Anlage 1 – Vom Auftragsverarbeiter bei sich ergriffene technisch-organisatorische (TOMs) Maßnahmen

Ziffer 6 der Vereinbarung zur Auftragsdatenverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Datenschutzmaßnahmen auf diesen Anhang.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1. Zutrittskontrolle

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist	vorhanden ja
Anmelden von Besuchern beim Empfang	☒
Aufbewahrung der Datenträger unter Verschluss bzw. in abgeschlossenen Räumen	☒
Aufbewahrung der Server in verschlossenen Räumen	☒
Begleitung von Besuchern	☒
Gesondert gesicherter Zutritt zum Rechenzentrum, Serverraum, Patch-Raum	☒
Schlüsselregelung, Dokumentierte Ausgabe	☒
Videoüberwachung	☒
Zutrittsberechtigungskonzept	☒
Sonstiges:	☐

1.2. Zugangskontrolle

Das Eindringen Unbefugter in die Datenverarbeitung bzw. deren unbefugte Nutzung ist zu verhindern.	vorhanden ja
Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität	☒
Funktionelle und/oder zeitlich limitierte Vergabe von Benutzerberechtigungen	☒
Kontrollierte Vernichtung von Datenträgern	☒
Passwortsicherung von Bildschirmarbeitsplätzen	☒
* Passwort-Policy:	☒
Prozess zur Rechtevergabe Eintritt - Abteilungswechsel - Austritt des Mitarbeiters	☒
Verpflichtung zur Vertraulichkeit	☒
Verschlüsseln von Datenträgern	☒
Sonstiges:	☐

secom edv services gmbh
Alte Straße 2a, 9431 St. Stefan
F: 04352/81 332 | **M**: info@secom.co.at | www.secom.co.at
FN: 373433 t | **UID-Nummer**: ATU66882144

1.3. Zugriffskontrolle

Unerlaubte Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen sind zu verhindern.	vorhanden ja
Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken	☒
Clear-Desk/Clear-Screen Policy	☒
Festlegung der Zugriffsberechtigungen, Berechtigungskonzept	☒
Firewall	☒
Regelmäßig durchgeführte Wiederherstellungstests	☒
Regelmäßige Überprüfung von Berechtigungen	☒
Regelung zur Wiederherstellung von Daten aus Backups	☒
SPAM-Filter	☒
Verschlüsselte Speicherung von Daten	☒
Virenscanner	☒
Sonstiges:	☐

1.4. Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.	vorhanden ja
Trennung von Kunden	☒
Trennung von Entwicklungs-, Test- und Produktivsystemen	☒
Sonstiges:	☐

1.5. Pseudonymisierung

Art. 32 Abs. 1 Lit. A DSGVO; Art. 25 Abs. 1 DSGVO	vorhanden ja
Dies ist die Verantwortung des Kunden	☒
Sonstiges:	☐

1.6. Klassifikationsschema für Daten

Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).	vorhanden ja
Klassifikation wird angewandt	☒
Sonstiges:	☐

secom edv services gmbh
Alte Straße 2a, 9431 St. Stefan
F: 04352/81 332 | **M**: info@secom.co.at | www.secom.co.at
FN: 373433 t | **UID-Nummer**: ATU66882144

2. Datenintegrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1. Weitergabekontrolle

Aspekte der Weitergabe (Übermittlung) pb-Daten sind zu regeln: Elektronische Übertragung, Datentransport, sowie deren Kontrolle.	vorhanden ja
Dokumentierte Verwaltung von Datenträgern, Bestandskontrolle	☒
Festlegung der Bereiche, in dem sich Datenträger befinden müssen	☒
Gesicherter Eingang für An- und Ablieferung	☒
Kontrollierte Vernichtung von Daten/Datenträgern	☒
Verschlüsselung von Laptopfestplatten	☒
Welche Versendungsarten der Daten bestehen	☒
* E-Mail Versand	☒
* Datenaustausch über https-Verbindung	☒
* Serverplattform	☒
* Externe Cloud	☒
Sonstiges:	☐

2.2. Eingabekontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.	vorhanden ja
Dezidierter Log-Server	☒
Differenzierte Benutzerberechtigungen	☒
Dokumentenmanagement	☒
Festsetzung von Benutzerberechtigungen (Profile)	☒
Regelung der Zugriffsberechtigungen für Log-Server (Log-Admin)	☒
Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke	☒
Verpflichtung auf das Datengeheimnis	☒
Sonstiges:	☐

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1. Verfügbarkeitskontrolle

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.	vorhanden ja
Datensicherungs- und Backupkonzepte	☒
Blitz-/Überspannungsschutz	☒
Brandmeldeanlage in Serverräumen	☒
CO2-Feuerlöscher in unmittelbarer Nähe der Serverräumlichkeit	☒
Durchführung der Datensicherungs- und Backupkonzepte	☒
Gewährleistung der technischen Lesbarkeit von Backupspeichermedien	☒
Klimatisierung in Serverräumen	☒
Rauchmelder in Serverräumen	☒

Unterbringung von Backupsystem in separaten Räumlichkeiten und Brandabschnitten	☒
USV-Anlage	☒
Wasserlose Brandbekämpfung in Serverräumen	☒
Zutrittsbegrenzung in Serverräume	☒
Sonstiges:	☐

3.2. Rasche Widerherstellbarkeit

Die Daten müssen rasch widerherstellbar sein um den Betrieb/Fortbestand zu gewährleisten.	vorhanden ja
Dauerhaft beauftragter interner IT-Experte	☒
Regelmäßige Widerherstellungstests	☒

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. b DSGVO; Art. 25 Abs. 1 DSGVO)

4.1. Kontrollverfahren

Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Datensicherungsmaßnahmen ist zu implementieren.	vorhanden ja
Alle Mitarbeiter werden mind. jährlich und Anlass bezogen geschult	☒
Es besteht ein Prozess zur Vorbereitung auf Sicherheitsverletzungen (Angriffen) und Systemstörungen sowie zur Identifizierung, Eingrenzung, Beseitigung und Erholung von selbigen (Incident-Response-Prozess)	☒
Es werden datenschutzfreundliche Voreinstellungen gewählt	☒
Getroffene Sicherheitsmaßnehmen werden regelmäßig internen Kontrollen unterzogen	☒
Interne Datenschutzdokumentation wird mind. jährlich aktualisiert	☒
Meldung neuer/veränderter Datenverarbeitungsverfahren an den DSK/DSB	☒
Meldung neuer/veränderter Datenverarbeitungsverfahren an den IT-Sicherheitsbeauftragten	☒
Prozess zur Meldung neuer/veränderter Verfahren sind dokumentiert	☒
Bei negativem Verlauf der zuvor genannten Überprüfung werden die Sicherheitsmaßnahmen risikobezogen angepasst, erneuert und umgesetzt	☒
Regelmäßige Auditierung durch einen externen Datenschutzbeauftragten	☒
Sonstiges:	☐

secom edv services gmbh
Alte Straße 2a, 9431 St. Stefan
F: 04352/81 332 | **M**: info@secom.co.at | www.secom.co.at
FN: 373433 t | **UID-Nummer**: ATU66882144

4.2. Auftragskontrolle

Es ist sicherzustellen, dass Daten die im Auftrag durch Dienstleister (Subauftragnehmer) verarbeitet werden, nur gemäß der Weisung des Auftragnehmers verarbeitet werden.	vorhanden ja
Sichtung vorhandener IT-Sicherheitszertifikate der Auftragnehmer	☒
Vertragsgestaltung gem. Art. 28 DSGVO	☒
Zentrale Erfassung vorhandener Dienstleister (einheitliches Vertragsmanagement)	☒
Sonstiges:	☐

4.3. Incident-Response-Management

Vorfall-Management	vorhanden ja
Prozess zur Meldung von Vorfällen an die DSK/DSB	☒
Prozess zur Abarbeitung von Vorfällen	☒

4.4. Datenschutzfreundliche Voreinstellungen

	vorhanden ja
Berechtigungskonzept	☒

Sollten Sie noch Fragen dazu haben, kontaktieren Sie unsere Datenschutzkoordinatorin:

Ansprechperson für den Datenschutz:

Externer Datenschutzbeauftragter
MMag. Dr. Gerhard T. Gfrerer
Tel: 0664 1880724
Mail: gfrerer@chronoberatung.at