Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag (Auftragsverarbeitung gem. Artikel 28 DSGVO)

zwischen

(im Folgenden „Auftraggeber“)

und

ZMI GmbH

Adolf-Kolping-Straße 11

97725 Elfershausen

(im Folgenden „Auftragnehmer“)

1. Gegenstand und Dauer des Auftrags

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers.

(2) Gegenstand des Auftrags ist die Installation und Betreuung bzw. Bereitstellung der erworbenen ZMI Software durch den Auftragnehmer. Der Auftrag kann im Bedarfsfall durch Einzelaufträge erweitert werden.

(3) Geltungsdauer der Vereinbarung: Die Geltungsdauer richtet sich nach der Laufzeit der zugrundeliegenden Leistungsvereinbarung(en). Diese Vereinbarung zur Auftragsverarbeitung wird automatisch Bestandteil sämtlicher in Ziffer 1 Absatz 2 bezeichneten Einzelaufträge und ergänzt diese. Diese Vereinbarung geht den datenschutzrechtlichen Regelungen der Einzelaufträge vor.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Auftragsbestätigung und den allgemeinen Nutzungsbedingungen.

(2) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

Das angemessene Schutzniveau kann wie folgt hergestellt werden:

- durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DSGVO);
- durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. 47 DSGVO);
- durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DSGVO);
- durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. 40 DSGVO);
- durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DSGVO).
- durch sonstige Maßnahmen.

(3) Bei Bedarf werden Datentransfer-Folgenabschätzungen im Rahmen der Verarbeitung personenbezogener Daten in unsicheren Drittländern durchgeführt.

3. Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien, die davon abhängen, welches Produkt/Modul Sie bei uns beauftragen und welche Daten Sie in der Software erfassen:

- Personalstammdaten (z.B. Vorname, Nachname, Geschlecht, Geburtsdatum, Familienstand, Staatsangehörigkeit, Personalnummer, Konfession)
- Adress- und Kommunikationsdaten (z.B. Straße. Hausnummer, PLZ, Ort sowie Telefon oder E-Mail)
- Qualifikationsdaten (z.B. Lebenslauf, Zeugnisse, Fähigkeiten)
- An-/Abwesenheitsdaten (z.B. Arbeitszeiten, Fehlzeiten und -gründe)
- Bankdaten (z.B. IBAN, BIC)
- Steuer- und Sozialversicherungsdaten (z.B. Steuer-ID, Kinder, SV-Nummer, Krankenkasse)

4. Kategorien betroffener Personen

Betroffen von der Verarbeitung sind nachstehende Kreise von Betroffenen:

- Mitarbeitende inkl. Aushilfen, Teilzeitkräfte sowie Praktikanten und Schüler
- Externe Arbeitskräfte wie z.B. Freelancer oder Leiharbeiter

5. Pflichten des Auftragnehmers

a) Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen. Hierfür gelten die in der Anlage 1 festgelegten technischen und organisatorischen Maßnahmen, mit denen sich der Auftraggeber einverstanden erklärt [Einzelheiten in Anlage 1 TOM].

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

b) Unterstützungspflicht

(1) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber, an der Erstellung des Verzeichnisses von Verarbeitungstätigkeiten des Auftraggebers sowie bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen. Er hat die dazu erforderlichen Angaben jeweils unverzüglich an den Auftraggeber weiterzuleiten.

Hierzu gehören u.a.

- a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
- b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
- c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind und über die gesetzlichen Pflichten des Auftragnehmers hinausgehen, kann der Auftragnehmer eine angemessene Vergütung beanspruchen. Hinsichtlich der Vergütungshöhe wird auf die entsprechende Vergütungsklausel verwiesen.

c) Verarbeitung personenbezogener Daten im Home- bzw. Mobile-Office

Der Auftraggeber stimmt der Verarbeitung von Daten außerhalb der Betriebsräume (z.B. Telearbeit, Heimarbeit, Home-Office, mobiles Arbeiten) zu. Der Auftragnehmer verpflichtet sich

- zur Unterstützung seiner Beschäftigten bei der Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen in ihren privaten Räumlichkeiten, um die Sicherheit der Daten zu garantieren.
- zur angemessenen Unterrichtung seiner Beschäftigten bezüglich der Einhaltung der technischen und organisatorischen Maßnahmen und sonstigen Sorgfaltspflichten, die es bei der Verarbeitung der Daten in privaten Räumlichkeiten einzuhalten gilt.

d) sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer gewährleistet die schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt.
Die Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers lauten: SiDIT GmbH, info@sidit.de und sind auch auf der Webseite des Auftragnehmers einsehbar.

