AUFTRAGSVERARBEITUNGS-VERTRAG (AVV)

Zwischen	und
	Candis GmbH
	Friedrichstraße 200
	10117 Berlin
– nachfolgend: **„Auftraggeber“** –	– nachfolgend: **„Auftragnehmer“** –

Präambel

Diese Anlage konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der im Vertragsverhältnis der Allgemeinen Geschäftsbedingungen vom 03.2019 in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertragsverhältnis in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

Die Anhänge 1 und 2 sind Bestandteil dieser Vereinbarung.

1. Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

1.1 Aus dem Vertrag ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Art der Daten	**Art und Zweck der Datenverarbeitung**	**Kategorien betroffener Personen**
Bankdaten (Kontoverbindungen, PIN / Passwort, Bankumsatzdaten, Kreditkartennummern, Paypal-Mailadressen, [Vertragspartner und Vertragsdaten des Kunden, ggf. Art des Vertrages, ggf. Daten von Dritten aus Kontoübersicht: Name, IBAN, Überweisungszweck, Betrag])	Verarbeitung zum Zweck der Vertragserfüllung und gewährleistung der CANDIS Funktionen.	Kunden, ggf. Interessenten
Firmendaten (Name, Anschrift, Ansprechpartner, Umsatzsteuer-ID, Telefonnummern, E-Mail-Adressen, Faxnummern, IP‘s)	Verarbeitung zum Zweck der Vertragserfüllung und gewährleistung der CANDIS Funktionen.	Kunden, ggf. Interessenten

1.2 Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüber hinausgehende Verpflichtungen ergeben.

2. Anwendungsbereich und Verantwortlichkeit

2.1 Der Auftragnehmer verarbeitet die Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 EU-Datenschutzgrundverordnung (DSGVO).

2.2 Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

2.3 Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit des Vertragsverhältnisses und nach dessen Beendigung jederzeit die Berichtigung, Löschung, Sperrung und Herausgabe von Daten verlangen.

2.4 Die Inhalte dieser Vereinbarung gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

3. Pflichten des Auftragnehmers

3.1 Der Auftragnehmer darf die Daten nur im Rahmen des Vertrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

3.2 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragnehmer wird angemessene technische und organisatorische Maßnahmen treffen, die den Anforderungen der DSGVO (vgl. Art 32. DSGVO) entsprechen. Dies beinhaltet insbesondere:

3.2.1 Die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen,

3.2.2 die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,

3.2.3 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

3.3 Maßnahmen hierzu sind insbesondere die Verwendung dem Stand der Technik entsprechenden Verschlüsselungs-verfahren bzw. Pseudonymisierung.

3.4 Der Auftragnehmer stellt auf Anforderung des Auftraggebers die für die Übersicht nach Art. 30 Abs. 1 DSGVO notwendigen Angaben zur Verfügung.

3.5 Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten befassten Mitarbeiter zur Vertraulichkeit verpflichtet und in die Schutzbestimmungen der DSGVO eingewiesen worden sind. Die Vertraulichkeitsverpflichtung besteht auch nach Beendigung der Tätigkeit fort.

3.6 Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 37 DSGVO nachzukommen, wie z.B. seiner Pflicht, einen Datenschutzbeauftragen zu bestellen, soweit vom Gesetz vorgeschrieben.

3.7 Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten des betrieblichen Datenschutzbeauftragten mit.
Die Kontaktdaten des betrieblichen Datenschutzbeauftragten lauten: datenschutz@candis.io

3.8 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 32 bis 36 DS-GVO genannten Pflichten.

Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

3.9 Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit die Daten und Unterlagen betroffen sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe. Des Weiteren behält sich der Auftragnehmer das Recht vor, entsprechende Datensätzen gemäß seiner gesetzlichen Aufbewahrungspflichten (wie nach den Grundsätzen zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in Elektronischer Form sowie zum Datenzugriff, kurz GoBD) für bis zu 10 Jahre weiterhin sicher zu bewahren.

3.10 Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und in geeigneter Weise nachzuweisen.

3.11 Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

3.12 Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

3.13 Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung.

4. Pflichten des Auftraggebers

4.1 Auftraggeber und Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

4.2 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

4.3 Dem Auftraggeber obliegen die aus Art. 33, 34 DSGVO resultierenden Informationspflichten.

4.4 Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Vertragsverhältnisses vertraglich oder durch Weisung fest.

5. Anfragen Betroffener an die Auftraggeber

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

6. Kontrollrechte und -pflichten

6.1 Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen von Auftragnehmer und dokumentiert das Ergebnis. Hierfür kann der Auftraggeber nach freier Wahl Selbstauskünfte vom Auftragnehmer einholen, sich ein Testat eines Sachverständigen vorlegen lassen oder sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich überzeugen.

6.2 Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung oder Anforderung in Textform innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

7. Subunternehmer

7.1 Der Einsatz von Subunternehmern als weitere Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

7.2 Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer informiert der Auftragnehmer den Auftraggeber durch die Aktualisierung der Liste der beauftragten Subunternehmer. Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist - aus wichtigem Grund – gegenüber der vom Auftragnehmer genannten Stelle: datenschutz@candis.io schriftlich widersprechen.

7.3 Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt:

Name und Anschrift des Subunternehmers	Beschreibung der Teilleistung
Amazon Web Services EMEA Sàrl 5 Rue Plaetis L-2338 Luxemburg	Hosting in der Datenzone Frankfurt in Deutschland
Gini GmbH Lyonel-Feininger-Str. 28 80807 München	Erkennung von relevanten Informationen aus PDF's und gescannten Textdokumenten
finleap connect GmbH Gaußstraße 190c 22765 Hamburg	Anbindung & Synchronisierung von Zahlungskonten
finAPI Adams-Lehmann-Str. 44 80797 München	Verarbeiten von Konto- und Transaktionsdaten. Ausführung von Kundenzahlungen in CANDIS.
Mailjet SAS 13-13 bis, rue de l'Aubrac, 75012 Paris, France	Verschicken von Benachrichtigungs-Emails

7.4 Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

7.5 Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

7.6 Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO). Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich unterstellter Personen erfüllt hat.

7.7 Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

7.8 Ein Subunternehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei externem Personal, Post- und Versanddienstleistungen oder Wartung.

Der Auftragnehmer wird mit diesem Dritten im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Datenschutz zu gewährleisten.

8. Informationspflichten

Sollten die Daten bei Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegen.

9. Schriftformklausel & anwendbares Recht

9.1 Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile bedürfen einer schriftlichen Vereinbarung oder Vereinbarung in Textform und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

9.2 Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

9.3 Es gilt deutsches Recht.

10. Ansprechpartner

10.1 Ansprechpartner beim Auftragnehmer:
Abteilung Datenschutz,
datenschutz@candis.io, +49 030 311 930 40

Für Auftraggeber	**Für Auftragnehmer**
	Bamberg 03 / 30 / 2021
Ort, Datum	Ort, Datum
	Candis GmbH
Firmenname	Firmenname
	Christopher Becker
Name des Unterzeichners, Funktion	Name des Unterzeichners, Funktion
Unterschrift	Unterschrift

Anhang 1: Technische und organisatorische Maßnahmen der Candis GmbH

A. Zutrittskontrollmaßnahmen zu Büroräumen

(bitte entnehmen Sie Hinweise zu den Zutrittskontrollmaßnahmen zu den Serverräumen der Dokumentation von Amazon Web Services hier. Amazon Web Services verfügt über die ISO27001 Zertifizierung, die hohe Sicherheitsstandards an den Zertifizierten hinsichtlich der Zutrittskontrollmaßnahmen stellt.)

A.1. Standorte der Clientarbeitsplätze, von denen auf personenbezogene Daten zugegriffen wird.

Name	Büros CANDIS
Adresse	Friedrichstraße 200, 10117 Berlin / Ottostraße 11, 96047 Bamberg
E-Mail:	info@CANDIS.io
Tel:	030 311 930 40

A.2. Existiert ein Pförtnerdienst / ständig besetzter Empfangsbereich zum Gebäude bzw. zu Ihren Büros?

☒ Ja

A.3. Ist das Gebäude oder sind die Büroräume mittels einer Einbruchmeldeanlage (EMA) alarmgesichert?

