Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vertrag

Zwischen

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

MACH GmbH

Wielandstraße 14

23558 Lübeck

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt –

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

☐ Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung/ SLA/..... vom ....., die/den/das hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

☐ Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: (Beschreibung der Aufgaben)

☐ Bereitstellung der Web-Anwendung MACH formsolutions im SaaS-Model

☐ Bereitstellung Infrastrukturschnittstelle eID / Identitätsmanagement

☐ Bereitstellung Infrastrukturschnittstelle E-Payment

☐ Bereitstellung Infrastrukturschnittstelle Transport

☐ Bereitstellung Security Paket

☐ Bereitstellung Assistenten

☐ Bereitstellung Fachverfahrensschnittstellen

☐ Bereitstellung …….

(2) Dauer

☒ Der Vertrag wird für unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von 3 Monaten zum Jahresende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

(3) Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange wie der Auftrag-nehmer 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:

☒ Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: Siehe 1 (1).

(2) Art der Daten

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

☒ Personenstammdaten/Adressdaten/Kontaktdaten

☒ 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)

(3) Kategorien betroffener Personen

☒ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- ☒ Kunden
- ☐ Interessenten
- ☐ Abonnenten
- ☒ Beschäftigte
- ☒ Lieferanten
- ☐ Handelsvertreter
- ☒ Ansprechpartner

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 Auftrag-geber 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 zu 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.

j) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artt. 32-36 DSGVO genannten Pflichten.

k) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt:

Als Datenschutzbeauftragter ist beim Auftragnehmer Herr Oliver Volk, datenschutz@mach.de benannt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen. Die jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.

6. Unterauftragsverhältnisse

(1) Der Auftragnehmer ist berechtigt, Unterauftragnehmer für die Verarbeitung von Daten im Auftrag einzusetzen. Der Wechsel von Unterauftragnehmern oder die Beauftragung weiterer Unterauftragnehmer ist unter den folgenden Voraussetzungen zulässig (allgemeine Genehmigung):

a) Der Auftragnehmer informiert den Auftraggeber rechtzeitig, spätestens vier Wochen vor dem geplanten Einsatz, Wechsel oder Ersatz eines Unterauftragsverarbeiters in Textform („Information"). Der Auftraggeber kann innerhalb von drei Wochen in Textform und mit zwingender datenschutzrechtlicher Begründung widersprechen. Das Ausbleiben eines Widerspruchs gilt als Genehmigung. Ein Widerspruch kann jederzeit zurückgenommen werden.

b) Im Falle eines Widerspruchs prüft der Auftragnehmer, ob die Leistung auch ohne die Hinzuziehung des neuen Unterauftragnehmers möglich ist. Ist dies nicht der Fall, kann der Auftragnehmer das Vertragsverhältnis mit dem Auftraggeber mit einer Frist von mindestens 14 Tagen zum Ende eines Kalendermonats kündigen. Der Auftragnehmer wird bei der Kündigungsfrist die Interessen des Auftraggebers angemessen berücksichtigen.

(2) Die zum Zeitpunkt des Abschlusses dieser Vereinbarung genehmigten Unterauftragsverarbeiter sind in Anhang 2 aufgeführt. Der Auftragnehmer führt die Liste fort, aktualisiert sie bei Änderungen (z.B. bei neuen Unterauftragnehmern oder Wechsel von Unterauftragnehmern) und dokumentiert Art und Umfang der übertragenen Verarbeitung.

(3) Neue Unterauftragnehmer gelten erst nach Ablauf der Widerspruchsfrist und nach vollständiger Erfüllung der DSGVO-Vorgaben als zugelassen.

(4) Nicht als zustimmungspflichtige Unterauftragsverhältnisse gelten Dienstleistungen Dritter, die reine Nebenleistungen darstellen und keinen spezifischen personenbezogenen Datenbezug zum Auftrag des Auftraggebers haben (z. B.: Reinigungsdienste, Telekommunikationsleistungen ohne Datenzugriff, Post-, Kurier- und Transportdienste, Bewachungsdienste).

(5) Der Auftragnehmer wählt Unterauftragnehmer sorgfältig aus und prüft vor und regelmäßig während der Vertragslaufzeit, ob diese die vertraglichen und gesetzlichen Anforderungen einhalten. Insbesondere ist sicherzustellen, dass der Unterauftragnehmer angemessene technische und organisatorische Maßnahmen nach Art. 32 DSGVO getroffen hat.

(6) Der Auftragnehmer verpflichtet alle Unterauftragnehmer vertraglich zur Einhaltung sämtlicher Pflichten aus diesem Vertrag. Der Auftragnehmer schließt mit dem Unterauftragnehmer einen den Anforderungen des Art. 28 DSGVO entsprechenden Vertrag ab.

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. In der Anlage 2 werden die 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.

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 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.

11. Haftung

(1) Auftraggeber und Auftragnehmer haften im Außenverhältnis nach Art. 82 Abs. 1 und 4 DSGVO für materielle und immaterielle Schäden, die eine Person wegen eines oder mehrerer Verstöße gegen die DSGVO erleidet. Sind für einen solchen Schaden Auftraggeber und Auftragnehmer verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall eine Partei ganz oder überwiegend auf Schadensersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit es ihrem Anteil an der Verantwortung für den Schaden entspricht.

(2) Der Auftragnehmer haftet dem Verantwortlichen gegenüber entsprechend auch für die Einhaltung datenschutzrechtlicher Vorgaben durch die Subunternehmer, die er zur Erfüllung seiner Aufgaben einsetzt. Das Verschulden von Subunternehmern ist dem Auftragnehmer wie eigenes Verschulden zuzurechnen.

(3) Der Auftragnehmer unterstützt den Auftraggeber mit Auskünften zu allen ihm zur Verfügung stehenden Informationen, wenn der Auftraggeber einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder anderen Ansprüchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist.

12. Gerichtsstand

(1) Gerichtsstand ist der Ort des Auftraggebers.

_____	_____
Ort, Datum, Unterschrift	Ort, Datum, Unterschrift
Auftraggeber	Auftragnehmer

Anlage 1 – Technische- und organisatorische Maßnahmen

Nach Art. 32 DSVGO

Einführung

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen haben nach Art. 32 DSGVO der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Technische Maßnahmen beziehen sich auf den Datenverarbeitungsprozess als solchen. Diese bezeichnen alle Maßnahmen, die sich physisch umsetzen lassen.

Organisatorische Maßnahmen beziehen sich auf die Rahmenbedingungen der Datenverarbeitung. Sie umfassen Regeln, Vorgaben und Handlungsanweisungen, die dazu dienen, dass Mitarbeitende den Datenschutz gesetzestreu einhalten.

Zutrittskontrolle

Maßnahmen, um nur autorisierten Personen Zugriff auf personenbezogene Daten zu gewähren:

Umgesetzt/Vorhanden

- Es sind schriftliche Regelungen vorhanden, welche regeln, wer Zugang zu welchen Unternehmensbereichen hat.
- Auf die Trennung von Bearbeitungs- und Publikumszonen wird streng geachtet.
- Die Räumlichkeiten werden überwacht.
- Es gibt einen Empfang.
- Jeder Schlüsselhalter ist in einer Liste aufgeführt.
- Es findet eine Quittierung bei der Schlüsselausgabe statt.
- Es sind Alarmanlagen vorhanden.
- Die Zugänge der Räume sind ausreichend abgesichert (z. B. Türen, Lichtschächte).
- Die Räume werden bei Arbeitsbeginn bzw. -ende, auf- bzw. abgeschlossen.
- Es ist eine Videoüberwachungsanlage vorhanden.
- Mit dem Reinigungspersonal sind entsprechende Regelungen getroffen, um Zugriff auf personenbezogene Daten zu verhindern.
- Die Anwesenheit wird überprüft (z. B. Stechuhren, Schichtbuch).
- Bei fernangebundenen Arbeitsplätzen wird für ausreichende Sicherheit gesorgt.
- Ggf. findet eine Beratung durch kriminalpolizeiliche Beratungsstellen oder spezialisierte Dienstleister statt.
- Abwesenheiten werden protokolliert.
- Ein Zugangskontrollsystem wird benutzt.
- Mit IT-Dienstleistern bei Wartungen sind entsprechende Regelungen getroffen, um Zugriff auf personenbezogene Daten zu verhindern.
- Die Zugänge sind über Chipkarten/Transponder gesperrt.
- Es kommen Sicherheitsschlösser zum Einsatz.
- Besucher werden durch Mitarbeiter begleitet.

- Das Reinigungspersonal wird mit Sorgfalt ausgewählt.
- Es existiert eine Richtlinie "Clean Desk".

Zugangskontrolle

Sicherungsmaßnahmen, um unbefugten Personen keinen Zugriff auf IT-Systeme zu gewähren:

Umgesetzt/Vorhanden

- Es existiert eine zentrale Firewall.
- Ausreichend sichere Passwörter werden verwendet (z. B. keine Eigennamen und Wörter aus dem Wörterbuch, auch Sonderzeichen verwenden, empfohlene Länge von zehn Stellen, usw.).
- Falscheingabe von Passwörtern wird protokolliert.
- Regelmäßiger Passwortwechsel ist verpflichtend.
- Jeder Mitarbeiter hat ein eigenes Benutzerkonto.
- Das genutzte Verschlüsselungsverfahren ist auf dem Stand der Technik.
- Bei mehr als drei Anmelde-Fehlversuchen wird der Zugang gesperrt.
- Datenträger werden verschlüsselt.
- Es erfolgt eine automatische Sperrung der Bildschirme mit Passwortschutz, wenn Pausen gemacht werden.
- Zwei-Faktor-Authentifizierung wird eingesetzt.
- Es findet eine Auswertung der Protokolleinträge bei Falscheingaben des Passworts statt.
- Login erfolgt mit Benutzername und Passwort.
- Es existiert eine Richtlinie "Sicheres Passwort".
- Das BIOS wird durch ein separates Passwort geschützt.
- Es kommen Intrusion Detection Systeme zum Einsatz.
- Firewall- und Virenschutzprogramme werden eingesetzt.
- E-Mail-Verschlüsselung kommt wie folgt zum Einsatz: (Standard-TLS-Verschlüsselung)

Zugriffskontrolle

Maßnahmen, die angewendet werden, um sicherzustellen, dass ausschließlich Personal mit der nötigen Befugnis zur Nutzung der Verarbeitungsanlagen Zugriff auf personenbezogene Daten haben und dass diese bei der Bearbeitung genutzten personenbezogenen Daten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden:

Umgesetzt/Vorhanden

- Es bestehen Schutzmaßnahmen gegen unbefugte interne und externe Zugriffe (z. B. durch Verschlüsselung, Firewalls).
- Es findet eine Auswertung der Protokolle statt.
- Die Datenträger sind inventarisiert.
- Der Eingang, Ausgang sowie Bestand von Datenträgern werden festgehalten.
- Es existieren firmeninterne Richtlinien für das Kopieren von Datensätzen bzw. das vollständige Kopieren von Datenträgern.
- Die Geräte der Mitarbeitenden mit fernangebundenen Arbeitsplätzen werden regelmäßig gewartet.
- Datenträger verschiedener Auftraggeber werden getrennt behandelt (logische Datentrennung).
- Veraltete Datenträger werden geregelt und datenschutzkonform vernichtet.

- Datenträger werden vor neuer Verwendung vollständig von bestehenden Daten bereinigt.
- Es finden regelmäßige Kontrollen der tatsächlichen Vernichtung von Datenträgern statt.
- Es werden regelmäßige Penetrationstests gegen Attacken von Hackern durchgeführt.
- Es werden Verfahren zur Erkennung unerwünschter Datenabflüsse eingesetzt.
- Der Einsatz privater Datenträger ist untersagt.
- Fehldrucke werden sorgfältig entsorgt (Datenvernichtungstonnen).
- Zugriffe bzw. Zugriffsversuche werden protokolliert.
- Es gibt Regeln für die Verwendung von mobilen Datenträgern und Geräte.
- Das Konzept entspricht, sowohl für Anwender als auch für Administratoren, den aufgabenbedingten- und datenschutzrechtlichen Erfordernissen.
- BYOD-Kultur (Bring-Your-Own-Device) wird in der Organisation nicht gelebt.
- Es kommen geeignete Aktenvernichter zum Einsatz.
- Es kommt ein externer Aktenvernichter (z.B. nach ISO 21964) zum Einsatz.
- Es kommen Berechtigungskonzepte zum Einsatz.
- Es gibt nur die notwendige Anzahl an Administratoren.
- Datenträger werden physisch gelöscht.
- Benutzerrechte werden durch Administratoren verwaltet.

Weitergabekontrolle

Maßnahmen, welche gewährleisten, dass personenbezogene Daten während eines Transportes, bei elektronischer Übertragung oder bei Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

Umgesetzt/Vorhanden

- Der Eingang/Ausgang von Datenträgern wird schriftlich festgehalten.
- Die Abruf- und Übermittlungsvorgänge werden dokumentiert.
- Elektronische Datentransporte sind Ende-zu-Ende verschlüsselt.

Eingabekontrolle

Maßnahmen, die absichern, dass nachträglich überprüft und festgestellt werden kann, ob und durch welche Person personenbezogene Daten im Verarbeitungssystem eingegeben, verändert oder entfernt worden sind:

Umgesetzt/Vorhanden

- Die Eingabe neuer Daten wird protokolliert.
- Im Rahmen der Protokollierung wird aufgezeichnet, wer Daten eingeben hat.
- Im Rahmen der Protokollierung wird aufgezeichnet, wann Daten eingeben wurden.
- Im Rahmen der Protokollierung wird aufgezeichnet, was für Daten eingeben wurden.
- Bei der Dokumentation der Eingabeverfahren werden auch Informationen über die Person erfasst, die die Änderungen gemacht hat (nicht der Name, aber z. B. die Stellenbeschreibung).
- Protokolle werden manuell oder automatisiert kontrolliert.
- Es existiert eine Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können.
- Formulare, von denen Daten in automatisierte Verarbeitungen übernommen wurden, werden aufbewahrt.
- Zuständigkeiten für Löschungen sind klar verteilt.

Auftragskontrolle

Maßnahmen, die erforderlich sind, um die Daten nur zu den Zwecken und im notwendigen Umfang nach Weisung des Auftraggebers zu verarbeiten:

Umgesetzt/Vorhanden

- Es findet eine sorgfältige Auswahl der Auftragnehmer statt.
- Es gibt eine Liste von Auswahlkriterien.
- Die Unterauftragnehmer des Auftragnehmers werden sorgfältig ausgewählt.
- Es bestehen detaillierte schriftliche Regelungen über die Verpflichtungen aller Auftragsverarbeiter (auch im Bezug auf Subunternehmen).
- Es gibt eindeutige Regelungen über Zuständigkeiten und Verantwortlichkeiten.
- Es erfolgt eine formalisierte Auftragserteilung.
- Es findet eine regelmäßige Kontrolle der Arbeitsergebnisse von Auftragnehmern statt (formal, inhaltlich).
- Notwendigen Vereinbarungen zur Auftragsverarbeitung bzw. EU-Standard-Vertragsklauseln werden abgeschlossen.
- Die Benennung des Datenschutzbeauftragten beim Auftragnehmer wird überprüft.
- Es werden wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart.
- Die Vernichtung von Daten nach Beendigung eines Auftrags wird sichergestellt.
- Der Auftragnehmer und sein Schutzniveau werden regelmäßig überprüft.

Verfügbarkeitskontrolle

Maßnahmen, welche die Verfügbarkeit erhöhen:

Umgesetzt/Vorhanden

- Es gibt Feuerlöscher, Rauch- und Brandmelder.
- Sicherungsdatenträger werden getrennt aufbewahrt.
- Eine unterbrechungsfreie Stromversorgung (USV) ist etabliert.
- Die Daten werden auf Sicherungsträgern gespeichert.
- Speichereinheiten werden redundant ausgelegt.
- Die Datensicherungen sind verschlüsselt.
- Für einen Katastrophenfall gibt es entsprechende Vorkehrungen (z. B. durch Angriffe von intern/extern, Schäden durch Feuer).
- Im Serverraum werden Temperatur und Feuchtigkeit überwacht.
- Es kommen RAID-Systeme zum Einsatz.
- Betriebssysteme und Daten werden auf getrennten Partitionen gespeichert.
- Backup-Vorgänge werden kontrolliert.
- Es finden regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse statt.
- Sicherungsmedien werden an einem sicheren Ort außerhalb des Serverraums aufbewahrt.
- Der Serverraum ist klimatisiert.
- Im Serverraum kommen Schutzsteckdosen zum Einsatz.
- Der Serverraum hat ein eigenes Zutrittskontrollsystem mit Alarmanlage/Alarmmeldung.
- Es gibt keine sanitären Anschlüsse im oder oberhalb des Serverraums.

Trennungskontrolle

Maßnahmen, die unterstützen, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben werden, getrennt verarbeitet werden können:

Umgesetzt/Vorhanden

- Von allen Daten unter unserer Verantwortung gibt es mindestens einen Satz getrennt gelagerte Backups.
- Produktion- und Testumgebungen sind stets voneinander getrennt.
- Daten mit hohem Schutzbedarf werden besonders umsichtig behandelt.
- Es besteht ein Konzept zur Mandantentrennung.
- Es gibt ein System für die Veränderung, Löschung und Übermittlung von Daten mit unterschiedlichen Vertragszwecken.
- Es werden Systeme verwendet, die eine interne Mandantenaufteilung ermöglichen (Zweckbindung).

Organisationskontrolle

Innerbetriebliche Maßnahmen, welche dazu dienen, ein entsprechendes Datenschutzniveau zu gewährleisten:

Umgesetzt/Vorhanden

- Sicherungen des Datenbestandes erfolgen nach festgelegtem Schema.
- Es wird auf etablierte hohe Standards für IT-Sicherheit bzw. Abwicklung von IT-Projekten zurückgegriffen.
- Im Urlaubs- und Krankheitsfall ist für eine Vertretung gesorgt.
- Es gibt regelmäßige Hinweise und Ermahnungen, um das Problembewusstsein zu fördern.
- Mitarbeiter werden über den sicheren Umgang mit den Daten entsprechend geschult.
- Mobile Datenträger der Mitarbeiter sind standardmäßig verschlüsselt.
- Es gibt weitere Sicherungsmaßnahmen, wenn sensible Daten verarbeitet werden. (Verschlüsselung wird immer eingesetzt).
- Es bestehen schriftliche Regelungen über den Verlauf der Datenverarbeitung sowie zu den verschiedenen Datensicherheitsmaßnahmen.

Pseudonymisierung

Folgende Maßnahmen sind implementiert, damit Daten nicht mehr einer Person zugeordnet werden können:

Umgesetzt/Vorhanden

- Bei Pseudonymisierung werden Zuordnungsdaten und personenbezogene Daten in getrenntem und abgesichertem System aufbewahrt.

Datenschutz-Management

Maßnahmen, die dazu dienen, die Verarbeitung personenbezogener Daten zu regeln, zu dokumentieren und zu überprüfen:

Umgesetzt/Vorhanden

- Mitarbeitende sind geschult und auf die Wahrung der Vertraulichkeit verpflichtet.
- Mitarbeitende werden regelmäßige (mindestens jährlich) sensibilisiert.
- Die Organisation kommt den Informationspflichten nach.
- Es existiert ein formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener.

- Es existiert eine zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung.
- Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt.
- Es kommen Software-Lösungen für Datenschutz-Management zum Einsatz.
- Es gibt eine zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung.
- Die Datenschutz-Folgenabschätzung (DSFA) wird bei Erforderlichkeit stets durchgeführt.

Privacy by Design

Diese Voreinstellungen sollen gewährleisten, dass nur personenbezogene Daten verarbeitet werden, welche für den jeweiligen Zweck erforderlich sind:

Umgesetzt/Vorhanden

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.
- Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen ist möglich.

Incident-Response-Management

Folgende Maßnahmen sind bei bzw. zu Sicherheitsvorfällen implementiert:

Umgesetzt/Vorhanden

- Es existiert ein dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde).
- Es existiert eine dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen.
- Der/Die ISB wird in Sicherheitsvorfälle und Datenpannen eingebunden.
- Der/Die DSB wird in Sicherheitsvorfälle und Datenpannen eingebunden.
- Sicherheitsvorfälle und Datenpannen werden dokumentiert.
- Es existiert ein formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen.

Anlage 2 - Genehmigte Unterauftragsverhältnisse

Firma Unterauftrag-nehmer	**Anschrift/Land**	**Leistung**	**Angaben zu geeigneten Garantien bei Datenübermittlungen in ein Drittland**
T-Cloud (T-Systems International GmbH)	Hahnstraße 43d D-60528 Frankfurt am Main	Serverhosting und Support im Störungsfall auf Anfrage	Eine Datenübermittlung in Drittländer erfolgt nicht.
T-Cloud (T-Systems International GmbH)	Hahnstraße 43d D-60528 Frankfurt am Main	Backup‘s	Eine Datenübermittlung in Drittländer erfolgt nicht.