Vereinbarung zur Auftragsdatenvereinbarung

zwischen der

Smart Enterprise Solutions GmbH
Stuttgarter Str. 13a
75179 Pforzheim
(nachstehend: Auftragnehmer)

und dem im Hauptvertrag, der Auftragsbestätigung oder in einem Angebot näher bestimmten

Kunden bzw. Nutzern unserer Produkte *smenso Cloud* und *Smart Project Manager*
(nachstehend: Auftraggeber).

Präambel
Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz im Zusammenhang mit dem Umgang des Auftragnehmers mit personenbezogenen Daten des Auftraggebers oder dessen Ansprechpartner (Kunden, Lieferanten, etc.). Sie findet Anwendung auf alle Tätigkeiten, bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können. Darüber hinaus werden dem Auftragnehmer im Rahmen des Hauptvertrages, oder sonstiger Geschäftsbeziehungen zwischen den Parteien, vertrauliche Informationen aus dem Unternehmen des Auftraggebers zur Verfügung gestellt bzw. es ist nicht ausgeschlossen, dass der Auftragnehmer in den Geschäftsräumen des Auftraggebers in Kontakt mit solchen Informationen kommt.

1. Gegenstand der Vereinbarung

1. Art, Umfang und Zweck der Datenerhebung, -verarbeitung oder -nutzung werden in **Anlage 1** konkretisiert. Der Auftragnehmer darf nur die in **Anlage 1** genannten Kategorien an Daten, der dort genannten Betroffenen zu den dort oder in einem eventuell vorhandenen Hauptvertrag genannten Zwecken verarbeiten. Das Vorhandensein eines eventuellen Hauptvertrages wird in der **Anlage 1** vermerkt.
2. Jede davon abweichende oder darüber hinaus gehende Erhebung oder Verwendung von Daten ist dem Auftragnehmer untersagt, insbesondere eine Verwendung der Daten zu eigenen Zwecken.
3. Die Dauer dieser Vereinbarung gilt für die Dauer eines bestehenden Vertragsverhältnisses, insbesondere einem bestehenden Wartungsvertrag, oder einem eventuell vorhandenen Hauptvertrag.

2. Rechte und Pflichten des Auftraggebers

1. Für die Einhaltung der gesetzlichen Datenschutzbestimmungen bei erteilten Weisungen sowie für die Wahrung der Rechte und Freiheiten der Betroffenen und Dritten ist der Auftraggeber verantwortlich. Die Verantwortlichkeiten des Auftragnehmers gem. Art. 28 Abs. 10, 82, 83 und 84 der Verordnung (EU)

2016/679 (Datenschutzgrundverordnung, nachfolgend DSGVO) bleiben unberührt. Der Auftraggeber ist im Verhältnis der Parteien zueinander Eigentümer der Daten und Inhaber aller Rechte an den Daten.

2. Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen (anfänglich festgelegt durch **Anlage 1**) sind gemeinsam abzustimmen und schriftlich festzulegen. Mündliche Weisungen können in dringenden Fällen erteilt werden, sind jedoch im Nachgang unverzüglich schriftlich zu bestätigen. Zur Initiierung oder Bestätigung von Änderungen/Ergänzungen autorisierte Personen der Vertragsparteien sind in **Anlage 3** aufgeführt.
3. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei den Verarbeitungsergebnissen feststellt, insbesondere wenn er Grund zu der Annahme hat, dass die Art und Weise der Verarbeitung der Daten durch den Auftragnehmer gegen datenschutzrechtliche Anforderungen verstößt.
4. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrags bestehen.
5. Der Auftraggeber ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Der Auftraggeber dokumentiert das Ergebnis dieser Kontrollen. Hierfür kann der Auftraggeber z.B. Auskünfte des Auftragnehmers einholen oder - grundsätzlich nach Terminvereinbarung - zu den üblichen Geschäftszeiten vor Ort in den Geschäftsräumen des Auftragnehmers prüfen oder durch einen Dritten prüfen lassen.
6. Der Auftragnehmer gewährt dem Auftraggeber oder einem von ihm beauftragten Dritten die zur Durchführung der Kontrollen erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte und wirkt bei der Kontrolle in angemessenem Umfang aktiv mit, wobei der Auftraggeber bei Ausübung des Prüfungsrechts auf die betrieblichen Belange des Auftragnehmers Rücksicht nehmen wird.

