

Technisch-organisatorische Maßnahmen zur IT-Sicherheit nach Art. 32 DSGVO Anlage zu den Allgemeinen Geschäftsbedingungen für SaaS-Verträge

A. Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität

1.	Zutrittskontrollmaßnahmen zu Serverräumen
1.0	Werden personenbezogene Daten des Verantwortlichen auf Servern gespeichert, die nicht vom Auftragsverarbeiter, sondern von weiteren Dienstleistern betrieben werden? <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein
	Mit den weiteren Dienstleistern aus Anhang IV wurde ein Vertrag nach Art. 28 DSGVO abgeschlossen, der angemessene technische und organisatorische Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität gemäß Art. 32 DSGVO in Bezug auf den Serverraum vorsieht.

2.	Zutrittskontrollmaßnahmen zu Büroräumen
2.1	Standort der Clientarbeitsplätze, von denen auf personenbezogene Daten zugegriffen wird: Martinistraße 74-49, 28195 Bremen
2.2	Existiert ein Pförtnerdienst / ständig besetzter Empfangsbereich zum Gebäude bzw. zu Ihren Büros? <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein
2.3	Wird ein Besucherbuch geführt? <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein
2.4	Ist das Gebäude oder sind die Büroräume mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein
2.5	Wenn 2.4 ja: Wer wird informiert, wenn die EMA auslöst? <input checked="" type="checkbox"/> beauftragter Wachdienst <input checked="" type="checkbox"/> Administrator <input checked="" type="checkbox"/> Leiter IT <input type="checkbox"/> Sonstiges: bitte eintragen
2.6	Werden das Bürogebäude bzw. seine Zugänge videoüberwacht? <input checked="" type="checkbox"/> ja, ohne Bildaufzeichnung <input type="checkbox"/> ja, mit Bildaufzeichnung <input type="checkbox"/> 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? <input checked="" type="checkbox"/> ja, Gebäude und Büroräume sind elektronisch verschlossen <input type="checkbox"/> ja, aber nur das Gebäude, nicht der Eingang zu den Büros bzw. zur Büroetage. <input type="checkbox"/> ja, aber nur der Eingang zu den Büros / zur Büroetage, nicht das Gebäude insgesamt. <input type="checkbox"/> nein
2.9	Wenn 2.8 ja: Welche Zutrittstechnik kommt zum Einsatz? Mehrfachantworten möglich! <input checked="" type="checkbox"/> RFID <input type="checkbox"/> PIN <input type="checkbox"/> Biometrie <input type="checkbox"/> Sonstiges: Elektronisches Schließsystem

2.10	Wenn 2.8 ja: Werden die Zutrittsrechte personalisiert vergeben? <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein
2.11	Wenn 2.8 ja: Werden die Zutritte im Zutrittssystem protokolliert? <input checked="" type="checkbox"/> ja, sowohl erfolgreiche als auch erfolglose Zutrittsversuche <input type="checkbox"/> ja, aber nur erfolgreiche positive Zutritte <input type="checkbox"/> ja, aber nur erfolglose Zutrittsversuche <input type="checkbox"/> nein, das Schloss wird nur freigegeben oder nicht
2.12	Wenn 2.11 ja: Wie lange werden diese Protokolldaten aufbewahrt? 30 Tage
2.13	Wenn 2.11 ja: Werden die Protokolle regelmäßig ausgewertet? <input type="checkbox"/> ja <input checked="" type="checkbox"/> nein, eine Auswertung wäre aber im Bedarfsfall möglich
2.14	Existiert ein mechanisches Schloss für die Gebäude / Büroräume? <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein
2.15	Wenn 2.14 ja: Wird die Schlüsselausgabe protokolliert, wer gibt die Schlüssel aus? <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein Ausgabestelle: Personalabteilung des Dienstleisters
2.16	Gibt es offizielle Zutrittsregelung für betriebsfremde Personen (bspw. Besucher) zu den Büroräumen? <input type="checkbox"/> nein <input checked="" type="checkbox"/> 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 bei der Neueinstellung und beim Ausscheiden von Mitarbeitern bzw. bei organisatorischen Veränderungen? <input checked="" type="checkbox"/> definierter Freigabeprozess <input type="checkbox"/> kein definierter Freigabeprozess, auf Zuruf <input type="checkbox"/> Sonstige Vergabeweise: bitte angeben
3.2	Werden die Vergabe bzw. Änderungen von Zugriffsberechtigungen protokolliert? <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein
3.3	Authentisieren sich die Mitarbeiter über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst? <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein
3.4	Existieren verbindliche Passwortparameter im Unternehmen? <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein
3.5	Passwort-Zeichenlänge: 8 Muss das Passwort Sonderzeichen enthalten? <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein Mindest-Gültigkeitsdauer in Tagen: 100