(2) Der Auftragnehmer gewährleistet die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Diese Vertraulichkeitsverpflichtung der Mitarbeiter gilt auch nach Beendigung ihres jeweiligen Arbeitsvertrages fort.

(3) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

(4) Der Auftragnehmer gewährleistet die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(5) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen. Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind und über die gesetzlichen Pflichten des Auftragnehmers hinausgehen, kann der Auftragnehmer eine angemessene Vergütung beanspruchen. Hinsichtlich der Vergütungshöhe wird auf die entsprechende Vergütungsklausel verwiesen.

(6) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

6. Pflichten und Rechte des Auftraggebers

a) Verantwortlichkeit

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

(2) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

b) Weisungsbefugnis

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt.

(2) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Sofern technisch und nach dem Zweck der Leistungsvereinbarung erforderlich, darf der Auftragnehmer Daten von Geräten auch ohne diesbezügliche Weisung löschen (z.B. bei einem schnell erforderlichen, technisch notwendigen Austausch eines Gerätes). Entstehen dem Auftragnehmer Kosten bei Löschung der Daten, so trägt diese der Auftraggeber.

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(4) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

c) Kontrollrechte

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen zur Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Dem Auftragnehmer steht es frei, zur Erfüllung dieses Überprüfungsrechts dem Auftraggeber entsprechende Kontrollberichte oder ähnliche Dokumentationen, die eine datenschutzkonforme Datenverarbeitung belegen, vorzulegen. Soweit dem Auftraggeber Zweifel an der Datenschutzkonformität der Datenverarbeitungen verbleiben, hat er das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Auftragnehmer ist berechtigt, den Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI Grundschutz).

zu erbringen.

7. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Die Auslagerung auf Unterauftragnehmer oder der Wechsel bestehender Unterauftragnehmer sind zulässig, soweit der Auftragnehmer dies dem Auftraggeber mindestens vier Wochen vor dem geplanten Wechsel auf folgender Unterseite seiner Webseite (*https://zmi.de/unterauftragnehmer/*) anzeigt sowie per E-Mail informiert und der Auftraggeber nicht innerhalb von 2 Wochen ab der Anzeige gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung oder den Wechsel erhebt. Der Auftraggeber verpflichtet sich dazu, die o.g. Auflistung der eingesetzten Unterauftragnehmer regelmäßig zu überprüfen. Der Auftragnehmer wird mit dem Unterauftragnehmer eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO schließen. Verweigert der Auftraggeber durch seinen Einspruch die Zustimmung aus anderen als aus wichtigen Gründen, kann der Auftragnehmer den Vertrag zum Zeitpunkt des geplanten Einsatzes des Unterauftragnehmers kündigen.

(3) Der Auftraggeber stimmt der Beauftragung der unter (*https://zmi.de/unterauftragnehmer/*) aufgeführten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zu.

(4) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

8. Löschung und Rückgabe von personenbezogenen Daten

(1) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen. Entstehen dem Auftragnehmer Kosten bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

9. Vergütungshöhe für weitergehende Kontroll- und Unterstützungsmaßnahmen

Die vom Auftragnehmer nach den vorangegangenen Klauseln möglicherweise zu verlangenden Vergütungsansprüche müssen angemessen sein. Als angemessen gilt die Abrechnung des entstandenen Aufwands nach den vom Auftragnehmer üblicherweise verlangten Stundensätzen.

10. Haftung und Schadensersatz

Der Auftraggeber gewährleistet in seinem Verantwortungsbereich bei der Verarbeitung personenbezogener Daten die Umsetzung der sich aus den einschlägigen geltenden rechtlichen Bestimmungen ergebenden Verpflichtungen.

