

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Vertragsparteien

Diese Vereinbarung wird zwischen dem Auftraggeber/Vertragspartner (nachfolgend „Auftraggeber“) und der KRISS MICUS 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 mit dem Auftraggeber geschlossenen Vertrag über entsprechende Nutzungsrechte an der Software KRISS MICUS (im Folgenden Leistungsvereinbarung). Der Auftraggeber nutzt hierbei die Buchhaltungssoftware Buchhaltung Butler als White-Label-Lösung. 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 Vertragsinhalts

(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 Mitgliedstaat 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 Art. 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 Benutzerverwaltung/-berechnung sowie ggf. im Rahmen der Buchhaltung)

- Vorname und Nachname
- ggf. Poison / Funko

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 Vorbereitungsstätigkeiten, 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 oder ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Dies gilt jedoch nur, soweit dies für den Auftragnehmer wirtschaftlich und für das angestrebte beziehungsweise tatsächlich erforderliche Schutzniveau angemessen sowie erforderlich ist.

2) Der Auftragnehmer stellt die Sicherheit gemäß Artikel 28 Absatz 3 Buchstabe c sowie 32 DSGVO insbesondere in Verbindung mit Artikel 5 Absatz 1, Absatz 2 DS GVO 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 Artikel 32 Absatz 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 der Leistungsumfang umfasst, sind Löschkonzepte, 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 gemäß Artikel 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 gemäß Artikel 38 und 39 DSGVO ausübt. Die aktuellen Kontaktdaten sind auf der Website des Auftragnehmers leicht zugänglich .

b) Die Wahrung der Vertraulichkeit gemäß Artikel 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, darf 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 gemäß Artikel 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 Ordnungswidrigkeiten- 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 Ordnungswidrigkeiten- 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 Artikel 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.

(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 Driland: Angaben zu geeigneten Garantien
1	ABBY 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.-Vor Anmeldung	-
3	Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy L-1855 Luxembourg	Web Hosting (SaaS) am Serverstandort Frankfurt a. M.	-
4	ZOH0 CORPORATION B. V. Hoogoorddreef 15, 1101 BA Amsterdam, Niederlande und ZOH0 CORPORATION PVT. LTD., Estancia IT Park, Plot No. 140 & 151, GST Road, Vallanchery Village, Chengalpattu Taluk, Kanchipuram District 603 202, Indien	CRM/ERP auf europäischen Servern von zoho.eu	technischer Support: erfolgt durch ZOH0 CORPORATION PVT. LTD.: <u>Standardvertrag klauseln vereinbart</u>
5	Google Ireland Limited Gordon House, Barrow Street Dublin 4 Ireland	Google G Suite, CRM	<u>Standardvertrag klauseln vereinbart</u>

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

(5) Gemäß 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 Auftraggeber zu kündigen. Dies gilt insbesondere, sofern dem Auftragnehmer infolge des Widerspruchs ein Verzicht auf dieses/diese Unterauftragsverhältnis/e aufgrund von Mehrkosten oder sonstigem Mehraufwand nicht zumutbar ist.

(6) Sofern Unterauftragnehmer personenbezogene Daten in ein Drittland übermitteln, stellt der Auftragnehmer sicher, dass dies auf Grundlage von geeigneten Schutzvorrichtungen, wie einem Angemessenheit Beschluss der EU-Kommission gemäß 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 gemäß Art. 40 DSGVO sowie unter Umständen aktuelle Testate, Berichte oder Berichte Auszüge 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-Folgenabschätzungen und vorherigen Konsultationen. Hierzu gehören unter anderem:

- 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 Verletzung Ereignissen ermöglichen.

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden.

c) die Verpflichtung, den 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 sind oder auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggeber

(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, dass eine Weisung verstößt 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 Nutzung Ergebnisse 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 / Transponder System
- Besucher: Anmeldung und Protokoll am Empfang
- Besucher nur in Begleitung durch Mitarbeiter
- Empfang, 24/7 Security im Eingang 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 Besuchsregelung, die unter anderem vorsieht, dass jeder Besucher sich ohne Begleitung durch die Büroräume bewegen kann.

Im Rechenzentrum sind folgende Maßnahmen getroffen:

- Zutritt zum Gebäude nur durch Legion 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 Wracks 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:

- Ein Login mit Benutzername sowie geeignetem Kennwort Verfahren (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 Remote Zugriffen
- Sperre von externen Schnittstellen (insbesondere USB)
- Automatischer Bildschirm- bzw. Desktopsperre
- Verschlüsselung von Datenträgern (insbesondere Festplatten)
- Verschlüsselung von Datenträgern in mobilen Endgeräten (u.a. Notebooks, Tablets, Smartphones)
- Einsatz moderner Firewall-Technologien (Beispiel: 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 Berechnungen rechtzeitig wieder entzogen werden.

Die Zugriffsrechte von Datenbank-Nutzern 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 zur Sicherstellung, dass personenbezogene Daten bei elektronischer Übertragung, Transport oder Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass festgestellt werden kann, an welche Stellen eine Übermittlung vorgesehen ist:

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

Der Auftragnehmer gibt grundsätzlich keine Daten an Dritte weiter, außer dies ist Teil der Vertragspflichten gegenüber dem Auftraggeber. Verschlüsselte Verbindungen werden zur Nutzung der Applikation verwendet.

B) Eingabekontrolle

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

- Stichproben- und anlassbasierte Kontrolle von Protokollen
- Sicherstellung durch Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten basierend auf einem Berechtigungskonzept
- Klare Zuständigkeiten für Vornahme, Kontrolle und Protokollierung von Löschungen
- Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschungen (durch Logfiles). Zugriff auf Datenbestände basiert auf Berechtigungen, um unbemerkte Datenveränderungen zu verhindern.

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

Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Maßnahmen zum Schutz der Daten gegen zufällige Zerstörung oder Verlust:

- Moderne Feuer- und Rauchmeldeanlage (Büros / Rechenzentrum)
- Inertgas-Löschanlage (Rechenzentrum)
- Klimatisierter Serverraum (Rechenzentrum)
- USV (Unterbrechungsfreie Stromversorgung, insbesondere Rechenzentrum)
- RAID-System (gespiegelte Festplatten, Rechenzentrum)
- Serverräume sind hochwasser geschützt (Rechenzentrum)
- Videoüberwachung im Serverraum (Rechenzentrum)
- Alarmmeldung bei unberechtigtem Zutritt zu Serverräumen (Rechenzentrum)
- Sprinkleranlage (Rechenzentrum)
- Brandklasseneinteilung (Kennzeichnung gefährdeter Räume, Rechenzentrum)
- Feuerlöscher in PC-Arbeitsräumen (Rechenzentrum / Büros)

- Einsatz eines geeigneten Antiviren-Programms
- Bestehendes Backup & Recovery-Konzept
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Backups und Sicherungsmedien werden örtlich getrennt aufbewahrt
- Keine sanitären Anschlüsse im oder oberhalb der Serverräume
- Vorhandensein eines geeigneten Notfallplans
- Getrennte Partitionen für Betriebssysteme und Daten

Server Systeme arbeiten mit gespiegelten Festplatten Systemen (RAID) und haben ein Backup-Konzept mit täglicher inkrementeller und wöchentlicher Vollsicherung. Backups werden örtlich getrennt und verschlüsselt aufbewahrt. Die Server Systeme im Rechenzentrum verfügen über unterbrechungsfreie Stromversorgung (Akkus und Dieselgeneratoren) sowie ein inertes Gas basiertes Feuerlöschsystem mit Anbindung an örtliche Feuerwehr Leitstellen.

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

A) Datenschutz-Management

Zusammenfassend beinhaltet das Datenschutz-Management folgende Maßnahmen:

- Zentrale Dokumentation aller Datenschutzverfahren und -regelungen, zugänglich für Mitarbeiter je nach Bedarf und Berechtigung (z.B. via Intranet, Collaboration-Software).
- Jährliche Überprüfung der Wirksamkeit technischer Schutzmaßnahmen.
- Bestehende Sicherheitszertifizierungen (ISO 27001, BSI-Grundsicherheitszertifikat, VDS-Zertifikat).
- Bestellung eines externen Datenschutzbeauftragten, dessen Kontaktdaten öffentlich einsehbar sind.
- Regelmäßige, bedarfsangepasste Mitarbeiter-Schulungen zum Datenschutz.
- Durch Einführung von Datenschutz-Folgenabschätzungen, wenn erforderlich.
- Erfüllung der Informationspflichten gemäß Art. 13 und 14 DSGVO.
- Formalisierter Prozess zur Bearbeitung von Auskunftersuchen von betroffenen Personen.

B) Incident-Response-Management

Das Incident-Response-Management umfasst:

- Einsatz und regelmäßige Aktualisierung von Firewalls, Spamfiltern und Antivirus-Software.
- Einsatz eines Intrusion Detection Systems (IDS) und eines Intrusion Prevention Systems (IPS).
- Dokumentierter Prozess zur Erkennung, Meldung und Bearbeitung von Sicherheitsvorfällen und Datenpannen, einschließlich Meldepflichten.
- Einbindung des Datenschutzbeauftragten und der IT-Sicherheit bei Sicherheitsvorfällen.
- Dokumentation von Sicherheitsvorfällen und Datenpannen (z.B. über ein Ticketsystem).

- Definierte Prozesse und Verantwortlichkeiten für die Nachbearbeitung von Sicherheitsvorfällen und Datenpannen.

C) Datenschutzfreundliche Voreinstellungen (Privacy by Design & Privacy by Default)

- Gestaltung und Voreinstellungen von Software und Verarbeitungsvorgängen so, dass nur die für den jeweiligen Zweck erforderlichen personenbezogenen Daten verarbeitet werden.
- Technische Maßnahmen zur Gewährleistung der einfachen Ausübung des Widerrufsrechts von Betroffenen.

D) Auftragskontrolle (Outsourcing)

Für das Outsourcing gelten folgende Richtlinien:

- Vorabprüfung der Sicherheitsmaßnahmen und Dokumentation des Auftragnehmers.
- Sorgfältige Auswahl des Auftragnehmers, insbesondere hinsichtlich Datenschutz und Datensicherheit.
- Abschluss notwendiger Vereinbarungen zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln.
- Weisungen an den Auftragnehmer erfolgen grundsätzlich schriftlich oder in Textform.
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datenschutz und Vertraulichkeit.
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer, falls erforderlich.
- Vereinbarung effektiver Kontrollrechte gegenüber dem Auftragnehmer.
- Regelungen 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 Vorab-Überzeugung Pflicht.

Stand: 02.2023