ANHANG C
Technisch-organisatorische Maßnahmen (TOM / Version 03-2021)

1 Organisation

1.1 Wie ist die Umsetzung des Datenschutzes organisiert? Ein externer Datenschutzbeauftragter wird zur Wahrnehmung der Kontrollfunktion aus dem DSGVO eingesetzt.

1.2 Unser Datenschutzbeauftragter ist in den untenstehenden Kontaktdaten aufgeführt. Philip Essinger, Essinger Consulting, Telefonnummer Tel: 089-461389-13, E-Mail: datenschutz@essinger.consulting.de

1.3 Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt? Mitarbeiter Verpflichtungen wurden schriftlich, zur Wahrnehmung des Datenschutzes, vereinbart. Die Mitarbeiter werden regelmäßig zum Datenschutz geschult.

1.4 Wie stellen Sie sicher, dass die internen Prozesse gemäß den aktuellen Datenschutzbestimmungen ablaufen und regelmäßig geprüft werden? Eine konstante monatliche Sensibilisierung der Mitarbeiter und regemäßige Prüfungen der Abläufe im Unternehmen wird durchgeführt.

1.5 In welcher Form werden die Mitarbeiter auf die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen geschult, die für diese Verarbeitung in Anwendung kommen? Mitarbeiter erhalten eine Datenschutz-unterweisung.

Regelmäßige Datenschutzschulung aller Mitarbeiter.

1.6 Sind die Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit dokumentiert. Die Datenströme sind dokumentiert und die Zulässigkeit der Nutzung und Verarbeitung nach DSGVO nachgewiesen.

2 Zutrittskontrolle

2.1 Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert? Das Gebäude ist mit einer Sicherheits-Schließanlage, Alarmanlage, ausgestattet. Verschlossener Eingang mit Klingel. Empfang mit Gästebuch und Portiere.

2.2 Wie werden die Räume/Büros, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert? Alarmanlage im Gebäudeanteil der Firma. Die Räume werden ebenfalls durch das Sicherheitsschließsystem gesichert. Ein Videoüberwachungssystem überwacht die Zugänge.

2.3 Wie werden die Verarbeitungsanlagen vor unbefugtem Zugriff geschützt? Abschließbare, dezentrale Serverschränke, dokumentierte Zutrittskontrolle für Externe.

2.4 Wie werden die umgesetzten Zutrittskontrollen auf Tauglichkeit geprüft? Im Rahmen der Kontrollen durch den Datenschutzbeauftragten werden auch die Zutrittskontrollmaßnahmen überprüft.

3 Zugangskontrolle

3.1 Wie erfolgt die Vergabe von Benutzerzugängen? Benutzerzugänge werden nur sehr selektiv und nach Genehmigung durch die GF und Abteilungsleiter vergeben. Rechtevergabe und Änderungen sind dokumentiert. Zugriff auf kaufmännische Dokumente und Kommunikationsinformationen sind Passwort geschützt. Mitarbeiter erhalten bei Eintritt MS AD-Accounts, die Berechtigungen werden über AD-Gruppen geregelt.

3.2 Wie wird die Gültigkeit von Benutzerzugängen überprüft? Eine regelmäßige Revision der vergebenen Rechte ist ein Teil der Prüfung und der Maßnahmen. Dieser Vorgang wird zusammen mit dem Datenschutzbeauftragten durchgeführt. Die Abteilungsleiter bzw. GF sind verpflichtet, relevante Änderungen in Beschäftigungsverhältnissen rechtzeitig der Administration anzuzeigen.

3.3 Wie werden Benutzerzugänge inkl. Antragstellung, Genehmigungsverfahren etc. dokumentiert? Anforderungen zu Benutzerzugängen können nur von den Abteilungsleitern bzw. GF per Mail beantragt bzw. genehmigt werden. Dies wird von der Administration per Mail bestätigt. Der Verlauf wird über Mail-Archivierung festgehalten.

3.4 Wie wird sichergestellt, dass die Anzahl von Administrationszugängen ausschließlich auf die notwendige Anzahl reduziert ist und nur fachlich und persönlich geeignetes Personal hierfür eingesetzt wird? Es wird streng auf Datensparsamkeit geachtet, um nach Art. 5 Abs. 1 lt. C dem Grundsatz "Datenminimierung" zu folgen. Der Systemadministrator arbeitet nach dem "Need-to-Know"-Prinzip und überprüft regelmäßig die Zugänge und deren Berechtigungen. Alle betreffenden und infrage kommenden Personen besitzen einen nachweislich fachlichen IT-Hintergrund. Sie sind weder temporär noch als externe Mitarbeiter beschäftigt, befinden sich nicht in der Probezeit, und wurden auf die "Verpflichtung auf das Datengeheimnis nach gesetzlichen Vorgaben der DSGVO" des Unternehmens verpflichtet.

3.5 Ist ein Zugriff auf die Systeme/Anwendungen von außerhalb des Unternehmens möglich (Heimarbeitsplätze, Dienstleister etc.)? Wie ist der Zugang gestaltet? Der Zugriff ist über eine verschlüsselte VPN-Verbindung (L2TP) für explizit freigegebene Mitarbeiter möglich. Die Authentifizierung erfolgt über MS-AD Anmeldedaten.

4 Zugriffskontrolle

4.1 Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind? Die PW werden vom jeweiligen Mitarbeiter selbst vergeben. Jeder Mitarbeiter hat einen eigenen Zugang. Es gibt für die Regelung der Passwörter eine Passwort-Policy.

4.2 Welche Anforderungen werden an die Komplexität von Passwörtern gestellt? Das Passwort wird regelmäßig gewechselt. Das Passwort entspricht der Passwort-Policy und der darin festgelegten Sicherheitsmerkmale, wie Sonderzeichen, Groß u. Kleinschreibung, Zahlen. Mind. 8 Stellen, es müssen mind. 3 der erwähnten Regeln erfüllt sein.

4.3 Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann/muss?
Durch Gruppenrichtlinien wird ein Wechsel des Passwortes nach 60 Tagen erzwungen oder der Zugriff gesperrt. Das neue Passwort darf nicht einem der drei vorherigen entsprechen.

4.4 Welche organisatorischen Vorkehrungen werden zur Verhinderung von unberechtigten Zugriffen auf personenbezogene Daten am Arbeitsplatz getroffen?
Alle Zugänge sind kennwortgeschützt. Automatische Bildschirmsperre ist fest eingerichtet. Schulung und Sensibilisierung der Mitarbeiter. Die Mitarbeiter sind unterwiesen, bei Verlassen des Arbeitsplatzes keine sichtbaren bzw. freizugängliche, personenbezogene Daten zu hinterlassen (Clean-Desk-Prinzip).

4.5 Wie wird sichergestellt, dass Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden?
Der GF prüft in regelmäßigen Abständen die Rechte der Benutzerstruktur.

4.6 Wie erfolgt die Dokumentation von Zugriffsberechtigungen?
Regelmäßiger Report der IT-Verantwortlichen aus dem Berechtigungssystem der Access-Control-List.

4.7 Wie wird sichergestellt, dass Zugriffsberechtigungen nicht missbräuchlich verwendet werden?
Stichprobenartige Durchsicht der Systemprotokolle durch den GF.

4.8 Wie lange werden Protokolle aufbewahrt? Wer hat Zugriff auf die Protokolle? Wie oft werden sie ausgewertet?
Protokolle werden für 6 Monate ausbewahrt. Im Standard gelten die definierten Fristen der Verarbeitungsvorgänge. Zugriff auf die Protokolle sind auf die Administratoren beschränkt. Eine Auswertung erfolgt verdachtsbezogen, z.B. auf Grund einer automatisierten Zugriffssperre, sowie stichprobenartig.

5 Trennungskontrolle

5.1 Wie wird sichergestellt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet werden? Zur Trennung der Daten wird ein dezidiertes Rechte-System eingesetzt.

6 Pseudonymisierung

6.1 Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung personenbezogener Daten gesetzeskonform erfolgt? Alle, mit der Verarbeitung von personenbezogenen Daten betrauten Personen, wurden entsprechend verpflichtet. Ein Datenschutzkonzept wird im Unternehmen eingesetzt und ist allen Mitarbeitern bekannt und schriftlich fixiert. Datenschutzunterweisungen/ Sensibilisierungen finden regemäßig statt.

6.2 Wie werden personenbezogene Daten verarbeitet/ aufbewahrt, sodass diese nicht den betroffenen Personen zugeordnet werden können?
Die Verarbeitung personenbezogener Daten kann in den meisten Fällen einer betroffenen Person zugeordnet werden.

7 Weitergabekontrolle

7.1 Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten? Die Weitergabe erfolgt über verschlüsselte Kanäle und/ oder die Verschlüsselung der Daten selbst. Eine Zustellung oder Bekanntgabe erfolgt nur an den vorhergesehenen Empfänger.

7.2 Werden Verschlüsselungssysteme bei der Weitergabe von personenbezogenen Daten eingesetzt? Wenn ja, welche?
Verschlüsselte USB-Sticks, verschlüsselte ZIP-Archive (AES-256) und verschlüsselte E-Mail-Übertragung. Ein Versenden per Mail oder die Bereitstellung per Internet erfolgt über Server mit Transportverschlüsselung (SSL/TLS).

