Auftragsdatenverarbeitungsvereinbarung

zwischen

der moncardo GmbH

- nachfolgend Provider -

und

(Kunde)

- nachfolgend Auftraggeber -

gem. Art. 28 DSGVO

**Präambel**

Diese Vereinbarung über die Datenverarbeitung im Auftrag konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus den Nutzungsbedingungen über die vom Provider vertriebene Software moncardo in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit den Nutzungsbedingungen in Zusammenhang stehen und bei denen Beschäftigte des Providers oder durch den Provider Beauftragte personenbezogenen Daten des Auftraggebers (Kunde) verarbeiten.

# **§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsdatenverarbeitung**

(1) Aus den Nutzungsbedingungen ergeben sich Gegenstand und Dauer des Auftrags sowie Zweck und Art der Datenverarbeitung. Im Einzelnen sind insbesondere die Teilnehmerdaten des Auftraggebers Bestandteil der Datenverarbeitung. Hierzu zählen Name, Anschrift, Telefonnummer, E-Mail-Adresse und ggf. weitere Daten. Die Daten werden vom Auftraggeber zum Zweck der Erbringung seiner Dienstleistungen seinen Kunden (Teilnehmer und Verbraucher) gegenüber erhoben. Des Weiteren werden personenbezogene Daten der Kunden der Teilnehmer (Verbraucher) des Auftraggebers verarbeitet. Hierzu zählen insbesondere Name, Anschrift, Telefonnummer, E-Mail-Adresse und ggf. weitere Daten. Zweck dieser Verarbeitung ist ebenfalls die Erfüllung vertraglicher Pflichten aus der Nutzungsvereinbarung für moncardo.

(2) Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit der Nutzungsbedingungen für moncardo, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen ergeben.

# **§ 2 Anwendungsbereich und Verantwortlichkeit**

(1) Der Provider verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die in den Nutzungsbedingungen, dort insbesondere in § 3 konkretisiert sind. Der Auftraggeber ist im Rahmen dieser Nutzungsbedingungen für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Provider sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO). Dies gilt insbesondere auch für Daten, die dem Berufsgeheimnis unterliegen, § 203 StGB.

(2) Die Weisungen werden anfänglich durch die Nutzungsbedingungen festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

# **§ 3 Technische und organisatorische Maßnahmen**

(1) Der Provider wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutzgrundverordnung (Art. 32 DSGVO)) genügen. Der Provider hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. 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 DS-GVO zu berücksichtigen (siehe Anlage zu dieser Vereinbarung).

(2) Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

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

#

# **§ 4 Pflichten des Providers**

(1) Der Provider darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Art. 28 Abs. 3 lit. a) DSGVO vor. Der Provider informierte den Auftragsgeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Provider darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wird.

(2) Der Provider unterstützt so weit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel 3 der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

(3) Der Provider gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Provider tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Provider, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(4) Der Provider unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Der Provider trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

(5) Der Provider nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

(6) Der Provider gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(7) Der Provider berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Provider die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien aufgrund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

(8) Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

(9) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Provider den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

# **§ 5 Pflichten des Auftraggebers**

(1) Der Auftraggeber hat den Provider unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt §3 Abs. 9 entsprechend.

(3) Der Auftraggeber nennt dem Provider den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

# **§ 6 Anfragen Betroffener**

(1) Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Verarbeitung von Daten dieser Person zu erteilen, wird der Provider den Auftraggeber dabei unterstützen, diese Informationen bereitzustellen. Dies setzt voraus, dass der Auftraggeber den Provider hierzu schriftlich oder in Textform aufgefordert hat und der Auftraggeber dem Provider die durch diese Unterstützung entstandenen Kosten erstattet. Der Provider wird keine Auskunftsverlangen beantworten und den Betroffenen insoweit an den Auftraggeber verweisen.

(2) Wendet sich ein Betroffener mit Forderungen zur Berichtigung, Löschung oder Sperrung an den Provider, wird der Provider den Betroffenen an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Provider leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Provider unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Provider haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

# **§ 7 Kontrollrechte des Auftraggebers**

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Provider 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 Provider in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Provider stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Providers nach Art. 28 DSGVO überzeugen kann. Der Provider 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) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Provider einen Vergütungsanspruch geltend machen.

# **§ 8 Unterauftragsverhältnisse**

(1) Die Weitergabe von Aufträgen im Rahmen der in dem Vertrag vereinbarten Tätigkeiten an Subunternehmer durch den Provider bedarf der vorherigen ausdrücklichen schriftlichen bzw. dokumentierten Zustimmung des Auftraggebers. Der Provider wird Subunternehmer nach deren Eignung sorgfältig auswählen.

(2) 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 Provider 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 Provider 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.

Im Übrigen liegt ein zustimmungspflichtiges Subunternehmerverhältnis vor, wenn der Provider weitere Provider mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Erteilt der Provider Aufträge an Subunternehmer, so obliegt es dem Provider, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

(3) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung eines Subunternehmers durchgeführt, und zwar:

|  |  |
| --- | --- |
| Name und Anschrift des Subunternehmers | Beschreibung der Teilleistungen |
|  |  |

Für diese Subunternehmer gilt die Einwilligung für das Tätigwerden als erteilt. Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt der Provider die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf.

# **§ 9 Informationspflichten, Schriftformklausel, Rechtswahl**

(1) Sollten die Daten des Auftraggebers beim Provider durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Provider den Auftraggeber unverzüglich darüber zu informieren. Der Provider 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 Datenschutzgrundverordnung liegen.

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

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen der Nutzungsbedingungen vor. Sollten einzelne Teile hiervon unwirksam sein, so berührt dies die Wirksamkeit im Übrigen nicht.

(4) Es gilt deutsches Recht.

(5) Gerichtsstand für alle Streitigkeiten aus dieser Vereinbarung ist der Sitz des Anbieters, der moncardo GmbH.

**§ 10 Haftung und Schadensersatz**

(1) Eine zwischen den Parteien in den Nutzungsbedingungen vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, sofern und soweit nicht ausdrücklich etwas anderes vereinbart wurde.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 - Ort und Datum -

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 - Provider -

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 - Ort und Datum -

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 - Auftraggeber -

**Anlage**

**Technische und Organisatorische Maßnahmen**

**zum Vertrag zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO vom 24.05.2019**

**Zutrittskontrolle**

Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

|  |  |
| --- | --- |
| **Maßnahme** | **vorhanden** |
| ja | nein |
| Berechtigungsausweise |   | X |
| Zutrittscodekarten/ Zutrittstransponder  |   | X |
| Zutrittsberechtigungskonzept*.* |   | X |
| Überwachungseinrichtungen (z.B. Videoüberwachung) |   | X |
| Schlüsselregelung | X |   |
| Regelung für Firmenfremde, Besucherausweise |   | X |
| Anwesenheitsaufzeichnungen, Dokumentationspflicht |   | X |
| Sicherung auch außerhalb der Arbeitszeit durch Alarmanlage und/oder Werkschutz | X |   |
| Definierte Sicherheitsbereiche und kontrollierter Zutritt |   | X |
| Gesicherter Eingang für An‑ und Ablieferung | X |   |
| Türsicherung (elektrischer Türschließer, Ausweisleser, Fernsehmonitor, Pförtner) |   | X |
| Kontrolle durch die Mitarbeiter (4‑Augen‑Prinzip) | X |   |
| Maßnahmen zur Objektsicherung (z. B. Spezialverglasung, Alarmanlage, Geländebewachung) | X |   |
| Sicherung des RZ-Zutritt |   | X |
| Aufbewahrung der Server in abschließbaren Räumen |   | X |
| Aufbewahrung der Datenträger unter Verschluss bzw. in abgeschlossenen Räumen |   | X |
| Aufbewahrung von Datensicherungen (z.B. Bänder, CDs) im zutrittsgeschützten Safe |   | X |
| Anweisung zur Ausgabe von Schlüsseln | X |   |
| **Sonstiges:**  |   |   |

**Zugangskontrolle**

Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

|  |  |
| --- | --- |
| **Maßnahme** | **vorhanden** |
| ja | nein |
| Verschlüsselung von Netzwerken | X |   |
| Verschließbarkeit von Datenverarbeitungsanlagen |   | X |
| Identifizierung eines Terminals und/oder eines Terminalbenutzers gegenüber der Datenverarbeitungsanlage |   | X |
| Vergabe und Sicherung von Identifizierungsschlüsseln |   | X |
| Sicherung von Bildschirmarbeitsplätzen | X |   |
| Funktionelle und/oder zeitlich beschränkte Nutzung von Terminals und ldentifizierungsmerkmalen |   | X |
| Regelung der Benutzerberechtigung | X |   |
| Verwendung von individuellen Passwörtern | X |   |
| Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern |   | X |
| Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner) | X |   |
| Passwortpolicy | X |   |
| Verpflichtung auf das Datengeheimnis nach Art. 32 Abs. 4 DSGVO. | X |   |
| Richtlinien für die Dateiorganisation | X |   |
| Protokollierung und Auswertung der Systembenutzung |   | X |
| Kontrollierte Vernichtung von Datenträgern | X |   |
| Arbeitsanweisung und Bearbeitungsverfahren für Datenerfassung | X |   |
| Prüf-, Abstimm- und Kontrollsysteme | X |   |
| Programmprüfungs- und Freigabeverfahren | X |   |
| **Sonstiges:**  |   |   |

**Zugriffskontrolle**

Unerlaubte Tätigkeiten in DV-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.

|  |  |
| --- | --- |
| **Maßnahme** | **vorhanden** |
| ja | nein |
| Festlegung der Zugriffsberechtigung, Berechtigungskonzept | X |   |
| Festlegung der Befugnis zur Dateneingabe, -änderung, -löschung | X |   |
| Besteht eine Trennung von Berechtigungsbewilligung (organisatorisch) und Berechtigungsvergabe (technisch)? | X |   |
| Konzept der Laufwerksnutzung und -zuordnung  | X |   |
| Regelung zur Wiederherstellung von Daten aus Backups (wer darf wann auf wessen Anforderung Back-up-Daten einspielen?) in einem verbindlichen Verfahren | X |   |
| Überprüfung der Berechtigung | X |   |
| Beschränkung der freien und unkontrollierten Abfragemöglichkeit von Datenbanken | X |   |
| Auswertung von Protokollen*.* |   | X |
| Ausweisleser am Terminal |   | X |
| Zeitliche Begrenzung der Zugriffsmöglichkeiten |   | X |
| Teilzugriffsmöglichkeiten auf Datenbestände und Funktionen |   | X |
| Kontrolle des Zugriffs | X |   |
| Protokollierung des Datenzugriffs | X |   |
| Prinzip "Aufgeräumter Schreibtisch" | X |   |
| **Sonstiges:**  |   |   |

**Weitergabekontrolle**

Aspekte der Weitergabe personenbezogener Daten sind zu regeln: Elektronische Übertragung, Datentransport, sowie deren Kontrolle.

|  |  |
| --- | --- |
| **Maßnahme** | **vorhanden** |
| ja | nein |
| Werden Daten vom Provider an den Auftraggeber geschickt? | X |   |
| Erhält der Provider Daten vom Auftraggeber? | X |   |
| Welche Versendungsart der Daten besteht zwischen Auftraggeber und Provider?  |   |   |
| § Citrix-Verbindung (128 Bit verschlüsselt) |   |   |
| § VPN-Verbindung |   |   |
| § E-Mail Versand mit verschlüsselten ZIP-Dateien | X |   |
| Verschlüsselung von Daten und Verbindungen beim Transport | X |   |
| Berechtigungskonzept vorhanden | X |   |
| Kontrolle durch Mitarbeiter (4 Augen Prinzip) | X |   |
| Gesicherter Eingang für An- und Ablieferung |   | X |
| Verwaltung von Datenträgern, Bestandskontrolle | X |   |
| Festlegung der Bereiche, in dem sich Datenträger befinden müssen |   | X |
| Verschlüsselung vertraulicher Datenträger | X |   |
| Sicherheitsschränke |   | X |
| Verbot der Mitnahme von Taschen und sonstigen Gepäckstücken in die Sicherheitsbereiche |   | X |
| Kontrollierte Vernichtung von Datenträgern (Datenträgervernichtungsregelung) | X |   |
| Regelung zur Anfertigung von Kopien |   | X |
| Sicherungskopien von Datenträgern, die transportiert werden müssen |   | X |
| Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege |   | X |
| Verpackungs- und Versandvorschriften, verschlüsselter E-Mail-Versand | X |   |
| Direktabholung, Kurierdienst, Transportbegleitung | X |   |
| Plausibilitätsprüfung | X |   |
| Vollständigkeits- und Richtigkeitsprüfung | X |   |
| Verschlüsselung v. Festplatten (Laptops) |   | X |
| Verschlüsselung WLAN | X |   |
| **Sonstiges:**  |   |   |

**Eingabekontrolle**

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.

|  |  |
| --- | --- |
| **Maßnahme** | **vorhanden** |
| ja | nein |
| Kennzeichnung erfasster Daten | X |   |
| Sind die Benutzerberechtigungen (Profile) festgelegt? | X |   |
| Sind die Benutzerberechtigungen differenziert? | X |   |
| § Lesen, Ändern, Löschen | X |   |
| § Teilzugriff auf Daten bzw. Funktionen | X |   |
| § Feldzugriff bei Datenbanken | X |   |
| Organisatorische Festlegung der Zuständigkeiten für die Eingabe | X |   |
| Protokollierung von Eingaben | X |   |
| Protokollauswertungssystem |   | X |
| Ist eine Verfahrens-, Programm- und Arbeitsablauforganisation vorhanden? | X |   |
| Kontrolle der Dateneingabe |   | X |
| Verpflichtung auf das Datengeheimnis | X |   |
| Regelung der Zugriffsberechtigungen  | X |   |
| Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke | X |   |
| **Sonstiges:**  |   |   |

**Verfügbarkeitskontrolle**

Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

|  |  |
| --- | --- |
| **Maßnahme** | **vorhanden** |
| ja | nein |
| Datensicherungs- und Backupkonzepte | X |   |
| Begrenzung der Zutrittsrechte in Serverräumlichkeiten auf notwendiges Personal |   | X |
| Installation von Brandmeldeanlagen in Serverräumlichkeiten | X |   |
| Wasserlose Brandbekämpfungssysteme für Server |   | X |
| Klimatisierte Serverräumlichkeiten |   | X |
| Blitz-/ Überspannungsschutz |   | X |
| Serverräumlichkeiten in separaten Brandabschnitt |   | X |
| Unterbringung von Backupsystemen in separaten Räumlichkeiten und Brandabschnitt | X |   |
| Gewährleistung der technischen Lesbarkeit von Backupspeichermedien für die Zukunft | X |   |
| Lagerung von Archiv-Speichermedien unter notwendigen Lagerbedingungen (Klimatisierung, Schutzbedarf etc.) |   | X |
| CO2 Feuerlöscher in unmittelbarer Nähe der Serverräumlichkeiten |   | X |
| Durchführung der Datensicherungs- und Backupkonzepte | X |   |
| Gibt es eine Vereinbarung bzgl. Übergabe der (Daten-) Sicherungen? |   | X |
| Katastrophen- oder Notfallplan (Wasser, Feuer, Explosion, Androhung von Anschlägen, Absturz, Erdbeben) |   | X |
| Erfolgt eine Festplattenspiegelung? |   | X |
| Einbeziehung des Einflusses angrenzender baulicher Einrichtungen |   | X |
| Schwachstellenanalyse (Geländeschutz, Gebäudeschutz, Eindringen in Rechner, Rechnernetze) |   | X |
| Aufbewahrung der Daten in Datensicherungsschränken, Tresoren |   | X |
| Sind Ausweich-Rechenzentren vorhanden (Hot- bzw. Cold-Stand-by)? |   | X |
| Gibt es eine USV-Anlage (Unterbrechungsfreie Stromversorgung)? |   | X |
| Werden unberechtigte Benutzer abgewiesen? | X |   |
| Werden entsprechende Sicherheitssysteme (Software/Hardware) eingesetzt? | X |   |
| § Virenscanner | X |   |
| § Firewalls | X |   |
| § SPAM-Filter | X |   |
| § Verschlüsselungsprogramme |   | X |
| **Sonstiges:**  |   |   |

**Trennungskontrolle**

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

|  |  |
| --- | --- |
| **Maßnahme** | **vorhanden** |
| ja | nein |
| Trennung von Kunden | X |   |
| Dateiseparierung bei Datenbanken | X |   |
| Werden die Daten des Auftraggebers und anderer Kunden von unterschiedlichen Mitarbeitern beim Provider verarbeitet? | X |   |
| Erfolgen die Datensicherungen der Auftraggeber-Daten auf separaten Datenträgern (ohne Daten anderer Kunden)? |   | X |
| Existiert ein Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeber-Daten von Daten anderer Kunden Rechnung trägt? |   | X |
| Funktionstrennung |   | X |
| Trennung von Entwicklungs-, Test- und Produktivsystem |   | X |
| **Sonstiges:**  |   |   |

 [f1]Welche Daten erheben Ihre Kunden von den nachgelagerten Benutzern, insbesondere den Karteninhabern?

 [f2]s.o.