Auftragsverarbeitungsvertrag

V.20180522

zwischen **Ihnen**

im Sinne der DS-GVO „Verantwortlicher“, nachstehend **Auftraggeber** genannt

und der

hundertzehn GmbH

Aeschstrasse 131F

8123 Ebmatingen

Schweiz

im Sinne der DS-GVO „Auftragsverarbeiter“ - nachstehend **Auftragnehmer** genannt

Inhalt

Präambel

Der Auftragnehmer verarbeitet für den Auftraggeber entsprechend des zwischen diesen Parteien bestehenden Vertrags *(vgl. Ziff.1, Gegenstand)* (**„Leistungsvertrag**“) personenbezogene Daten.

Die Parteien stellen fest, dass möglicherweise die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung „**DS-GVO**“) eine Anwendung auf die vereinbarte Datenverarbeitung findet (wie z.B. bei Verarbeitung von personenbezogenen Daten von in der EU wohnhaften Personen). Daher einigen sich die Parteien, dass die Verarbeitung von Personendaten auf der Grundlage dieses Auftragsverarbeitungsvertrags („**AVV**“) erfolgt, welcher die Bestimmungen der DS-GVO berücksichtigt. Die Datenverarbeitung muss ausserdem die einschlägigen Schweizer Datenschutzregeln gemäss geltendem Datenschutzgesetz (DSG) sicherstellen, sofern diese durch Einhaltung der DS-GVO Vorgaben nicht ohnehin erfüllt werden.

Gegenstand

Der Gegenstand des Auftrags ergibt sich aus der Verfahrensbeschreibung des Produkts MOCO („Leistungsbeschrieb“):

MOCO ist eine B2B Cloud Software für kleine bis mittlere Dienstleistungsunternehmen, die auf Projektbasis arbeiten. MOCO ist die Abkürzung von "MObile COmpany" und umfasst die Bereiche Akquise & Angebote, Projektcontrolling, Ressourcenplanung, Zeiterfassung, Abrechnung und Kontaktverwaltung. Darüber hinaus liefern übergeordnete Berichte Zahlen und Fakten visualisiert zur Entscheidungsgrundlage für Geschäftsleitung und leitende Angestellte. Querschnittsthemen wie Urlaub und Arbeitszeiten finden ebenso Betrachtung. Mobil-Apps und Integrationen in andere Cloud-Lösungen runden das Produkt ab. Bis auf wenigen Ausnahmen kann das Produkt modulweise verwendet werden – die komplette Nutzung aller Bereiche ist keine Voraussetzung.

Dauer

Der Auftrag ist unbefristet erteilt und kann von beiden Parteien jederzeit (MOCO Cloud) bzw. mit einer Frist von 3 Monaten (MOCO Private Cloud) zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

Konkretisierung des Auftragsinhaltes

1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

- Speicherung der Daten zur Erbringung der Leistungen gemäss *Leistungsbeschrieb und Leistungsvertrag/AGB (Allgemeine Geschäftsbedingungen für die Nutzung des Dienstes MOCO)*

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet in der Schweiz statt. Ein angemessenes Datenschutzniveau wurde von der EU-Kommission in einer förmlichen Entscheidung für die Schweiz festgestellt: 2000/518/EC.

2) Art der Daten

Der Auftragnehmer führt selbst keine aktive Verarbeitung von Personendaten durch. Der Zugriff auf die Daten erfolgt nur zur Behebung von Fehlern gemäss AGB. Im Rahmen dieser Fehlerbehebung ist es möglich, dass der Auftragnehmer Zugriff auf Daten des Auftraggebers erhält. Davon können auch Personendaten betroffen sein.

Der Auftraggeber bestätigt, dass folgende Personendaten Gegenstand der Bearbeitung bilden können.

- Personal Stammdaten
- Kunden Stammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail, IP Adresse)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Planungs- und Steuerungsdaten
- Akquisitionsdaten (CRM)

Der Auftraggeber bestätigt, dass die folgenden Personendaten-Kategorien Gegenstand der Bearbeitung bilden können:

- Kunden
- Interessenten
- Mitarbeiter
- Lieferanten
- Ansprechpartner

Der Auftraggeber stellt sicher, dass keine Daten nach Art. 9 DS-GVO gespeichert werden. Dies umfasst die folgenden Datenkategorien:

Rassische und ethnische Herkunft / politische Meinungen / religiöse oder weltanschauliche Überzeugungen / Gewerkschaftszugehörigkeit / genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

Bei der Speicherung solcher Daten ist der Auftragnehmer unverzüglich zu informieren. Der Auftragnehmer behält sich vor, in diesem Fall den Vertrag unverzüglich, einseitig und ohne Kostenfolge sofort zu beenden.

Technische / Organisatorische Massnahmen

1) Der Auftragnehmer hat die erforderlichen technischen und organisatorischen Massnahmen vor Beginn der Verarbeitung in Kraft gesetzt.

2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 litt. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO hergestellt. 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 wurden der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO berücksichtigt [Einzelheiten in Anlage 1].

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.

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 unmittelbar 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 unmittelbar durch den Auftraggeber sicherzustellen. Der Auftragnehmer unterstützt den Auftraggeber gegen Entschädigung bei der Erbringung dieser Leistungen.

Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäss Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

1) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten nach DS-GVO verpflichtet. Als Ansprechpartner wird: Tobias Miesel, hundertzehn GmbH, Aeschstrasse 131F, 8123 Ebmatingen, Schweiz benannt. Dieser kann unter privacy@mocoapp.com erreicht werden.

2) Die Wahrung der Vertraulichkeit gemäss Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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.

3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Massnahmen gemäss Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage 1].

4) Soweit der Auftraggeber 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 Auftragnehmer ausgesetzt ist, wird ihn der Auftragnehmer nach besten Kräften zu unterstützen. Dem Auftragnehmer steht für diese Unterstützung eine aufwandsbasierte Entschädigung zu.

5) 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 Person gewährleistet wird.

6) Nachweisbarkeit der getroffenen technischen und organisatorischen Massnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrages.

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 z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Massnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ergreift zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmassnahmen.

2) Die folgenden Unterauftragnehmer sind für die Erbringung der Leistungen eingebunden:

    a) Intercom (USA, Auftragsverarbeitung gem. Art. 28 DS-GVO). Intercom registriert Nutzungsdaten (Vorname, Nachname, E-Mail, erstes & letztes Anmeldedatum via Browser, Mobilgerät, API, CardDAV und MOCO-Browsererweiterung, Browser, Browserversion, Sprache, Betriebssystem, Bildschirmbreite, letzter Kontakt, letzte gelesene E-Mail, Anzahl Anmeldungen, Zugriffsrechte in MOCO), mit denen der Betreiber dem Benutzer von MOCO eine bestmögliche und persönliche Betreuung bieten kann, opt-out möglich.

    b) Stripe (USA, Auftragsverarbeitung gem. Art. 28 DS-GVO). Stripe bietet die Abwicklung von Lastschrift und Kreditkartenbelastungen als Service zur Verfügung. Alle Kreditkartendaten werden seitens Stripe gespeichert.

    c) Ably (UK, Auftragsverarbeitung gem. Art. 28 DS-GVO). Um Kunden von MOCO neue Informationen oder geänderte Daten mitzuteilen ohne das Neuladen des Browsers notwendig ist, werden solche Aktualisierungen über WebSockets im Hintergrund ausgeliefert. Ably stellt die Infrastruktur zur Verfügung. Die Daten werden vor der Übertragung an Ably verschlüsselt.

d) Amazon (Irland & Deutschland, Auftragsverarbeitung gem. Art. 28 DS-GVO). Alle Daten (Datenbank) und Dateien (Belege, Rechnungen, Uploads) werden regelmässig auf externen Datenspeichern gesichert. Die Daten werden auf den Systemen des Auftragnehmers verschlüsselt und auf Amazon-S3-Speicher abgelegt. Der Schlüssel liegt nur in der Hand des Auftragnehmers und ist dadurch dem Zugriff ausländischer Behörden entzogen; keine Option.

e) Zapier (USA, Auftragsverarbeitung gem. Art. 28 DS-GVO). Zapier stellt ein Workflow-System zur Verfügung um verschiedene Webservices über eine einheitliche Schnittstelle miteinander verbinden zu können. Zapier kann optional durch den Auftraggeber verwendet werden (opt-in).

f) Netskin GmbH und IWB: hundertzehn betreibt die notwendige IT Infrastruktur für die MOCO Cloud auf zwei identischen Systemen in einem Rechenzentrum der IWB. Dazu hat sich die hundertzehn bei dem RZ Anbieter IWB über die Netskin GmbH eingemietet und individuell konfigurierte Serverhardware bei Netskin angemietet (Managed Individual Server). Vom RZ Anbieter IWB werden die infrastrukturellen Dienstleistungen wie Strom, Klima, Überwachung und eine performante sowie gespiegelte Netzwerkanbindung bezogen. Die IWB (https://www.IWB.ch/) ist ein Institut des öffentlichen Rechts (IOR) mit Sitz in Basel. Die IWB ist neben dem Energie-Kerngeschäft auch ein Internet Service Provider für Firmenkunden und betreibt Rechenzentren in der Schweiz.

g) Die Netskin GmbH ist ein Schweizer Anbieter für Netzwerkdienstleistungen mit Sitz in Freienbach/SZ

3) Die Unterauftragnehmer erbringen die im Zusammenhang mit der Hauptleistung notwendigen Nebenleistungen, die für das korrekte und vertragsgemässe Funktionieren der Lösung notwendig sind. Der Auftraggeber nimmt davon Kenntnis und ist ausdrücklich mit der Vergabe der beschriebenen Aufgaben einverstanden.

4) Erbringt der Unterauftragnehmer die vereinbarte Leistung ausserhalb der EU/des EWR, der Schweiz stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Massnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

Information des Auftraggebers

1) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen.

2) Der Nachweis solcher Massnahmen, kann erfolgen durch

a) die Einhaltung genehmigter Verhaltensregeln gemäss Art. 40 DS-GVO;

b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäss Art. 42 DS-GVO;

c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

e) Für Kosten, die dem Auftragnehmer durch die Ausübung der Kontrollrechte und durch die Erbringung der geforderten Nachweise entstehen, kann der Auftragnehmer eine Vergütung beanspruchen.

Mitteilung bei Verstössen des Auftragnehmers

1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO 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 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 alle Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

Weisungsbefugnis des Auftraggebers

1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. 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.

Löschung und Rückgabe von personenbezogenen Daten

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.

Schlussbestimmungen

1) Diese Vereinbarung ersetzt keine bisher geschlossenen Vereinbarungen.

2) Nebenabreden oder Änderungen dieses Auftrags bedürfen der Schriftform.

3) Bezugnahmen auf Gesetze, Vorschriften, Dokumente und Anhänge gelten, soweit nicht ausdrücklich etwas Anderes bestimmt ist, für die Gesetze, Vorschriften, Dokumente und Anhänge in ihrer jeweils geltenden Fassung, also einschliesslich etwaiger Änderungen nach dem Vertragsdatum.

4) Die Anhänge sind integraler Bestandteil dieses Auftrags. Im Falle eines Widerspruchs zwischen den Bestimmungen des eigentlichen Vertragstextes und seiner Anhänge, gehen die Bestimmungen des Vertragstextes vor. Zwingende gesetzliche Vorschriften bleiben hiervon jedoch unberührt.

5) Sollten einzelne Bestimmungen dieses Auftrags unwirksam oder undurchführbar sein oder werden, so wird dadurch die Wirksamkeit der übrigen Teile nicht berührt. Die Parteien verpflichten sich in einem solchen Falle, die unwirksame oder undurchführbare Bestimmung durch eine sol-che zu ersetzen, die dem angestrebten Zweck in rechtlich zulässiger Weise möglichst nahekommt, gleiches gilt bei Regelungslücken.

6) Der Auftraggeber bestätigt, dass er die Bestimmungen der DS-GVO und des DSG vollumfänglich einhält und keine Inhalte zur Verarbeitung anbietet, welche die Verletzung der Persönlichkeitsrechte von Betroffenen bedeuten könnten.

7) Im Aussenverhältnis haftet der Auftraggeber gemäss den datenschutzrechtlichen Haftungsbestimmungen für den Schaden, der durch eine nicht gesetzeskonforme Verarbeitung verursacht wurde. Der Auftragnehmer haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen Verpflichtungen aus diesem Vertrag nicht nachgekommen ist oder gegen die Instruktionen des Auftraggebers gehandelt hat. Im Innenverhältnis haften die Parteien für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall eine Partei ganz oder

überwiegend auf Schadenersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit dies ihrem Anteil an der Verantwortung entspricht.

8) Der Auftragnehmer ist als in der Schweiz tätiges Unternehmen ausschliesslich gegenüber Schweizer Behörden auskunfts- und rechenschaftspflichtig. Die Unterstützung oder Befolgung behördlicher oder hoheitlicher Akte ausländischer Staaten und Behörden ist ihm strafrechtlich verboten (Art. 271 StGB).

9) Auf diesen Vertrag findet ausschliesslich das Schweizer Recht Anwendung. Gerichtsstand ist Zürich.

Anlage 1

Technische / Organisatorische Massnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle

  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen:

  ☒ Magnet- oder Chipkarten

  ☒ Schlüssel

  ☒ elektrische Türöffner

  ☒ Werkschutz bzw. Pförtner

  ☒ Alarmanlagen

  ☒ Videoanlagen

  ☒ Automatisches Zugangskontrollsystem

  ☒ Schliesssystem mit Codesperre

  ☒ Manuelles Schliesssystem

  ☐ Sicherheitsschlösser

  ☒ Schlüsselregelung (Schlüsselausgabe etc.)

  ☒ Protokollierung der Besucher

  ☒ Sorgfältige Auswahl von Reinigungspersonal

  ☒ Sorgfältige Auswahl von Wachpersonal

  ☐ Tragepflicht von Berechtigungsausweisen

  ☒ Besucher werden beaufsichtigt

  ☒ Jeder kennt jeden (KMU)

- Zugangskontrolle

  Keine unbefugte Systembenutzung:

  ☒ (sichere) Kennwörter

  ☐ automatische Sperrmechanismen

  ☒ Zwei-Faktor-Authentifizierung

  ☐ Verschlüsselung von Datenträgern

  ☒ Zuordnung von Benutzerrechten

  ☐ Erstellen von Benutzerprofilen

  ☒ Authentifikation mit Benutzername / Passwort

  ☒ Gehäuseverriegelungen

  ☒ Einsatz von VPN-Technologie

☐ Sperren von externen Schnittstellen (USB etc.)

☒ Verschlüsselung von mobilen Datenträgern

☐ Verschlüsselung von Smartphone-Inhalten

☐ Einsatz von zentraler Smartphone-Administrations-Software

☒ Einsatz von Anti-Viren-Software

☒ Verschlüsselung von Datenträgern in Laptops / Notebooks,

☒ Einsatz einer Hardware/Software-Firewall

- Zugriffskontrolle

  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

  ☒ Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte

  ☒ Protokollierung von Zugriffen

  ☐ Erstellen eines Berechtigungskonzepts

  ☒ Verwaltung der Rechte durch Systemadministrator

  ☒ Reduzierung der Anzahl der Administratoren

  ☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

  ☒ Sichere Aufbewahrung von Datenträgern

  ☒ Sicheres Wipen von Datenträgern vor Wiederverwendung

  ☒ Ordnungsgemässe Vernichtung von Datenträgern (DIN 66399)

  ☒ Verschlüsselung von Datenträgern

- Trennungskontrolle

  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden:

  ☒ Sandboxing

  ☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

  ☒ Softwarebasierte Mandantentrennung

  ☐ Erstellung eines Berechtigungskonzepts

  ☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden

  ☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei

  ☒ Festlegung von Datenbankrechten

- Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

  ☐ Die Verarbeitung personenbezogener Daten 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.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle

  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

  ☒ Verschlüsselung

  ☒ Virtual Private Networks (VPN)

  ☐ elektronische Signatur

  ☒ Weitergabe von personenbezogenen Daten in anonymisierter oder pseudonymisierter Form

  ☐ Erstellen einer Übersicht von regelmässigen Abruf- und Übermittlungsvorgängen

  ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

  ☐ Beim physischen Transport: sichere Transportbehälter/-verpackungen

- Eingabekontrolle

  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

  ☒ Protokollierung der Eingabe, Änderung und Löschung personenbezogener Daten

  ☒ Dokumentenmanagement

  ☒ Erstellen einer Übersicht, mit welchen Applikationen welche personenbezogenen Daten eingegeben, geändert und gelöscht werden können.

  ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung personenbezogener Daten durch individuelle Benutzernamen

  ☐ Aufbewahrung von Formularen, von denen personenbezogene Daten in automatisierte Verarbeitungen übernommen worden sind

  ☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung personenbezogener Daten auf Basis eines Berechtigungskonzepts

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle

  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:

  ☒ Backup-Strategie (online/offline; on-site/off-site)

☒ unterbrechungsfreie Stromversorgung (USV)

☒ Virenschutz

☒ Firewall

☒ Meldewege und Notfallpläne

☒ Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

☒ Klimaanlage in Serverräumen

☒ Schutzsteckdosenleisten in Serverräumen

☒ Feuer- und Rauchmeldeanlagen

☒ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen

☒ Erstellen eines Backup-Konzepts

☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen / privacy by design (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle

  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers:

  ☒ Eindeutige Vertragsgestaltung

  ☐ formalisiertes Auftragsmanagement

  ☐ strenge Auswahl des Dienstleisters

  ☐ Vorabüberzeugungspflicht

  ☒ Nachkontrollen