7.3 Wie wird die Weitergabe personenbezogener Daten dokumentiert?
Ist vom jeweiligen Prozess (Personal, Kundendaten, etc.) abhängig und wird im Verfahrensverzeichnis individuell geregelt.

7.4 Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?
Eine strikte Rechtevergabe sichert die Daten vor unberechtigtem Zugriff.

7.5 Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann?
Dies wird im Rahmen der Zugriffskontrolle geprüft.

8 **Eingabekontrolle**

8.1 Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie lange auf Applikationen zugegriffen hat?
Zugriffs-Logs der Server und Systeme.

8.2 Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?
Zugriffs-Logs der einzelnen Applikationen.

8.3 Welche Maßnahmen werden ergriffen, damit die Verarbeitung durch die Mitarbeiter nur gemäß der Weisung des Auftraggebers erfolgen kann?
Stichproben zur Prüfung und Unterweisung der Mitarbeiter zur Einhaltung. Regelmäßige Datenschutz-Veranstaltungen bzw. Personalgespräche.

8.4 Welche Maßnahmen werden getroffen, damit auch Unterauftragnehmer ausschließlich im vereinbarten Umfang personenbezogene Daten des Auftraggebers verarbeiten? Die Datenverarbeitung von Unterauftragnehmern erfolgt mit eindeutigen Auftragsdefinitionen und einer formalisierten Auftragserteilung (AV-Verträge nach Art. 28 DSGVO). Die Pflichten zur Überprüfung der Unterauftragnehmer übernimmt der Datenschutzbeauftragte des Unternehmens. Er ist auch bei der Wahl der beauftragten Firmen beteiligt.

8.5 Wie wird die Löschung/Sperrung von personenbezogenen Daten am Ende der Aufbewahrungsfrist bei Unterauftragnehmern sichergestellt?
Feststellung durch Vertragsbindung, bei Wegfall des Zwecks ist ebenfalls eine Löschung der Daten indiziert.

9 **Verfügbarkeitskontrolle**

9.1 Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten?
Eingerichtetes Backup-Verfahren (Restore-Konzept/Wiederanlaufkonzept).

9.2 Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetischer Abstrahlung etc.) geschützt sind?
Die Backup-Datenträger werden in einem Safe in einer anderen Räumlichkeit aufbewahrt.

9.3 Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt? Wie werden deren Aktualität gewährleistet?
Firewall-Systeme mit Servicevertrag, Session Border Controller zur IT-Sicherheit für VoIP, diese werden zentral automatisiert ausgerollt und aktualisiert. Anti-Viren und Firewall-Lösungen werden auf den Client- und Server-Systemen eingesetzt. Eingehende Mails werden vor Zustellung durch den Exchange-Server auf Schadsoftware und SPAM geprüft.

9.4 Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden? Physische Löschung bei funktionsfähigen Datenträgern und mechanische Zerstörung defekter Datenträger werden zentral durch die IT-Abteilung gemeinsam mit einem ISO-zertifizierten Entsorgungsfachbetrieb entsorgt.

10 **Wiederherstellbarkeit**

10.1 Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten? (rasche Wiederherstellbarkeit nach Art. 32 Abs. 1 lit. C DS-GVO) Ein streng konzipiertes Backupsystem. Die Server und Stromversorgungssysteme der Verarbeitungsanlage sind redundant ausgelegt, um einem Ausfall vorzubeugen.

Backup-Wiederherstellungen können im Vertretungsfall von verschiedenen IT-Mitarbeitern durchgeführt werden.

11 **Auftragskontrolle**

11.1 Welche Verfahren gibt es zur regelmäßigen Bewertung/Überprüfung, um die Sicherheit der Datenverarbeitung zu gewährleisten (Datenschutz-Management)? Der externe Datenschutzbeauftragte überprüft regelmäßig und stichprobenartig, die Einhaltung der technisch organisatorischen Maßnahmen.

11.2 Wie wird auf Anfragen bzw. Probleme reagiert (Incident-Response-Management)? Einsatz eines eigenen Ticket-Systems. Zusätzlich Telefon-Hotline und automatisierte Systemüberwachung.

11.3 Welche datenschutzfreundlichen Voreinstellungen gibt es (Art. 25 Abs. 2 DS-GVO)? Keine Vorbelegung, der Benutzer muss die Anmeldeinformationen jeweils eintragen.

11.4 Welche Vorgänge gibt es zur Weisung bzw. dem Umgang mit der Auftragsdatenvereinbarung (Datenschutz-Management)? Das Vertragswerk wurde entsprechend den neuen Richtlinien zur Auftragsdatenverarbeitung gestaltet. Der externe Datenschutzbeauftragte nimmt entsprechende Beratungs- und Kontrollfunktionen wahr