☒ Ja

A.4. Wer wird informiert, wenn die EMA auslöst?

☒ beauftragter Wachdienst

A.5. Werden das Bürogebäude bzw. seine Zugänge videoüberwacht?

☒ ja, mit Bildaufzeichnung – Nur Zugänge

A.6. Ist das Gebäude/die Büroräume mit einem elektronischen Schließsystem versehen?

☒ ja, aber nur der Eingang zu den Büros / zur Büroetage, nicht das Gebäude insgesamt.

A.7. Wenn B.8 ja: Welche Zutrittstechnik kommt zum Einsatz?

☒ RFID

A.8. Existiert ein mechanisches Schloss für die Gebäude / Büroräume?

☒ Ja

A.9. Wird die Schlüsselausgabe protokolliert, wer gibt die Schlüssel aus?

☒ Ja

A.10. Gibt es eine offizielle Zutrittsregelung für betriebsfremde Personen (bspw. Besucher) zu den Büroräumen?

☒ ja, betriebsfremde Personen werden am Eingang bzw. Empfang vom Ansprechpartner abgeholt und dürfen sich im Gebäude nur begleitet bewegen.

Sind die dokumentierten Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?

☒ geeignet

B. Zugangs- und Zugriffskontrollmaßnahmen

B.1. Existiert ein Prozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitern bzw. bei organisatorischen Veränderungen?
☒ definierter Freigabeprozess

B.2. Authentisieren sich die Mitarbeiter über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst?
☒ Ja

B.3. Existieren verbindliche Passwortparameter im Unternehmen?
☒ Ja

B.4. Wie lang muss das Passwort sein und Muss es Sonderzeichen enthalten?
Länge 12

B.5. Zwingt das IT System den Nutzer zur Einhaltung der oben genannten Passwort Vorgaben?
☒ Ja

B.6. Wird der Bildschirm bei Inaktivität des Benutzers gesperrt? Wenn ja, nach wie viel Minuten?
☒ Ja, nach einer Minute

B.7. Welche Maßnahmen ergreifen Sie bei Verlust, Vergessen oder Ausspähen eines Passworts?
☒ Admin vergibt neues Initialpasswort

B.8. Wie erfolgt die Authentisierung bei Fernzugängen?
☒ Passwort

B.9. Werden die Systeme, auf denen personenbezogene Daten verarbeitet werden, über eine Firewall abgesichert?

☒ Ja

B.10. Wird die Firewall regelmäßig aktualisiert?

☒ Ja

B.11. Wer administriert Ihre Firewall?

☒ eigene IT

B.12. Wenn ein externer DL zum Einsatz kommt: Kann sich dieser ohne Aufsicht durch Ihre IT auf die Firewall aufschalten?

☒ ja

Sind die dokumentierten Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?

☒ geeignet

C. Maßnahmen zur Sicherung von Papier-Unterlagen, mobilen Datenträgern und mobilen Endgeräten

C.1. Wie werden nicht mehr benötigte Papier-Unterlagen mit personenbezogenen Daten (bspw. Ausdrucke / Akten / Schriftwechsel) entsorgt?

☒ Es stehen hierfür Schredder zur Verfügung, deren Nutzung angewiesen ist.

C.2. Wie werden nicht mehr benötigte Datenträger (USB Sticks, Festplatten), auf denen personenbezogene Daten gespeichert sind, entsorgt?

☒ Löschen der Daten

C.3. Dürfen im Unternehmen mobile Datenträger verwendet werden (z.B. USB-Sticks)?

☒ Ja

C.4. Dürfen die Mitarbeiter private Datenträger (z.B. USB Sticks) verwenden?

☒ nein, alle benötigten Speichermedien werden vom Unternehmen gestellt.

C.5. Werden personenbezogene Daten auf mobilen Endgeräten verschlüsselt?

☒ Ja

Sind die dokumentierten Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?

☒ geeignet

D. Maßnahmen zur sicheren Datenübertragung

D.1. Erfolgt der Transfer personenbezogener Daten durchgängig verschlüsselt?

☒ per SSL

D.2. Wer verwaltet die Schlüssel bzw. die Zertifikate?

☒ eigene IT

☒ Externer Dienstleister

D.3. Werden die Übertragungsvorgänge protokolliert?

☒ Ja

D.4 Werden die Protokolle regelmäßig ausgewertet?

☒ nein, eine Auswertung wäre aber im Bedarfsfall möglich

D.5. Wer ist für die Netzanbindung des Unternehmens verantwortlich?

☒ Eigene IT

☒ Externer Dienstleister

Sind die dokumentierten Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?

☒ geeignet

E. Backup- und Notfall-Konzept, Virenschutz

E.1. Existiert ein Backupkonzept?

☒ Ja

E.2. Wird die Funktionalität der Backup-Wiederherstellung regelmäßig getestet?

☒ Ja

E.3. In welchem Rhythmus werden Backups von Systemen angefertigt, auf denen personenbezogene Daten gespeichert werden?

☒ Echtzeitspiegelung

E.4. Auf was für Sicherungsmedien werden die Backups gespeichert?

☒ Zweiter redundanter Server

E.5. Wo werden die Backups aufbewahrt?

☒ Zweiter redundanter Server steht an einem anderen Ort

E.6. Im Falle eines Transports der Backups: Wie wird dieser durchgeführt?

☒ Mitnahme durch einen MA der IT / Geschäftsleitung

E.7. Sind die Backups verschlüsselt?

☒ Ja

E.8. Befindet sich der Aufbewahrungsort der Backups in einem vom primären Server aus betrachtet getrennten Brandabschnitt bzw. Gebäudeteil?

☒ Ja

E.9. Existiert ein dokumentierter Prozess zum Software- bzw. Patchmanagement?

☒ ja

E.10. Wer ist für das Software- bzw. Patchmanagement verantwortlich?

☒ Eigene IT

☒ Externe Dienstleister

E.11. Existiert ein Notfallkonzept (bspw. Notfallmaßnahmen bei Hardwaredefekte / Brand / Totalverlust etc.)?

☒ Ja

E.12. Sind die IT Systeme technisch vor Datenverlusten / unbefugten Datenzugriffen geschützt? Ja, mittels stets aktualisiertem

☒ Virenschutz

☒ Anti-Spyware

☒ Spamfilter

E.13. Wer ist für den aktuellen Virenschutz, Anti-Spyware und Spamfilter verantwortlich?

☒ Externer Dienstleister

Sind die dokumentierten Maßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten?

☒ geeignet

F Weitere Sicherheitsmaßnahmen

F.1. Zutrittskontrolle

- Alarmanlage
- Aufbewahrungsdauer Bildmaterial < 50 Tage
- Automatisches Zugangskontrollsystem
- Besucher nur in Begleitung durch Mitarbeiter
- Empfang mit Pförtner
- Gebäude ist ein reines Bürogebäude

F.2. Zugangskontrolle

- Allgemeine Richtlinie Datenschutz und / oder Sicherheit
- Anti-Viren-Software
- Anwendung einer 2-Faktor-Authentifikation (wenn möglich)
- Automatische Desktopsperre
- Intrusion Detection Systeme
- Login mit Benutzername und Passwort
- Verschlüsselung von Notebooks / Tablet
- Zuordnung von Benutzerrechten

F.3. Zugriffskontrolle

- Differenzierte Berechtigungen (Anwendungen)
- Differenzierte Berechtigungen (Daten)
- Verwaltung der Benutzerrechte durch Administratoren

F.4. Trennungskontrolle

- Festlegung von Datenbankrechten
- Logische Mandantentrennung (softwareseitig)
- Steuerung über ein Berechtigungskonzept
- Trennung von Produktiv- und Testumgebung

F.5. Weitergabekontrolle

- Email-Verschlüsselung

- Bereitstellung über verschlüsselte Verbindungen wie sftp, https

F.6. Eingabekontrolle

- Technische Protokollierung der Änderung von Daten
- Vergabe von Rechten zur Bearbeitung von Daten

F.7. Verschlüsselung

- Verschlüsselter Zugriff auf Datenbanken von Kunden
- Verschlüsselter Zugriff auf Server von Kunden
- Verschlüsselter Zugriff auf Web-Portale
- Verschlüsselung des Transports von E-Mails

F.8. Verfügbarkeit (der Daten)

- Backup & Recovery-Konzept
- Betrieb von Hochverfügbarkeits-Webservern
- RAID System / Festplattenspiegelung
- Tägliche Backups
- Unterbrechungsfreie Stromversorgung (USV)

F.9. Belastbarkeit (der Systeme)

- Einsatz von Hardware Firewalls
- Einsatz von Intrusion Detection Systemen
- Einsatz von Software Firewalls
- Einspielen von aktuellen Sicherheitsupdates auf allen Applikationsservern
- Einspielen von Sicherheitsupdates auf allen Entwicklersystemen

F.10. Wiederherstellbarkeit (der Daten / der Systeme)

- Alarmmeldung bei unberechtigtem Zutritt zum Serverraum
- Brandschutztüren
- Feuer- und Rauchmeldeanlagen
- Feuerfeste Schränke
- Feuerlöscher im Serverraum

F.11. Auftragskontrolle

- Abschluss der notwendigen Auftragsverarbeitungsvereinbarungen
- Abschluss der notwendigen Standard-Vertragsklauseln
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Überprüfung des Schutzniveaus des Auftragnehmers (kontinuierlich)

F.12. Datenschutz-Management

- Bestellung eines externen Datenschutzbeauftragten
- Einsatz von Softwarelösungen für Datenschutz-Management

- Schulung der Mitarbeiter zum Datenschutz
- Verpflichtung der Mitarbeiter zur Wahrung der Vertraulichkeit

F.13. Incident-Response-Management

- Dokumentation von Sicherheitsvorfällen
- Einbindung von Datenschutzbeauftragten in Sicherheitsvorfälle
- Einsatz von Firewall und deren regelmäßige Aktualisierung
- Einsatz von Virenscanner und deren regelmäßige Aktualisierung

F.14. Datenschutzfreundliche Voreinstellungen

- Personenbezogene Daten werden nur zweckerforderlich erhoben

ANHANG 2: DATENVERARBEITUNG

Der Auftragnehmer speichert unter anderem folgende Daten zum Zweck der CANDIS-Nutzung. Je nach Nutzungsgrad durch den Auftraggeber werden mehr oder weniger Daten gespeichert und verarbeitet.

a) Transaktionsinformationen

- Basisinformationen verknüpfter Bankkonten, Kreditkarten und PayPal-Konten, bestehend aus:
    - Konto/Kartenbezeichnung
    - IBAN, BIC
    - Kreditkartennummer
    - PayPal-Mailadresse
- Einzeltransaktionen verknüpfter Bankkonten, Kreditkarten und PayPal-Konten, bestehend aus:
    - Datum
    - Summe
    - Verwendungszweck
    - Informationen zum Sender/Empfänger-Konto

b) Beleginformationen

- Belege und E-Mails, die vom Auftraggeber an die zur Verfügung gestellte CANDIS-Mailadresse geschickt oder manuell per Upload hochgeladen werden, bestehend aus:
    - E-Mail Header
    - E-Mail Body
    - E-Mail Anhänge
- Einzel-Beleginformationen, maximal bestehend aus:
    - Dokumentenlayout
    - Zu zahlender Betrag
    - Postleitzahl
    - Kontonummer
    - BIC
    - Unternehmensregisternummer des Rechnungstellers
    - Kundennummer
    - Dokumenttyp
    - Dokumentendatum
    - Dokumentendomäne
    - IBAN
    - Rechnungsnummer
    - Verwendungszweck
    - Absenderstadt
    - Absender
    - Absendernamenszusatz
    - Absenderpostfach
    - Absenderpostleitzahl
    - Absenderadresse
    - Steuernummer
    - Umsatzsteuer-ID
    - Website

c) Sonstige Informationen

- Kommentare
- Sucheingaben
- Angaben zu eingeladenen Nutzern (jeweils Name, Mailadresse)

d) Abrechnungsinformationen

- Firma
- Adresse
- Ansprechpartner (Mailadresse)
- Abrechnungsinformationen

e) Nutzungsverhalten

- Logdaten
- Nutzungsstatistiken