PRIVACY Central

02.01.2021

Allgemeine Lizenzbedingungen privacy port

der

PRIVACY Central GmbH

Konsul-Smidt-Str. 88, 28217 Bremen

(Lizenzgeber)

Präambel

Der Lizenzgeber stellt dem Lizenznehmer das Datenschutz-Managementsystem privacy port als sogenannte Software-as-a-Service (SaaS) zur Nutzung im Unternehmensumfeld (B2B) („Software“) zur Verfügung. Der Lizenzgeber ist Urheber und Inhaber sämtlicher Nutzungsrechte an der Software. Der Lizenzgeber unterbreitet dem Lizenznehmer hierzu ein individuelles Angebot. Nimmt der Lizenznehmer das Angebot an, so kommt ein Lizenzvertrag zu den nachstehenden Bedingungen zustande.

§ 1 Vertragsgegenstand

(1) Der Lizenzgeber gewährt die Nutzung der Software privacy port in der jeweils aktuellen Version sowie in dem jeweiligen Funktionsumfang, wie er sich aus dem individuell für den Lizenznehmer erstellten Angebot sowie der Funktionsbeschreibung in **Anlage A.1.** ergibt. Die in dieser Anlage enthaltenen Angaben sind als Leistungsbeschreibung zu verstehen und nicht als Garantien. Der Lizenzgeber behält sich vor, weitere Funktionalitäten und Leistungsverbesserungen im Laufe des Lizenzvertrages zur Verfügung zu stellen.

(2) Gegenstand dieses Vertrages ist die Gewährung von Nutzungsrechten an der gewählten Software entsprechend der angebotenen Lizenzklasse. Nutzung in diesem Zusammenhang bedeutet die Ermöglichung des Zugriffs auf die im Rechenzentrum des Lizenzgebers installierte Software mit der in § 3 definierten Verfügbarkeit. Eine Aushändigung auf Datenträger oder Downloadmöglichkeit ist nicht Gegenstand der Nutzung.

(3) Installations- und Konfigurationsleistungen sind nicht Gegenstand dieses Vertrages. Etwaige Workshops bzw. Schulungen, die dem Lizenznehmer Kenntnisse zur fachgerechten Nutzung der Software vermitteln, werden separat vereinbart, dies gilt auch für Anwenderunterstützung (Support) während der Laufzeit des Vertrages.

§ 2 Nutzungsrechte

(1) Der Lizenzgeber gewährt dem Lizenznehmer ein entgeltliches, durch die Vertragsdauer zeitlich befristetes, nicht ausschließliches Recht zur Nutzung der Software (Lizenz). Die Lizenz berechtigt zur Nutzung der Software im Rahmen eines normalen Gebrauchs. Auf andere Nutzungsarten erstreckt sich die Lizenz nicht.

(2) Zur Nutzung erhält der Lizenznehmer eine zwischen den Parteien vereinbarte Anzahl von Zugriffsmöglichkeiten für dedizierte Nutzer. Eine Nutzung dieser Zugriffsmöglichkeiten durch andere Nutzer innerhalb desselben Unternehmens bedarf der Absprache mit dem Lizenzgeber.

(3) Der Lizenznehmer darf die Software nicht in sonstiger Weise unterlizensieren, sie öffentlich wiedergeben oder zugänglich machen oder aber Dritten zur Verfügung stellen, sei es entgeltlich oder unentgeltlich.

§ 3 Verfügbarkeit

(1) Mit Ausnahme von geplanten Nicht-Verfügbarkeiten aufgrund notwendiger Updates und ähnlicher Veränderungen der Software auf Veranlassung des Lizenzgebers, sichert der Lizenzgeber eine durchschnittliche jährliche Verfügbarkeit von 99,5 % zu.

(2) Updates und ähnliche Leistungsverbesserungen bzw. Fehlerbehebungen, die die Verfügbarkeit der Software für einen definierten Zeitraum einschränken, werden dem Lizenznehmer mit einer Vorlaufzeit von mindestens zwei Werktagen mitgeteilt.

§ 4 Vertragslaufzeit, Kündigung

(1) Der Vertragsbeginn ergibt sich aus der Erklärung des Lizenznehmers, das Angebot des Lizenzgebers anzunehmen, und wird zunächst für einen Zeitraum von 12 Jahr fest geschlossen. Wenn der Vertrag nicht spätestens drei Monate vor Ablauf dieser Zeit schriftlich gekündigt wird, verlängert er sich jeweils automatisch um weitere 12 Monate.

