Vertrag über Auftragsverarbeitung (AVV)

Zwischen

– nachfolgend „Verantwortlicher“ genannt –

und

dbh Logistics IT AG

Martinistraße

4728195 Bremen

– nachfolgend „Auftragsverarbeiter“ genannt

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

§ 1 Gegenstand und Dauer des Auftrags

(1) 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 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 darf Unterauftragsverarbeiter, die nicht in Anhang 2 benannt sind, nur beauftragen, wenn der Verantwortliche in die Beauftragung vorher schriftlich eingewilligt hat. Der Auftragsverarbeiter stellt die Informationen, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden, rechtzeitig, mindestens jedoch drei Wochen vor der Beauftragung des betreffenden Unterauftragsverarbeiters, zur Verfügung. 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.

§ 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. 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.

(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:

a. Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Anzahl der betroffenen Personen und Datensätze,
b. Name und Kontaktdaten von Kontaktpersonen für weitere Informationen,
c. Beschreibung der wahrscheinlichen Folgen der Verletzung sowie
d. 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

(1) 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.

Auftraggeberin

_____

Bremen,

Auftragnehmerin
dbh Logistics IT AG

_____ _____

Anhang 1: Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

Gegenstand der Verarbeitung	Der Gegenstand der Verarbeitung personenbezogener Daten ergibt sich aus dem mit dem Auftraggeber geschlossenen Vertrag.
Art und Zweck der Verarbeitung	Art und Zweck der Aufgaben des Auftragnehmers sind im Folgenden der dem Auftrag zu Grunde liegenden Leistungsvereinbarungen beschrieben.
Art der Daten	Adress- und Kommunikationsdaten, Personenstammdaten, Vertragsstammdaten, Abrechnungs- und Zahlungsdaten des Auftraggebers, Planungs- und Steuerungsdaten, Auskunftsangaben (öffentliche Verzeichnisse).
Kategorien betroffener Personen	Beschäftigte, Kunden, Interessenten, Lieferanten, Vertriebs- und Kooperationspartner, Ansprechpartner
Dauer der Verarbeitung	Entspricht der Dauer des Hauptvertrages

Name und Kontaktdaten des Datenschutz-beauftragten der Auftraggeberin (sofern benannt)	
Name und Kontaktdaten des Datenschutz-beauftragten der Auftragnehmerin (sofern benannt)	Dr. Uwe Schläger c/o datenschutz nord GmbH Konsul-Smidt-Straße 88 28217 Bremen Tel.: 0421 69 66 32 0 Fax: 0421 69 66 32 11 office@datenschutz-nord.de

Anhang 2: Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

Unterauftragnehmer (Name, Rechtsform, Sitz der Gesellschaft)	**Verarbeitungsstandort**	**Art der Dienstleistung**
Bremen Briteline GmbH, Wiener Str. 5 28359 Bremen	Wiener Str. 5, 28359 Bremen, Deutschland	Housing IT-Infrastruktur, Bereitstellung Internetleitungen keine Auftragsverarbeitung

dbh speichert und hostet Kundendaten ausschließlich in den genannten Rechenzentren in Bremen, Deutschland.