3.6	Zwingt das IT System den Nutzer zur Einhaltung der oben genannten PW Vorgaben? <input checked="" type="checkbox"/> ja <input type="checkbox"/> 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? <input checked="" type="checkbox"/> Admin vergibt neues Initialpasswort <input type="checkbox"/> keine
3.9	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen? <input checked="" type="checkbox"/> ja, 5 Versuche <input type="checkbox"/> nein
3.10	Wenn 3.9 ja, Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht wurde? <input type="checkbox"/> Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt <input checked="" type="checkbox"/> Die Zugänge bleiben für 15 Minuten gesperrt.
3.11	Wie erfolgt die Authentisierung bei Fernzugängen: Authentisierung mit <input type="checkbox"/> Token <input checked="" type="checkbox"/> VPN-Zertifikat <input checked="" type="checkbox"/> Passwort
3.12	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen bei Fernzugängen? <input checked="" type="checkbox"/> ja, 5 Versuche <input type="checkbox"/> nein
3.13	Wenn 3.12 ja, Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht worden ist? <input type="checkbox"/> Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt <input checked="" type="checkbox"/> Die Zugänge bleiben für 15 Minuten gesperrt.
3.14	Wird der Fernzugang nach einer gewissen Zeit der Inaktivität automatisch getrennt? <input checked="" type="checkbox"/> ja, nach 30 Minuten <input type="checkbox"/> nein
3.15	Werden die Systeme, auf denen personenbezogene Daten verarbeitet werden, über eine Firewall abgesichert? <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein
3.16	Wenn 3.15 ja: Wird die Firewall regelmäßig upgedatet? <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein
3.17	Wenn 3.15 ja: Wer administriert Ihre Firewall? <input type="checkbox"/> eigene IT <input checked="" type="checkbox"/> Externer Dienstleister
3.18	Wenn ein externer DL zum Einsatz kommt: Kann sich dieser ohne Aufsicht durch Ihre IT auf die Firewall aufschalten? <input type="checkbox"/> ja <input checked="" type="checkbox"/> nein, die Aufschaltung ist nur im 4 Augenprinzip mit einem Mitarbeiter der eigenen IT möglich.

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?

	<input type="checkbox"/> Altpapier / Restmüll <input checked="" type="checkbox"/> Es stehen hierfür Schredder zur Verfügung, deren Nutzung angewiesen ist. <input checked="" type="checkbox"/> Es sind verschlossene Datentonnen aufgestellt, die von einem Entsorgungsdienstleister zur datenschutzkonformen Vernichtung abgeholt werden. <input type="checkbox"/> Sonstiges: bitte angeben
4.2	<p>Wie werden nicht mehr benötigte Datenträger (USB Sticks, Festplatten), auf denen personenbezogene Daten gespeichert sind, entsorgt?</p> <input type="checkbox"/> Physische Zerstörung durch eigene IT. <input checked="" type="checkbox"/> Physische Zerstörung durch externen Dienstleister. <input checked="" type="checkbox"/> Löschen der Daten <input type="checkbox"/> Löschen der Daten durch bitte Anzahl angeben Überschreibungen <input type="checkbox"/> Sonstiges: bitte angeben
4.3	<p>Dürfen im Unternehmen mobile Datenträger verwendet werden (z.B. USB-Sticks)</p> <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein
4.4	<p>Dürfen die Mitarbeiter private Datenträger (z.B. USB Sticks) verwenden?</p> <input type="checkbox"/> generell ja <input type="checkbox"/> ja, aber nur nach Genehmigung und Überprüfung des Speichermediums durch die IT. <input checked="" type="checkbox"/> nein, alle benötigten Speichermedien werden vom Unternehmen gestellt.
4.5	<p>Werden personenbezogene Daten auf mobilen Endgeräten verschlüsselt?</p> <input checked="" type="checkbox"/> Verschlüsselung der Festplatte <input type="checkbox"/> Verschlüsselung einzelner Verzeichnisse <input type="checkbox"/> keine Maßnahmen
4.6	<p>Verarbeiten Mitarbeiter personenbezogene Daten auch auf eigenen privaten Geräten (bring your own device)?</p> <input type="checkbox"/> ja <input checked="" type="checkbox"/> nein
5	<p>Maßnahmen zur sicheren Datenübertragung</p>
5.1	<p>Erfolgt der Transfer personenbezogener Daten durchgängig verschlüsselt?</p> <input type="checkbox"/> gar nicht <input type="checkbox"/> nein, Datenübertragung erfolgt per MPLS <input type="checkbox"/> nur vereinzelt <input type="checkbox"/> per verschlüsselter Datei als Mailanhang <input type="checkbox"/> per PGP / S/MIME <input type="checkbox"/> per verschlüsseltem Datenträger <input checked="" type="checkbox"/> per VPN

	<input checked="" type="checkbox"/> per https/TLS <input checked="" type="checkbox"/> per SFTP <input type="checkbox"/> Sonstiges: bitte angeben
5.2	Wer verwaltet die Schlüssel bzw. die Zertifikate? <input type="checkbox"/> Anwender selbst <input type="checkbox"/> eigene IT <input checked="" type="checkbox"/> Externer Dienstleister
5.3	Werden die Übertragungsvorgänge protokolliert? <input checked="" type="checkbox"/> ja <input type="checkbox"/> nein
5.4	Wenn 5.3 ja: Wie lange werden diese Protokolldaten aufbewahrt? 30 Tage
5.5	Wenn 5.3 ja: Werden die Protokolle regelmäßig ausgewertet? <input type="checkbox"/> ja <input checked="" type="checkbox"/> nein, eine Auswertung wäre aber im Bedarfsfall möglich

B. Maßnahmen zur Sicherstellung der Verfügbarkeit

Sicherungsmaßnahmen stammen vom Unterauftragnehmer dbh logistics IT AG, in die der Auftragsverarbeiter eingebunden ist.

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

Sicherungsmaßnahmen stammen vom Unterauftragnehmer dbh logistics IT AG, in die der Auftragsverarbeiter eingebunden ist.

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

Sicherungsmaßnahmen stammen vom Unterauftragnehmer dbh logistics IT AG, in die der Auftragsverarbeiter eingebunden ist.