Vertrag zur Auftragsverarbeitung personenbezogener Daten (gem. DSGVO) zwischen

CleverReach GmbH & Co. KG
Schafjückenweg 2
26180 Rastede
- nachstehend Auftragnehmerin genannt -

und

heidee Lifestyle + Design
Kundennummer 264066
Rosenstraße 10
97276 Margetshöchheim, Deutschland
- nachstehend Auftraggeberin genannt -

§ 1 Gegenstand und Dauer des Auftrags

(1) Die Auftragnehmerin führt die im Anhang 1 beschriebenen Dienstleistungen für die Auftraggeberin durch. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien werden dort beschrieben.

(2) Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Unterzeichnung beider Parteien in Kraft und gilt, solange die Auftragnehmerin für die Auftraggeberin personenbezogene Daten verarbeitet. Dieser Vertrag ersetzt gleichzeitig alle bisherigen Verträge zur Auftragsdatenverarbeitung zwischen den Vertragsparteien, sofern vorhanden.

§ 2 Weisungen der Auftraggeberin

(1) Die Auftraggeberin ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen bleiben hiervon unberührt.

(2) Die Auftragnehmerin verarbeitet die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich nach den Weisungen der Auftraggeberin und im Rahmen der getroffenen Vereinbarungen. Daten dürfen nur berichtigt, gelöscht und gesperrt werden, wenn die Auftraggeberin dies anweist. Die Auftragnehmerin darf hiervon abweichend in Ausnahmefällen die Daten, die sie im Auftrag der Auftraggeberin verarbeitet, berichtigen, löschen oder sperren, wenn sie aus rechtlichen Gründen dazu verpflichtet ist, E-Mail-Adressen aus der Datenbank zu entfernen und auf eine schwarze Liste zu setzen, wenn eine E-Mail an eine bestimmte und gleiche E-Mail-Adresse dreimal in Folge als unzustellbar zurückkommt (sog. Hardbounces) oder Beschwerden von Empfängern vorliegen.

(3) Die Verarbeitung erfolgt nur auf Weisung der Auftraggeberin, es sei denn, die Auftragnehmerin ist durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem die Auftragnehmerin unterliegt, zur Verarbeitung dieser Daten verpflichtet. In einem solchen Fall teilt die Auftragnehmerin der Auftraggeberin diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(4) Grundsätzlich können Weisungen mündlich erteilt werden. Mündliche Weisungen sind anschließend von der Auftraggeberin zu dokumentieren. Weisungen sind schriftlich oder in Textform zu erteilen, wenn die Auftragnehmerin dies verlangt.

(5) Ist die Auftragnehmerin der Ansicht, dass eine Weisung der Auftraggeberin gegen datenschutzrechtliche Vorschriften verstößt, hat sie die Auftraggeberin unverzüglich darauf hinzuweisen.

§ 3 Technische und organisatorische Maßnahmen

(1) Die Auftragnehmerin verpflichtet sich, für die zu verarbeitenden Daten angemessene technische und organisatorische Sicherheitsmaßnahmen zu treffen und im Anhang 3 dieses Vertrages zu dokumentieren. Die Sicherheitsmaßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die getroffenen Maßnahmen können im Laufe der Zeit der technischen und organisatorischen Weiterentwicklung angepasst werden. Die Auftragnehmerin darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Sicherheitsniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss die Auftragnehmerin der Auftraggeberin nur wesentliche Anpassungen mitteilen.

(3) Die Auftragnehmerin unterstützt die Auftraggeberin bei der Einhaltung aller gesetzlichen Pflichten hinsichtlich der einzuhaltenden technischen und organisatorischen Maßnahmen. Die Auftragnehmerin hat auf Anfrage an der Erstellung und der Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten der Auftraggeberin mitzuwirken. Die Auftragnehmerin wirkt bei der Erstellung einer Datenschutz-Folgenabschätzung und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden mit. Sie hat der Auftraggeberin alle erforderlichen Angaben und Dokumente auf Anfrage offenzulegen.

§ 4 Pflichten der Auftragnehmerin

(1) Die Auftragnehmerin bestätigt, dass ihr die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Sie gestaltet in ihrem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Die Auftragnehmerin bietet hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften und den Rechten der betroffenen Person steht.

