Vertrag über Auftragsverarbeitung (AVV)

zwischen

Firma	
Anschrift	
PLZ, Ort	
Land	

– nachfolgend „Verantwortlicher" genannt –

und

Firma

Personizer GmbH & Co. KG

vertreten durch die HILCHNER & BOGENA Beteiligungs GmbH, diese vertreten durch die Geschäftsführer Sebastian Schwarz, Sebastian Strzelecki & Jens Klibingat

Schafjückenweg 2, 26180 Rastede, Deutschland / Germany

– nachfolgend „Auftragsverarbeiter" genannt

und gemeinsam als „Vertragsparteien" bezeichnet – wird Folgendes vereinbart:

§ 1 Gegenstand und Dauer des Auftrags

Der Auftragsverarbeiter führt die im Anhang 1 aufgeführten Datenverarbeitungen durch. Darin werden Gegenstand, Art, Zweck und Dauer der Verarbeitung sowie die Kategorien verarbeiteter Daten und betroffener Personen beschrieben.

§ 2 Weisungen der Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur für in Anhang 1 aufgeführte Zwecke bzw. nur auf Grund dokumentierter Weisungen des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine erteilte Weisung gegen geltende Datenschutzbestimmungen der Union oder eines Mitgliedstaats verstößt.

(3) Eine Verarbeitung der überlassenen personenbezogenen Daten durch den Auftragsverarbeiter für andere, insbesondere für eigene Zwecke ist unzulässig.

§ 3 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft mindestens die im Anhang 3 aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Die Maßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Beurteilung des angemessenen Schutzniveaus tragen die Vertragsparteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen, den Zwecken der Verarbeitung und der Datenkategorien (insbesondere nach Art. 9 Abs. 1 bzw. Art. 10 DSGVO) sowie den unterschiedlichen Eintrittswahrscheinlichkeiten und der Schwere des Risikos für die betroffenen Personen gebührend Rechnung.

(2) Die in Anhang 3 aufgeführten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Diese sind durch den Auftragsverarbeiter anzupassen, wenn das bei Vertragsschluss festgelegte Sicherheitsniveau nicht mehr gewährleistet werden kann. Durch die Anpassung muss mindestens das Schutzniveau der bisherigen Maßnahmen erreicht werden. Soweit nichts anderes bestimmt ist, teilt der Auftragsverarbeiter die Anpassungen dem Verantwortlichen unaufgefordert mit.

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass er den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Soweit gesetzlich vorgeschrieben, bestellt der Auftragsverarbeiter einen Beauftragten für den Datenschutz und teilt dessen Kontaktdaten im Anhang 1 mit. Der Auftragsverarbeiter informiert unverzüglich und unaufgefordert über den Wechsel des Datenschutzbeauftragten.

(4) Der Auftragsverarbeiter erbringt die Auftragsverarbeitung im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder innerhalb des Europäischen Wirtschaftsraums. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf stets der vorherigen dokumentierten Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen der DSGVO erfüllt sind.

(5) Sofern der Auftragsverarbeiter Daten des Verantwortlichen im Auftrag verarbeitet, die dem Schutzbereich des § 203 StGB bzw. einem Berufsgeheimnis unterliegen, darf der Auftragsverarbeiter nur dann auf derartige Daten zugreifen, soweit dies im Einzelfall erforderlich ist. Der Auftragsverarbeiter verpflichtet sich in diesem

Zusammenhang, alle Personen, die im Rahmen der beauftragten Tätigkeit die in Satz 1 genannten Daten verarbeiten, auf die Geheimhaltung nach § 203 StGB zu verpflichten. Dem Auftragsverarbeiter ist bekannt, dass hinsichtlich der Daten, die dem Schutzbereich des § 203 StGB unterliegen, ein Zeugnisverweigerungsrecht nach § 53a StPO besteht. Über die Ausübung des Rechtes auf Zeugnisverweigerung entscheidet der Berufsgeheimnisträger der Verantwortlichen. Dem Auftragsverarbeiter ist bekannt, dass die dem Berufsgeheimnis unterliegenden Daten, die sich im Gewahrsam des Auftragsverarbeiters zur Erhebung, Verarbeitung oder Nutzung befinden, dem Beschlagnahmeverbot des § 97 Abs. 1, 3 StPO unterliegen. Einer Sicherstellung ist zu widersprechen. Der Verantwortliche ist unverzüglich zu informieren, wenn eine Beschlagnahme der Daten zu erwarten ist oder bevorsteht.

