Anlage 1 – Beschreibung der personenbezogenen Datenkategorien

☒ Abrechnungsdaten	☒ Kennzeichen KFZ
☒ Accountdaten	☒ Kontaktdaten
☒ Adressdaten geschäftlich	☒ Kontakthistorie
☒ Adressdaten privat	☒ Krankmeldungen
☒ Angaben zu Lohnpfändungen	☐ Krankheitsdaten
☒ Angaben zu Angehörigen	☒ Leistungsnachweise
☒ Arbeitgeber	☒ Lohn- und Gehaltsdaten
☒ Arbeitszeiten	☒ Mobilnummer geschäftlich
☒ Arbeitszeugnisse	☒ Mobilnummer privat
☒ Authentifizierungen	☒ Name / Vorname
☒ Bankverbindungsdaten	☒ Name Unternehmen
☒ Berufliche Laufbahn	☒ Nutzungsdaten
☒ Berufsabschluss	☒ Personalnummer
☒ Besucherlisten	☒ Position
☒ Bilder / Fotos	☒ Qualifikationen
☒ Daten Warenkauf / Dienste	☒ Reisekosten
☒ E-Mail Adresse geschäftlich	☒ Schulabschlussdaten
☒ E-Mail Adresse privat	☒ Sicherheitsdaten
☒ Familienstand	☒ Sozialversicherungsdaten
☒ Faxnummer	☒ Steuerdaten
☒ Fortbildungen	☒ Telefonnummer geschäftlich
☒ Führerscheindaten	☒ Telefonnummer privat
☒ Internetadresse	☒ Termindaten
☒ Hosting	☒ Titel
☒ Urlaubszeiten	☐ Überwachungsbilder / Videos
☒ Vertragsdaten	☒ Umsatzdaten
☒ Videos	☒ UST Nummer
☒ Vorgangsdaten	☐ Zeiterfassung
☒ Werbung	☐ Sonstiges:
☒ Zahlungsdaten	_____

Kategorien der von der Datenverarbeitung betroffenen Personen

Bei dem Auftragsverarbeiter zur Verarbeitung zugewiesenen Daten könnte es sich um personenbezogene Daten folgender Personenkreise handeln:

- Ansprechpartner
- Beschäftigte
- Dienstleister
- Interessenten
- Kunden
- Lieferanten
- Vermittler

Anlage 2 – Beschreibung der besonders schutzbedürftigen Datenkategorien

- [x] Angaben über Gesundheit
- [ ] Angaben über eine Gewerkschaft
- [ ] Politische Angaben
- [ ] Rassische oder Ethnische Herkunft
- [x] Religiöse oder weltanschauliche Überzeugungen
- [ ] Angaben über Strafen / Vorstrafen
- [ ] Angaben über Sexualverhalten
- [ ] Sonstiges

_____

Geschäftsführer:
Marco Gusenburger
Andreas Piper

Hausanschrift:
Kurt-Schumacher-Straße 27
66130 Saarbrücken
HRB 5667

Postanschrift:
Postfach 45 03 64
66061 Saarbrücken

Telefon: 0681 88311 – 0
Telefax: 0681 88311 – 11
St.-Nr.: 040 119 01269

Internet: http://www.schwindt.de
eMail: info@schwindt.de
USt IDNr: DE 138 100 581
Amtsgericht Saarbrücken

Anlage 3 – Weisungsberechtigte Personen

Weisungsberechtigte Personen beim Auftraggeber (Verantwortlicher) sind

(Name, Vorname, E-Mail-Adresse, Tel.)

1 ……

2. ……

3. ……

4. ……

5. ……

Weisungsempfänger beim Auftragnehmer (Auftragsverarbeiter) sind

Gusenburger Marco, Geschäftsführer, 06 81 – 88 311-13
Piper Andreas, Geschäftsführer, 0681 – 88311-44

Anlage 4 - Allgemeine technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

Anforderungen an die technischen und organisatorischen Maßnahmen des Auftragnehmers (TOMs)

Verantwortlicher: SCHWINDT GmbH, Kurt-Schumacher-Str. 27, 66130 Saarbrücken

Gesetzliche Grundlagen zu technisch organisatorischen Maßnahmen.

1.1 Art 28 (1) DSGVO – „Technische und organisatorische Maßnahmen“

> Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

Dabei sind insbesondere Maßnahmen zu treffen, die geeignet sind unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren **(Zutrittskontrolle),**

zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle),**

zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können **(Zugriffskontrolle),**

zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung von personenbezogenen Daten durch Einrichtungen zur Datenübertragung vorgesehen ist **(Weitergabekontrolle),**

zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind **(Eingabekontrolle)**,

zu gewährleisten, dass personenbezogene Daten, die im Auftrag erhoben, verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden können **(Auftragskontrolle)**,

zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind **(Verfügbarkeitskontrolle)**,
zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. **(Trennungsgebot)**

Übersicht der zur Datenverarbeitung eingesetzten IT-Systeme:

Eingesetzte Hardware

X Interne Fileserver X Interne Serverräume

X Netzwerkinfrastruktur

- X W-LAN
- X NetzwerkinfrastrukturVPN
- X Netzwerkinfrastruktur: LANs: Menge: 4

X Desktop Clients Betriebssysteme

- X MS Windows: Version 10 & Version 11
- X MS Server: Version 2019, 2020

Eingesetzte Software

X Teamviewer X Virenschutz Kaspersky X Warenwirtschaft SAGE X MS Office Version 2016, 2019, 365

X Sonstiges: DocuWare & Asana

1. Zutrittskontrolle

Ziel ist es Unbefugten keinen räumlichen Zutritt zu Datenverarbeitungsanlagen, mit welchen personenbezogene Daten verarbeitet werden, zu verschaffen.

Zutrittskontrolle des Gebäudes während Tages- und Nachtzeit durch Perimetersicherung

X Zaun X Glasbruchsensoren X Alarmanlage X Zutrittskontrollsystem

X Bewegungsmelder

Gebäudesicherung

X Bewegungsmelder X Glasbruchsensoren X Alarmanlage X Sicherheitstüren- Fenster

X RFID/Bluetooth/NFC-Transp.

Innenraumsicherung

X Bewegungsmelder X Alarmanlage X Glasbruchsensoren X Sicherheitstüren- Fenster

Organisatorische Maßnahmen

X Mitarbeiterschulung X Sperrbereiche und Sicherheitszonen X Schlüsselregelung

X Dokumentierte Schlüsselausgabe

2. Zugangskontrolle

Welche Maßnahmen werden getroffen um das Eindringen in das eigentliche EDV System zu verhindern?

Technische Maßnahmen

X Zentrale Steuerung von Berechtigung (Verzeichnisdienst und Identitätsmanagement)

X Schnittstellen – Sperren (USB, Firewire, etc)

X Benutzeranmeldung mit Kennung und Passwort

X Netzwerkbasiertes Intrusion-Detection-System

X Software Firewall

X Hardware Firewall

X keine Administrator-Konten für normale Nutzer

X Regelmäßiges Einspielen sicherheitsrelevanter Patches, Updates und Servicepacks

X VPN-Tunnel für Remote Zugriffe

X Segmentierung z.B. V-LANs oder Layer 3 Switches

X Port-Sperren

X Sperren von Clients bei Inaktivität

Organisatorische Maßnahmen

X Passwortregelung X Berechtigungskonzept

X Passwortrichtlinie (zur Komplexität, Änderung und Geheimhaltung)

X Restriktive Vergabe von Admin Rechten auf Clients Mails mit unbekanntem Absender

X Mitarbeiterschulung

3. Zugriffskontrolle

Maßnahmen zur Sicherstellung, dass nur Befugte Zugriff auf die Datenverarbeitungs-programme und Daten Zugriff haben, wobei die Berechtigungen für Lesen, Löschen, Ändern und kopieren eingehalten werden müssen.

Technische Maßnahmen

X Ordnungsgemäße Vernichtung von Datenträgern

X Protokollierung der Vernichtung von Datenträgern

X Vernichtung von Papierdokumenten und Akten (Aktenvernichter, Dienstleister)

Organisatorische Maßnahmen

X Rechteverwaltung durch eine minimale Gruppe von Administratoren

4. Weitergabekontrolle

Maßnahmen, die sicherstellen, dass bei der Übertragung und Weitergabe von personenbezogenen Daten keine Löschungen, Änderungen oder unbefugte Zugriffe stattfinden können.

Technische Maßnahmen

X zentrale Steuerung von Berechtigung X Getunnelte Datenfernverbindungen (VPN)

X SSL Verschlüsselung bei WEB Access

Organisatorische Maßnahmen

X Berechtigungskonzept X Mitarbeiterschulung

X Sorgfältige Auswahl von Transportpersonal und Fahrzeugen

5. Eingabekontrolle

Nachträgliche Möglichkeit eines Zugriffs auf Daten welche das Löschen, Anlegen oder Ändern betreffen.

Technische Maßnahmen

X zentrale Steuerung von Berechtigung (z.B. per Verzeichnisdienst) X personenscharfe Nutzerkonten

Organisatorische Maßnahmen

X Passwortregelung X Berechtigungskonzept X Mitarbeiterschulung

X Dokumentation der Verarbeitungsprozesse einschließlich der eingesetzten Software und der damit jeweils verarbeiteten Daten (Verarbeitungsübersicht)

6. Auftragskontrolle

Maßnahmen der Überwachung, dass die Bearbeitung personenbezogener Daten nur laut Anweisung vorgenommen werden.

Technische Maßnahmen

X zentrale Steuerung von Berechtigung (z.B. per Verzeichnisdienst) X Protokollierung von Systemzugriffen

Organisatorische Maßnahmen

X Auswahl von Auftragnehmern nach definierten Sorgfaltsgesichtspunkten X Kontrolle von Auftragnehmern getroffener Datensicherheitsmaßnahmen X Mitarbeiterschulung

7. Verfügbarkeitskontrolle

Maßnahmen zum Schutz des Verlustes oder der Zerstörung personenbezogener Daten beim Auftragnehmer.

Technische Maßnahmen

X Unterbrechungsfreie Stromversorgung (USV) X Externe Datensicherung

X Redundante Systeme in unterschiedlichen Brandabschnitten

Organisatorische Maßnahmen

X Backup-Konzept

X Recovery-Konzept

8. Trennungskontrolle

Die Verarbeitung von Daten muss unabhängig voneinander gehalten werden.

Technische Maßnahmen

X physikalisch getrennte Speicherung

Organisatorische Maßnahmen

X Mitarbeiterschulung