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

1.1 Zutrittskontrolle:

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

Umgesetzte Maßnahmen:

	Maßnahme	Personenkreise
Eingangstür	Codeschloss	Mitarbeiter*innen
Serverraum	zusätzliches, getrenntes Codeschloss mit Sicherheitstoken	GL
Räume der Sigma-IT GmbH	Videoüberwachung	
Räume der Sigma-IT GmbH	Empfangsbereich mit Sekretariat (Empfang)	Empfang

2 Datenträgerkontrolle:

Unter Datenträgerkontrolle sind Maßnahmen zu verstehen, die geeignet sind zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können. Auch bei der Weitergabe, dem Austausch, der Reparatur oder der Entsorgung von magnetischen Datenträgern muss einem solchen Missbrauch vorgebeugt werden.

Umgesetzte Maßnahmen:

	Maßnahme	Personenkreise
Notebooks	• Einsatz von TPM Modul • Mobiles Device Management (MDM durch Sophos Central), • Festplatten Verschlüsselung	Mitarbeiter*innen
Smartphone	• Mobiles Device Management (MDM durch Sophos Central), • Arbeitsanweisung zur Trennung von Privat und Geschäftsdaten	Mitarbeiter*innen
Server	RAID Systeme, Monitoring verschiedener Sensoren mittels Server-Eye	GL
mobiler Datenträger	Verwendung für KundenDaten ist untersagt.	Mitarbeiter*innen
Entsorgung von Datenträgern	Entsorgung der Datenträger nur durch Zertifizierte Firmen mit Entsorgungsprotokoll / Zertifikat.	Mitarbeiter*innen

3 Zugangskontrolle:

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

Umgesetzte Maßnahmen:

	Maßnahme	Personenkreise
ERP mit CRM	Personenkreise und entsprechenden Berechtigungen nach Gruppen (Vertrieb, GL, Technische Einsatzplanung)	Mitarbeiter*innen
Ticketsystem	Personenkreise und entsprechenden Berechtigungen nach Gruppen (Vertrieb, GL, Mitarbeiter*innen) 2 Faktor Authentifizierung, Protokollierung der Zugriffe	Mitarbeiter*innen
Fernwartung	2 Faktor Authentifizierung, Protokollierung der Zugriffe	Techniker
automatische Überwachung der Kundensysteme	2 Faktor Authentifizierung, Protokollierung der Zugriffe	Techniker
IT-Systeme der Sigma-IT	• Passwortrichtlinie vorhanden, • Sperre nach 3 Fehlversuchen • Berechtigungen nach Gruppen • Beschränkte Anzahl an Administratoren • Office 365 Zugriffe nur mit 2 Faktor Authentifizierung • Passwortmanager nur mit 2 Faktor Authentifizierung	Mitarbeiter*innen, GL

4 Zugriffskontrolle:

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

	Maßnahme	Personenkreise
ERP mit CRM und DMS, Ticketsystem	• Stellenbeschreibung • differenzierte Berechtigungen • regeln für Benutzer*innen-rechte • Beschränkung der Löschberechtigung • Auswertungen der Veränderungen • Einsatz von Anwendungssoftware mit “Rollenberechtigungskonzepten” • Einsatz von Anwendungssoftware mit “differenzierbaren Rechten” • 2-Faktor Authentifizierung	Mitarbeiter*innen

5 Trennungskontrolle:

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing.

Umgesetzte Maßnahmen:

	Maßnahme	Personenkreise
ERP	Trennung der Kundendaten nach Notwendigkeit. • ERP System (GF, Finanzdaten, Rechnungsempfänger, Belege)	Mitarbeiter*innen
Ticketsystem (Leads)	Trennung von Kunden und Interessenten. • Kunden (Mitarbeiter*innen*innen des Kunden, Telefonnummern, E-Mail Adressen) • Interessenten (keine Erfassung im ERP, bis zur Angebotserstellung)	Vertrieb/Verwaltung

6 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.

Umgesetzte Maßnahmen:

	Maßnahme
ERP	Buchhaltungsbelege können nicht pseudonymisiert erstellt oder verarbeitet werden. Andere Personenbezogene Daten werden nicht erhoben oder gespeichert. Rechnungsempfänger werden mit Name, Geschlecht (Herrr Frau), Telefonnummer, E-Mail Adresse gespeichert. Dies ist für die Dokumentation von Geschäftsvorfällen notwendig.

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

7.1 Weitergabekontrolle:

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

Umgesetzte Maßnahmen:

	Maßnahme
Datenweitergabe	Ein transparentes Verschlüsselungssystem erlaubt Verschlüsselte E-Mails oder per SSL Verschlüsselte Übertragungen von Daten. Die Übertragung bei Fernwartungen ist SSL Verschlüsselt zwischen den Endgeräten (Techniker PC und Kunden PC). Alle Download-Links haben eine Gültigkeit und das Passwort wird auf einem 2. Weg übergeben.
E-Mail	E-Mail Signaturen und E-Mail-Verschlüsselung
Kennzeichnung von schutzwürdigen Informationen	Alle Dokumente werden mit dem TLP Verfahren gekennzeichnet. TLP ist eine standardisierte Vereinbarung zum Austausch von schutzwürdigen Informationen.
Passwörter von Kundensystemen	Verwenden eines Passwortmanagement-Servers.

8 Eingabekontrolle:

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

Umgesetzte Maßnahmen:

	Maßnahme
ERP, DMS und Ticketsystem	Protokoll durch die Systeme. Im DMS werden auch die hinterlegten digitale Prozesse protokolliert.

9 Datenintegrität:

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Umgesetzte Maßnahmen:

	Maßnahme
Betriebssysteme und aktive Daten	Alle Serversysteme der Sigma-IT GmbH befinden sich im Rechenzentrum der TerraCloud in Hüllhorst. Das Backup ist Katastrophensicher ausgelegt (Tier 3) und hat 12 Monate Rückwirkend eine Monatssicherung und 30 Tage Rückwirkend eine Sicherung aller Systeme. Alle Systeme werden redundant mit Strom und Netzwerk versorgt. Alle Systeme werden proaktiv 27/7 überwacht.
Internet	Im Rechenzentrum sind die Server mit Redundanten Internetverbindungen anschlossen. Am Standort Ludwigsburg werden 2 Unterschiedliche Provider verwendet. Ein automatisches Umschalten der Verbindungen ist eingerichtet. Am Standort Owingen besteht eine einfache Internetanbindung. Die Verbindung zu der Zentrale in Ludwigsburg findet mittels VPN Gateway verschlüsselt statt.

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

10.1 Verfügbarkeitskontrolle:

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne.

Umgesetzte Maßnahmen:

	Maßnahme
IT- Systeme	• tägliches Backup mit regelmäßigen Wiederherstellungstests • Web Proxy mit AV und Spam FIlter • Spam Filter für E-Mail Verkehr • IDS System • Intrusion prevention System • interne Malware detection • Antivirensoftware auf PC und Servern • Notfallplan bei Systemausfall der Sigma-IT GmbH • personal Firewalls • Netztrennung (VLAN)
Extern Datenträger	Die Verwendung ist untersagt.
Mobile Geräte	Ein Mobile-Device-Management ist eingeführt und umgesetzt.

11 Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Die rasche Wiederherstellbarkeit unserer IT-Systeme ist gewährleistet.

Umgesetzte Maßnahmen:

	Maßnahme
IT- Systeme	• Server Systeme im Rechenzentrum der Wortmann AG. (Tier 3 RZ, Hüllhorst, Deutschland) • Datenwiederherstellung mittels Software und Backupkonzept <4h (getestet)

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

Die Sigma-IT GmbH prüft durch interne Audits regelmäßig die verwendeten Verfahren und verwendet dazu das PDCA Verfahren. Ferner ist die Etablierung eines ISMS in Arbeit und eine ISO 27001 Zertifizierung wird derzeit vorbereitet (Stand Jan. 2022).

13 Datenschutz-Management:

- Internes ISMS wird seit Januar 2022 eingeführt.
- Incident-Response-Management (Eigenes System an ITIL angelehnt)
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.