3. Rechte und Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers und nur im Gebiet der Europäischen Union und des Europäischen Wirtschaftsraumes. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke als für die Erfüllung des Hauptvertrags, insbesondere nicht für eigene Zwecke.
2. Der Auftragnehmer darf Daten ohne vorherige Zustimmung in Schriftform durch den Auftraggeber nicht an Dritte oder andere Empfänger aushändigen. Hiervon ausgenommen sind Datenweitergaben an Unterauftragnehmer nach Maßgabe von Ziff. 4.
3. Der Auftragnehmer erklärt, dass er aufgrund gesetzlicher Anforderungen der Europäischen Union oder eines Mitgliedsstaats der Europäischen Union nicht verpflichtet ist, Daten auch ohne Weisung des Auftraggebers zu verarbeiten. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er dennoch eine entsprechende Aufforderung zur Datenverarbeitung erhält. Dies gilt nicht, wenn der Auftragnehmer aufgrund gesetzlicher Vorschriften zur Geheimhaltung verpflichtet ist.
4. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Auffassung nach gegen datenschutzrechtliche Anforderungen

verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

5. Der Auftragnehmer stellt sicher und kontrolliert regelmäßig, dass die Datenverarbeitung in seinem Verantwortungsbereich, der etwaige Unterauftragnehmer einschließt, im Einklang mit den Bestimmungen dieser Vereinbarung, den besonderen gesetzlichen Anforderungen des Datenschutzgesetzes und den Weisungen des Auftraggebers erfolgt und die technischen und organisatorischen Maßnahmen für die Dauer dieses Vertrags eingehalten werden. Dabei ist der aktuelle Stand der Technik unter Berücksichtigung des Risikos zu beachten. Diese Maßnahmen werden in **Anlage 4** festgelegt. Eine Änderung der getroffenen Maßnahmen bleibt dem Auftragnehmer nachgelassen, sofern sichergestellt ist, dass das vereinbarte Schutzniveau nicht unterschritten wird. Bei wesentlichen Änderungen wird der Auftraggeber über die Änderungsabsichten des Auftragnehmers rechtzeitig vor deren Umsetzung in Textform informiert. Auf Verlangen weist der Auftragnehmer dem Auftraggeber die Einhaltung dieser Maßnahmen durch Vorlage von Dokumentationsmaterial nach.
6. Der Auftragnehmer versichert, dass ihm alle einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind und gewährleistet deren Umsetzung. Der Auftragnehmer hat, sofern nicht bereits geschehen, alle mit der Verarbeitung der Daten beschäftigten Personen schriftlich zur Verschwiegenheit gem. DSGVO zu verpflichten, soweit diese Personen nicht bereits einer vergleichbaren, auch gesetzlichen, Verschwiegenheitspflicht unterliegen. Der Auftragnehmer hat diese Personen dabei in die wesentlichen gesetzlichen Bestimmungen über den Datenschutz einzuweisen und sie zu verpflichten, diese Bestimmungen zu beachten. Auf Verlangen des Auftraggebers wird der Auftragnehmer dies durch Vorlage der Verpflichtungserklärungen nachweisen.
7. Der Auftragnehmer berichtigt, löscht oder sperrt die Daten unverzüglich, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Löschung von Daten bzw. Vernichtung von Datenträgern übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber, sofern dies nicht bereits einem eventuellen Hauptvertrag vereinbart ist. Im Falle von Test- und Ausschussmaterialien ist eine Einzelbeauftragung zur Löschung nicht erforderlich. Gesetzliche Aufbewahrungsverpflichtungen bleiben unberührt.
8. Nach Beendigung des Auftragsverhältnisses hat der Auftragnehmer sämtliche in seinen Besitz sowie an Unterauftragnehmer gelangte personenbezogene Daten, die in Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an ihn zu übergeben oder zu löschen, es sei denn, der Auftragnehmer ist zu einer Speicherung aufgrund anderer Vorschriften verpflichtet. Der Auftragnehmer hat an den Daten kein Zurückbehaltungsrecht, es sei denn, sein Gegenanspruch ist rechtskräftig festgestellt oder unbestritten.
9. Der Auftragnehmer gewährleistet, einen Datenschutzbeauftragten zu bestellen und zumindest während der Dauer dieser Vereinbarung zu beschäftigen. Der Name des Datenschutzbeauftragten sowie die Kontaktdaten können der Datenschutzerklärung auf der Homepage des Auftragnehmers (www.smenso.de/datenschutz) entnommen werden. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
10. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten des Auftraggebers aus Art. 32 DSGVO (TOM), aus Art. 33 und 34 DSGVO (Meldeverpflichtungen bei Datenpannen) und