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

Liste der technisch-organisatorischen Maßnahmen

A Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität

1.	**Zutrittskontrollmaßnahmen zu Serverräumen**
1.0	Werden personenbezogene Daten auf Servern gespeichert, die von Ihnen betriebenen werden? ☒ ja ☐ nein
	Wenn 1.0 nein: In diesem Fall müssen die weiteren Fragen zu A1 nicht beantwortet werden, sondern sogleich die Fragen ab A2. Auch die Fragen zu B1 und B2 entfallen.
1.1	Standort des Serverraums / Rechenzentrums (RZ). Martinistr. 47-49, 28195 Bremen
1.2	Sind die personenbezogenen Daten auf mehr als einen Serverstandort / Rechenzentrum verteilt (z. B. Backup Server/ Nutzung von Cloud-Dienstleistungen)? ☒ ja ☐ nein
1.3	**Falls 1.2 ja: Machen Sie bitte die entsprechenden Standortangaben auch bzgl. weiterer Server.** Weitere Serverstandorte: Bremen Briteline GmbH, Wiener Str. 5, 28359 Bremen
1.4	Gelten die folgenden Angaben zu Zutrittskontroll-Maßnahmen für **alle** im Einsatz befindlichen Server- / RZ Standorte? ☒ ja ☐ nein
1.5	**Falls 1.4 nein: Beantworten Sie bitte die Fragen 1.6 bis 1.21 und B für weitere RZ- / Serverstandorte.**
1.6	Ist der Serverraum fensterlos? ☒ ja ☐ nein
1.7	Wenn 1.6 nein: Wie sind die Fenster vor Einbruch geschützt? ☐ vergittert ☐ alarmgesichert ☐ abschließbar ☐ gar nicht ☐ Sonstiges: bitte eintragen
1.8	Ist der Serverraum mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? ☒ ja ☐ nein
1.9	Wenn 1.8 ja: Wer wird informiert, wenn die EMA auslöst? **Mehrfachantworten möglich!** ☒ beauftragter Wachdienst ☒ Administrator ☒ Leiter IT ☐ Sonstiges: bitte eintragen
1.10	Ist der Serverraum videoüberwacht? ☐ ja, ohne Bildaufzeichnung ☒ ja, mit Bildaufzeichnung
1.11	**Wenn 1.10 ja, mit Bildaufzeichnung**: Wie lange werden die Bilddaten gespeichert? **30** Tage
1.12	Wie viele Personen haben Zutritt zum Serverraum und welche Funktionen haben diese inne? Anzahl der Personen: ca. 10 Personen Funktion im Unternehmen: Administratoren und deren Vertreter

1.13	Ist der Serverraum mit einem elektronischen Schließsystem versehen? ☒ ja ☐ nein, mit mechanischem Schloss
1.14	**Wenn 1.13 ja**: Welche Zutrittstechnik kommt zum Einsatz? **Mehrfachantworten möglich!** ☒ RFID ☒ PIN ☐ Biometrie ☐ Sonstiges: bitte eintragen
1.15	**Wenn 1.13 ja**: Werden die Zutrittsrechte personifiziert vergeben? ☒ ja ☐ nein
1.16	**Wenn 1.13 ja**: Werden die Zutritte zum Raum im Zutrittssystem protokolliert? ☒ ja, sowohl erfolgreiche als auch erfolglose Zutrittsversuche ☐ ja, aber nur erfolgreiche Zutritte ☐ ja, aber nur erfolglose Zutrittsversuche ☐ nein, das Schloss wird nur freigegeben oder nicht
1.17	**Wenn 1.16 ja**: Wie lange werden die Zutrittsdaten ungefähr gespeichert? 100 Tage
1.18	**Wenn 1.13 nein**, wie viele Schlüssel zum Serverraum existieren, wo werden diese aufbewahrt, wer gibt die Schlüssel aus? Anzahl Schlüssel: Schlüsselanzahl Aufbewahrungsort: Aufbewahrungsort eintragen Ausgabestelle: bitte Ausgabestelle angeben
1.19	Aus welchem Material besteht die Zugangstür zum Serverraum? ☒ Stahl / Metall ☐ sonstiges Material
1.20	Wird der Serverraum neben seiner eigentlichen Funktion noch für andere Zwecke genutzt? ☐ ja ☒ nein
1.21	**Wenn 1.20 ja**: Was wird in dem Serverraum noch aufbewahrt? ☐ Lagerung Büromaterial ☐ Lagerung Akten ☐ Archiv ☐ Lagerung von IT Ausstattung ☐ Sonstiges: bitte eintragen
	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 Mit einer regelmäßigen Bewertung und Anpassung der eingesetzten Enterprisetechnologien, sowie einem umfangreichen IT-Sicherheitsmanagement gem. ISO27001 in Verbindung mit regelmäßigen externen Audits wird der Betrieb sichergestellt.
2.	**Zutrittskontrollmaßnahmen zu Büroräumen**
2.1	Standort der Clientarbeitsplätze, von denen auf personenbezogene Daten zugegriffen wird: Bremen
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: bitte eintragen
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: Elektronisches Schließsystembitte 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? 2 Jahre
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: Personalabteilung
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 Im Rahmen eines umfangreichen IT-Sicherheitsmanagement gem. ISO27001 in Verbindung mit regelmäßigen externen Audits wird die Einhaltung der Prozesse und die regelmäßige Überprüfung des Schutzniveaus durchgeführt.
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:** mindestens 8 **Muss das Passwort Sonderzeichen enthalten?** ☒ ja ☐ nein **Mindest-Gültigkeitsdauer in Tagen:** max. 100 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? Wenn ja, nach wieviel Minuten? 3 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, 5 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 5 Versuche ☐ nein
3.13	**Wenn 3.12 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 30 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 Im Rahmen eines umfangreichen IT-Sicherheitsmanagement gem. ISO27001 in Verbindung mit regelmäßigen externen Audits wird die Einhaltung der Prozesse und die regelmäßige Überprüfung des Schutzniveaus durchgeführt.
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 Im Rahmen eines umfangreichen IT-Sicherheitsmanagement gem. ISO27001 in Verbindung mit regelmäßigen externen Audits wird die Einhaltung der Prozesse und die regelmäßige Überprüfung des Schutzniveaus durchgeführt.
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: bitte angeben
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 5.3 ja**: Wie lange werden diese Protokolldaten aufbewahrt? Je nach gesetzlicher Aufbewahrungspflicht.
5.5	**Wenn 5.3 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 Im Rahmen eines umfangreichen IT-Sicherheitsmanagement gem. ISO27001 in Verbindung mit regelmäßigen externen Audits wird die Einhaltung der Prozesse und die regelmäßige Überprüfung des Schutzniveaus durchgeführt.

B. Maßnahmen zur Sicherstellung der Verfügbarkeit

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? **Mehrfachantworten möglich!** ☒ ja, CO2 Löscher ☐ ja, Halon / Argon Löschanlage ☒ Sonstiges: Mini-max 1230
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, 1.6, 1.7 und 1.8, sofern vorhanden, 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 Im Rahmen eines umfangreichen IT-Sicherheitsmanagement gem. ISO27001 in Verbindung mit regelmäßigen externen Audits wird die Einhaltung der Prozesse und die regelmäßige Überprüfung des Schutzniveaus durchgeführt.
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 Systemen angefertigt, auf denen personenbezogene Daten gespeichert werden? ☐ Echtzeitspiegelung ☒ täglich ☐ ein bis dreimal pro Woche ☐ Sonstiges: bitte angeben
2.4	Auf was für Sicherungsmedien werden die Backups gespeichert? ☒ Zweiter redundanter Server ☐ Sicherungsbänder ☒ Festplatten ☐ Sonstiges: bitte angeben
2.5	Wo werden die Backups aufbewahrt? ☒ Zweiter redundanter Server steht an einem anderen Ort ☐ Safe, feuerfest, datenträger- und dokumentensicher ☐ einfacher Safe ☐ Bankschließfach ☐ abgeschlossener Aktenschrank / Schreibtisch ☐ Im Serverraum ☐ Privathaushalt ☐ Sonstiges: bitte Art der Aufbewahrung angeben
2.6	**Zu 2.5:** Im Falle eines Transports der Backups: Wie wird dieser durchgeführt? ☐ Mitnahme durch einen MA der IT / ~~Geschäftsleitung / Sekretärin~~ ☐ Abholung durch Dritte (bspw. Bankmitarbeiter / Wachunternehmen) ☒ Sonstiges: Backups werden nicht manuell transportiert
2.7	Sind die Backups verschlüsselt? ☐ ja ☒ nein
2.8	Befindet sich der Aufbewahrungsort der Backups in einem vom primären Server aus betrachtet getrennten Brandabschnitt bzw. Gebäudeteil? ☒ ja ☐ nein
2.9	Existiert ein dokumentierter Prozess zum Software- bzw. Patchmanagement? ☒ ja ☐ nein ☐ Prozess existiert, ist jedoch nicht dokumentiert
2.10	**Wenn 2.9 ja**, wer ist für das Software- bzw. Patchmanagement verantwortlich? ☐ Anwender selbst ☒ eigene IT ☐ Externer Dienstleister
2.11	Existiert ein Notfallkonzept (bspw. Notfallmaßnahmen bei Hardwaredefekte / Brand / Totalverlust etc.)? ☒ ja ☐ nein
2.12	Sind die IT Systeme technisch vor Datenverlusten / unbefugten Datenzugriffen geschützt? Ja, mittels stets aktualisiertem ☒ Virenschutz ☒ Anti-Spyware ☒ Spamfilter
2.13	**Wenn 2.12 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

	Im Rahmen eines umfangreichen IT-Sicherheitsmanagement gem. ISO27001 in Verbindung mit regelmäßigen externen Audits wird die Einhaltung der Prozesse, die Leistungsfähigkeit der eingesetzten Systeme und die regelmäßige Überprüfung des Schutzniveaus durchgeführt.
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 Im Rahmen eines umfangreichen IT-Sicherheitsmanagement gem. ISO27001 in Verbindung mit regelmäßigen externen Audits wird die Einhaltung der Prozesse und die regelmäßige Überprüfung des Schutzniveaus durchgeführt. Alle für die Netzanbindung benötigten System sind redundant ausgelegt. Die redundante Internetanbindung erfolgt über unterschiedliche Trassenführungen und Internetprovider.

C. Pseudonymisierung/Verschlüsselung, Art. 32 Abs. 1 lit. a DSGVO

1.	**Einsatz von Pseudonymisierung**
1.1	Werden verarbeitete personenbezogene Daten pseudonymisiert? ☐ ja Bitte Kategorien der Daten angeben. ☒ nein
	Wenn 1.1 nein: In diesem Fall müssen die weiteren Fragen zu C1 nicht beantwortet werden, sondern sogleich die Fragen ab C2.
1.2	Werden Algorithmen zur Pseudonymisierung eingesetzt? ☐ ja ☐ nein
1.3	**Wenn 1.1 ja:** Welcher Algorithmus wird zur Pseudonymisierung eingesetzt? Klicken Sie hier, um Text einzugeben.
1.4	Erfolgt eine Trennung der Zuordnungsdaten und eine Aufbewahrung in getrennten Systemen? ☐ ja ☐ nein
1.5	Wie kann die Pseudonymisierung bei Bedarf Rückgängig gemacht werden? **Mehrfachantworten möglich!**

	☐ gemäß einem definierten Verfahren ☐ im Mehr-Augen-Prinzip ☐ Direktzugriff auf nicht pseudonymisierte Rohdaten ☐ Auf Weisung des Vorgesetzten ☐ Sonstiges: bitte eintragen
2.	**Einsatz von Verschlüsselung**
2.1	Werden verarbeitete personenbezogene Daten über die bereits beschriebenen Maßnahmen hinaus verschlüsselt? ☐ ja Bitte Kategorien der Daten angeben. ☒ nein
	Wenn 2.1 nein: In diesem Fall müssen die weiteren Fragen zu C2 nicht beantwortet werden, sondern sogleich die Fragen ab D1.
2.2	Welcher Arten der Verschlüsselung werden eingesetzt? **Mehrfachantworten möglich!** Im Fall der Mehrfachantworten beschreiben Sie bitte im Feld „Sonstige“, welche Art der Verschlüsselung für welche Daten eingesetzt wird. ☐ Ende-zu-Ende-Verschlüsselung ☐ Transportverschlüsselung ☐ Data-at-Rest-Verschlüsselung ☐ Sonstige: bitte eintragen.
2.3	Welche kryptographischen Algorithmen werden zur Verschlüsselung oder für verschlüsselungsartige Maßnahmen (z. B. Hashen von Passwörtern) eingesetzt? ☐ AES ☐ SHA-256 ☐ RSA-2048 oder höher ☐ Sonstige: bitte eintragen
2.4	Wer hat Zugriff auf die Verschlüsselten Daten? Mitarbeiter aus den Abteilungen: bitte eintragen. Insgesamt haben … Mitarbeiter Zugriff auf die verschlüsselten Daten
	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: ISO27001

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

1.	**Belastbarkeit**
	Es existieren Maßnahmen, die die Fähigkeit gewährleiten, die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. ☐ nein ☒ ja bitte Maßnahmen beschreiben.

2	**Wiederherstellbarkeit**
	Existieren Notfall- oder Recoverykonzepte und Maßnahmen über B.2.11 hinaus, die die Fähigkeit gewährleisten, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen? ☒ nein ☐ ja bitte Maßnahmen beschreiben.
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? ☐ nein ☒ ja ISO27001 - Audits
3.2	**Wenn 3.1 ja:** In welchen Abständen finden die Überprüfungen statt? 1 mal pro Jahr
3.3	**Wenn 3.1 ja:** Werden die Ergebnisse der Prüfungen dokumentiert? ☒ ja ☐ nein
3.4	Gibt es Zertifizierungen mit Bezug zu den technisch-organisatorischen Maßnahmen und wenn ja, welche? ☒ ja, ISO27001 ☐ 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: ISO27001