Vertrag zur Auftragsdatenverarbeitung

Gemäß Art. 28 DSGVO

Die

…… *[NAME VERTRAGSPARTNER]*

…… *[STRASSE]*

…… *[PLZ, ORT]*

- nachstehend **„Auftraggeber“** genannt -

und

DEHN SE
Hans-Dehn-Str. 1
92318 Neumarkt

- nachstehend **„Auftragnehmer“** genannt -

schließen folgenden Vertrag zur Auftragsdatenverarbeitung

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Der Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Bereitstellung einer SaaS-Plattform im Bereich Blitz- und Überspannungsschutz

(2) Dauer

Die Dauer dieses Auftrags entspricht der Laufzeit der Leistungsvereinbarung

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers:

Online-Tools zur digitalen Projektverwaltung mit Applikationen zur Konzeption, Planung, Installation und Wartung von Projekten im Bereich von Blitz- und Überspannungsschutz.

(2) Ort der Verarbeitung von Daten

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union statt.

(3) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien):

- Personenstammdaten (z.B. Firma, Name, Vorname, Anschrift, Telefonnr., E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt-/Vertragsinteresse)
- Kundenhistorie

(4) Kategorien betroffener Personen

- Kunden
- Beschäftigte
- Projektbeteiligte und Ansprechpartner

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) 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 (Einzelheiten in Anlage 1).

(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.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) 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.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(1) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

(2) 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.

(3) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (Einzelheiten hierzu siehe Anlage 1).

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

(5) 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.

(6) 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.

(7) 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.

(8) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

(9) Wendet sich eine betroffene Person mit Anträgen gemäß Art. 15 bis 21 DS-GVO an den Auftragnehmer, wird der Auftragnehmer die betroffene Person unverzüglich an den Auftraggeber verweisen und leitet den Antrag an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung dieser Anträge der betroffenen Personen im erforderlichen Umfang

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 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) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) einsetzen.

Zum Zeitpunkt des Vertragsschlusses stimmt der Auftraggeber der Beauftragung der nachfolgenden Unterauftragnehmer zu, unter der Bedingung, dass mit diesen jeweils vertragliche Vereinbarungen nach Maßgabe des Art. 28 Abs. 2–4 DSGVO bestehen:

Unterauftragnehmer	Anschrift/Land	Leistung
Dehn Digital Solutions GmbH	Hans-Dehn-Str. 1 92318 Neumarkt	Entwicklung und Betrieb von Softwareprodukten für die DEHN SE.

Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit 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

- mit dem Unterauftragnehmer eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2–4 DSGVO abgeschlossen 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.

(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 bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. 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 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 solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen 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).

(4) Durch Unterstützungsleistungen, welche über die Vertragliche Vereinbarung hinaus gehen, kann der Auftragnehmer einen angemessenen Vergütungsanspruch geltend machen.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. 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, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

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

10. 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 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.

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

11. Haftung

Auf Art. 82 DSGVO wird verwiesen.

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 Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

Anlage 1 – Technische und organisatorische Maßnahmen (TOM)

Unter Berücksichtigung des

- Stands der Technik,
- der Implementierungskosten und
- der Art, des Umfangs, der Umstände und
- der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

trifft der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Der Auftragsverarbeiter ergreift folgende Maßnahmen:

Maßnahmen zur Sicherstellung der Vertraulichkeit

Zutrittskontrolle

Die Maßnahmen der Zutrittskontrolle stellen sicher, dass ein Unbefugter sich keinen Zutritt in Gebäude oder einzelne Räume verschaffen kann, in denen personenbezogene Daten verarbeiten werden. Im Einzelnen bestehen insbesondere folgende Maßnahmen:

- Festlegung befugter Personen inklusive Umfang der jeweiligen Befugnisse
- Existenz von Regelungen für Unternehmensexterne
- Umsetzung einer Schlüsselregelung
- Empfang / Rezeption / Pförtner
- Besucherbuch / Protokollierung der ein- und ausgehenden Personen
- Mitarbeiter- / Besucherausweise
- Besucher in Begleitung durch Mitarbeitende
- Unterteilung in verschiedene Sicherheitszonen
- Physische Maßnahmen vorhanden und regelmäßig überprüft
- Gesicherter Eingang – abschließbare Türen, Ausweisleser

- Gerätesicherung gegen Diebstahl, Manipulation oder Beschädigung
- Überwachungseinrichtung – Alarmanlage, Videoüberwachung
- Sorgfalt bei Auswahl des Wach- und Reinigungspersonals
- Richtlinie zur Datenklassifizierung mit Handlungsanweisung

Zugangskontrolle

Mit den Maßnahmen der Zugangskontrolle wird sichergestellt, dass keine unbefugte Benutzung der Systeme erfolgen kann, mit denen die personenbezogenen Daten verarbeitet werden. Im Einzelnen bestehen insbesondere folgende Maßnahmen:

- Konzeption und Implementierung eines Berechtigungskonzeptes
    - Berechtigungskonzept nach Rollenprofil
    - Berechtigungskonzept für Endgeräte (Client)
    - Berechtigungskonzept für Software (Apps) und Systeme (Server)
- Identifikation und Berechtigungsprüfung eines Benutzers
- Monitoring der Zugangsversuche mit Reaktion auf Sicherheitsvorfälle
- Festlegung und Kontrolle der Zugangsbefugnisse
- Authentisierungsverfahren dem Schutzbedarf der Informationen entsprechend
    - Multifaktor-Authentication
- Angemessener Passwortschutz – Verhaltensregeln, verschlüsselte Archive
- Sicherheitssoftware – Anti-Malware, Application Control, DNS-Gateway, VPN, Firewall
- Mobile Device Management
- Verschlüsselung von mobilen Endgeräten und Datenträgern
- Regelungen für Unternehmensexterne
- Umsetzung von Regelungen zum Umgang mit elektronischen Speichermedien
- Umsetzung von Regelungen zur Entsorgung von Speichermedien
- Allgem. Richtlinie zu IT-Sicherheit und Datenschutz
- Anleitung „Manuelle Desktopsperre“

- Secure Print (FollowMe-Printing, Pull-Printing)

Zugriffskontrolle

Die Maßnahmen zur Zugriffskontrolle stellen sicher, dass innerhalb des Systems nur befugte Personen die jeweiligen personenbezogenen Daten verarbeiten können. Insbesondere erhalten die Mitarbeiter nur Zugriff auf die personenbezogenen Daten, die sie für die Erledigung ihrer Aufgaben im Unternehmen des Auftragsverarbeiters benötigen. Im Einzelnen bestehen insbesondere folgende Maßnahmen:

- Berechtigungs- und Rollenkonzept für Applikationen
- Umsetzung von Regelungen zur Zugriffs- und Benutzerberechtigung
- Überprüfung der Berechtigungen
- Funktionsbegrenzung (funktional/zeitlich)
- Zugriffsbeschränkungen (gemäß „Need-to-Know“ und „Least Privilege“)
- Protokollierungen
- Umsetzung von Regelungen zur Vernichtung und Löschung von Daten

Trennungskontrolle

Die Maßnahmen zur Trennungskontrolle stellen sicher, dass personenbezogene Daten getrennt voneinander gespeichert und verarbeitet werden. Dadurch wird das Risiko eines unbefugten Zugriffs auf die Daten reduziert, da jeder Datenbestand separat geschützt ist. Die Trennungskontrolle trägt somit dazu bei, die Vertraulichkeit von personenbezogenen Daten zu gewährleisten und das Datenschutzniveau insgesamt zu erhöhen.

- Dokumentation der Funktionstrennung
- Vorhandensein von Richtlinien und Arbeitsanweisungen
- Vorhandensein von Verfahrensdokumentationen
- Mandantenfähigkeit
- Physische Trennung
- Trennung auf Systemebene
- Trennung auf Datenebene
- Regelmäßige Prüfung der bestimmungsgemäßen Nutzung der Informationen und IT-Systeme

Maßnahmen zur Sicherstellung von Integrität

Zum Schutz vor unrechtmäßiger oder ungewollter Veränderung bzw. Löschung von personenbezogenen Daten werden technische und organisatorische Maßnahmen eingesetzt, die die Integrität sichern. Im Einzelnen bestehen insbesondere folgende Maßnahmen:

Weitergabekontrolle

Die Weitergabe-Kontrolle bezieht sich auf die Regelungen zur Weitergabe von personenbezogenen Daten an Dritte. Um diese Kontrolle umzusetzen, können beispielsweise folgende Maßnahmen ergriffen werden:

- Bereitstellung über verschlüsselte Verbindungen und Datenspeicher, z. B. VPN, SharePoint, OneDrive
- Dokumentation der Formen der Weitergabe von Daten (z. B. Ausdruck, Datenträger, automatisierte Übermittlung)
- Auflistung der Empfänger der Daten
- Dokumentation der Schnittstellen und der Abruf- und Übermittlungsprogramme
- Durchführung von Plausibilitäts-, Vollständigkeits- und Richtigkeitsprüfungen
- Maßnahmen zur Verhinderung von unkontrollierten Informationsflüssen
- Protokollierung der Zugriffe

Eingabekontrolle

Die Eingabekontrolle bezieht sich auf die Regelungen zur Erfassung von personenbezogenen Daten. Um diese Kontrolle umzusetzen, können beispielsweise folgende Maßnahmen ergriffen werden:

- Technische Protokollierung der Eingabe
- Session Recording bei Tunnel-VPN-Zugriffen von externen Dienstleistern
- Organisatorische festgelegte Zuständigkeiten für die Eingabe
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen

Maßnahmen zur Sicherstellung und Wiederherstellung von Verfügbarkeit

Die personenbezogenen Daten werden durch Maßnahmen zur Sicherstellung und Wiederherstellung der Verfügbarkeit vor zufälliger oder mutwilliger Zerstörung bzw. Verlust gesichert. Die Maßnahmen sind dabei so gewählt, dass Schadensereignisse, die zu einem Datenverlust führen können (z.B. Virenbefall, Überhitzung) bereits präventiv verhindert werden, aber auch so, dass bei einem Zwischenfall der Datenbestand möglichst vollständig wiederhergestellt werden kann. Im Einzelnen bestehen insbesondere folgende Maßnahmen:

- Regelmäßige Kontrolle des Systemzustandes (Monitoring)
- Backup- und Recovery-Konzept (regelmäßige Datensicherung)
- Datenarchivierungskonzept
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- Vorhandensein eines allgem. Notfallkonzeptes
- Vorhandensein von redundanten IT-Systemen (z. B. Business Continuity, Disaster Recovery)
- Regelmäßige Tests des Notfallkonzepts
- Vorhandensein von redundanten IT-Systemen (z. B. Server, Speicher)
- Funktionsfähige physische Schutzeinrichtungen (Brandschutz, Energie, Klima)

Incident Responce Management

Das Incident Response Management ist eine Maßnahme im Datenschutz, die dazu beiträgt, die Verfügbarkeit von personenbezogenen Daten sicherzustellen. Es umfasst die schnelle Identifizierung und Reaktion auf Sicherheitsvorfälle oder Störungen in der Verarbeitung von Daten sowie die Wiederherstellung der normalen Verarbeitung. Durch effektives Incident Response Management wird sichergestellt, dass personenbezogene Daten auch im Fall eines Sicherheitsvorfalls oder einer Störung weiterhin verfügbar sind und dass angemessene Maßnahmen zur Wiederherstellung der Daten ergriffen werden können:

- Prozess zur Erkennung, Meldung, Behandlung und Dokumentation von Sicherheitsvorfällen / Datenpannen
- Externer 24/7 1st-Level-Support durch IT Service Desk
- Externer 24/7 Support für digitale Forensik und Incident Response (DFIR)
- Einbindung des externen ISB und DSB in Sicherheitsvorfälle und Datenpannen

Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutzmanagement

Das Datenschutz-Management ist eine wichtige Maßnahme im Rahmen der Wirksamkeitskontrolle, die sicherstellt, dass geltende Datenschutzvorschriften und -richtlinien eingehalten werden und angemessene Maßnahmen zur Gewährleistung der Datensicherheit ergriffen werden. Durch regelmäßige Überprüfungen und Kontrollen des Datenschutz-Managements wird sichergestellt, dass die Datensicherheit und der Datenschutz kontinuierlich verbessert werden und mögliche Schwachstellen im System frühzeitig erkannt und behoben werden:

- Externer Datenschutzbeauftragter
- Datenschutzmanagementsystem
- Zentrale Dokumentation aller Verfahrensanweisungen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für alle Mitarbeitenden
- Erfüllung der Informationspflichten nach Art. 13 und 14 DSGVO
- Regelmäßige Schulung der Mitarbeitenden und Verpflichtung auf Vertraulichkeit / Datengeheimnis
- Regelmäßige Bewertung und Kontrolle der Technischen und organisatorischen Maßnahmen

Maßnahmen zur Sicherstellung der Zweckbindung und Datensparsamkeit

Die Maßnahmen zur Sicherstellung der Zweckbindung und Datensparsamkeit stellen sicher, dass personenbezogene Daten nur für spezifische und legitime Zwecke verarbeitet werden und dass nur die für diese Zwecke erforderlichen Daten erhoben und verarbeitet werden.

- Privacy by design / Privacy by default
- Zweckgebundene, datensparsame Verarbeitung personenbezogener Daten

Weisungskontrolle / Auftragskontrolle (Outsourcing an Dritte)

Die Maßnahmen der Weisungs- bzw. Auftragskontrolle dienen grundsätzlich dazu sicherzustellen, dass sich der Auftragsverarbeiter bei der Erbringung seiner Dienstleistung an die Weisungen des Verantwortlichen hält, aber auch dazu die Tätigkeit der eingesetzten Unterauftragsverarbeiter regelmäßig zu überprüfen und sicherzustellen, dass diese die personenbezogenen Daten nur nach dem gegebenen Vertrag zur Auftragsverarbeitung Weisungen verarbeiten. Die eigenen Mitarbeiter hat der Auftragsverarbeiter auf die Vertraulichkeit verpflichtet und sensibilisiert:

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standard-Vertragsklauseln
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Regelung zum Einsatz weiterer Subunternehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus