KUNDENINFORMATION ZUR DATENVERARBEITUNG GEM. EU-DSGVO

1. ALLGEMEINE INFORMATIONEN

1.1. Verantwortliche für die Datenverarbeitung (Art. 13 DSGVO)

dbh Logistics IT AG
Martinistr. 47-49
28195 Bremen
Telefon +49 421 30902-0
E-Mail info(at)dbh.de

1.2. Kontaktdaten des Datenschutzbeauftragten

Herr Dr. Uwe Schläger
datenschutz nord GmbH
Konsul-Smidt-Straße 88
28217 Bremen
Tel.: 0421 69 66 32 0
Fax: 0421 69 66 32 11
E-Mail: office@datenschutz-nord.de

1.3. Information zur Datenverarbeitung

Wir verarbeiten Ihre personenbezogenen Daten gem. Art.28 DSGVO, um den Vertrag zu erfüllen.

1.4. Technisch-organisatorische Maßnahmen

Anhang 1: Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

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

Name und Kontaktdaten des Datenschutz-beauftragten der Auftraggeberin (sofern benannt)	
Name und Kontaktdaten des Datenschutz-beauftragten der Auftragnehmerin (sofern benannt)	Herr Dr. Uwe Schläger 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	Bremen, Deutschland	Housing IT-Infrastruktur, Bereitstellung Internetleitungen keine Auftragsverarbeitung

Anhang 3: 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
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
3.2	Authentisieren sich die Mitarbeiter über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst? ☒ ja ☐ nein
3.3	Existieren verbindliche Passwortparameter im Unternehmen? ☒ ja ☐ nein
3.4	**Passwort-Zeichenlänge:** mindestens 8 **Muss das Passwort Sonderzeichen enthalten?** ☒ ja ☐ nein **Mindest-Gültigkeitsdauer in Tagen:** max. 100 Tage
3.5	Zwingt das IT System den Nutzer zur Einhaltung der oben genannten PW Vorgaben? ☒ ja ☐ nein
3.6	Wird der Bildschirm bei Inaktivität des Benutzers gesperrt? Wenn ja, nach wieviel Minuten? 3 Minuten
3.7	Welche Maßnahmen ergreifen Sie bei Verlust, Vergessen oder Ausspähen eines Passworts? ☒ Admin vergibt neues Initialpasswort ☐ keine

3.8	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen? ☒ ja, 5 Versuche ☐ nein
3.9	**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.
3.10	Wie erfolgt die Authentisierung bei Fernzugängen: Authentisierung mit ☐ Token ☒ VPN-Zertifikat ☒ Passwort
3.11	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen bei Fernzugängen? ☒ ja 5 Versuche ☐ nein
3.12	**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.
3.13	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
	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
5.2	Werden die Übertragungsvorgänge protokolliert? ☒ ja ☐ nein
5.3	**Wenn 5.2 ja**: Wie lange werden diese Protokolldaten aufbewahrt? Je nach gesetzlicher Aufbewahrungspflicht.
5.4	**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 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.