§ 5 Unterstützungspflichten des Auftragsverarbeiters

(1) Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragsverarbeiter bei der Durchführung einer Datenschutz-Folgenabschätzung sowie einer ggf. erforderlichen Konsultation der Aufsichtsbehörden und bei Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jede Geltendmachung von Rechten durch die von den Datenverarbeitungen betroffenen Personen.

(2) Eine Unterstützung sichert der Auftragsverarbeiter bei der Prüfung von Datenschutzverletzungen und der Umsetzung etwaiger Melde- und Benachrichtigungspflichten zu sowie bei der Einhaltung der Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind.

(3) Ferner unterstützt der Auftragsverarbeiter mit geeigneten technischen und organisatorischen Maßnahmen, damit der Verantwortliche seine bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann.

§ 6 Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens drei Wochen im Voraus in Textform über alle beabsichtigten Beauftragungen von Unterauftragsverarbeitern, damit der Verantwortliche vor der Beauftragung Einwände erheben kann. Der Auftragsverarbeiter stellt die Informationen, die der Verantwortliche benötigt, um über die Wahrnehmung seines Einspruchsrechts zu entscheiden mit der Unterrichtung über die geplante Beauftragung zur Verfügung. Im Falle des begründeten, fristgerechten Einspruchs steht dem Verantwortlichen ein Sonderkündigungsrecht zu. Die Inanspruchnahme der in Anhang 2 zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragsverarbeiter gilt als genehmigt, sofern die in § 6 Abs. 2 dieses Vertrages genannten Voraussetzungen umgesetzt werden.

(2) Ein Zugriff auf personenbezogene Daten durch den Unterauftragsverarbeiter darf erst erfolgen, wenn der Auftragsverarbeiter durch einen schriftlichen Vertrag, der auch in einem elektronischen Format abgeschlossen werden kann, mit dem Unterauftragsverarbeiter sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber dem Unterauftragsverarbeiter gelten. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Verlangen eine Kopie des Vertrags und

etwaiger späterer Änderungen zur Verfügung. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen vollumfänglich dafür, dass der Unterauftragsverarbeiter seinen vertraglichen Pflichten nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen über vertragliche Pflichtverletzungen des Unterauftragsverarbeiters.

(3) Der Auftragsverarbeiter stellt bei einer Unterbeauftragung, die eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhaltet, die Einhaltung der Regelungen der Artikel 44 ff. DSGVO sicher, indem – sofern erforderlich - geeignete Garantien gemäß Artikel 46 DSGVO getroffen werden.

(4) Der Auftragsverarbeiter verpflichtet sich in den Fällen, in denen er einen Unterauftragsverarbeiter in Anspruch nimmt und in denen die Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhalten, mit dem Unterauftragsverarbeiter Standardvertragsklauseln nach Art. 46 DSGVO zu schließen, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

(5) Im Falle des § 6 Abs. 4 führt der Auftragsverarbeiter eine Prüfung nach den Klauseln 14 und 15 der Standardvertragsklauseln durch und stellt diese dem Verantwortlichen unaufgefordert zur Verfügung. Kommen Auftragsverarbeiter oder Verantwortlicher zu dem Ergebnis, dass weitere Maßnahmen getroffen werden müssen, um ein angemessenes Schutzniveau zu erreichen, sind diese Maßnahmen vom Auftragsverarbeiter bzw. vom Unterauftragsverarbeiter zu ergreifen. Der Unterauftragsverarbeiter darf erst dann in die Datenverarbeitung eingebunden werden, wenn ein angemessenes Schutzniveau sichergestellt ist.

(6) Der Auftragsverarbeiter hat die Verpflichtung der weiteren mitwirkenden Personen und der Unterauftragsverarbeiter auf die Geheimhaltung gem. § 203 StGB und § 4 Abs. 5 dieses Vertrages sicherzustellen.

§ 7 Kontrollrechte des Verantwortlichen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesem Vertrag festgelegten oder sich unmittelbar aus der DSGVO ergebenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diesen Vertrag fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen im Sinne des Art. 28 Abs. 5 DSGVO des Auftragsverarbeiters berücksichtigen.