ggf. aus Art. 35 DSGVO (Datenschutz-Folgenabschätzung) sowie Art. 36 DSGVO (Konsultation der Aufsichtsbehörde).

4. Unterauftragnehmer

1. Unterauftragnehmer sind Vertragspartner des Auftragnehmers, die ihrerseits personenbezogene Daten des Auftraggebers verarbeiten, sowie deren Auftragnehmer.
2. Der Auftragnehmer darf geeignete Unterauftragnehmer im Gebiet der Europäischen Union oder des Europäischen Wirtschaftsraums mit der Verarbeitung von Daten im Auftrag und nach Weisung betrauen, wenn der Auftraggeber dem im Einzelfall schriftlich (z.B. per E-Mail) vor Beauftragung des Unterauftragnehmers zugestimmt hat. Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder den Austausch von Unterauftragnehmern informieren. Der Auftraggeber kann der Hinzuziehung oder dem Austausch von Unterauftragnehmern nach Information durch den Auftragnehmer widersprechen. Ein Widerspruch darf nur aus wichtigem Grund erfolgen.
3. Eine Beauftragung von Unterauftragnehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
4. Der Auftragnehmer stellt vertraglich sicher, dass dem Unterauftragnehmer die gleichen Datenschutzpflichten aus dieser Vereinbarung auferlegt werden. Insbesondere ist sicherzustellen, dass die geeigneten technischen und organisatorischen Maßnahmen vom Unterauftragnehmer so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des Datenschutzrechts erfolgt. Der Auftraggeber muss berechtigt sein, Kontrollen vor Ort beim Unterauftragnehmer durchzuführen oder durch Dritte durchführen zu lassen.
5. Die in **Anlage 2** mit Namen, Anschrift und Auftragsinhalt genannten Unterauftragnehmer werden zum Zeitpunkt des Abschlusses dieser Vereinbarung durch den Auftragnehmer eingesetzt. Die Unterauftragnehmer unterscheiden sich wesentlich je nach eingesetztem Produkt bzw. genutzter Leistungen, weshalb in **Anlage 2** zwei getrennte Auflistungen von Unterauftragnehmern aufgenommen wird. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

5. Besondere Pflichten des Auftragnehmers bei Störungen der Verarbeitung oder Verletzungen des Schutzes personenbezogener Daten

1. Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen oder Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder diese Vereinbarung mit, wenn Anhaltspunkte bestehen, dass personenbezogene Daten unrechtmäßig verarbeitet worden sind. Der Auftragnehmer trifft außerdem die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen.
2. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenzverfahren 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 liegen.

6. Anfragen Betroffener

1. Für den Fall, dass ein Betroffener gegenüber dem Auftraggeber berechtigte datenschutzrechtliche Ansprüche geltend macht, wird der Auftragnehmer den Auftraggeber unter Berücksichtigung der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, der Erfüllung dieser Ansprüche nachzukommen.
2. Sollten Betroffene oder sonstige Dritte datenschutzrechtliche Anfragen unmittelbar an den Auftragnehmer richten oder Datenschutzrechte gegenüber dem Auftragnehmer geltend machen, wird der Auftragnehmer diese Anfragen unverzüglich an den Auftraggeber weiterleiten.

7. Haftung

1. Auftraggeber und Auftragnehmer haften im Rahmen ihrer Verantwortlichkeiten gemäß den gesetzlichen Bestimmungen des Art. 82 DSGVO gegenüber Dritten für Schäden, die durch eine nicht der DSGVO entsprechenden Datenverarbeitung entstanden sind.

8. Schlussbestimmungen

1. Änderungen oder Ergänzungen dieser Vereinbarung oder ihrer Anlagen bedürfen der Schriftform.
2. Wenn und soweit der Hauptvertrag Regelungen enthält, die denjenigen dieser Vereinbarung entgegenstehen, so haben die Regelungen dieser Vereinbarung Vorrang, soweit in dieser Vereinbarung nicht etwas anderes geregelt ist.
3. Es gilt deutsches Recht.
4. Sollten einzelne dieser Bestimmungen unwirksam sein, berührt dies die Gültigkeit der übrigen Bestimmungen nicht.

9. Unterschriften

Auftraggeber		**Auftragnehmer**	
Name		Name	
Funktion		Funktion	
Ort, Datum		Ort, Datum	
Unterschrift		Unterschrift	

Übersicht Anlagen

Anlage	Inhalt
Anlage 1	Gegenstand, Art, Umfang und Zweck der Datenverarbeitung / Kreis der Betroffenen
Anlage 2	Unterauftragnehmer
Anlage 3	Autorisierte Personen
Anlage 4	Technische und organisatorische Maßnahmen

10. Anlagen

Anlage 1: Gegenstand, Art, Umfang und Zweck der Datenverarbeitung / Kreis der Betroffenen

Gegenstand der Datenerhebung, -verarbeitung oder -nutzung

- Hauptvertrag zwischen Auftraggeber und Auftragnehmer
- Hilfsweise Angebot (mit Leistungsbeschreibung) oder Auftragsbestätigung

Art, Umfang und Zweck der Datenerhebung, -verarbeitung oder -nutzung

- Erstellung und Verwaltung von Benutzerprofilen
- Kommunikation mit Nutzern zu unseren Services, Updates oder Angeboten
- Zugriff auf Daten im Rahmen des Supports/Remotezugriffs
- Aufnahme von Fehlermeldungen im Helpcenter des Auftragnehmers
- Aufnahme von Fehlermeldungen per E-Mail an den Auftragnehmer
- Auftrags- und Subskriptionsverwaltung

Art der Daten

- Personenbezogene Stammdaten:
  - Vor- und Nachnamen
  - Positionen / Organisationseinheiten
  - Kundennummern
- Kontaktdaten
  - Telefonnummer(n)
  - E-Mail-Adresse(n)
  - Postadressen
- Account-Informationen
  - Benutzernamen
  - Berechtigungen
  - Tarifinformationen
- Nutzungsdaten
  - Gerätekennungen
  - Systemzustände
  - IP-Adressen
  - Gerätekennungen
  - Genutzte Browser (Hersteller, Version)
  - Browser Historie, Seitenaufruf-Statistiken
  - Informationen zu Erstanmeldung, letzter Login, Logindauer
  - Zugriffsinformationen
  - Log-Dateien

  - Cookies
- Planungs- und Steuerungsdaten im Projektumfeld (z.B. Daten von Projekten/Aufgaben, Kunden-/Lieferantennamen)
- Kommunikationsinhalte
  - E-Mail-Inhalte
- Transaktionsdaten
  - Rechnungsinformationen
  - Unternehmens-/Abteilungszugehörigkeiten
  - Kreditkartendaten
  - Transaktions- und Rechnungsdaten
  - Kontonummer(n)/IBAN

Kreis der Betroffenen

- Beschäftigte des Auftraggebers
- Ansprechpartner des Auftraggebers (Kunden/Lieferanten/Partner/potenzielle Kunden)
- Nutzer und Kunden von Kunden des Auftragsverarbeiters

Anlage 2: Unterauftragnehmer

Unterauftragnehmer in Bezug auf die Webanwendung "**smenso Cloud**"

Name, Adresse	Auftragsinhalt
Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA	Teile der Software werden in den Rechenzentren von Microsoft im Gebiet der Europäischen Union gehostet. Im Rahmen dessen werden diverse Dienste und Daten verarbeitet. Die Datenspeicherung erfolgt ebenfalls in Rechenzentren von Microsoft im Gebiet der Europäischen Union. https://azure.microsoft.com/de-de/ https://privacy.microsoft.com/de-de/privacystatement https://www.microsoft.com/de-de/trust-center/privacy/gdpr-overview
Auth0, Inc. 10800 NE 8th Street Suite 700 Bellevue, WA 98004 USA	Auth0 ist ein Anbieter von Services für das Identity-Management. Wir nutzen Auth0 zur Authentifizierung und Anmeldung von Benutzern und zur Pflege von Benutzerprofilen. Die Daten werden dabei im Gebiet der Europäischen Union gehostet. https://auth0.com/privacy/
mongoDB, Inc. 3rd Floor 3 Shelbourne Building Crampton Avenue Ballsbridge Dublin Ireland	Wir nutzen Hosting-Services von mongoDB für Datenbanken. Physisch werden die Datenbanken jedoch in Rechenzentren von Microsoft Azure im Gebiet der Europäischen Union gehostet. https://www.mongodb.com/legal/privacy-policy
Zendesk International Ltd 55 Charlemont Place Saint Kevin's Dublin D02, F985 Ireland	Die Dienste von Zendesk nutzen wir zum Betreiben unseres Helpcenters und zur Aufnahme von Supportanfragen unserer Benutzer. https://www.zendesk.de/company/customers-partners/privacy-policy/ Vertragsgrundlage: Data Processing Agreement vom 11.03.2020
Atlassian Corporation Plc C/O Herbert Smith Freehills Llp Exchange House, Primrose Street, London, EC2A 2EG United Kingdom	Wir nutzen das Ticketmanagement-System Jira Software in Kombination für die Bearbeitung von Feature Requests unserer Benutzer. https://de.atlassian.com/legal/privacy-policy
The Rocket Science Group, LLC	MailChimp ist ein Mailingservice der The Rocket Science Group.

Name, Adresse	Auftragsinhalt
675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 USA	Wir setzen MailChimp für Marketing-Kampagnen, Werbung und Informationen zu Updates ein und nutzen den Service für Webanalysen und in unseren Marketingkampagnen. https://mailchimp.com/legal/privacy/ https://mailchimp.com/legal/data-processing-addendum/

Unterauftragnehmer in Bezug auf die On-Premise-Anwendung "**Smart Project Manager**"

Name, Adresse	Auftragsinhalt
Atlassian Corporation Plc C/O Herbert Smith Freehills Llp Exchange House, Primrose Street, London, EC2A 2EG United Kingdom	Wir nutzen das Ticketmanagement-System Jira Software in Kombination mit Jira Service Desk für die Bearbeitung von Supportanfragen unserer Benutzer. https://de.atlassian.com/legal/privacy-policy
The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 USA	MailChimp ist ein Mailingservice der The Rocket Science Group. Wir setzen MailChimp für Marketing-Kampagnen, Werbung und Informationen zu Updates ein und nutzen den Service für Webanalysen und in unseren Marketingkampagnen. https://mailchimp.com/legal/privacy/ https://mailchimp.com/legal/data-processing-addendum/
itelligence AG Königsbreede 1, 33605 Bielefeld Deutschland	Wir nutzen die itelligence AG zur Unterstützung bei SAP-Beratungs- und Entwicklungsleistungen. https://itelligencegroup.com/de/privacy/
itmX GmbH Stuttgarter Str. 8 75179 Pforzheim Deutschland	Wir nutzen die itmX GmbH zur Unterstützung bei SAP-Beratungs- und Entwicklungsleistungen. https://itmx.de/datenschutzerklaerung/
enosiX, Inc. 250 E Fifth Street Suite 1500 Cincinnati, OH 45202 USA	enosiX ist Hersteller des enosiX Frameworks, welches Daten aus SAP ERP / S4 in Frontend-Systeme integriert. Wir nutzen das enosiX Framework für die Integration von SAP in unsere Software. https://enosix.com/company/

Anlage 3: Verantwortliche in Fragen des Datenschutzes

Autorisierte Personen des Auftraggebers

Name, Vorname	Funktion	Kontaktdaten

Autorisierte Personen des Auftragnehmers

Name, Vorname	Funktion	Kontaktdaten
De Tullio, Marco	Geschäftsführer **Smart Enterprise Solutions GmbH** Stuttgarter Str. 13a 75179 Pforzheim	+49 7231 77857 53 marco.detullio@smenso.de
Riermeier, Philipp	Geschäftsführer **Smart Enterprise Solutions GmbH** Stuttgarter Str. 13a 75179 Pforzheim	+49 7231 77857 51 philipp.riermeier@smenso.de
Ernst, Volker	Datenschutzbeauftragter **Just-IT GmbH** Schwebelstraße 10 75172 Pforzheim	+49 7231 133 6008 datenschutzbeauftragter@justitgmbh.de

Anlage 4: Technische und organisatorische Maßnahmen

Zutrittskontrolle

Maßnahmen, die verhindern, dass Unbefugte räumlich Zutritt zu den Verarbeitungsanlagen/-räumen personenbezogener Daten oder sonstigen personenbezogenen Unterlagen, z. B. Akten oder Datenträgern erhalten.

- Zutrittskontrolle wird über Schlüsselregelung (Schlüsselausgabe etc.) gewährt
- Einsatz von Sicherheitsschlössern
- Sorgfältige Auswahl von Reinigungspersonal
- Zugang zu internen Servern mit zusätzlicher Sicherung - nur dedizierte Mitarbeiter dürfen Bereich betreten
- Aufbewahrung von sensiblen Datenträgern und Papierakten in abschließbaren Schränken

Zugangskontrolle

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

- Authentifizieren mit personalisiertem Benutzername / Passwort und dedizierten Benutzerrechten
- Passwortvergabe mit technisch unterstützter Passwortrichtlinie
- Begrenzung Anmeldeversuche an der Domäne
- Einsatz von VPN-Technologie inklusive Zwei-Faktor-Authentifizierung
- Einsatz von Intrusion-Detection-System
- Einsatz von Anti-Viren-Software
- Einsatz einer Software-Firewall
- Einsatz einer Hardware-Firewall
- Gewährleistung von Sicherheitspatches
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Umgehende Deaktivierung von nicht mehr genutzten Benutzerkonten
- Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)

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.

- Nutzung eines Berechtigungskonzepts (Active Directory von Microsoft inkl. Gruppenzuordnungen)
- Anzahl der Administratoren auf das "Notwendigste" reduziert
- Einsatz von VPN-Technologie
- Physische Löschung von Datenträgern vor Wiederverwendung
- Verwaltung der Rechte durch Anforderung beim internen IT-Support
- Sichere Aufbewahrung von Datenträgern
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)

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.

- Einsatz von VPN-Tunneln inkl. Zwei-Faktor-Authentifizierung
- Beim physischen Transport: Auswahl sicherer Transportbehälter/-verpackungen,
- Beim physischen Transport: Auswahl sicheren Transportpersonals, sicherer Transportfahrzeuge (z.B. Kurierdienste)
- Verschlüsselung von zum Transport verwendeten Datenträgern
- Überwachung und Protokollierung des Datenverkehrs mittels Software- und Hardware-Firewall
- Einsatz von Anti-Viren-Software

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.

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Protokollierung von VPN-Verbindungen (Firewall)

Auftragskontrolle

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

- Auswahl von Unterauftragnehmern unter besonderer Berücksichtigung von Art. 28 DSGVO und somit der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen
- Erhebung, Verarbeitung, Berichtigung und Löschung der Daten erfolgt streng gebunden an Auftrag und Einzelweisungen des Auftraggebers gemäß den hier getroffenen, vertraglichen Vereinbarungen
- Schriftliche Verpflichtung von Beschäftigten sowie eingesetzten Unterauftragnehmern auf das Datengeheimnis bzw. zur Vertraulichkeit, bei denen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann
- Schriftliche Weisungen an den Auftragnehmer
- Wirksame Kontrollrechte gegenüber dem Unterauftragnehmer werden vereinbart
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Abschluss von Verträgen mit Unterauftragnehmern in Drittstaaten nur unter Anwendung der EU-Standardvertragsklauseln

Verfügbarkeitskontrolle

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

- Unterbrechungsfreie Stromversorgung (USV)

- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Einsatz von Virtualisierungslösungen für Server sowie Backup- & Recovery Maßnahmen
- Feuer- und Rauchmeldeanlagen
- Regelmäßige Überwachung wesentlicher Systeme
- Einsatz von Intrusion-Detection-Systemen und einer zentralen Firewall
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Klimaanlage in Serverräumen
- Feuerlöschgeräte in Serverräumen
- Serverräume nicht unter sanitären Anlagen

Trennungsgebot

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

- Logische Mandantentrennung (softwareseitig), getrennt löschbar
- Trennung von Produktiv- und Testsystemen
- Versehen der Datensätze mit Zweckattributen/Datenfeldern