Technisch-organisatorische Maßnahmen der EWS GmbH Besselstraße 10, 68219 Mannheim nach Art. 25 Abs. 1 und Art. 32 Datenschutz-Grundverordnung (DSGVO)

zur Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO der

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen:

- Empfang (EG/1.OG)
- Zutrittskontrollsystem: RFID-Chips
- Verantwortliche Person für die Vergabe der Berechtigungen und Schlüsselvergabe, inkl. Vertretungsregelung.
- Ständige Erreichbarkeit einer Schlüsselperson, auch an Wochenenden.
- Sorgfältige Auswahl von Reinigungspersonal:
- Überwachungseinrichtung: Alarmanlage für Lager, Werkstatt und Bürogebäude mit Aufschaltung auf Alarmzentrale (Anlage mit Wartungsvertrag)

Zugangskontrolle
Keine unbefugte Systembenutzung:

- Identifizierung und Authentifizierung des Nutzers- am lokalen System und im Netzwerk.
- Kennwortverfahren (Sonderzeichen, Mindestlänge, 8 Stellen inkl. Groß- und Kleinbuchstaben, regelmäßiger Wechsel und Wiederverwendbarkeit erst nach mehreren Generationen)
- Regelungen bei Ausscheiden eines Mitarbeiters zur Kontosperrung
- Automatische Sperrung des Bildschirms (z.B. Kennwort oder Pausenschaltung). Mitarbeiter sind zusätzlich angehalten den Bildschirm zu sperren wenn diese Ihren Arbeitsplatz verlassen.
- Verschlüsselung von Datenträgern: Support mit Festplatten/Hardlock, Technik nutzt USBsticks für Firmware-Updates an Maschinen ohne Verschlüsselung. Mobile Arbeitsplatzsysteme mit verschlüsseltem Container.

Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems bzw. Systemverbunds.

- Differenzierte Berechtigungen (Profile, Rollen, Objekte) über serverbasiertes Rechte- und Rollenkonzept.
- Verantwortliche Person für die Vergabe der Berechtigungen inkl. Vertretungsregelung steht fest.
- Regelungen bei Ausscheiden eines Mitarbeiters zur Kontosperrung
- Löschung von Datenträgern vor Wiederverwendung: Mitarbeiter sind sensibilisiert.
- Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399).
- Kennwortverfahren (Sonderzeichen, Mindestlänge, 8 Stellen inkl. Groß- und Kleinbuchstaben, regelmäßiger Wechsel und Wiederverwendbarkeit erst nach mehreren Generationen)
- Sichere Aufbewahrung von externen Datenträgern
- Einsatz von Anti-Viren-Software inkl. Updatevertrag
- Einsatz von Hardware-Firewall

Trennbarkeit
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden:

- Datenspeicherung erfolgt in getrennten Verzeichnissen. Bei der Verarbeitung in Datenbanksystemen werden die Daten logisch bzw. über Instanzen getrennt.
- Zugriffe erfolgen im Rahmen von Aufgabenerfüllung und notwendiger Berechtigungen
- Funktionstrennung: Produktions- & Testumgebung

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen:

Im Vordergrund stehen immer die schutzwürdigen Interessen der betroffenen Personen. Soweit dies mit vertretbarem Aufwand technisch und organisatorisch möglich ist, findet eine Pseudonymisierung der Daten der betroffenen Personen statt.

Im Rahmen von Auftragsverarbeitungen ist der Auftraggeber für die Pseudonymisierung der zur Verfügung gestellten personenbezogenen Daten verantwortlich.

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport:

- Bei physischem Transport: Transportsicherung/ Verschlüsselung der Datenträger und sorgfältige Auswahl von Transportpersonal und –fahrzeug.
- Datenschutzgerechte Entsorgung von Datenträgern (intern/extern)

Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Entfällt, da außer Löschung und Testdruck in Anwesenheit des Auftraggebers keine Verarbeitung personenbezogener Daten im Kundenauftrag direkt beim Auftragnehmer erbracht wird.
- Bei Remote-Supporttätigkeiten erfolgt die Verarbeitung im System bzw. Systemverbund und mit der jeweiligen Rolle des Mitarbeiters beim Auftraggeber.

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:

- Backup- & Recoverykonzept
- Spiegeln von Festplatten, RAID-System
- Testen der Datenwiederherstellung durch Datenwiederherstellung.
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort (mind. anderer Brandschutzbereich)
- Unterbrechungsfreie Stromversorgung im Serverräumen (USV)
- Klimaanlage in Serverräumen
- Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosen in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Serverräume nicht unter sanitären Anlagen
- Virenschutzsoftware

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)
Gewährleisten, dass einzelne Systeme im Störfall wiederhergestellt werden können:

- Nutzung einfacher Sicherungsverfahren
- Einsatz kurzfristig zu beschaffender Standard-Hardware
- Einsatz redundanter Hardwarekomponenten
- Einsatz virtueller Arbeitsplätze und Server
- Regelmäßiges Testen der Wiederherstellbarkeit der Daten

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleitung der Sicherheit der Verarbeitung:

- Interne Tests mit Dokumentation der Ergebnisse
- Regelmäßige Datenschutzaudits

Incident-Response-Management
IT relevante Aspekte einer Prüfung von Datenschutz Compliance:

- Notfallpläne
- Regelmäßige Kontrollen

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

- Arbeitsanweisungen und Schulungen zur Nutzung der Systeme
- Differenziertes Berechtigungskonzept
- Definition der Speicherfristen

Auftragskontrolle
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers:

- Eindeutige Vertragsgestaltung nach Art. 28 DS-GVO - Auftragsverarbeitung
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
- Vorabüberzeugungspflicht
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit

Hiermit bestätigen wir die Richtigkeit dieser Angaben.

Mannheim im Mai 2018

Franz Schüler, Geschäftsführer