(3) Die Auftragnehmerin sichert zu, dass sie die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Sie überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(4) Die Auftragnehmerin darf im Rahmen der Auftragsverarbeitung nur dann auf personenbezogene Daten der Auftraggeberin zugreifen, wenn dies für die Durchführung der Auftragsverarbeitung zwingend erforderlich ist.

(5) Soweit gesetzlich vorgeschrieben, bestellt die Auftragnehmerin einen Beauftragten für den Datenschutz. Die Kontaktdaten des Beauftragten für den Datenschutz werden der Auftraggeberin zum Zweck der direkten Kontaktaufnahme mitgeteilt.

(6) Die Auftragnehmerin darf die ihr zur Verfügung gestellten personenbezogenen Daten ausschließlich im Gebiet der Bundesrepublik Deutschland oder in einem Mitgliedsstaat der Europäischen Union verarbeiten. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung der Auftraggeberin und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen erfüllt sind.

(7) Die Auftragnehmerin unterstützt die Auftraggeberin mit geeigneten technischen und organisatorischen Maßnahmen, damit diese ihren bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann, z.B. die Information und Auskunft an die betroffene Person, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch. Die Auftragnehmerin benennt einen Ansprechpartner, der die Auftraggeberin bei der Erfüllung von gesetzlichen Informations- und Auskunftspflichten, die im Zusammenhang mit der Auftragsverarbeitung entstehen, unterstützt und teilt der Auftraggeberin dessen Kontaktdaten unverzüglich mit. Soweit die Auftraggeberin besonderen gesetzlichen Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten unterliegt, unterstützt die Auftragnehmerin die Auftraggeberin hierbei. Auskünfte an die betroffene Person oder Dritte darf die Auftragnehmerin nur nach vorheriger Weisung der Auftraggeberin erteilen. Soweit eine betroffene Person ihre datenschutzrechtlichen Rechte unmittelbar gegenüber der Auftragnehmerin geltend macht, wird die Auftragnehmerin dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

§ 5 Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Die Auftragnehmerin darf Unterauftragnehmer nur beauftragen, wenn sie die Auftraggeberin immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter vorab informiert, wodurch die Auftraggeberin die Möglichkeit erhält, gegen derartige Änderungen innerhalb von 30 Tagen Einspruch zu erheben. Der Einspruch darf nur aus wichtigem Grund erfolgen.

(2) Ein Unterauftragsverhältnis liegt insbesondere vor, wenn die Auftragnehmerin weitere Auftragnehmer in Teilen oder im Ganzen mit Leistungen beauftragt, auf die sich dieser Vertrag bezieht. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die die Auftragnehmerin bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen oder Reinigungskräfte. Die Auftragnehmerin ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten der Auftraggeberin auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen

(3) Ein Zugriff auf Daten darf durch den Unterauftragnehmer erst dann erfolgen, wenn die Auftragnehmerin durch einen schriftlichen Vertrag sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber den Unterauftragnehmern gelten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den datenschutzrechtlichen Vorschriften erfolgt.

(4) Die Inanspruchnahme der in Anhang 2 zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragnehmer gilt als genehmigt, sofern die in § 5 Abs. 3 dieses Vertrages genannten Voraussetzungen umgesetzt werden.

§ 6 Kontrollrechte der Auftraggeberin

Die Auftragnehmerin erklärt sich damit einverstanden, dass die Auftraggeberin oder eine von ihr beauftragte Person berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und Anforderung von relevanten Unterlagen oder durch Zutritt zu den Arbeitsräumen der Auftragnehmerin zu den ausgewiesenen Geschäftszeiten nach vorheriger Anmeldung. Durch geeignete und gültige Zertifikate zur IT-Sicherheit (z.B. IT-Grundschutz, ISO 27001) kann auch der Nachweis einer ordnungsgemäßen Verarbeitung erbracht werden, sofern hierzu auch der jeweilige Gegenstand der Zertifizierung auf die Auftragsverarbeitung im konkreten Fall zutrifft. Die Vorlage eines relevanten Zertifikats ersetzt jedoch nicht die Pflicht der Auftragnehmerin zur Dokumentation der Sicherheitsmaßnahmen im Sinne des § 3 dieser Vereinbarung.