(2) Die Kündigung aus wichtigem Grund bleibt unberührt.

(3) Im Falle der Kündigung des Vertrags können die im Datenschutz-Managementsystem privacy port gespeicherten Daten auf Verlangen als Export in einem gängigen maschinenlesbaren Format zur Verfügung gestellt werden.

§ 5 Lizenzgebühr privacy port

(1) Die monatliche Lizenzgebühr für das Produkt privacy port ergibt sich aus dem Angebot. Der Lizenznehmer ist insoweit verpflichtet, dem Lizenzgeber bei Vertragsbeginn wahrheitsgemäß die für die jeweilige Lizenzklasse erforderlichen Angaben hinsichtlich der Anzahl der nutzungsberechtigten Unternehmen sowie der Anzahl der Anwender zu machen.

(2) Jede Veränderung dieser für die gewählte Lizenzklasse relevanten Angaben ist dem Lizenzgeber unverzüglich anzuzeigen. Der Lizenzgeber behält sich vor, die

weitere Nutzung der Software bei Überschreiten der maximal in der gewählten Lizenzklasse vorgesehenen Anzahl von Unternehmen oder der Anzahl von Anwendern technisch einzuschränken.

(3) Der Lizenzgeber ist befugt, das Lizenzmodell im Januar eines jeden Jahres an den Preissteigerungs-Index anzupassen, erstmalig im Januar des übernächsten Jahres nach Vertragsschluss. Sofern der Lizenznehmer hiermit nicht einverstanden ist, obliegt ihm ein außerordentliches Kündigungsrecht, das er innerhalb von vier Wochen nach Bekanntgabe der Preisangleichung wahrnehmen kann. Die Bekanntgabe von Preisanpassungen erfolgt per eMail.

(4) Die Zahlung der Lizenzgebühr ist für das jeweilige Vertragsjahr (vgl. oben § 4) mit Vertragsschluss fällig und kann nach Wahl des Lizenznehmers mittels der angebotenen Zahlungsverfahren gezahlt werden. Sämtliche Preise sind Nettopreise.

§ 6 Gewährleistung

(1) Der Lizenzgeber gewährleistet, dass die Software der Produktbeschreibung entspricht und mit der gebotenen Sorgfalt und Fachkenntnis erstellt worden ist. Dennoch ist nach dem derzeitigen Stand der Technik der völlige Ausschluss von Softwarefehlern nicht möglich.

(2) Der Lizenzgeber wird Fehler der Software berichtigen, die die bestimmungsgemäße Benutzung erheblich beeinträchtigen. Die Fehlerberichtigung erfolgt durch den Lizenzgeber, je nach Stellenwert des Fehlers, durch die Bereitstellung einer verbesserten Softwareversion.

(3) Der Lizenzgeber leistet Gewähr für die vereinbarte Beschaffenheit der Software und dafür, dass der Lizenznehmer die Software ohne Verstoß gegen Rechte Dritter nutzen kann. Die Gewährleistung ist nicht anwendbar auf Mängel, die in der Soft- bzw. Hardwareumgebung des Lizenznehmers begründet sind.

(4) privacy port ist ein online-Datenschutz-Managementsystem, welches den Lizenznehmer bei der Dokumentation und Strukturierung datenschutzrechtlicher Anforderungen unterstützt. Der Lizenznehmer bleibt auch mit der Nutzung der Software datenschutzrechtlich verantwortlich im Sinne des Art. 4 Nr. 7 der Datenschutzgrundverordnung (DSGVO). Ansprüche gegen den Lizenzgeber aufgrund der Verletzung datenschutzrechtlicher Pflichten des Lizenznehmers sind ausgeschlossen.

§ 7 Auftragsverarbeitung

Im Rahmen der Nutzung von privacy port ist der Lizenzgeber für den Lizenznehmer als Auftragsverarbeiter gemäß Art. 28 Datenschutzgrundverordnung tätig. Die Pflichten beider Parteien werden in dem diesem Vertrag als **Anlage A.2.** beigefügten Vertrag zur Auftragsverarbeitung geregelt.

§ 8 Haftung

(1) Der Lizenzgeber haftet für Schäden, die durch Vorsatz oder grober Fahrlässigkeit entstanden sind, sowie für die schuldhafte Verletzung wesentlicher Vertragspflichten nach den Vorschriften des ProdHaftG, soweit diese Verletzung in einer das Erreichen des Vertragszwecks gefährdenden Weise verursacht wurde.

(2) Bei Verletzung einer Kardinalpflicht (Pflicht, die wesentlich für die Erreichung des Vertragszwecks ist) ist die Haftung des Lizenzgebers begrenzt auf den Schaden, der nach der Art des fraglichen Geschäfts vorhersehbar und typisch ist und mit dessen Entstehen der Lizenzgeber aufgrund der ihm zu jenem Zeitpunkt bekannten Umstände typischerweise rechnen musste. Eine weitergehende Haftung des Lizenzgebers besteht nicht.

(3) Die vorgenannte Haftungsbeschränkung bezieht sich auch auf die persönliche Haftung der Mitarbeiter, Vertreter und Organe des Lizenzgebers.

§ 9 Schlussbestimmungen

(1) Sollte eine der vorliegenden Regelungen unwirksam sein, berührt dies nicht die Wirksamkeit der übrigen Bestimmungen.

(2) Die unwirksame Regelung wird in diesem Fall durch die gesetzliche Regelung ersetzt, die nach dem angenommenen Willen der Parteien dem wirtschaftlichen Zweck der unwirksamen Regelung am nächsten kommt.

(3) Es gilt deutsches Recht. Gerichtsstand ist Bremen.

A.1. Funktionsbeschreibung privacy port

- Verwaltung der Stammdaten des Lizenznehmers einschließlich verbundener Unternehmen,
- Verwaltung der Stammdaten und der Benutzerrechte des Datenschutzbeauftragten und des Koordinators des Lizenznehmers,
- Dokumentation und Bewertung der Verarbeitungstätigkeiten (Verfahrensverzeichnis) sowohl für Verantwortliche als auch für Auftragsverarbeiter,
- Dokumentation und Bewertung der Videosysteme, Down- und Upload von Kamera-Screenshots und Lageplänen,
- Dokumentation und Bewertung der Auftragsverarbeiter, Down- und Upload von Verträgen und Zertifikaten,
- Dokumentation und Bewertung der Datenempfänger außerhalb der EU, Down- und Upload von Verträgen,
- Dokumentation und Bewertung der technisch-organisatorischen Maßnahmen
- Dokumentation und Bewertung der Webseiten,
- Dokumentation der Auskünfte von Betroffenen, Down- und Upload von relevanten Dokumenten,
- Dokumentation meldepflichtiger Vorfälle, Down- und Upload von relevanten Dokumenten,
- Dokumentation von Datenschutz-Schulungen, Down- und Upload von Schulungsmaterial und Teilnehmerlisten,
- Dokumentation von Datenschutz-Projekten (u.a. Audits),
- Down- und Upload von Tätigkeitsberichten, Vertragsmustern und Merkblättern,
- Export von Formularen in pdf- oder xlsx-Format,
- Abbildung von Unternehmensgruppen und Konzernstrukturen,
- Mandantenfähigkeit.

A.2. Vertrag zur Auftragsverarbeitung

Zwischen dem im Hauptvertrag bezeichneten **Lizenzgeber** (hier nachfolgend als **Auftragnehmerin** bezeichnet) und dem im Hauptvertrag bezeichneten **Lizenznehmer (Auftraggeberin).**

§ 1 Gegenstand und Dauer des Auftrags

(1) Die Auftragnehmerin führt die in **Anlage A.3.** beschriebenen Dienstleistungen für die Auftraggeberin durch. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien betroffener Personen werden dort beschrieben.

(2) Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Abschluss des Hauptvertrages in Kraft und gilt, solange die Auftragnehmerin für die Auftraggeberin personenbezogene Daten verarbeitet.

§ 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.

(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 der Auftragsverarbeiter 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 hat für die zu verarbeitenden Daten angemessene technische und organisatorische Sicherheitsmaßnahmen getroffen und diese in **Anlage A.4.** dieses Vertrages dokumentiert. Die Sicherheitsmaßnahmen gewährleisten ein dem Risiko angemessenes Schutzniveau.

(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 ihre 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 hat zum Zeitpunkt des Vertragsschlusses folgende Unterauftragnehmer beauftragt:

Unterauftragnehmer (Name, Rechtsform, Sitz der Gesellschaft)	**Verarbeitungsstandort**	**Art der Dienstleistung**
PLUTEX GmbH, Bremen	Bremen	Hosting, Managed Services
ScaleUp Technologies GmbH & Co. KG, Hamburg	Berlin, Hamburg	Hosting, Managed Services
Mailjet SAS, Paris (Frankreich)	Frankfurt/Main, Saint-Ghislain (Belgien)	Bereitstellung von E-Mail-Services

Der Lizenzgeber sichert zu, nur solche externen Hosting-Dienstleister einzusetzen, die nach ISO/IEC 27001 oder anderen gleichwertigen Standards zertifiziert sind. Weitere Unterauftragnehmer dürfen nur beauftragt werden, wenn die Auftragnehmerin immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informiert wird. Ein Einspruch gegen die weitere Beauftragung 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 die 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.

§ 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, die Einsichtnahme in die Verarbeitungsprogramme 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.

A.3. Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

Gegenstand der Verarbeitung	Betrieb eines Datenschutz-Managementsystems
Art und Zweck der Verarbeitung	Dokumentation von Verfahren, Videosystemen, externen Dienstleistern, technisch-organisatorischen Maßnahmen, Schulungen, Auskunftsersuchen von Betroffenen, meldepflichtigen Vorfällen der Auftraggeberin gemäß Datenschutz-Grundverordnung
Art der personenbezogenen Daten	E-Mail-Adressen der Nutzer mit dezidierten Zugängen zum System. In aller Regel keine darüberhinausgehenden personenbezogenen Daten der Auftraggeberin, in Ausnahmefällen Anfragen von Betroffenen der Datenverarbeitung der Auftraggeberin
Kategorien betroffener Personen	Mitarbeiter, Kunden der Auftraggeberin

Name und Kontaktdaten des Datenschutzbeauftragten der Auftragnehmerin	Joanna Maxine Stünkel, Konzerndatenschutzbeauftragte der DSN Holding GmbH, office@datenschutz-nord.de

A.4. Technische und organisatorische Sicherheitsmaßnahmen

Die Auftragnehmerin garantiert gegenüber der Auftraggeberin folgende technisch-organisatorische Sicherheitsmaßnahmen:

- Das Hosting des Datenschutz-Managementsystems und die Administration der Server, Datenbanksysteme erfolgt durch einen nach ISO/IEC 27001 zertifizierten Dienstleister, der der Auftragnehmerin hoch verfügbare und sichere Managed Server bereitstellt.
- Auf die Anwendung führt die Auftragnehmerin regelmäßige Penetrationstests durch, die dem Auftraggeber bei Bedarf zur Verfügung gestellt werden können.
- Der Zugriff auf das Datenschutz-Managementsystem durch die Auftragnehmerin erfolgt verschlüsselt per SSL/TLS.
- Der temporäre Zugriff auf einzelne Web-Formulare erfolgt per Deep-Link; dieser wird über eine ausreichend lange ID abgesichert, die nicht erraten werden kann.
- Die Authentisierung von Mitarbeitern der Auftraggeberin erfolgt durch eine Multi-Faktor-Authentisierung. Neben Abfrage von Benutzernamen und Passwort wird einer der folgenden drei zusätzlichen Faktoren zur Authentisierung genutzt:

  1. über Abfrage und Filterung der IP-Adresse oder
  2. über ein one-time password-Verfahren oder
  3. über ein browser fingerprinting-Verfahren.

- Die durchschnittliche jährliche Verfügbarkeit des Systems beträgt 99,5 %.

A.4.1. Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität

1.	Zutrittskontrollmaßnahmen zu Serverräumen
1.0	Werden personenbezogene Daten des Verantwortlichen auf Servern gespeichert, die von Ihnen oder etwaigen Dienstleistern betrieben 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). ScaleUp Technologies GmbH &Co. KG ScaleUp Rechenzentrum Hamburg Hammerbrook, Süderstr. 198, 20537 Hamburg ScaleUp Rechenzentrum Hamburg Airport, Obenhauptstr. 1c, 22335 Hamburg
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	Gelten die folgenden Angaben zu Zutrittskontroll-Maßnahmen für **alle** im Einsatz befindlichen Server- / RZ Standorte? ☒ ja ☐ nein
1.4	Hat der Serverraum Fenster? ☐ ja ☒ nein
1.5	Ist der Serverraum mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? ☒ ja ☐ nein
1.6	Wenn 1.5 ja: Wer wird informiert, wenn die EMA auslöst? **Mehrfachantworten möglich!** ☐ beauftragter Wachdienst ☐ Administrator ☐ Leiter IT ☒ Sonstiges: Sicherheits-Leitstelle
1.7	Ist der Serverraum videoüberwacht? ☐ ja, ohne Bildaufzeichnung ☒ ja, mit Bildaufzeichnung ☐ nein
1.8	Wie viele Personen haben Zutritt zum Serverraum und welche Funktionen haben diese inne? Anzahl der Personen: Funktion im Unternehmen: Director of Infrastructure od. dessen Beauftragte; Rechenzentrumsbetreiber; Feuerwehr
1.9	Ist der Serverraum mit einem elektronischen Schließsystem versehen? ☒ ja ☐ nein, mit mechanischem Schloss
1.10	**Wenn 1.9 nein**, wie viele Schlüssel zum Serverraum existieren, wo werden diese aufbewahrt, wer gibt die Schlüssel aus? Anzahl Schlüssel: Aufbewahrungsort: Ausgabestelle:
1.11	Aus welchem Material besteht die Zugangstür zum Serverraum? ☒ Stahl / Metall ☐ sonstiges Material
1.12	Wird der Serverraum neben seiner eigentlichen Funktion noch für andere Zwecke genutzt? ☐ ja ☒ nein

2. Zutrittskontrollmaßnahmen zu Büroräumen

2.1	Standort der Clientarbeitsplätze, von denen auf personenbezogene Daten zugegriffen wird: PRIVACY Central GmbH, Konsul-Smidt-Str. 88, 28217 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: Polizei und Geschäftsführung, wenn außerhalb der Geschäftszeiten
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 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
2.8	**Wenn 2.8 ja**: Welche Zutrittstechnik kommt zum Einsatz? **Mehrfachantworten möglich!** ☒ RFID ☒ PIN ☐ Biometrie ☐ Sonstiges: bitte eintragen
2.9	**Wenn 2.8 ja**: Werden die Zutrittsrechte personifiziert vergeben? ☒ ja ☐ nein
2.10	**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
2.11	**Wenn 2.10 ja**: Wie lange werden diese Protokolldaten aufbewahrt? Anlassbezogen, abhängig vom Zweck der Speicherung
2.12	**Wenn 2.10 ja**: Werden die Protokolle regelmäßig ausgewertet? ☐ ja ☒ nein, eine Auswertung wäre 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: die Ausgabe wird mittels eines Formulars/Schlüsselbuch dokumentiert und durch den Schlüsselbeauftragten ausgegeben.
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.

3	Zugangs- und Zugriffskontrollmaßnahmen
3.1	Existiert ein Prozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen im Rahmen der Penetrationstests bei den eingesetzten 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:** mind. 8 Zeichen **Muss das Passwort Sonderzeichen enthalten?** ☒ ja ☐ nein **Mindest-Gültigkeitsdauer in Tagen:** 90 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? 15 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, 3 Versuche ☐ 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 30 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, bitte Anzahl eintragen 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 bitte Wert in Minuteneintragen 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

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? ☐ Physische Zerstörung durch eigene IT. ☒ Physische 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
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 / S/MIME ☐ per verschlüsseltem Datenträger ☐ per VPN ☒ per https/TLS ☐ per SFTP ☒ Sonstiges: hängt beim Penetrationstest von der Art der Schnittstelle ab, die geprüft wird.
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? bis zum Ende des jeweiligen Auftrags
5.5	**Wenn 5.3 ja**: Werden die Protokolle regelmäßig ausgewertet? ☐ ja ☒ nein, eine Auswertung wäre aber im Bedarfsfall möglich

A.4.2. 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, CO_2 Löscher ☒ ja, Halon / Argon Löschanlage ☐ Sonstiges: bitte angeben
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
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 von Systemen angefertigt, auf denen personenbezogene Daten gespeichert werden? ☐ Echtzeitspiegelung ☒ täglich ☐ ein bis dreimal pro Woche ☐ Sonstiges: alle zwei Stunden
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: bitte angeben
2.7	Sind die Backups verschlüsselt? ☐ ja ☒ nein *Anmerkung:*
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
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

A.4.3. 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

A.4.4. 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 Monitoring der betreffenden Systeme i.V.m. Kubernetes-Mechanismen für Bereitstellung ausreichender Serverinstanzen
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 automatisierte Recovery-Prozesse

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 Überwachung der IT-Infrastruktur, Benennung mehrerer Ansprechpartner, Austausch mit externen Sachverständigen
3.2	**Wenn 3.1 ja:** In welchen Abständen finden die Überprüfungen statt? Fortlaufend.
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, Klicken Sie hier, um Text einzugeben. ☒ nein