(2) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können gegebenenfalls auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden mit angemessener Vorankündigung und unter Einhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragsverarbeiters sowie nach Möglichkeit ohne Störung des Betriebsablaufs durchgeführt.

(3) Die Vertragsparteien stellen den zuständigen Aufsichtsbehörden die in diesem Vertrag genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

§ 8 Mitzuteilende Verstöße

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Verantwortlichen mit sich bringen, sowie bei Bekanntwerden von Datenschutzverletzungen im Zusammenhang mit den Daten des Verantwortlichen. Gleiches gilt, wenn der Auftragsverarbeiter feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen.

(2) Dem Auftragsverarbeiter ist bekannt, dass der Verantwortliche verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person zu melden. Er wird Verletzungen an den Verantwortlichen unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

- Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Anzahl der betroffenen Personen und Datensätze,
- Name und Kontaktdaten von Kontaktpersonen für weitere Informationen,
- Beschreibung der wahrscheinlichen Folgen der Verletzung sowie
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung oder zur Abmilderung der sich daraus ergebenden nachteiligen Auswirkungen.

§ 9 Beendigung des Auftrags

(1) Mit Beendigung der Auftragsverarbeitung hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht, dies gilt auch für etwaige Sicherungskopien nach Maßgabe der getroffenen technischen und organisatorischen Maßnahmen. Die Löschung hat der Auftragsverarbeiter dem Verantwortlichen in Textform anzuzeigen.

(2) Der Verantwortliche kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragsverarbeiter einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und dem Verantwortlichen aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

(3) Der Auftragsverarbeiter kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Verantwortliche auf die Erfüllung seiner Weisungen besteht, obwohl diese Weisungen gegen geltende rechtliche Anforderungen oder gegen diesen Vertrag verstoßen und der Auftragsverarbeiter den Verantwortlichen darüber in Kenntnis gesetzt hat.

§ 10 Beitritt zum Vertrag

Diesem Vertrag können mit Zustimmung aller Parteien über eine Beitrittserklärung jederzeit weitere Parteien als Verantwortliche oder als Auftragsverarbeiter beitreten. Zusätzlich zur Beitrittserklärung sind – soweit erforderlich – die Anhänge 1 bis 3 auszufüllen. Ab dem Zeitpunkt des Beitritts gelten die beitretenden Parteien als Vertragsparteien dieses Vertrags mit den entsprechend ihrer Bezeichnung bestehenden Rechten und Pflichten.

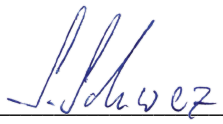
§ 11 Schlussbestimmungen

(1) Sollte das Eigentum des Verantwortlichen bei dem Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Verantwortlichen ausgeschlossen.

(2) Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(3) Im Falle eines Widerspruchs zwischen diesen Vertragsklauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

(4) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

Ort, Datum	Verantwortlicher
Rastede, 05.09.2022	
Ort, Datum	Auftragsverarbeiter

Hinweis

Bitte senden Sie dieses Dokument per E-Mail an contract@personizer.com oder per Briefpost an Personizer GmbH & Co. KG, Abteilung Recht, Schafjückenweg 2, 26180 Rastede, Germany.

Vielen Dank

Anhang 1

Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

Gegenstand der Verarbeitung	Bereitstellung der Software Personizer für die Urlaubs- und Abwesenheitsplanung und -verwaltung und die Erfassung von Arbeitszeiten
Art und Zweck der Verarbeitung	Verarbeitung von Daten von Arbeitnehmern und sonstigen Kontaktpersonen des Verantwortlichen zur Planung und Verwaltung von Urlaubs- und sonstiger Abwesenheit und zur Erfassung von Arbeitszeiten
Art der personenbezogenen Daten	Pflichtfelder: - Vorname - Name Optional: - E-Mail - Adresse - Urlaubstage - Krankheitstage - Arbeitszeiten - sonstige vom Anwender definierte optionale Angaben
Kategorien betroffener Personen	- Arbeitnehmer - sonstige Teilnehmer und Nutzer der Urlaubs- und Abwesenheitsplanung und -verwaltung und Arbeitszeiterfassung
Dauer der Verarbeitung	Entspricht der Dauer der Vertragsbeziehung

Datenschutzbeauftragte/r des Verantwortlichen	
Datenschutzbeauftragte/r des Auftragsverarbeiters	Dr. Uwe Schläger datenschutz nord GmbH Konsul-Smidt-Straße 88 28217 Bremen Tel.: 0421 696632-0 Fax: 0421 696632-11 E-Mail: office@datenschutz-nord.de

Anhang 2

Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

UNTERAUFTRAGNEHMER	VERARBEITUNGSSTANDORT	BESCHREIBUNG DER VERARBEITUNG
Amazon Web Services EMEA Sàrl Ave J-F Kennedy 381855 Luxembourg, Luxemburg	in der EU	Cloud Dienstleistung
Mailgun Technologies, Inc535 Mission St.San Francisco, CA 94105United States	in der EU	E-Mail Dienstleistung

Anhang 3

Technisch-organisatorische Maßnahmen zur IT-Sicherheit nach Art. 32 DSGVO

A) Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität

1.	**Zutrittskontrollmaßnahmen zu Serverräumen**
1.0	Werden personenbezogene Daten auf Servern gespeichert, die von Ihnen betrieben werden? ☐ ja ☒ nein
2.	**Zutrittskontrollmaßnahmen zu Büroräumen**
2.1	Standort der Clientarbeitsplätze, von denen auf personenbezogene Daten zugegriffen wird: Schafjückenweg 2, 26180 Rastede, Deutschland
2.2	Existiert ein Pförtnerdienst / ständig besetzter Empfangsbereich zum Gebäude bzw. zu Ihren Büros? ☒ ja ☐ nein
2.3	Wird ein Besucherbuch geführt? ☐ ja ☒ nein
2.4	Ist das Gebäude oder sind die Büroräume mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? ☒ ja ☐ nein
2.5	**Wenn 2.4 ja**: Wer wird informiert, wenn die EMA auslöst? ☒ beauftragter Wachdienst ☒ Administrator ☐ Leiter IT ☒ Sonstiges: Geschäftsführung
2.6	Werden das Bürogebäude bzw. seine Zugänge videoüberwacht? ☐ ja, ohne Bildaufzeichnung ☐ ja, mit Bildaufzeichnung ☒ nein
2.7	**Wenn 2.6 „ja, mit Bildaufzeichnung“,** wie lange werden die Bilddaten gespeichert? bitte Wert in Tagen eintragen Tage
2.8	Ist das Gebäude / die Büroräume mit einem elektronischen Schließsystem versehen? ☒ ja, Gebäude und Büroräume sind elektronisch verschlossen ☐ ja, aber nur das Gebäude, nicht der Eingang zu den Büros bzw. zur Büroetage. ☐ ja, aber nur der Eingang zu den Büros / zur Büroetage, nicht das Gebäude insgesamt. ☐ nein
2.9	**Wenn 2.8 ja**: Welche Zutrittstechnik kommt zum Einsatz? **Mehrfachantworten möglich!** ☒ RFID ☐ PIN ☐ Biometrie ☐ Sonstiges: bitte eintragen
2.10	**Wenn 2.8 ja**: Werden die Zutrittsrechte personifiziert vergeben? ☒ ja ☐ nein
2.11	**Wenn 2.8 ja**: Werden die Zutritte im Zutrittssystem protokolliert? ☐ ja, sowohl erfolgreiche als auch erfolglose Zutrittsversuche ☐ ja, aber nur erfolgreiche positive Zutritte

	☐ ja, aber nur erfolglose Zutrittsversuche ☒ nein, das Schloss wird nur freigegeben oder nicht
2.12	**Wenn 2.11 ja**: Wie lange werden diese Protokolldaten aufbewahrt? bitte Wert in Tagen eintragen Tage
2.13	**Wenn 2.11 ja**: Werden die Protokolle regelmäßig ausgewertet? ☐ ja ☐ nein, eine Auswertung wäre aber im Bedarfsfall möglich
2.14	Existiert ein mechanisches Schloss für die Gebäude / Büroräume? ☒ ja ☐ nein
2.15	**Wenn 2.14 ja**: Wird die Schlüsselausgabe protokolliert, wer gibt die Schlüssel aus? ☒ ja ☐ nein Ausgabestelle: Buchhaltung
2.16	Gibt es offizielle Zutrittsregelung für betriebsfremde Personen (bspw. Besucher) zu den Büroräumen? ☐ nein ☒ ja, betriebsfremde Personen werden am Eingang bzw. Empfang vom Ansprechpartner abgeholt und dürfen sich im Gebäude nur begleitet bewegen.
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht 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 ☐ begrenzt geeignet ☐ ungeeignet Begründung: Der Zutritt für betriebsfremde Personen ist nur in Begleitung möglich. Eine Alarmanlage schützt vor Einbruch. Darüber hinaus würden selbst bei Erreichen eines physikalischen Zugriffs zu einem Clientrechner noch diverse weitere Sicherheitsmaßnahmen greifen, um einen unautorisierten Zugriffs auf schützenswerte Daten zu verhindern.
3	**Zugangs- und Zugriffskontrollmaßnahmen**
3.1	Existiert ein Prozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitern bzw. bei organisatorischen Veränderungen? ☒ definierter Freigabeprozess ☐ kein definierter Freigabeprozess, auf Zuruf ☐ Sonstige Vergabeweise: bitte angeben
3.2	Werden die Vergabe bzw. Änderungen von Zugriffsberechtigungen protokolliert? ☐ ja ☒ nein
3.3	Authentisieren sich die Mitarbeiter über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst? ☒ ja ☐ nein

3.4	Existieren verbindliche Passwortparameter im Unternehmen? ☒ ja ☐ nein
3.5	**Passwort-Zeichenlänge:** 10 **Muss das Passwort Sonderzeichen enthalten?** ☒ ja ☐ nein **Mindest-Gültigkeitsdauer in Tagen:** mindestens 0 Tage, maximal 90 Tage gültig
3.6	Zwingt das IT System den Nutzer zur Einhaltung der oben genannten PW Vorgaben? ☒ ja ☐ nein
3.7	Wird der Bildschirm bei Inaktivität des Benutzers gesperrt? Nein Wenn ja, nach wieviel Minuten? bitte Wert in Minuteneintragen Minuten
3.8	Welche Maßnahmen ergreifen Sie bei Verlust, Vergessen oder Ausspähen eines Passworts? ☒ Admin vergibt neues Initialpasswort ☐ keine
3.9	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen? ☒ ja, 10 Versuche ☐ nein
3.10	**Wenn 3.8 ja**, Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht wurde? ☐ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt ☒ Die Zugänge bleiben für 15 Minuten gesperrt.
3.11	Wie erfolgt die Authentisierung bei Fernzugängen: Authentisierung mit ☐ Token ☒ VPN-Zertifikat ☒ Passwort
3.12	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen bei Fernzugängen? ☒ ja, 10 Versuche ☐ nein
3.13	**Wenn 3.11 ja**, Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht worden ist? ☐ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt ☒ Die Zugänge bleiben für 15 Minuten gesperrt.
3.14	Wird der Fernzugang nach einer gewissen Zeit der Inaktivität automatisch getrennt? ☐ ja, nach bitte Wert in Minuteneintragen Minuten ☒ nein
3.15	Werden die Systeme, auf denen personenbezogene Daten verarbeitet werden, über eine Firewall abgesichert? ☒ ja ☐ nein
3.16	**Wenn 3.15 ja:** Wird die Firewall regelmäßig upgedatet? ☒ ja ☐ nein
3.17	**Wenn 3.15 ja**: Wer administriert Ihre Firewall? ☐ eigene IT ☒ Externer Dienstleister

3.18	**Wenn ein externer DL zum Einsatz kommt**: Kann sich dieser ohne Aufsicht durch Ihre IT auf die Firewall aufschalten? ☒ ja ☐ nein, die Aufschaltung ist nur im 4 Augenprinzip mit einem Mitarbeiter der eigenen IT möglich.
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht 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 ☐ begrenzt geeignet ☐ ungeeignet Begründung: Verschiedene Maßnahmen schützen vor unautorisierten Client-Logins. Darüber hinaus ist ein erfolgreicher Login auf einem Client-Rechner alleine nicht ausreichend, um Zugang zur Kundendatenbank zu erlangen. Weitere Sicherheitsmechanismen greifen an diesem Punkt.
4	**Maßnahmen zur Sicherung von Papier-Unterlagen, mobilen Datenträgern und mobilen Endgeräten**
4.1	Wie werden nicht mehr benötigte Papier-Unterlagen mit personenbezogenen Daten (bspw. Ausdrucke / Akten / Schriftwechsel) entsorgt? ☐ Altpapier / Restmüll ☒ Es stehen hierfür Schredder zur Verfügung, deren Nutzung angewiesen ist. ☐ Es sind verschlossene Datentonnen aufgestellt, die von einem Entsorgungsdienstleister zur datenschutzkonformen Vernichtung abgeholt werden. ☐ Sonstiges: bitte angeben
4.2	Wie werden nicht mehr benötigte Datenträger (USB Sticks, Festplatten), auf denen personenbezogene Daten gespeichert sind, entsorgt? ☒ Physikalische Zerstörung durch eigene IT. ☐ Physikalische Zerstörung durch externen Dienstleister. ☒ Löschen der Daten ☐ Löschen der Daten durch bitte Anzahl angeben Überschreibungen ☐ Sonstiges: bitte angeben
4.3	Dürfen im Unternehmen mobile Datenträger verwendet werden (z.B. USB-Sticks) ☒ ja ☐ nein
4.4	Dürfen die Mitarbeiter private Datenträger (z.B. USB Sticks) verwenden? ☐ generell ja ☐ ja, aber nur nach Genehmigung und Überprüfung des Speichermediums durch die IT. ☒ nein, alle benötigten Speichermedien werden vom Unternehmen gestellt.

4.5	Werden personenbezogene Daten auf mobilen Endgeräten verschlüsselt? ☒ Verschlüsselung der Festplatte ☐ Verschlüsselung einzelner Verzeichnisse ☐ keine Maßnahmen
4.6	Verarbeiten Mitarbeiter personenbezogene Daten auch auf eigenen privaten Geräten (bring your own device)? ☐ ja ☒ nein
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht 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 ☐ begrenzt geeignet ☐ ungeeignet Begründung: Die Daten auf physikalischen Datenträgern werden durch diverse Maßnahmen geschützt, um auch bei unrechtmäßigem Zugriff auf die Hardware einen Missbrauch zu verhindern.
5	**Maßnahmen zur sicheren Datenübertragung**
5.1	Erfolgt der Transfer personenbezogener Daten durchgängig verschlüsselt? ☐ gar nicht ☐ nein, Datenübertragung erfolgt per mpls ☐ nur vereinzelt ☐ per verschlüsselter Datei als Mailanhang ☐ per PGP/SMime ☐ per verschlüsseltem Datenträger ☒ per VPN ☒ per https/TLS ☐ per SFTP ☒ Sonstiges: SSH
5.2	Wer verwaltet die Schlüssel bzw. die Zertifikate? ☐ Anwender selbst ☒ eigene IT ☐ Externer Dienstleister
5.3	Werden die Übertragungsvorgänge protokolliert? ☐ ja ☒ nein

5.4	**Wenn 5.2 ja**: Wie lange werden diese Protokolldaten aufbewahrt? bitte Wert in Tagen eintragen Tage
5.5	**Wenn 5.2 ja**: Werden die Protokolle regelmäßig ausgewertet? ☐ ja ☐ nein, eine Auswertung wäre aber im Bedarfsfall möglich
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht 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 ☐ begrenzt geeignet ☐ ungeeignet Begründung: Sämtliche Verbindungen, über die personenbezogene Daten übermittelt werden, werden nach dem Stand der Technik verschlüsselt.

B) Maßnahmen zur Sicherstellung der Verfügbarkeit

1	**Netzanbindung**
1.1	Verfügt das Unternehmen über eine redundante Internetanbindung? ☒ ja ☐ nein
1.2	Sind die einzelnen Standorte des Unternehmens redundant miteinander verbunden? ☐ ja ☒ nein
1.3	Wer ist für die Netzanbindung des Unternehmens verantwortlich? ☐ eigene IT ☒ Externer Dienstleister
	Sind die dokumentierten Maßnahmen aus Ihrer Sicht 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 ☐ begrenzt geeignet ☐ ungeeignet Begründung: Die Netzanbindung wird durch den externen Dienstleister professionell geschützt und abgesichert.