§ 7 Mitzuteilende Verstöße der Auftragnehmerin

Die Auftragnehmerin unterrichtet die Auftraggeberin unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten der Auftraggeberin mit sich bringen, sowie bei Verdacht auf Datenschutzverletzungen im Zusammenhang mit den Daten der Auftraggeberin. Gleiches gilt, wenn die Auftragnehmerin feststellt, dass die bei ihr getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen. Der Auftragnehmerin ist bekannt, dass die Auftraggeberin verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person unverzüglich zu melden. Sofern es zu solchen Verletzungen gekommen ist, wird die Auftragnehmerin die Auftraggeberin bei der Einhaltung ihrer Meldepflichten unterstützen. Sie wird die Verletzungen der Auftraggeberin unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

a) eine Beschreibung der Art der Verletzung, der Kategorien und ungefähre Anzahl der betroffenen Personen und Datensätze,

b) Name und Kontaktdaten eines Ansprechpartners für weitere Informationen,

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung sowie

d) eine Beschreibung der ergriffenen Maßnahmen zur Behebung oder Abmilderung der Verletzung.

§ 8 Beendigung des Auftrags

(1) Nach Abschluss der Auftragsverarbeitung hat die Auftragnehmerin alle personenbezogenen Daten nach Wahl der Auftraggeberin entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

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

§ 9 Schlussbestimmungen

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

(2) Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was ab dem 25.05.2018 auch in einem elektronischen Format erfolgen kann.

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

(4) Als Gerichtsstand vereinbaren die Parteien, sofern gesetzlich zulässig, den Firmensitz der Auftragnehmerin.

Ort, Datum	Ort, Datum
Margetshöchheim, 21.07.2020	Rastede, 21.07.2020
Unterschrift Auftraggeberin	Unterschrift Auftragnehmerin
	
	Geschäftsführung

Anhang 1: Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

Gegenstand der Verarbeitung	Bereitstellung der CleverReach-Software für den E-Mail-Versand/-Auswertung und Verwaltung durch die Auftraggeberin. Judith Rasp
Art und Zweck der Verarbeitung	Erhebung, Speicherung, Nutzung, Verarbeitung und Übermittlung von Account- und individuelle Nutzerverwaltungsdaten der Auftraggeberin. Speicherung, Verarbeitung und Übermittlung von Empfängerdaten zum Zweck der Zusendung/Auswertung von E-Mails. Judith Rasp
Art der personenbezogenen Daten	Account-Daten der Auftraggeberin - Ansprache - Vor- und Nachname - Firma, Rechnungsanschrift Empfängerdaten (E-Mail-Adresse, Vor- und Zuname) - E-Mail-Adresse - Vor- und Nachname - Anschrift - Personenstammdaten (z. B. Adresse, Geburtstag, Interessen) - Kommunikationsdaten (z. B. Telefon-/Faxnummer, Mobiltelefon) - Vertragsstammdaten (z. B. Käufe, Abos, Rechnungsdaten) - Protokolldaten (z. B. Log-Infos, Aktivierungsinformationen)
Kategorien betroffener Personen	- Ansprechpartner/Handelnde Personen der Auftraggeberin - Newsletter-Empfänger - Käufer und Interessenten - Kunden und Interessenten
Name und Kontaktdaten des Datenschutz-beauftragten der Auftraggeberin (sofern vorhanden)	Judith Rasp
Name und Kontaktdaten des Datenschutz-beauftragten der Auftragnehmerin	Dr. Uwe Schläger, datenschutz nord GmbH Konsul-Smidt-Str. 88 28217 Bremen Deutschland Ansprechpartner: Conrad S. Conrad, Justiziar E-Mail: cconrad@datenschutz-nord.de

Anhang 2: Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

Unterauftragnehmer (Name, Rechtsform, Sitz der Gesellschaft)	**Verarbeitungsstandort**	**Art der Dienstleistung**
PlusServer GmbH	Deutschland	Versand der E-Mails
Amazon Web Services, Inc.	Irland Deutschland	Speicherung und Verarbeitung der Auftragsdaten, Versand der E-Mails
Hetzner Online GmbH	Deutschland	Versand der E-Mails

Anhang 3: Technisch-organisatorische Maßnahmen bei der CleverReach GmbH & Co. KG

A Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität (1.1 Standort 1)

