Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

Zwischen der

Firmenname, Straße, PLZ, Ort

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

ITM systems GmbH & Co. KG
Hauptstraße 43
48712 Gescher

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt -

Inhalt

1. Gegenstand und Dauer des Vertrags

(1) Gegenstand der Vereinbarung ist die Verarbeitung personenbezogener Daten (nachstehend „Daten“ genannt) durch den Auftragnehmer für den Auftraggeber in dessen Auftrag und nach dessen Weisung im Zusammenhang mit einem Dienstleistungsvertrag oder entsprechend jeweiliger Einzelaufträge (im Folgenden Leistungsvereinbarung). Die Vereinbarung gilt für Leistungen im Zusammenhang mit der Bereitstellung eines Hinweisgebermeldesystems.

(2) Die Dauer dieses Vertrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

(3) Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

(4) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, soll dieser Vertrag zur Auftragsverarbeitung vorrangig gelten, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

2. Konkretisierung des Vertragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Auftragnehmer führt für den Auftraggeber folgende Leistungen durch:

- Bereitstellung einer webbasierten Oberfläche für den Eingang und die Verwaltung von Hinweisen (Hinweisgebermeldesystem)
- Administration und Verwaltung der Nutzer
- Support

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien):

☒ Personenstammdaten (z.B. Namen, Adresse Firmenzugehörigkeit)

☒ Kommunikationsdaten (z.B. Telefon, E-Mail)

☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

☐ Kundenhistorie

☐ Vertragsabrechnungs- und Zahlungsdaten

☐ Planungs- und Steuerungsdaten

☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien oder aus öffentlichen Verzeichnissen)

☐ Verbindungsdaten zur Erkennung und Abwehr von Störungen der Infrastruktur und des Missbrauchs der Dienste

☒ Inhaltsdaten

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☐ Kunden

☐ Interessenten

☐ Abonnenten

☒ Beschäftigte

☐ Lieferanten

☐ Handelsvertreter

☒ Ansprechpartner

☒ Meldesystemnutzer

☐

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorische Maßnahmen gem. Art. 32 DS-GVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung [Anlage 1]. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags.

(2) Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(3) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber unverzüglich in Kenntnis zu setzten.

4. Rechte von betroffenen Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, 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.

(2) Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. 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 berechtigterweise 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.

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

c) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag 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.

d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationsersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

e) 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.

f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrags.

g) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Artt. 33, 34 DS-GVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.

h) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung.

i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

(2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DS-GVO.

6. 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 in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen.

Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. 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 zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a) ☐ Eine Unterbeauftragung ist unzulässig.

b) ☒ Der Auftraggeber stimmt der Beauftragung der in Anhang 2 bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO mit dem Unterauftragnehmer zu.

Die vertragliche Vereinbarung wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

c) ☒ Die Auslagerung auf Unterauftragnehmer oder
☒ der Wechsel der gemäß Anhang 2 bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

(4) 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.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☐ ist nicht gestattet;

☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

☒ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform).

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Internationale Datentransfers

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO.

☒ 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.

☐ Der Auftraggeber gestattet eine Datenübermittlung in ein Drittland an die in Anlage 2 genannten Empfänger. In der Anlage werden die vom Auftraggeber genehmigten Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus aus Art. 44 ff. DS-GVO im Rahmen der Unterbeauftragung spezifiziert.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

8. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb während der üblichen Geschäftszeiten zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO 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 Nachweis der technisch-organisatorischen Maßnahmen zur Einhaltung der besonderen Anforderungen des Datenschutzes allgemein sowie solche, die den Auftrag betreffen, kann erfolgen durch

☒ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;

☒ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;

☒ 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).

9. Weisungsbefugnis des Auftraggebers

(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 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 solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(3) Der Auftraggeber kann weisungsberechtigte Personen benennen. Diese sind dem Auftragnehmer zu Beginn des Auftrages mitzuteilen und können im Folgenden dokumentiert werden. Weisungsberechtigte Personen des Auftraggebers sind:

Vorname, Name	**E-Mail-Adresse**

Vorname, Name	**E-Mail-Adresse**

(4) Weisungsempfänger beim Auftragnehmer sind:

Ansprechpartner bei Auftragnehmer ist: Markus Lammerding sowie im Tagesbetrieb das Techniker-Team, das per E-Mail an ticket@itm-gruppe.com oder über die Zentrale unter der Tel.-Nr. 02542 917 918 0 erreichbar ist

10. Haftung und Schadensersatz

(1) Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DS-GVO entsprechende Verarbeitung verursacht wird gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.

(2) Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der

a) er den aus der DS-GVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist oder
b) er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte oder
c) er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat.

(3) Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.

(4) Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er

a) seinen ihm speziell durch die DS-GVO auferlegten Pflichten nicht nachgekommen ist oder
b) unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.

(5) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

11. Löschung und Rückgabe von personenbezogenen Daten

(1) 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.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens aber 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.

12. Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die 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 und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung den Regelungen des Haupt-Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

(5) Gerichtsstand ist der Sitz des Auftragnehmers.

13. Salvatorische Klausel

(1) Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen der Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, bleiben die übrigen Vertragsbestimmungen und die Wirksamkeit des Vertrages im Ganzen hiervon unberührt.

(2) An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

(3) Erweist sich der Vertrag als lückenhaft, gelten die Bestimmungen als vereinbart, die dem Sinn und Zweck des Vertrages entsprechen und im Falle des Bedachtwerdens vereinbart worden wären.

(4) Existieren mehrere wirksame und durchführbare Bestimmungen, welche die unter 18 Abs. 1 genannte unwirksame Regelung ersetzen können, so muss die Bestimmung gewählt werden, welche den Schutz der Daten im Sinne dieses Vertrages am besten gewährleistet.

14. Unterschriften

Ort, Datum	Unterschrift Auftraggeber
Gescher, 24.11.2023	
Ort, Datum	Unterschrift Auftragnehmer

15. Anlagen

Anlage 1: Unterauftragnehmer

Anlage 2: Technische und organisatorische Maßnahmen

Anlage 1 - Genehmigte Unterauftragsverhältnisse

Unterauftragnehmer	Anschrift/Land	Leistung	Angaben zu geeigneten Garantien bei Datenübermittlungen in ein Drittland
DPMS – Data Protection Management System	Haagscher Weg 17 47608 Geldern Deutschland	Software-Anbieter (Software as a Service)	*Nicht erforderlich*
ITM Networks GmbH	Roßmarkt 13 9400 Wolfsberg Österreich	IT-Dienstleistungen, Support	ITM Networks GmbH

Anlage 2 – Technische und organisatorische Maßnahmen

Beschreibung der technisch-organisatorischen Maßnahmen des Auftragnehmers unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener Personen.

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

Zutrittskontrolle

Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren.

Der generelle Zutritt zu den Geschäftsräumen der ITM design GmbH wird – während der Geschäftszeiten – dadurch gewährleistet, dass die hintere Eingangstür zum Bürogebäude stets verschlossen ist. Der Haupteingang wird durch einen stetig besetzten Empfang kontrolliert.

Der Besucher wird hier durch einen Mitarbeiter empfangen, der den gewünschten Ansprechpartner informiert und ggf. ins Besprechungszimmer begleitet.

Da die Mitarbeiterzahl überschaubar ist, ist eine gesonderte Kennzeichnung der Besucher nicht notwendig. Eine fremde Person fällt direkt als Besucher auf.

Es ist dokumentiert, welche Mitarbeiter Schlüssel zu den Bürogebäuden und einzelnen Büros erhalten haben. Ein Verlust muss direkt gemeldet werden.

Der Zutritt zum Serverschrank ist nur berechtigten Personen gestattet. Wartungsarbeiten werden durch internes Fachpersonal durchgeführt.

Um die Zutrittskontrolle auch außerhalb der Geschäftszeiten zu gewährleisten, werden alle Gebäudetüren mit einem Sicherheitsschloss verschlossen. Zusätzlich werden Durchgangstüren zu den verschiedenen Büroräumen verschlossen sowie die einzelnen Büros selbst.

Im Rahmen des für die tägliche Arbeit genutzten Rechenzentrums wird darauf geachtet, dass:

- der Zutritt zum Rechenzentrum nur autorisierten Personen gestattet ist
- der Zutritt durch ein materielles (RFID-Chip) und ein geistigen (PIN) Identifikationsmerkmal gesichert ist
- der Zutritt zu den einzelnen Kundenschränken oder -flächen ausschließlich durch den Kunden und durch das zuständige Personal möglich ist
- die Zutrittskontrollsysteme sowie die Raumüberwachung über USV und Netzersatzanlage gegen Stromausfall gesichert sind
- das Rechenzentrum, insbesondere der Zutritt zu Sicherheitsbereichen mit Raumüberwachung und Einbruchmeldeanlage ausgestattet ist
- es nach ISO/IEC 27001, EN 1047-2 und ECB-S zertifiziert ist

Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Der Zugang zu Anwendungen und Dokumenten ist grundlegend durch ein Berechtigungskonzept gewährleistet. Mit individuellen Benutzernamen und Kennwörtern erfolgt sowohl die Anmeldung am PC-Arbeitsplatz als auch der Login zu einzelnen Anwendungen. Es existiert eine Kennwortrichtlinie, nach der sich die Mitarbeiter richten müssen. Diese entspricht den Standards nach der DIN-Norm für Informationssicherheit – ISO 27001.

Zudem ist eine „Clean Desktop Policy“ etabliert, die regelt, dass alle Mitarbeiter bei Abwesenheit ihren Bildschirm durch einen Passwortschutz sperren und keine personenbezogenen oder vertraulichen Daten durch Unbefugte eingesehen werden können.

Das interne Netzwerk ist durch eine Firewall vor externen Zugriffen geschützt. Die regelmäßige Wartung übernimmt der interne IT-Verantwortliche.

Um den externen Zugriff auf das Netzwerk für Mitarbeiter zu gewährleisten, wird eine verschlüsselte VPN-Verbindung genutzt.

Die Arbeit mit Notebooks erfolgt unter der Anweisung, sämtliche personenbezogenen Daten nicht lokal, sondern auf dem Firmenserver zu speichern. Falls auf externen Datenträgern personenbezogene Daten transportiert werden, sind diese zu verschlüsseln.

Für den zuverlässigen Schutz vor Viren oder Trojanern ist ein Virenschutzkonzept umgesetzt, das sowohl für die Arbeitsplätze der Mitarbeiter als auch für die Notebooks der Mitarbeiter anwendbar ist.

Zugriffskontrolle

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

Im Zuge eines Berechtigungskonzeptes ist gewährleistet, dass die Mitarbeiter nur die Daten verarbeiten, die sie für ihre Arbeit benötigen. In diesem Konzept sind auch verschiedene Profile festgelegt, um den Benutzern entsprechende Rechte zum Lesen, Schreiben oder Löschen zuweisen zu können. Administrative Rechte besitzen lediglich die mit der Wartung vertrauten internen Mitarbeiter.

Im Falle der Verwendung von USB-Sticks werden nur solche genutzt, die durch den IT-Verantwortlichen ausgegeben wurden. Die Mitarbeiter wurden durch eine Richtlinie auf die datenschutzfreundliche Verwendung dieses Mediums hingewiesen. Falls der Einsatz von externen Festplatten nötig ist, werden diese ebenfalls kontrolliert durch den IT-Verantwortlichen ausgegeben. Für die Wiederverwendung wird für eine fachgerechte Löschung der nicht mehr benötigten Daten gesorgt. Ebenso ist eine fachgerechte Entsorgung der Hardware geregelt, wenn sie nicht mehr verwendet werden soll.

Papierdokumente werden ebenfalls fachgerecht entsorgt, wenn sie personenbezogene Daten enthalten. Dies erfolgt mit einem Aktenvernichter unter Einhaltung der Sicherheitsstufen nach DIN 66399.

Die für die Datenverarbeitung genutzten Anwendungen sind mit einer Historienfunktion ausgestattet, die eine Protokollierung von Eingabe, Änderung und Löschung von Daten gewährleistet.

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Datenerhebungen erfolgen stets zu einem bestimmten Zweck. Zu unterschiedlichen Zwecken erhobene Daten werden getrennt voneinander gespeichert.

Test- und Produktivdaten werden unterschieden. Produktivdaten werden in keiner Weise zu Testzwecken genutzt.

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

Weitergabekontrolle

Maßnahmen, die 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 personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Bei der Weitergabe von personenbezogenen Daten werden Verfahren genutzt, die eine verschlüsselte Übertragung gewährleisten. Dies umfasst die Nutzung von verschlüsselten VPN-Verbindungen sowie den Einsatz von Fernwartungstools, die eine Sitzungsverschlüsselung gewährleisten (derzeit werden Datenkanäle mit einem 2048 Bit RSA Public-/Private Key Exchange aufgebaut und mit 256 Bit AES verschlüsselt).

Wenn einzelne Dokumente mit personenbezogenen Daten per E-Mail übermittelt werden, sind die Mitarbeiter auf Grundlage einer Richtlinie dazu verpflichtet, diese mit Hilfe eines Passwortes zu verschlüsseln. Zusätzlich ist ein Outlook-Plugin installiert, das eine komplette Verschlüsselung des E-Mail-Inhalts inkl. Anhänge gewährleistet, sofern diese durch den Nutzer aktiviert wird. Standardmäßig werden E-Mails mittels einer TLS-Verschlüsselung verschlüsselt. Die Mitarbeiterrichtlinie enthält auch Regelungen, welche Übertragungswege genutzt werden dürfen und welche aus Datenschutzgründen nicht erlaubt sind.

Zur gesamtheitlichen Übersicht wird ein Verfahrensverzeichnis geführt, in dem jegliche Weitergabe von Daten dokumentiert ist.

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Durch eine systemseitige Protokollierung, welcher Benutzer wann eine bestimmte Änderung von Daten vorgenommen hat, wird die Eingabekontrolle sichergestellt.

Bei der Nutzung von Fernwartungstools wird darauf geachtet, dass die Mitarbeiter sich nicht ohne Absprache des Kunden auf die Systeme schalten. Es existiert eine Richtlinie zur Fernwartung, nach der die Supporttechniker die datenschutzkonforme Wartung durchführen.

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

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Im Falle eines Notfalls, der die gewohnte Arbeitsweise beeinträchtigt, greift ein Notfallkonzept, das die Wiederherstellung des IT-Betriebs sicherstellt.

Es ist außerdem ein umfangreiches Datensicherungskonzept eingeführt, das ein zuverlässiges Backup und die schnelle Wiederherstellbarkeit von Daten gewährleistet. Die Datensicherungen werden an einem sicheren, ausgelagerten Ort aufbewahrt. Durch regelmäßige Tests wird geprüft, ob die Datenrücksicherung einwandfrei funktioniert. Außerdem erfolgt eine automatische Überprüfung, ob die Sicherung erfolgreich durchgeführt worden ist. Bei Fehlern werden die Administratoren automatisch benachrichtigt.

In den Serverräumen sind eine USV sowie eine redundante Klimaanlage installiert, die an die Größe des Serverraumes angepasst sind. Für die zuverlässige Brandvorbeugung und -bekämpfung sind Rauchwarnmelder installiert und Feuerlöscher stehen bereit.

Um die Belastbarkeit der Systeme sicherzustellen, werden Betriebssysteme auf Client-Arbeitsplätzen sowie Servern regemäßig aktualisiert. Auch Hilfsprogramme wie der PDF-Reader oder zip-Programme werden regelmäßig aktualisiert. Ebenso werden Firmwareupdates von Firewall- und Routersystemen durchgeführt, wenn sie die Sicherheit des Netzwerkes erhöhen bzw. aufrechterhalten.

Dieses Vorgehen ist in der Richtlinie zur Betriebssicherheit festgehalten. Diese orientiert sich an Standards gemäß ISO 27001.

Im Rahmen des Rechenzentrumsbetriebes wird insbesondere darauf geachtet, dass:

- die Stromversorgung durch Redundanzen sichergestellt wird (Notstromaggregate sowie USV-Anlagen mit n+1 Redundanz; Überbrückungszeit mindestens 15 min. bis die Notstromaggregate die Stromversorgung wieder sicherstellen - Anlaufzeit inkl. Lastübernahme 1-2 min.)
- eine redundante Internetanbindung mit direktem Draht zu den wichtigsten Internetknoten eingerichtet ist
- das Rechenzentrum mit einer Raumklimatisierung ausgestattet ist (mittlere Temperatur 22° C +/- 4°, redundant ausgelegt (n+1), die installierten Luftfilter entsprechen DIN EN 779 G4)
- an den Kältebedarf anpassbare, redundante Klimaanlagen mit Warmgangeinhausung eingerichtet sind
- das Rechenzentrum über baulich getrennte Brandabschnitte verfügt und in den Räumlichkeiten eine Brandmeldeanlage installiert ist
- die Hochwasser- und Erdbebenkritikalität DIN-gerecht geprüft wurde
- die Messbarkeit der Prozesse durch permanente Systemüberwachung gegeben ist
- es insgesamt nach ISO/IEC 27001, EN 1047-2 und ECB-S zertifiziert ist

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Dienstleister, die die ITM design GmbH in ihrer Tätigkeit unterstützen, werden sorgfältig ausgewählt. Besonders der Bereich Datenschutz und Informationssicherheit ist ein wichtiges Kriterium bei der Auswahl. Im Zuge der Verwendung ausländischer Dienste ist sichergestellt, dass ein vergleichbar hoher

Datenschutzstandard eingehalten wird.

Es wird stets ein Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO geschlossen, wenn die Datenverarbeitung oder Dateneinsicht durch einen externen Dienstleister erfolgt.

Daten, die im Zuge einer Auftragsverarbeitung an die ITM design GmbH übermittelt werden, werden nach Auftragsende gelöscht, sofern dies nicht gegen gesetzliche Aufbewahrungspflichten verstößt. Außerdem ist vertraglich festgehalten, dass Daten, die die ITM design GmbH ihrerseits an Auftragsverarbeiter übermittelt, von diesen nach Auftragsende zuverlässig gelöscht werden. In diesem Zusammenhang sind auch Kontrollrechte auf Seiten der ITM design GmbH festgelegt. Von diesen wird in regelmäßigen Abständen Gebrauch gemacht, indem aktuelle Auditberichte eingeholt werden.

Sämtliche Dienstleister werden zur Verschwiegenheit verpflichtet, sollten sie mit personenbezogenen Daten in Kontakt kommen.

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

Datenschutz-Management

Für den Aufbau eines Datenschutzmanagementsystems wurde ein interner Mitarbeiter als Datenschutzbeauftragter bestellt. Dieser ist beratend tätig wirkt auf die Einhaltung der Datenschutzgesetze hin.

Mit Einführung eines Datenschutzmanagementsystems wurde auch eine Leitlinie zum Datenschutz veröffentlicht, die für das gesamte Unternehmen anwendbar ist. Gleichzeitig wurden mehrere Richtlinien und Vereinbarungen eingeführt, nach denen die Datenverarbeitung durch die Mitarbeiter erfolgt. Darunter fällt auch die Vertraulichkeitserklärung, die jeder Mitarbeiter im Zuge seiner Einstellung unterschreibt.

In diesem Zusammenhang werden neue Mitarbeiter über die Einhaltung der Datenschutzvorschriften unterrichtet und sensibilisiert. Außerdem finden 1 Mal pro Jahr Mitarbeiterschulungen statt, um die Sensibilisierung aufrechtzuerhalten bzw. weiter zu erhöhen.

Um jederzeit den Überblick zu haben, an welcher Stelle welche Daten verarbeitet werden, wird ein Verfahrensverzeichnis geführt und gepflegt, das alle Verarbeitungstätigkeiten dokumentiert. Hier sind ebenfalls Verarbeitungen aufgeführt, die im Auftrag erfolgen. Entsprechende Sicherheitsmaßnahmen sind dokumentiert und werden regelmäßig auf ihre Angemessenheit überprüft. Die Prüfung inkl. Berichterstellung erfolgt jedes Jahr durch den Datenschutzbeauftragten.

Umgesetzt wird das Datenschutzmanagement mit Hilfe einer Software. Berichte können jederzeit erstellt und exportiert werden.