# Anlage zur Vereinbarung zur Auftragsverarbeitung

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO zur Sicherheit personenbezogener Daten der

**Minol Messtechnik W. Lehmann GmbH & Co. KG**
**Nikolaus-Otto-Straße 25**
**70771 Leinfelden-Echterdingen** - Auftragnehmer -

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft die Minol Messtechnik geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmäßig - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

## 1. Vertraulichkeit (lt. Art. 32 Satz 1 a, b)

| |
|---|
| **1.1 Zutrittskontrolle** (Verhinderung des Zutritts Unbefugter zu DV-Anlagen, die der Verarbeitung personenbezogenen Daten dienen) |
| Einrichtung der Rechenzentren als Sicherheitsbereich, der stets verschlossen ist, mit Sonderzutrittsregelung (differierenden Zutrittsberechtigungen) |
| Festlegung zutrittsberechtigter Personen |
| Schlüsselregelung für Zutrittsberechtigte |
| Sonderzutrittsregelung für andere: nur in Begleitung Zutrittsberechtigter |
| Netzwerke (Verteilerkästen, Netzwerk-Management, Router, Switches, Verkabelung) gesichert |
| Einbruchmeldeanlage für Rechenzentren und angrenzende Räume |
| Gebäudesicherung durch Wachdienst |

| **1.2 Zugangskontrolle** (Verhinderung der Nutzung von DV-Systemen mit personenbezogenen Daten durch Unbefugte) |
|---|
| Nutzung von Legitimationsverfahren mit eindeutiger Nutzerauthentifizierung |
| Nutzerauthentifizierung beinhaltet unterschiedliche Zugangsrechte („Nutzer-Rollen“) |
| Definierte Vergabe, Sicherung, Änderung und Löschung von Nutzer-Rollen |
| Multifaktor-Authentifizierung bei der VPN-Einwahl und Anmeldung an Computern |
| Zusätzliche separate Passwortvergabe für DV-Systeme, mit denen personenbezogene Daten verarbeitet, genutzt und gespeichert werden |
| Prüfung der Passwörter auf Kompromittierung |
| Kontrolliertes Passwortverfahren (mit definierter Syntax), bei ggf. notwendigem Wechsel keine Wiederholung der Passwörter mit ähnlichem Beginn nicht zulässig |
| Nutzung zentraler Firewalls |
| Systemunterstützte / manuelle Tastatur- und Bildschirmsperre bei Nichtnutzung / Abwesenheit |
| Schutz vor Brute-Force-Angriffen mit dauerhafter Sperrung der Zugänge, bis zur Wiederfreigabe durch Administrator |
| Schutz durch Phishing-Test und Cyber Security Awareness-Kampagnen |

| **1.3 Zugriffskontrolle** (Verhinderung des Zugriffs auf oder die Veränderung von personenbezogenen Daten durch Unbefugte) |
|---|
| Dateiorganisation und Vergabe von Zugriffsrechten zentral geregelt, zusätzlich Freigabe Vorgesetzter erforderlich |
| Berechtigungssteuerung für den Zugriff auf Dateien, System- und Anwendungsprogramme durch Zugangsberechtigung über Freigabe durch Vorgesetzte und Rollenkonzepte (unter Berücksichtigung des Global Active Directory) |
| Nachvollziehbarkeit der Rechtevergabe für Nutzer, inklusive Administrationsrechte, gemäß Rollenkonzept („Need to know“ - Ansatz) |
| Zugangspolicy und Rechtevergabe für Administratoren zu Datenbanken und Rechenzentren gemäß Rollenkonzept und Einführung einer toolspezifischen Mulitfaktor-Authentifizierung |
| Mehrstufiges Berechtigungskonzept mit Segmentierung der Administratoren-Ebenen |

| **1.4 Trennungskontrolle** (Gewährleistung getrennter Verarbeitung zu unterschiedlichen Zwecken erhobener personenbezogener Daten) |
|---|
| Getrennte Bearbeitung jedes Auftrages |
| Getrennte Protokollierung einzelner Arbeitsschritte bei jedem Auftrag |
| Trennung von Test- und Produktionsbetrieb bei Programmen und Dateien |
| Berechtigungskonzepte stellen die zweckgebundene und mandantengetrennte Verarbeitung sicher. Zweckbindung: Logische Mandanten werden softwareseitig getrennt. |

| **1.5 Pseudonymisierung** (Verhinderung der Zuordnung von personenbezogenen Daten zu einer betroffenen Person ohne Hinzuziehung zusätzlicher Informationen) |
|---|
| Bei den Funk-Ableseverfahren radio$^{3}$ und radio$^{5}$ werden ausschließlich Geräteinformationen übertragen. Eine Zuordnung zu einer Nutzeinheit bzw. Personen ist nur im Backend (ERP-System) mit speziellen Zugriffs-Legitimationen möglich |
| Im Andruck von Rechnungen werden die für SEPA-Mandate notwendigen Bankdaten der IBAN maskiert (Setzen von X an mindestens 12 Stellen) |

## 2. Integrität (lt. Art. 32 Satz 1 b)

| **2.1 Weitergabekontrolle** (Verhinderung des unbefugten Lesens, Kopieren, Veränderns oder Entfernens personenbezogener Daten während der elektronischen Übertragung bzw. der Speicherung) |
|---|
| Weitergabe von Dateien nur an berechtige Personen oder Auftragsverarbeiter mit Vereinbarung nach Art. 28 EU-DSGVO |
| Dokumentation der Datenverarbeitungs-Endgeräte und der eingesetzten Software-Tools, die personenbezogenen Daten verarbeiten / nutzen |
| Berechtigungsregelung für Datenweitergabe |
| Interne Weitergabe: über internes Austauschlaufwerk mit VPN-Verschlüsselung |
| Zentrale Firewalls und Switche an den Rechenzentren sind redundant |
| Zugang zu allen Online-Services sind SSL verschlüsselt |
| Nutzung von Wechselmedien gemäß Berechtigungskonzept |
| Dokumenten Management System (DMS) mit Änderungshistorie |
| Externe Weitergabe: nach Absprache mit dem Empfänger (Regelung des DTA bzw. elektronischen Rechnungsversands) |

| **2.2 Eingabekontrolle** (Nachträgliche Prüfmöglichkeit darüber, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben / verändert / entfernt wurden) |
|---|
| ERP System mit Nutzergruppen |
| Automatisch Protokollierung der Dateinutzung |
| Protokollierung der Eingaberechte im ERP-System |
| Aufbewahrung bzw. Nachvollziehbarkeit der Protokollierung im ERP-System |
| Ein Ticketsystem im Support- und Administrationsbereich stellt die korrekte und zeitgerechte Erledigung aller Aufgaben sicher |

## 3. Verfüg- und Belastbarkeit (lt. Art. 32 Satz 1 b)

| **3.1 Verfügbarkeitskontrolle** (Schutz personenbezogener Daten vor zufälligem Verlust / zufälliger Zerstörung) |
|---|
| Richtlinien zur Datenarchivierung |
| Zentrales Backup-System mit Berechtigungskontrolle |
| Verfahrensanweisung für zentrales Backup (Backup-Richtlinie) |
| Firewall installiert |
| Automatischer Virenscan und Richtlinie zur Aktualisierung des Virenscanners |
| Verschlüsselung sämtlicher Firmenlaptops und -smartphones |
| Rechenzentren ist mit einer Brandmeldeanlage mit Verbindung zu VdS-zertifizierten Sicherheitszentrale und einer Löschanlage ausgestattet |

| **3.2 Belastbarkeit** (Gewährleitung, dass eingesetzte Systeme anforderungskonform genutzt und im Normbetrieb störungsfrei betrieben werden können) |
|---|
| Die Verfügbarkeit von IT-Systemen wird über ein Monitoring überwacht |
| Systeme werden 24/7 proaktiv erweitert |
| Datenleitungen verfügen über ein ‚Quality of Service‘ |
| Zentrale IT-Systeme verfügen über ein ‚Quality of Service‘ |
| Die IT-Systeme verfügen über dynamisch verfügbaren Speicherplatz und Rechenkapazitäten |

| **3.3 Wiederherstellbarkeit** (Gewährleitung, dass eingesetzte Systeme im Störungsfall wiederherstellt werden können) |
|---|
| gesichertes Herunterfahren des Systems bei Stromausfall (USV-Geräte installiert) |
| Aufbewahrung der Backup-Kopien in unterschiedlichen Gebäuden und abgeschlossenen Räumen |
| Regelmäßige Tests zur Wiederherstellung mit Backup-Dateien |

## 4. Richtlinien, Arbeitsanweisungen, regelmäßige Kontrollen (lt. Art. 32 Satz 1 d)

| **4.1 Organisationskontrolle** (Sicherstellung der Umsetzung der besonderen Anforderungen an den Datenschutz in der innbetrieblichen Organisation ) |
|---|
| Implementierung eines Datensicherheitsansatzes verbunden mit einem aktuell gehaltenen IT-Sicherheitskonzept |
| Fortschreiben und Nachhalten von Arbeitsanweisungen zum Datenschutz (insbesondere auch im Hinblick auf die HKVO, BetrKV, LBO und TrinkwasserV) |
| laufende Sensibilisierung und regelmäßige Unterweisungen der Mitarbeiter auf die Belange der EU-DSGVO |
| regelmäßige Prüfung der Verfahren, die der Nutzung, Verarbeitung und Speicherung personenbezogener Daten dienen |
| regelmäßige Prüfung, mindestens einmal jährlich, der technischen und organisatorischen Maßnahmen und deren innerbetriebliche Umsetzung |
| Löschkonzepte für vertrags- / auftragsbezogene sowie personen- / mitarbeiterbezogene Daten (wie SAP-, Personalabteilungs-Löschkonzept) |
| Führen von Verzeichnissen der Verarbeitungstätigkeiten |

| **4.2 Außenkontrolle** (Sicherstellung der Umsetzung der besonderen Anforderungen an den Datenschutz an die außerbetriebliche Organisation ) |
|---|
| Vorgabe zur Prüfung von Datenschutz-Standards bei Einführung neuer Dienstleister / Unterauftragnehmer |
| regelmäßige Prüfung von Unterauftragnehmer und deren technische und organisatorische Maßnahmen |