Aufstellung für Auftraggeber der Severins GmbH zu den bei der Severins GmbH getroffenen technischen und organisatorischen Maßnahmen im Datenschutz.

Diese Auflistung der bei der Severins GmbH getroffenen technischen und organisatorischen Maßnahmen im Datenschutz (TOMs) orientiert sich an den Vorgaben des § 9 BDSG(alt) und der Anlage zu § 9 Satz 1 BDSG(alt). Diese Dokumentation ermöglicht eine strukturierte Dokumentation der TOMs, da es weder in der EU-Datenschutzgrundverordnung (DSGVO) noch im neuen Bundesdatenschutzgesetz (BDSG-Neu) dazu Vorgaben für nicht öffentliche Stellen gibt (§ 64 BDSG-Neu findet bei nicht öffentlichen Stellen keine Anwendung). Diese Angaben dokumentieren auch die Forderungen des § 78a SGB X und des Art. 32 der DSGVO. Es soll Verantwortlichen (Auftraggebern) dazu dienen, ihre Prüf- und Dokumentationspflicht bei Auftragsverarbeitung gem. Art. 28 und 29 DSGVO und 80 SGB X zu erleichtern.

Diese Aufstellung ist auch als Ergänzung zu einem bestehenden oder neuen - Art. 28, 29 DSGVO konformen - Dienstleistungsvertrag gedacht und kann jedem Verantwortlichen (Auftraggeber) auf Anforderung zur Verfügung gestellt werden. Die getroffenen Maßnahmen unterliegen dem technischen Fortschritt und werden somit fortlaufend aktualisiert, wobei das bisher vorhandene Sicherheitsniveau nicht unterschritten wird.

Die Daten, die bei der Severins GmbH in Auftrag verarbeitet werden, sind als besonders sensibel eingestuft. Es handelt sich um personenbezogene Daten gemäß Art. 4 Nr. 1 und um Sozialdaten gemäß § 67 Abs. 1 SGB X in Verbindung mit besonderen Daten gemäß Art. 4 Nr. 15 DSGVO (Gesundheitsdaten).

Ergänzend sei noch erwähnt, dass es bei der Severins GmbH IT-Notfallpläne, Datensicherungs- und Berechtigungskonzepte und dokumentierte Prozessabläufe gibt.

Allgemeiner Teil:

1. Name und Anschrift des Unternehmens:

   Severins *GmbH*
   Am Lippeglacis 16-18
   46483 Wesel

2. Ansprechpartner mit Telefon, Fax und E-Mail:

   Herr Oliver Mentler, Datenschutzkoordinator
   Tel.: +49 281 16394 - 74
   Fax: +49 281 16394 – 20
   E-Mail: o.mentler@severins.de

3. Name des Geschäftsführers:

   Wilfried Engel und Sven Hebenbrock

Seite 2:

4. Name und Kontaktdaten des Datenschutzbeauftragten:

Joachim *Kramer*
Datenschutz Kramer & Kramer GmbH
Büro für Datenschutz und Datensicherheit
Elsternweg 24
42555 Velbert
Tel.: 02052 92897 -66
Fax: 02052 92897 -67
E-Mail: j.kramer@datenschutz-kramer.de

5. Datenschutzbeauftragter:

5.1. Bestellung:

- *externer Datenschutzbeauftragter gem. § 4 f Abs. 2 BDSG(alt) bzw. Art.37 DSGVO und § 38 BDSG-Neu*
- *schriftliche Bestellung vom 27.02.2017 liegt vor*
- *davor war Günter-Wolfgang Kramer, staatl. gepr. Betriebswirt EDV externer Datenschutzbeauftragter (15.04.2005-26.02.2017)*

5.2. Qualifikation:

- *Datenschutz-Auditorin (TÜV) Zertifizierungsstelle für Personal TAR-ZERT der TÜV Akademie Rheinland Nr. 19553*
- *regelmäßige Fortbildungen*
- *Mitglied im Erfa-Kreis MEO für Datenschutzbeauftragte*
- *GDD Mitglied*
- *Firma Kramer & Partner besitzt über 30 Jahre Erfahrung im Datenschutz*

6. Mitarbeiter der Severins GmbH:

- *alle Mitarbeiter sind schriftlich zur Wahrung des Datengeheimnisses, der Schweigepflicht nach § 203 StGB, der Vertraulichkeit nach DSGVO, BDSG-Neu und auf das Sozialgeheimnis nach § 35SGB I verpflichtet worden*
- *die Verpflichtung erfolgte auf einem extra Formular*
- *die der Verpflichtung zugrundeliegenden Gesetzestexte wurden allen Mitarbeitern gegen Unterschrift ausgehändigt*
- *die Verpflichtung wird bei Einstellung durch das Personalbüro des Mutterkonzerns vorgenommen*
- *Betriebsvereinbarung über die private Nutzung von E-Mail, Internet und Telefon*
- *alle Mitarbeiter werden in regelmäßigen Abständen durch den BDSB geschult*

7. Verfahrensverzeichnisse/Verzeichnis der Verarbeitungstätigkeiten:

- *das „Verzeichnis der Verarbeitungstätigkeiten" liegt vor und ist Bestandteil eines integrierten Managementsystems*

Seite 3:

Technische und organisatorische Maßnahmen:

8. In unserem Haus ist die räumliche **Zutrittskontrolle** folgendermaßen sichergestellt:

- *Closed-Shop-Betrieb*
- *Geschäftsräume befinden sich im EG, 1. OG und 2. OG*
- *Zutritt in die Geschäftsräume ist nur über Zahlenschlösser oder über Schlüssel möglich*
- *Besucher müssen klingeln*
- *Alarmanlage mit Bewegungsmeldern*
- *Technikraum zusätzlich mit Sicherheitsschloss verschlossen*
- *Wach- und Sicherheitsdienst für das gesamte Objekt*

9. Um das unbefugte Eindringen in unsere Systeme und Datenverarbeitungssystemen zu verhindern, verwenden wir folgende **Zugangskontrollen**:

- *Benutzername und Kennwort*
- *automatische Sperrung (Pausenschaltung)*
- *Sperrung des Accounts bei wiederholter Falschanmeldung*
- *datenschutzgerechte Passwortrichtlinien gem. BSI*
- *Active Directory mit Zugangsprotokoll*
- *Server mit zusätzlichen Administrator Passwörtern*

10. Wie wird der Zugriff (**Zugriffkontrolle**) auf verschiedene Daten bzw. Systeme geregelt:

- *durch differenzierte Berechtigungen, gesteuert durch die Anmeldung (Berechtigungskonzept)*
- *extra Administrationspasswörter für die Server, die nur dem IT-Leiter und dem EDV-Support bekannt sind (im Rechenzentrum der Muttergesellschaft)*

11. Wir kontrollieren die Weitergabe (**Weitergabekontrolle**) personenbezogener Daten bei Übermittlung bzw. Übertragung oder bei Transport mit folgenden Maßnahmen:

- *die Übermittlung von Daten in Papierform an die Rechnungsprüfstellen und Kostenträger erfolgt per Post, bzw. Paketdienst*
- *die Übermittlung zu den Rechnungsprüfstellen der Kostenträger, sowie direkt zu den Kostenträgern, erfolgt durch den so genannten DTA und wird verschlüsselt mit vom ITSG Trust Center zertifizierten Schlüsseln übertragen*
- *abrechnungsbegründende Unterlagen die gescannt werden müssen, gehen zur Muttergesellschaft und werden dort professionell gescannt (ADV-Vertrag gem. § 28 DSGVO vorhanden)*
- *der Zugriff von Kunden auf ihre eigenen Kundendaten bzw. Statistiken erfolgt via Internet und einer 2048 Bit SSL (TLS) Verschlüsselung nach Anmeldung mit Benutzernamen und Passwort im „Mein Kundenportal“*
- *Personaldaten und Buchhaltungsdaten werden an die Muttergesellschaft weitergegeben*
- *Daten in Schriftform (Schriftstücke bis DIN A4) werden durch einen Entsorgungsbetrieb nach DIN 66399 - P4 entsorgt*

12. Wir gewähren die Nachvollziehbarkeit bzw. Dokumentation der Wartungsarbeiten bzw. Systemzugriffe mit folgenden Maßnahmen (Eingabekontrolle). Dadurch kann nachvollzogen werden, wer auf ein System bzw. Daten zugegriffen hat und wann:

- *durch Protokolle am Domain-Controller*
- *durch Server Protokolle*
- *in den Programmen werden bei Erfassung bzw. Änderung von Daten die Mitarbeiterkürzel mit protokolliert*
- *Es werden Protokolle geschrieben, wer in die Bearbeitung eines Auftrags involviert war*

13. Die Aufträge (Auftragskontrolle) unserer Kunden kontrollieren wir anhand folgender Möglichkeiten:

- *die Auftraggeber der Severins GmbH kontrollieren die Abrechnung anhand der von der Severins GmbH versendeten Kundenunterlagen*
- *Kunden, die Zugriff auf „MeinKundenPortal" haben, können auch hier ihre Abrechnungsdaten einsehen und so eine Auftragskontrolle vornehmen*
- *Es werden Protokolle geschrieben, wer in die Bearbeitung eines Auftrags involviert war*

14. Folgende Sicherheitsmaßnahmen (Verfügbarkeitskontrolle) haben wir gegen zufällige oder mutwillige Zerstörung und gegen Verlust bzw. Sabotage von Daten ergriffen:

- *alle Server sind mit Raid-Systemen ausgestattet, die die Daten permanent spiegeln (im Rechenzentrum der Muttergesellschaft)*
- *die Raid-Systeme der Server und NAS-Systeme melden Plattenausfälle sofort, dass die Störung, ohne den Betriebsablauf der Kunden zu stören, behoben werden kann (im Rechenzentrum der Muttergesellschaft)*
- *alle Server sind an USVs angeschlossen (im Rechenzentrum der Muttergesellschaft)*
- *Dieselgenerator im Falle längerer Stromausfälle (im Rechenzentrum Muttergesellschaft)*
- *Serverraum mit Brand- / Rauchmelder und Klimaanlage (im Rechenzentrum Muttergesellschaft)*
- *automatisiertes Backupverfahren mit Protokollen (im Rechenzentrum Muttergesellschaft)*
- *Virenscanner mit automatischem Update Protokollen (im Rechenzentrum Muttergesellschaft)*
- *Datensicherungsprotokolle werden täglich von dem IT-Support ausgewertet Protokollen (im Rechenzentrum Muttergesellschaft)*
- *Datensicherungen in einem anderen Brandabschnitt (im Rechenzentrum Muttergesellschaft)*

15. Um Daten, die zu unterschiedlichen Zwecken erhoben wurden oder um die Daten von Mandanten voneinander zu trennen (Trennungskontrolle), haben wir folgende Maßnahmen ergriffen:

- *physikalische Server sind in VM-Server unterteilt*
- *durch interne Mandantenfähigkeit und Authentifizierung der Auftraggeber*
- *verschiedene Systeme sind auch auf unterschiedlichen Servern installiert*

16. Nicht mehr benötigte Daten in Papierform bzw. nicht mehr gebrauchte oder defekte Datenträger werden bei uns wie folgt entsorgt:

- *Daten in Papierform werden in verschlossenen Alu-Tonnen gesammelt und durch ein Entsorgungsunternehmen nach DIN 66399 P4 datenschutzgerecht entsorgt (quittiert)*
- *elektronische und optische Datenträger werden gesammelt und durch den EDV-Support nach DIN 66399 O3 T4 H4 entsorgt (quittiert)*

Zu erwähnen ist noch, dass die Severins GmbH eines der kleineren Unternehmen in einer Firmengruppe ist, zu der 22 Unternehmen aus dem Gesundheitssektor zählen. So werden, um vorhandene Ressourcen besser zu nutzen, mehrere Bereiche von der Muttergesellschaft mit übernommen. Dabei handelt es sich um das Personalbüro, die Finanzbuchhaltung, den zentralen Einkauf, der gesamten IT-Infrastruktur und um den EDV-Hard- und Software Support. Verträge, auch AV Verträge zwischen den einzelnen Gesellschaften über die zu erbringenden Dienstleistungen, existieren. Somit gibt es bei der Severins GmbH keine weiteren Untervertragsverhältnisse.

Velbert, 30.06.2023 _____

Ort, Datum Joachim Kramer (betrieblicher Datenschutzbeauftragter)

Wesel, 30.06.2023 _____

Ort, Datum Wilfried Engel und Sven Hebenbrock