1.	Zutrittskontrollmaßnahmen zu Serverräumen
1.1	Werden personenbezogene Daten auf Servern gespeichert, die von Ihnen betriebenen werden? ☒ ja ☐ nein
1.2	Nennen Sie bitte die Standorte des Serverraums / Rechenzentrums (RZ). **Standort 1**: Deutschland - **hier werden keine Auftragsdaten gespeichert** **Standort 2**: Amazon Web Services, Inc., Irland **Standort 3**: PlusServer GmbH, Deutschland **Standort 4**: Amazon Web Services, Inc., Deutschland **Standort 5**: Hetzner Online GmbH, Deutschland Mit allen externen Dienstleistern sind entsprechende datenschutzrechtliche Verträge nach Maßgabe von Art. 28 DSGVO geschlossen worden. Für die konkrete Datenverarbeitung durch die externen Dienstleister gelten deren jeweilige technisch-organisatorische Maßnahmen, auf die wir verweisen.
1.3	Sind die personenbezogenen Daten auf mehr als einen Serverstandort / Rechenzentrum verteilt (z. B. Backup Server/ Nutzung von Cloud-Dienstleistungen)? ☒ ja ☐ nein
1.4	**Falls 1.3 ja: Machen Sie bitte die entsprechenden Standortangaben auch bzgl. weiterer Server.** Weitere Serverstandorte: Amazon Web Services, Inc., Irland
1.5	Gelten die folgenden Angaben zu Zutrittskontroll-Maßnahmen für **alle** im Einsatz befindlichen Server- / RZ Standorte? ☐ ja ☒ nein, ausschließlich für Standort 1
1.6	Ist der Serverraum fensterlos? ☒ ja ☐ nein
1.7	Ist der Serverraum mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? ☒ ja ☐ nein
1.8	Wenn 1.7 ja: Wer wird informiert, wenn die EMA auslöst? ☒ beauftragter Wachdienst ☒ Administrator ☒ Leiter IT ☒ Sonstiges: Polizei
1.9	Ist der Serverraum videoüberwacht? ☐ ja, ohne Bildaufzeichnung ☐ ja, mit Bildaufzeichnung ☒ nein
1.10	Wie viele Personen haben Zutritt zum Serverraum und welche Funktionen haben diese inne? Anzahl der Personen: 6 Funktion im Unternehmen: Administratoren, Leiter IT
1.11	Ist der Serverraum mit einem elektronischen Schließsystem versehen? ☒ ja ☐ nein, mit mechanischem Schloss
1.12	Wie viele Schlüssel zum Serverraum existieren und wer gibt die Schlüssel aus? Anzahl Schlüssel: 6 Ausgabestelle: Administrator

1.13	Aus welchem Material besteht die Zugangstür zum Serverraum? ☒ Stahl / Metall / Brandschutztür Holz T-30 ☐ sonstiges Material
1.14	Wird der Serverraum neben seiner eigentlichen Funktion noch für andere Zwecke genutzt? ☐ 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 getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
2.	**Zutrittskontrollmaßnahmen zu Büroräumen**
2.1	Standort der Clientarbeitsplätze, von denen auf personenbezogene Daten zugegriffen wird: Arbeitsplätze der Mitarbeiter
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	Wer wird informiert, wenn die EMA auslöst? ☒ beauftragter Wachdienst ☒ Administrator ☒ Leiter IT ☒ Sonstiges: Polizei
2.6	Werden das Bürogebäude bzw. seine Zugänge videoüberwacht? ☒ ja, ohne Bildaufzeichnung ☐ ja, mit Bildaufzeichnung ☒ nein
2.7	Ist das Gebäude / die Büroräume mit einem elektronischen Schließsystem versehen? ☒ ja, Gebäude und Zutritt zu Büroräumen 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
2.8	**Wenn 2.7 ja**: Welche Zutrittstechnik kommt zum Einsatz? ☒ RFID ☒ PIN ☐ Biometrie ☐ Sonstiges:
2.9	**Wenn 2.7 ja**: Werden die Zutrittsrechte personifiziert vergeben? ☒ ja ☐ nein
2.10	**Wenn 2.7 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

2.11	**Wenn 2.10 ja**: Wie lange werden diese Protokolldaten aufbewahrt? 6 Monate
2.12	**Wenn 2.10 ja**: Werden die Protokolle regelmäßig ausgewertet? ☐ ja ☒ nein, eine Auswertung ist aber im Bedarfsfall möglich
2.13	Existiert ein mechanisches Schloss für die Gebäude / Büroräume? ☒ ja ☐ nein
2.14	**Wenn 2.13 ja**: Wird die Schlüsselausgabe protokolliert, wer gibt die Schlüssel aus? ☒ ja ☐ nein Ausgabestelle: Administration
2.15	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: Die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
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:
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	Wie lauten die Passwort-Vorgaben für Zugriff auf auftragsdatenbezogene Zugriffe? **PW Länge:** ☒ 10 Zeichen oder mehr ☐ Weniger als 8 Zeichen ☐ Weniger als 6 Zeichen **Welche Zeichenarten müssen erfüllt sein?** ☐ Sonderzeichen ☒ Ziffern ☒ Groß- / Kleinschreibung

	Gültigkeitsdauer des PW: ☐ 90 Tage oder weniger ☐ 180 Tage oder weniger ☒ mehr als 180 Tage
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? ☒ ja ☐ nein Wenn ja, nach wie vielen Minuten? Nach 10 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, nach 3 Versuchen ☐ nein
3.10	**Wenn 3.9 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 10 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 ☒ nein, ohne Zertifikat ist eine Anmeldeversuch nicht möglich
3.13	Wird der Fernzugang nach einer gewissen Zeit der Inaktivität automatisch getrennt? ☒ ja, nach 30 Minuten ☐ nein
3.14	Werden die Systeme über eine Firewall abgesichert? ☒ ja ☐ nein
3.15	**Wenn 3.14 ja:** Wird die Firewall regelmäßig upgedatet? ☒ ja ☐ nein
3.16	**Wenn 3.14 ja**: Wer administriert Ihre Firewall? ☒ 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 getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

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. ☒ Auftragsdaten der Auftraggeber liegen nicht in Papierform vor.
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
4.3	Dürfen im Unternehmen mobile Datenträger verwendet werden (z.B. USB-Sticks) ☒ ja, aber ausschließlich von der Auftragnehmerin gestellte Datenträger ☐ 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 von der Auftragnehmerin gestellt.
4.5	Werden Auftragsdaten der Auftraggeberin durch die Mitarbeiter auch auf mobilen Endgeräten verarbeitet? ☒ ja, aber nur auf Weisung der Auftraggeberin und auf Geräten der Auftragnehmerin ☐ nein
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 getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

5	**Maßnahmen zur sicheren Datenübertragung**
5.1	Erfolgt der Transfer personenbezogener Daten durchgängig verschlüsselt? ☐ gar nicht ☐ nein, Datenübertragung erfolgt per MPLS ☐ per verschlüsselter Datei als Mailanhang ☐ per PGP/SMime ☐ per verschlüsseltem Datenträger ☐ per VPN ☒ per SSL/TLS ☒ per SFTP ☐ Sonstiges:
5.2	Wer verwaltet die Schlüssel bzw. die Zertifikate? ☐ Anwender selbst ☒ eigene IT ☐ Externer Dienstleister
5.2	Werden die Übertragungsvorgänge protokolliert? ☒ ja ☐ nein
5.3	**Wenn 5.2 ja**: Wie lange werden diese Protokolldaten aufbewahrt? Dauerhaft
5.4	**Wenn 5.2 ja**: Werden die Protokolle regelmäßig ausgewertet? ☐ ja ☒ nein, eine Auswertung ist 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: Die getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

B. Maßnahmen zur Sicherstellung der Verfügbarkeit (A 1.1 Standort 1)

1.	Serveraum
1.1	Verfügt der Serverraum über eine feuerfeste bzw. feuerhemmende Zugangstür? ☒ ja ☐ nein
1.2	Ist der Serverraum mit Rauchmeldern ausgestattet? ☒ ja ☐ nein
1.3	Ist der Serverraum an eine Brandmeldezentrale angeschlossen? ☒ ja ☐ nein
1.4	Ist der Serverraum mit Löschsystemen ausgestattet? ☒ ja, CO2 Löscher ☐ ja, Halon / Argon Löschanlage ☐ Nein
1.5	Woraus bestehen die Außenwände des Serverraumes? ☐ Massivwand (bspw. Beton, Mauer) ☐ Leichtbauweise ☒ Brandschutzwand (bspw. F90)
1.6	Ist der Serverraum klimatisiert? ☒ ja ☐ nein
1.7	Verfügt der Serverraum über eine unterbrechungsfreie Stromversorgung (USV)? ☒ ja ☐ nein
1.8	Wird die Stromversorgung des Serverraums zusätzlich über ein Dieselaggregat abgesichert? ☐ ja ☒ nein
1.9	Werden die Funktionalität 1.2, 1.3, 1.4, 1.7 und 1.8 regelmäßig getestet? ☒ 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 getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
2	**Backup- und Notfall-Konzept, Virenschutz**
2.1	Existiert ein Backupkonzept? ☒ ja ☐ nein
2.2	Wird die Funktionalität der Backup-Wiederherstellung regelmäßig getestet? ☒ ja ☐ nein

