definierter Prozess sowie Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

Sämtliche genannten Maßnahmen werden umgesetzt sowie die Verfahren in einem angemessenen Umfang auf Aktualität und insbesondere deren Wirksamkeit hin überprüft.

C) Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
Privacy by design & Privacy by default:

- ⇨ Die Gestaltung und Voreinstellungen von Softwares und anderen Verarbeitungsvorgängen gewährleisten, dass lediglich solche personenbezogenen Daten verarbeitet, die für den jeweiligen Zweck auch tatsächlich erforderlich sind
- ⇨ Technische Maßnahmen gewährleisten die einfache Ausübung des Widerrufsrechts von Betroffenen

D) Auftragskontrolle (Outsourcing)

- ⇨ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen sowie der Dokumentation (Vorabüberzeugungspflicht)
- ⇨ Sorgfältige Auswahl des Auftragnehmers (insbesondere hinsichtlich Datenschutz und Datensicherheit)

- ⇨ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln
- ⇨ Weisungen an den Auftragnehmer erfolgen grundsätzlich ausschließlich schriftlich oder in Textform (mündliche Weisungen werden zusätzlich entsprechend schriftlich oder in Textform erteilt)
- ⇨ Verpflichtung der Mitarbeiter des Auftragnehmers auf den Datenschutz & Vertraulichkeit
- ⇨ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen einer Bestellpflicht
- ⇨ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- ⇨ Regelung zum Einsatz weiterer Subunternehmer
- ⇨ Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus bei längerer Zusammenarbeit
- ⇨ Sicherstellung der Löschung /Vernichtung von Daten nach Beendigung des Auftrags

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters und Vorabüberzeugungspflicht.

Stand: 02.2023