HOWOGE

Anlage 2
Technische und organisatorische Maßnahmen

Bewertung der Maßnahmen zum Zeitpunkt des Abschlusses dieser Vereinbarung:
Bewertung mit 0-2, wobei „**1**“ dem aktuellen Stand der Technik / üblicher Organisation entspricht, „2“ dem neusten Stand der Technik und „0“ einem früheren Stand der Technik. Die jeweilige Bewertung kann sich auch durch die konkrete Kombination mit anderen Maßnahmen ergeben.

Die hochgestellten Zahlen an den einzelnen Maßnahmen weisen diese dem bisherigen System nach der nach Anlage zu § 9 BDSG (2003) zu: (1) Zutrittskontrolle, (2) Zugangskontrolle, (3) Zugriffskontrolle, (4) Weitergabekontrolle, (5) Eingabekontrolle, (6) Auftragskontrolle, (7) Verfügbarkeitskontrolle, (8) Trennungskontrolle

Maßnahme	Bewertung 0	**1**	2
I. Vertraulichkeit			
1) Organisatorische Maßnahmen			
☐ Alle Mitarbeiter, die mit personenbezogenen Daten Umgang haben, sind gesondert (z.B. durch Vertrag, Verpflichtungserklärung) oder gesetzlich zur Verschwiegenheit verpflichtet. (4)	☐	☐	☐
☐ Türen, Tore und Fenster sind außerhalb der Betriebszeiten fest verschlossen. (1)	☐	☐	☐
☐ Zutritt zum Betriebsgelände ist nur mit ☐ Sicherheitsschlüssel / ☐ Magnetkarte möglich. (1)	☐	☐	☐
☐ Es wird eine Anwesenheitsliste geführt. (1)	☐	☐	☐
☐ Besucher werden registriert. (1)	☐	☐	☐
☐ Besucher dürfen sich nicht unbegleitet im Gebäude bewegen. (1)	☐	☐	☐
☐ Mitarbeiter von Dienstleistern, die sich auf dem Betriebsgelände frei bewegen können (z.B. Reinigungspersonal, Boten, Lieferanten) werden gesondert auf Vertraulichkeit verpflichtet. (1)	☐	☐	☐
☐ Mitarbeiter- und Besucherausweise müssen stets sichtbar getragen werden. (1)	☐	☐	☐
☐ Die Vergabe von Schlüsseln und/oder Magnetkarten ist schriftlich geregelt. (1)	☐	☐	☐
☐ Es besteht ein Pförtnerdienst / Empfang ☐ 24/7, ☐ werktags von , sonst von . (1)	☐	☐	☐
☐ Es besteht ein Wachschutz ☐ 24/7, ☐ werktags von , sonst von . (1)	☐	☐	☐
☐ Die organisatorische Berechtigungsbewilligung (z.B. durch den Vorgesetzten) und die technische Berechtigungsvergabe (z.B. durch den Administrator) erfolgen durch verschiedene Personen. (3)	☐	☐	☐
☐ Es besteht ein Rechte- und Rollenkonzept. (3)	☐	☐	☐
☐ Individuelle Zuweisung von Rechten pro Benutzer (Abgestufte Zugriffsberechtigung). (3)	☐	☐	☐
☐ Daten werden nicht auf mobilen Endgeräten oder mobilen Datenspeichern gespeichert. (4)	☐	☐	☐
☐ Daten, die als sensibel eingestuft sind, werden nicht auf mobilen Endgeräten oder mobilen Datenspeichern gespeichert. (4)	☐	☐	☐
☐ Mit allen Auftragsverarbeitern wird eine schriftliche Vereinbarung zur Auftragsverarbeitung abgeschlossen. (4)	☐	☐	☐
☐ Es besteht ein Konzept zur Datenlöschung für alle Systeme. (4)	☐	☐	☐
☐ Es besteht ein Konzept zur Datenlöschung für ausgewählte Datenverarbeitungen ([Verarbeitungen/Verarbeitungsgruppen angeben]). (4)	☐	☐	☐
☐ Es besteht ein dokumentierter Prozess zur fachgerechten Vernichtung von ausgedienten Datenträgern. (4)	☐	☐	☐
☐ Es besteht eine verbindliche Anweisung zur Datenerfassung. (4)	☐	☐	☐
☐ Programme, mit denen Dateneingaben erfolgen können, sind dokumentiert. (4)	☐	☐	☐
☐ Arbeitsanweisungen zum Umgang mit Daten werden dokumentiert. (4)	☐	☐	☐
☐ Arbeitsanweisungen zur Gewährleistung der Datensicherheit werden dokumentiert.	☐	☐	☐
☐ Es finden regelmäßig Schulungen zum Datenschutz und zur Datensicherheit statt.	☐	☐	☐
☐ Der Einsatz privater Datenträger (z.B. USB-Sticks, externe Festplattem) ist untersagt. (4)	☐	☐	☐
☐ Verbot der Weitergabe von Passwörtern (3)	☐	☐	☐
☐ Getrennte Aufbewahrung von Datenbeständen, die zu unterschiedlichen Zwecken erhoben wurden oder die zu unterschiedlichen Schutzbedarfskategorien gehören. (8)	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐

HOWOGE

Maßnahme	Bewertung 0	1	2
2) Technische Maßnahmen			
☐ Betriebsgelände ist vollständig durch Zaun oder Mauer umgeben. (1)	☐	☐	☐
☐ Fenster zu Räumen mit ☐ EDV-Anlagen / ☐ Servern sind vergittert. (1)	☐	☐	☐
☐ Serverräume sind durch einbruchsichere ☐ Stahltür / ☐ Sicherheitstür gesichert. (1)	☐	☐	☐
☐ Zutritt zu Serverräumen ist nur mit ☐ Sicherheitsschlüssel / ☐ Magnetkarte möglich. (1)	☐	☐	☐
☐ Zutritt zu Serverräumen ist nur nach biometrischer Identitätskontrolle möglich. (1)	☐	☐	☐
☐ Zutritt zu Serverräumen haben nur ausgewählte, fachlich zuständige Mitarbeiter. (1)	☐	☐	☐
☐ Jeder Zutritt zu einem Serverraum wird protokolliert. (1)	☐	☐	☐
☐ Es besteht zu Bürozeiten eine Videoüberwachung für ☐ das gesamte Betriebsgelände, ☐ den Eingangsbereich, ☐ sämtliche Zugänge, ☐ das Treppenhaus, ☐ alle die Flure, ☐ den Zugangsbereich von Serverräumen, ☐ alle Serverräume, ☐ Büroräume. (1)	☐	☐	☐
☐ Es besteht außerhalb der Bürozeiten eine Videoüberwachung für ☐ das gesamte Betriebsgelände, ☐ den Eingangsbereich, ☐ sämtliche Zugänge, ☐ das Treppenhaus, ☐ alle die Flure, ☐ den Zugangsbereich von Serverräumen, ☐ alle Serverräume, ☐ Büroräume. (1)	☐	☐	☐
☐ Es besteht eine Alarmanlage mit ☐ Signalton / ☐ Anschluss an Notrufzentrale. (1)	☐	☐	☐
☐ Pro Benutzer wird eine individuelle Benutzerkennung vergeben. (2)	☐	☐	☐
☐ Passwörter werden ausschließlich vom Benutzer erstellt. (2)	☐	☐	☐
☐ Passwörter können nicht vom Systemadministrator gelesen werden. (2)	☐	☐	☐
☐ Passwörter werden ausschließlich verschlüsselt gespeichert. (2)	☐	☐	☐
☐ Es besteht eine Passwort-Richtlinie mit Festlegung einer Mindestlänge und Vorgaben zur Komplexität von Passworten (z.B. Groß- und Kleinschreibung, Zahlen, Sonderzeichen) (2)	☐	☐	☐
☐ Eine Änderung des Passwortes wird in regelmäßigen Abständen technisch erzwungen. (2)	☐	☐	☐
☐ An allen Arbeitsplätzen ist die automatische Bildschirmsperre aktiviert. (2)	☐	☐	☐
☐ Jeder Systemzugriff wird protokolliert. (3)	☐	☐	☐
☐ Ein Fernzugriff auf die EDV-Systeme ist technisch nicht möglich. (3)	☐	☐	☐
☐ Jeder Fernzugriff wird protokolliert. (3)	☐	☐	☐
☐ Fernwartungen erfolgen ausschließlich über eindeutige Benutzerkennungen (keine Sammel-Accounts) (3)	☐	☐	☐
☐ Ein Datenexport ist nur nach Freigabe eines zweiten Benutzers mit entsprechender Berechtigung möglich („Vier-Augen-Prinzip“). (4)	☐	☐	☐
☐ Jeder Zugriff auf Daten wird technisch protokolliert. (4)	☐	☐	☐
☐ Jeder Zugriff auf Daten, die als sensibel eingestuft sind, wird technisch protokolliert. (4)	☐	☐	☐
☐ Die Speicherung von Daten erfolgt ausschließlich auf verschlüsselten Speichersystemen. (4)	☐	☐	☐
☐ Die Speicherung von Daten auf mobilen Endgeräten erfolgt ausschließlich auf verschlüsselten Speichersystemen und/oder in verschlüsselten Datencontainern. (4)	☐	☐	☐
☐ Daten werden nicht auf mobilen Endgeräten oder mobilen Datenspeichern gespeichert. (4)	☐	☐	☐
☐ Daten, die als sensibel eingestuft sind, werden nicht auf mobilen Endgeräten oder mobilen Datenspeichern gespeichert. (4)	☐	☐	☐
☐ Gescheiterte Zugriffsversuche auf die Datenverarbeitungssysteme werden protokolliert. (5)	☐	☐	☐
☐ Benutzerkonten werden bei mehreren gescheiterten Zugriffsversuchen automatisch gesperrt. (5)	☐	☐	☐
☐ USB-Ports sind technisch für nicht zugelassene Datenträger gesperrt. (4)	☐	☐	☐
☐ Fernzugriffe sind nur nach Zwei-Faktor-Authentifizierung möglich. (3)	☐	☐	☐
☐ Das Netzwerk ist separiert und in verschiedene Sicherheitsstufen unterteilt. (3)	☐	☐	☐
☐ Das Netzwerk und die Server sind durch eine Firewall geschützt. (3)	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐

II. Integrität

HOWOGE

Maßnahme	Bewertung 0	1	2
☐ ***Maßnahmen zur Integrität sind nicht erforderlich, da ausschließlich Lesezugriff besteht.***			
1) Organisatorische Maßnahmen			
☐ Alle Mitarbeiter werden regelmäßig geschult, um die Einhaltung der Vorschriften der DS-GVO und die Einhaltung von Weisungen sicherzustellen. (6)	☐	☐	☐
☐ Arbeitsanweisungen werden dokumentiert (☐ in Schriftform, ☐ in Textform). (6)	☐	☐	☐
☐ Arbeitsanweisungen zur Gewährleistung der Datensicherheit und der korrekten Ausführung von Aufträgen werden regelmäßig überwacht. (6)	☐	☐	☐
☐ Es bestehen Prozesse zur Aufrechterhaltung der Aktualität von Daten. (5)	☐	☐	☐
☐ Datenverarbeitungsprozesse werden durch regelmäßige Tests und/oder Stichprobenkontrollen auf korrekte Funktionalität hin überprüft.	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐
2) Technische Maßnahmen			
☐ Jede Dateneingabe und jede Datenänderung wird technisch protokolliert. (5)	☐	☐	☐
☐ Jede Eingabe oder Änderung von Daten, die als sensibel eingestuft wurden, wird technisch protokolliert. (5)	☐	☐	☐
☐ Jede Administratortätigkeit wird technisch protokolliert. (5)	☐	☐	☐
☐ Es werden Signaturen und/oder Zertifikate zur Sicherstellung Berechtigung des Zugriffs, der Speicherung oder Veränderung von Daten eingesetzt. (5)	☐	☐	☐
☐ Zur Validierung von Daten werden Prüfsummen oder vergleichbare Methoden eingesetzt.	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐

III. Verfügbarkeit

☐ ***Maßnahmen zur Verfügbarkeit sind nicht erforderlich, weil [kurze Begründung eintragen]***

1) Organisatorische Maßnahmen			
☐ Zentrale Beschaffung und/oder Freigabe von Hardwarekomponenten. (7)	☐	☐	☐
☐ Zentrale Beschaffung und/oder Freigabe von Software. (7)	☐	☐	☐
☐ Updates von Software werden zentral durchgeführt. (7)	☐	☐	☐
☐ Das Einspielen von Updates durch die Nutzer wird stichprobenartig kontrolliert. (7)	☐	☐	☐
☐ Es besteht ein Notfallkonzept für Datenschutz- und Sicherheitsvorfälle. (7)	☐	☐	☐
☐ Die IT-Systeme werden durch Fachkräfte betreut, die sich regelmäßig fortbilden. (7)	☐	☐	☐
☐ Datensicherungen werden regelmäßig auch an geografisch von den Servern unterschiedlichen Orten gespeichert / aufbewahrt. (7)	☐	☐	☐
☐ Ein Ausweichrechenzentrum für die zentralen Anwendungen ist verfügbar. (7)	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐
2) Technische Maßnahmen			
☐ Regelmäßige systematische Durchführung von Datensicherungen (BackUps) (7)	☐	☐	☐
☐ Die Datenwiederherstellung aus BackUps wird regelmäßig getestet. (7)	☐	☐	☐
☐ Unterbrechungsfreie Stromversorgung (USV) (7)	☐	☐	☐
☐ Für die wichtigsten Server-Räume besteht eine Notstromversorgung. (7)	☐	☐	☐

Maßnahme	Bewertung 0	1	2
☐ Netzwerk- und Serverinfrastruktur sind durch eine Firewall gesichert. (7)	☐	☐	☐
☐ Netzwerk- und Serverinfrastruktur verfügen über einen effektiven Viren- und Malwareschutz. (7)	☐	☐	☐
☐ Server sind über redundante Leitungen an das Internet angebunden. (7)	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐

IV. Belastbarkeit

☐ ***Maßnahmen zur Belastbarkeit nicht erforderlich, weil [kurze Begründung eintragen]***

1) Organisatorische Maßnahmen

☐ Regelmäßige Belastungstests der Datenverarbeitungssysteme	☐	☐	☐
☐ Speicher- und Rechenkapazitäten werden im Voraus und mit Sicherheitsaufschlägen geplant.	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐

2) Technische Maßnahmen

☐ Die Verfügbarkeit von IT-Systemen wird überwacht (Monitoring).	☐	☐	☐
☐ Zentrale IT-System verfügen über ein Load-Balancing.	☐	☐	☐
☐ Datenleitungen verfügen über ein Bandbreitenmanagement.	☐	☐	☐
☐ Die IT-Systeme sind verfügen über dynamisch verfügbaren Speicherplatz.	☐	☐	☐
☐ Die IT-Systeme sind verfügen über dynamisch verfügbare Rechenkapazität (Prozessoren).	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐

V. Regelmäßige Überprüfung

☐ Es findet eine regelmäßige Überprüfung statt, ob sich der Stand der Technik verändert hat und entsprechender Anpassungsbedarf der IT-Systeme besteht.	☐	☐	☐
☐ Es finden regelmäßig externe Prüfungen der IT-Systeme und/oder der Schutzmaßnahmen statte (z.B. Penetrationtests).	☐	☐	☐
☐ Die eingesetzte Hard- und Software wird regelmäßig auf Funktionsfähigkeit überprüft.	☐	☐	☐
☐ Die Schutzbedarfsklassifizierung für Datenverarbeitungen wird regelmäßig überprüft.	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐
☐	☐	☐	☐