2.3	In welchem Rhythmus werden Backups vom System angefertigt, auf denen personenbezogene Daten gespeichert werden? ☒ Echtzeitspiegelung ☒ täglich ☐ ein bis dreimal pro Woche
2.4	Auf was für Sicherungsmedien werden die Backups gespeichert? ☒ Zweiter redundanter Server ☐ Sicherungsbänder ☐ Festplatten
2.5	Wo werden die Backups aufbewahrt? ☒ Zweiter redundanter Server steht an einem anderen Ort ☐ Safe, feuerfest, datenträger- und dokumentensicher ☐ abgeschlossener Aktenschrank / Schreibtisch ☐ Im Serverraum
2.6	Sind die Backups verschlüsselt? ☒ ja ☐ nein
2.7	Befindet sich der Aufbewahrungsort der Backups in einem vom primären Server aus betrachtet getrennten Brandabschnitt bzw. Gebäudeteil? ☒ ja ☐ nein
2.8	Existiert ein dokumentierter Prozess zum Software- bzw. Patchmanagement? ☒ ja ☐ nein ☐ Prozess existiert, ist jedoch nicht dokumentiert
2.9	**Wenn 2.8 ja**, wer ist für das Software- bzw. Patchmanagement verantwortlich? ☐ Anwender selbst ☒ eigene IT ☐ Externer Dienstleister
2.10	Existiert ein Notfallkonzept (bspw. Notfallmaßnahmen bei Hardwaredefekte / Brand / Totalverlust etc.)? ☒ ja ☐ nein
2.11	Sind die IT Systeme technisch vor Datenverlusten / unbefugten Datenzugriffen geschützt? Ja, mittels stets aktualisiertem ☒ Virenschutz ☒ Anti-Spyware ☒ Spamfilter ☒ Firewall ☒ Backup
2.12	**Wenn 2.11 ja**, wer ist für den aktuellen Virenschutz, Anti-Spyware und Spamfilter verantwortlich? ☐ Anwender selbst ☒ 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 getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

3	**Netzanbindung**
3.1	Verfügt das Unternehmen über eine redundante Internetanbindung? ☐ ja ☒ nein
3.2	Sind die einzelnen Standorte des Unternehmens redundant miteinander verbunden? ☒ ja ☐ nein
3.3	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 getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

C. Sonstige Maßnahmen nach Art. 32 Abs. 1 lit. b, c, d DSGVO

1.	**Belastbarkeit**
	Existieren Maßnahmen, die die Fähigkeit gewährleisten, die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen? ☒ ja ☐ nein Die IT-Administration der Auftragnehmerin führt regelmäßige Stress- und Performancetests durch, um die Auftragsverarbeitung und die Systeme der Auftragnehmerin nach dem Stand der Technik aufrecht zu erhalten.
2	**Wiederherstellbarkeit**
	Existieren Notfall- oder Recovery-Konzepte und Maßnahmen, die die Fähigkeit gewährleisten, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen? ☒ ja ☐ nein
3	**Verfahren zur Überprüfung, Bewertung und Evaluierung der getroffenen Maßnahmen**
3.1	Existiert ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung? ☒ ja ☐ nein In Zusammenarbeit mit dem Datenschutzbeauftragten der Auftragnehmerin werden die technischen und organisatorischen Maßnahmen ständig dokumentiert, jährlich geprüft und bewertet sowie ggfs. angepasst.
3.2	Wird ein Datenschutz-Managementtool eingesetzt? ☒ ja ☐ nein Das Datenschutz-Managementtool dient der Dokumentation aller Verfahren und Prozesse (u. a. Verzeichnis der Verarbeitungstätigkeiten, Datenpannen-Meldung und Betroffenenanfragen) sowie deren Evaluierung.
3.3	Gibt es eine dokumentierte Richtlinie zum Vorgehen bei Datenpannen? ☒ ja ☐ nein
3.4	Existiert ein Verzeichnis der Verarbeitungstätigkeiten? ☒ 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 getroffenen Maßnahmen sind geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.