Es gelten grundsätzlich die Haftungsbeschränkungen aus dem Hauptvertrag. Der Auftraggeber stellt den Auftragnehmer von sämtlichen Ansprüchen frei, die Dritte wegen der Verletzung ihrer Rechte gegen den Auftragnehmer auf Grund der vom Auftraggeber beauftragten Verarbeitung personenbezogener Daten geltend machen, sofern nicht der Anspruch des Dritten auf einer rechtswidrigen Verarbeitung der personenbezogenen Daten durch den Auftragnehmer beruht. Im Übrigen bleibt Art. 82 DSGVO unberührt.

11. Sonstiges, Allgemeines

(1) Sollten die personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den personenbezogenen Daten des Auftraggebers bei dem Auftraggeber liegt.

(2) Die Regelungen dieser Vereinbarung gelten auch nach einer Beendigung des primären Leistungsverhältnisses bis zur vollständigen Vernichtung oder Rückgabe aller personenbezogenen Daten des Auftraggebers an den Auftraggeber fort.

(3) Sollten einzelne Teile der hier vorliegenden Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit dieser Vereinbarung im Übrigen nicht. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt.

.....	.....
Ort, Datum	Unterschrift Auftraggeber
.....	.....
Ort, Datum	Unterschrift Auftragnehmer

Anlage 1: Technische und organisatorische Maßnahmen gemäß Art. 32 Abs. 1 DSGVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO)

1.1. Zutrittskontrolle

Im Folgenden werden alle Maßnahmen aufgelistet, um Unbefugten den Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verhindern:

- Videogegensprechanlage am Haupteingang
- Bewegungsmelder an den Eingängen für die Lichtsteuerung
- Automatisches Zutrittskontrollsystem
- Chipkartensysteme zum Zutritt
- Manuelles Schließsystem
- Türen mit Knauf an der Außenseite
- Notausgang nur von innen zu öffnen
- Eigenes Rechenzentrum
- Eigener Serverraum und eigener Serverschrank
- Ausgaberegelung für Chipkarten
- Besucher / Externe in Begleitung durch Mitarbeiter
- Maßnahmen bei Verlust von Schlüssel und Chipkarte

1.2. Zugangskontrolle

Im Folgenden werden alle Maßnahmen aufgelistet, um Unbefugten den Zugang zu den Datenverarbeitungssystemen zu verhindern:

- Login mit Benutzername + Passwort
- 2-Faktor-Authentifizierung
- Sperrung Zugang des Benutzers nach definierter Anzahl von Falschanmeldungen
- Anti-Viren-Software Server
- Anti-Virus-Software Clients
- Anti-Virus-Software mobile Geräte
- Firewall - Server
- Firewall - Clients
- Intrusion Detection Systeme (IDS)
- Mobile Device Management
- Externer Zugang durch Mobile- / Homeoffice (bspw. PC / Laptop)
- Externer Zugang von externen Dienstleistern
- Externer Zugang durch Smartphones /Tablets
- Verschlüsselung bei WLAN-Benutzung (WPA2)
- Erstellen und Verwalten von Benutzerprofilen und -berechtigungen
- Anleitung „Manuelle Desktopsperre“
- Zentrale Passwortvergabe

- Richtlinie „Sicheres Passwort“
- Richtlinie „Löschen / Vernichten“
- Richtlinie „Clean desk“
- Richtlinie „Home-/Mobile-Office“
- Mobile Device Policy
- Allg. Richtlinie Datenschutz und Sicherheit

1.3. Zugriffskontrolle

Im Folgenden werden alle Maßnahmen aufgelistet, um Unbefugten das Lesen, Kopieren, Verändern oder Löschen innerhalb der Datenverarbeitungssysteme zu verhindern:

- Aktenschredder
- Physische Löschung von Datenträgern
- Protokollierung von Zugriffen auf Anwendungen in Log-Dateien
- Berechtigungskonzepte
- Minimale Anzahl an Administratoren
- Datenschutztresor
- Verwaltung Benutzerrechte durch Administratoren

1.4. Trennungskontrolle

Im Folgenden werden alle Maßnahmen aufgelistet, um die zu unterschiedlichen Zwecken erhobenen personenbezogenen Daten zu trennen:

- Trennung von Produktiv- und Testumgebung
- Virtuelle Trennung (Systeme / Datenbanken)
- Mandantenfähigkeit relevanter Anwendungen
- Bedarfsgerechte Zugriffsberechtigungen der Mitarbeiter
- Festlegung von Datenbankrechten

2. Integrität (Art. 32 Abs. 1 lit. b) DSGVO)

2.1. Weitergabekontrolle

Personenbezogene Daten müssen bei der elektronischen Übermittlung ausreichend geschützt werden, um nicht unbefugt gelesen, kopiert, verändert oder entfernt zu werden. Folgende technische und organisatorische Maßnahmen haben wir hierfür ergriffen:

- E-Mail-Verschlüsselung
- Bereitstellung von Tunnelverbindungen (VPN)
- Bereitstellung verschlüsselter Verbindungen

- Elektronische Signaturverfahren
- Protokollierung der Zugriffe und Abrufe in Log-Dateien
- Persönliche Übergabe mit Protokoll

2.2. Eingabekontrolle

Zur Kontrolle, ob und von wem personenbezogene Daten in das Datenverarbeitungssystem eingegeben, geändert, gesperrt oder gelöscht werden, setzen wir folgende Maßnahmen ein:

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Softwareliste mit Datenverarbeitungsprogrammen
- Vergabe individueller Benutzernamen
- Berechtigungskonzept mit Vergabe von bedarfsgerechten Benutzerrechten
- Sichere Aufbewahrung von Dokumenten in Papierform

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b) DSGVO)

3.1. Verfügbarkeitskontrolle

Zur Gewährleistung der Verfügbarkeit und Wiederherstellung der Verfügbarkeit personenbezogener Daten gegen zufällige oder mutwillige Zerstörung oder Verlust, setzen wir folgende Maßnahmen ein:

- Feuer- und Rauchmeldeanlagen
- Feuerlöscher
- Klimaanlage
- USV
- Schutzsteckdosenleisten Serverraum
- RAID System / Festplattenspiegelung
- Regelmäßige Archivierung / Backup der Daten
- Tägliche Snapshots im Rahmen der raschen Wiederherstellbarkeit der Daten
- Datenschutztresor
- Prozess zur raschen Wiederherstellbarkeit der Daten mittels täglicher Snapshots
- Kontrolle des Sicherungsvorgangs
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums (Cloud-Backup)
- Notfallpläne
- Getrennte Partitionen für Betriebssysteme und Daten

4. Verfahren zur regelmäßigen Überwachung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit d) DSGVO & Art. 25 Abs. 1 DSGVO)

Datum der Evaluierung der technischen und organisatorischen Maßnahmen: 31.10.2023

4.1. Datenschutz-Management

Zur Gewährleistung des Datenschutzes in unserem Unternehmen setzen wir folgende Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung ein:
Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt

- Externer Datenschutzbeauftragter
- Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
- Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich
- Interner IT-Sicherheitsbeauftragter

4.2. Incident-Response-Management (gemäß Art. 33 DSGVO)

Zur Verhinderung, zum Erkennen und zur Meldung von Datenschutzverletzungen sind folgende Maßnahmen im Einsatz:

- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virenscanner und regelmäßige Aktualisierung
- Patchkonzepte
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- Einbindung von DSB in Sicherheitsvorfällen und Datenpannen
- Einbindung von ISB in Sicherheitsvorfällen und Datenpannen
- Dokumentation von Sicherheitsvorfällen und Datenpannen
- Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.3. Datenschutzfreundliche Voreinstellungen

Im Rahmen datenschutzfreundlicher Voreinstellungen (Art. 25 Abs. 2 DSGVO) setzen wir folgende Maßnahmen ein:

- Datenminimierung und Zweckbindung
- Einfache Ausübung des Widerrufrechts des Betroffenen

4.4. Auftragskontrolle (Outsourcing)

Im Rahmen des Outsourcings der Verarbeitung personenbezogener Daten durch Auftragsverarbeiter setzen wir für die Gewährleistung eines angemessenen Schutzniveaus folgende Maßnahmen ein:

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- Auswahl des Auftragnehmers unter Sorgfalts-Gesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standard-Vertragsklauseln
- Schriftliche Weisungen an den Auftragnehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen der Bestellpflicht
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Regelung zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus