VERTRAG ÜBER DIE AUFTRAGSVERARBEITUNG PERSONENBEZOGENER DATEN

Zwischen dem CANEI-Kunden (der „**Verantwortliche**“), und der CANEI AG, Phoenixseestr. 22a, 44263 Dortmund (der „**Auftragsverarbeiter**“) wird der nachfolgende Vertrag geschlossen.

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsverarbeitungsverhältnis eingegangen. Dieser Vertrag über die Auftragsverarbeitung ("**AV-Vertrag**") i.S.d. Art. 28 Abs. 3 der Europäischen Datenschutz-Grundverordnung ("**DSGVO**") regelt die Verpflichtungen der Vertragsparteien zum Schutz der personenbezogenen Daten i.S.d. Art 4 Nr. 1 DSGVO, welche im Rahmen der Nutzung der Services des Auftragsverarbeiters verarbeitet werden.

Der AV-Vertrag findet Anwendung auf alle Tätigkeiten, die mit den AGB und den gebuchten Services (zusammen des "**Rahmenvertrags**") in Zusammenhang stehen und bei denen Beschäftigte des Auftragsverarbeiters oder durch den Auftragsverarbeiter Beauftragte Dritte personenbezogene Daten des Verantwortlichen verarbeiten. In diesem AV-Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der DSGVO zu verstehen.

Die Vertragsparteien schließen die nachfolgende Vereinbarung:

1. Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Gegenstand dieses Vertrages ist die Verarbeitung personenbezogener Daten (im Weiteren '**Daten**') durch den Auftragsverarbeiter für den Verantwortlichen im Zusammenhang mit der Nutzung der cloud-basierten Software-Lösungen von CANEI.

1.2 Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des abgeschlossenen Vertrags der CANEI Software-Lösungen.

2. Konkretisierung des Inhalts

2.1 Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Rahmenvertrag umfasst folgende Arbeiten und/oder Leistungen:

- Die Verarbeitung von Daten auf der Basis von insbesondere Summen- und Saldenlisten in der cloud-basierten Software-Lösung.
- Die Software analysiert auf der Basis dieser Listen die Ertrags-, Vermögens- und Liquiditätslage von Unternehmen, identifiziert wirtschaftlich relevante Potenziale und gibt Handlungsempfehlungen, wie diese Potenziale gehoben werden können.
- Erstellung von Finanz- und Planungsberichten
- Erstellung von unternehmerischen Finanzplänen
- Erstellung von Finanzberichten

2.2 Bereitstellung von Übersichten mittels einer mobilen Applikation

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

2.3 Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- E-Mail-Adresse der Systemnutzer
- Telefonnummer der Systemnutzer
- Firmierungen
- Eventuell in Summen- und Saldenlisten enthaltene personenbezogene Daten (Namen, Kennzeichen, Kontonummern etc.) vom Systemnutzer im Planungsmodul manuell gemachte Angaben zu personenbezogenen Daten

2.4 Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Mitarbeiter/Kunden/Mandanten des Verantwortlichen
- Dritte (sofern in den in das System geladenen Summen- und Saldenlisten enthalten)

3. Technisch-organisatorische Maßnahme

3.1 Der Auftragsverarbeiter hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Verantwortlichen zur Prüfung zu übergeben. Bei Akzeptanz durch den Verantwortlichen werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

3.2 Der Auftragsverarbeiter hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. 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 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 zu berücksichtigen (Einzelheiten in Anlage 1).

3.3 Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter 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

4.1 Der Auftragsverarbeiter darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Verantwortlichen berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

4.2 Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Daten Portabilität und Auskunft nach dokumentierter Weisung des Verantwortlichen unmittelbar durch den Auftragsverarbeiter sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragsverarbeiters

Der Auftragsverarbeiter 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:

5.1 Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragsverarbeiter 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 Auftragsverarbeiter und jede dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Verantwortlichen verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Die Vertraulichkeitsverpflichtung des Auftragnehmers und dessen Beschäftigte muss die besonderen Schweigepflichten für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte gem. § 203 Strafgesetzbuch beinhalten. Der Auftragnehmer stellt hierzu auf Anforderung des Auftraggebers geeignete Nachweise zur Verfügung.

5.2 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).

5.3 Der Verantwortliche und der Auftragsverarbeiter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

5.4 Die unverzügliche Information des Verantwortlichen 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 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.

5.7 Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

6.1 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 Auftragsverarbeiter 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 Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

6.2 Die Auslagerung auf Unterauftragsverarbeiter oder der Wechsel der bestehenden genehmigten Unterauftragsverarbeiter sind zulässig, soweit der Auftragsverarbeiter eine solchen Einschaltung von Unterauftragsverarbeiter dem Verantwortlichen eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und der Verantwortliche nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Verantwortlichen schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird. Im Falle des Einspruchs des Verantwortlichen steht dem Auftragsverarbeiter ein außerordentliches Kündigungsrecht sowohl hinsichtlich dieser Vereinbarung als auch bezüglich der Leistungsvereinbarung zu. Dem Verantwortlichen sind vor Beginn der Verarbeitung die Unterauftragsverarbeiter nach Anlage 2 mitgeteilt worden.

6.3 Die Weitergabe von personenbezogenen Daten des Verantwortlichen an den Unterauftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

6.4 Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragsverarbeiter aufzuerlegen.

7. Kontrollrechte des Verantwortlichen

7.1 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 durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen.

7.2 Der Auftragsverarbeiter stellt sicher, dass sich der Verantwortliche von der Einhaltung der Pflichten des Auftragsverarbeiters nach Art. 28 DS-GVO 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.

7.3 Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

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

8. Mitteilung bei Verstößen des Auftragsverarbeiters

8.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen 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.

- 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 die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Verantwortlichen zu melden
- die Verpflichtung, dem Verantwortlichen im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- die Unterstützung des Verantwortlichen für dessen Datenschutz-Folgenabschätzung
- die Unterstützung des Verantwortlichen im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

8.2 Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragsverarbeiters zurückzuführen sind, kann der Auftragsverarbeiter eine Vergütung beanspruchen.

9. Weisungsbefugnis des Verantwortlichen

9.1 Mündliche Weisungen bestätigt der Verantwortliche unverzüglich (mind. Textform).

9.2 Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.

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 der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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

11. Schlussbestimmungen

11.1 Änderungen und Ergänzungen dieser Vertragsregelung und all ihrer Bestandteile, einschließlich etwaiger Zusicherungen des Auftragsverarbeiters, bedürfen einer Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Vertragsregelung handelt.

11.2 Sollten einzelne Teile dieser Vertragsregelung unwirksam sein, so berührt dies die Wirksamkeit der Vertragsregelung im Übrigen nicht. Anstelle der unwirksamen Bestimmung soll eine Bestimmung vereinbart werden, die dem von den Partnern hiermit verfolgten wirtschaftlichen Zweck möglichst nahekommt. Entsprechendes gilt im Falle einer Regelungslücke.

11.3 Diese Vertragsregelung unterliegt ausschließlich dem formellen und materiellen Recht der Bundesrepublik Deutschland. Die Anwendung des internationalen Privatrechts sowie des einheitlichen UN-Kaufrechts (CISG) wird ausdrücklich ausgeschlossen.

Anlagen:

Anlage 1 - Technisch organisatorische Maßnahmen

Anlage 2- Unterauftragsverarbeiter

Anlage 1 – Technisch-organisatorische Maßnahmen

Der Auftragsverarbeiter gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes entspricht. Die Kundendaten werden im Rechenzentrum von AWS in Frankfurt verarbeitet und gespeichert. Es wurden alle nach Art. 32 DSGVO erforderlichen Maßnahmen ergriffen.

1. Zutrittskontrolle

Wie wird das Unternehmensgebäude, in dem die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?

- Die Schlüsselvergabe an Mitarbeiter wird dokumentiert
- Besucher werden vom Ansprechpartner (oder anderem Personal) in Empfang genommen und beaufsichtigt
- Das Gebäude ist mit einer Alarmanlage ausgestattet

Wie werden in Ihrem Unternehmen die Büroräume, in denen die personenbezogenen Daten verarbeitet werden, vor unbefugtem Zutritt gesichert?

- Türen sind bei Abwesenheit der Mitarbeiter verschlossen
- Fenster sind bei Abwesenheit der Mitarbeiter verschlossen

2. Zugangskontrolle

Welche Vorkehrungen werden bei Ihnen im Unternehmen getroffen, um unberechtigten Zugang zu personenbezogenen Daten zu verhindern?

- Die IT-Systeme sind passwortgeschützt
- Jeder meiner Mitarbeiter verfügt über ein eigenes nur ihm bekanntes und von ihm selbst gewähltes Passwort
- Die Nutzung der IT-Systeme wird protokolliert
- Es wird ein Monitoring-System eingesetzt
- Zugriffsberechtigungen und Rollen werden dokumentiert
- Rollen und Zugriffsberechtigungen werden anforderungsgerecht und zeitlich beschränkt vergeben
- Mobile Systeme (Notebook etc.) werden außerhalb der Bürozeiten unter Verschluss gehalten
- Bei Arbeitsunterbrechungen wird ein passwortgeschützter Bildschirmschoner aktiviert
- Es ist ein angemessener Virenschutz vorhanden
- Die IT-System/Nutzer Passwörter werden gesichert aufbewahrt

- Netzwerke werden ihrer Schutzbedürftigkeit nach eingeteilt
- Es wird eine sichere Übertragungstechnik verwendet (VPN)
- Es gilt das Prinzip der Minimalberechtigung. Jeder Benutzer erhält nur die Zugriffsrechte, die erforderlich sind, um seine vertraglichen Tätigkeiten durchzuführen.

Welche Anforderungen werden an die Komplexität von Passwörtern gestellt?

- Die Passwörter sind aus Zahlen, Buchstaben und Zeichen zusammengesetzt
- Die Passwörter müssen eine Mindestlänge aufweisen
- Trivialpasswörter werden nicht akzeptiert

Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändert und es zu keiner Wiederholung der Passwörter kommt?

- Der Nutzer kann sein Passwort jederzeit selbst ändern

Welche Maßnahmen werden bei gescheiterten Anmeldeversuchen ergriffen?

- Bei 3-maliger Falscheingabe des Passworts erfolgt eine automatische Sperrung des IT-Systems

3. Zugriffskontrolle

Wie stellen Sie eine differenzierte Zugriffsberechtigung bei den verschiedenen Mitarbeitern des Unternehmens sicher?

- Alle Mitarbeiter besitzen verschiedene Passwörter
- Bestimmte Berechtigungen werden durch eine Genehmigung erteilt

Wie wird sichergestellt, dass der Zugriff auf Datenträger wie USB-Sticks, Festplatten oder auch einfache Papierblätter ausschließlich durch berechtigte Personen erfolgt?

- Ausdrucke mit personenbezogenen Daten werden unmittelbar nach dem Ausdruck aus dem Drucker entnommen
- Datenträger werden in verschließbaren Schränken aufbewahrt
- Einzelne Dateien/Daten sind auf den IT-Systemen verschlüsselt Es ist ein angemessener Virenschutz vorhanden

Wie erfolgt die Kontrolle der Zugriffsberechtigungen?

- Unser Unternehmen besitzt ein Berechtigungskonzept

4. Weitergabekontrolle

Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten?

- Daten werden nur weitergegeben nach einer Prüfung der Rechtslage
- Nur ein bestimmter Personenkreis ist zur Weitergabe berechtigt
- Beim Verschicken personenbezogener Daten per Briefpost werden Sichtgeschützte Umschläge verwendet
- Die interne E-Mail-Kommunikation erfolgt über eine unternehmenseigene Domain
- Datenträger sind verschlüsselt
- Daten auf dem Datenträger sind verschlüsselt

Wie wird die Weitergabe von personenbezogenen Daten kontrolliert?

- Die Weitergabe personenbezogener Daten wird protokolliert

5. Verfügbarkeitskontrolle

Welche Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten?

- In regelmäßigen Zeitabständen werden Datensicherungen durchgeführt
- Es werden Protokolle geführt wann welche Daten gesichert wurden
- In unserem Unternehmen wird eine unterbrechungsfreie Stromversorgung sichergestellt
- Wir nutzen AWS (Amazon Web Services) als Hosting Partner. AWS ist nach DIN ISO 27001 zertifiziert.

Wie wird gewährleistet, dass die Datenträger vor Umwelteinflüssen (Feuer, Wasser etc.) geschützt sind?

- Das Gebäude und die Arbeitsräume sind mit Rauch- und Feuermeldern ausgestattet
- Serverräume sind Feuchtigkeitssensoren installiert
- Wichtige Räumlichkeiten sind mit Brandschutztüren ausgestattet
- Wir nutzen AWS (Amazon Web Services) und deren Rechenzentren in Frankfurt am Main als Hosting Partner. AWS ist nach DIN ISO 27001 zertifiziert.

Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet?

- Virenscanner
- Spam-Filter
- Anti-Spy-Programme – Firewalls

Wie wird gewährleistet, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?

- Datenträger werden zur Entsorgung immer an die IT-Abteilung abgegeben

6. Auftragskontrolle in Zusammenhang mit der Auftragsverarbeitung

Welche Maßnahmen werden ergriffen, damit die Verarbeitung der personenbezogenen Daten durch die damit betrauten Mitarbeiter nur gemäß den Weisungen des Auftraggebers erfolgen kann?

- Es erfolgt eine Angebots- und Auftragsbestätigung
- Die Mitarbeiter werden auf die Verpflichtung zum Datengeheimnis hingewiesen

Welche Maßnahmen werden getroffen, damit auch ggf. Unterauftragnehmer keine unbefugten Aktivitäten mit den zur Verfügung gestellten Daten durchführt?

- Unterauftragnehmer werden vertraglich zur Einhaltung der DS-GVO verpflichtet
- Mit Unterauftragnehmern sind entsprechende vertragliche Vereinbarungen (z.B. Verträge zur Auftragsverarbeitung) geschlossen.

Werden Maßnahmen getroffen, die am Ende des Aufbewahrungszwecks der personenbezogenen Daten deren Löschung/Sperrung sicherstellen?

- Unterauftragnehmer werden sorgfältig ausgewählt
- Unterauftragnehmer werden vertraglich zur Löschung/Sperrung verpflichtet

7. Amazon Web Services, Inc. und Amazon Web Services EMEA SARL

Es wurden alle erforderlichen Maßnahmen gemäß Art. 32 DSGVO ergriffen.

Anlage 2 - Verzeichnis der Unterauftragsverarbeiter

Der Verantwortliche stimmt der Beauftragung der nachfolgenden Unterauftragsverarbeiter zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855, Luxemburg	Rechenzentrums- und Hostingdienstleistungen
Stripe Inc.	510 Townsend Street, San Francisco, CA 94103, USA	Technische Anbindung von Online-Bezahlung
HubSpot CRM	HubSpot Irland Limited, Ground Floor, Two Dockland Central Guild Street, Dublin 1, Irland;	Verwaltung von Kundenkontakten und Verkaufsaktivitäten
Microsoft Teams	Microsoft Irland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	Audio- und Videokonferenzen, Chat, Dateifreigabe, Integration mit Office 365-Anwendungen, Echtzeit-Zusammenarbeit an Dokumenten, Kalenderfunktionen, Aufgabenverwaltung, Bildschirmfreigabe, optionale Aufzeichnung