1.1.1 Diese Auftragsdatenverarbeitung regelt die Rechte und Pflichten des/der Kunden/Kundin („Verantwortlicher”) und VISUAL WORLD GmbH („Auftragsverarbeiter") im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag (Vereinbarung).
Diese Vereinbarung ist so konzipiert, dass es den Bestimmungen der geltenden EU Datenschutz-Grundverordnung („DSGVO“) gerecht wird. Im Falle eines Widerspruchs zwischen den Bestimmungen diese Vereinbarung und des Vertrags haben die Bestimmungen dieser Vereinbarung Vorrang.

1.1.2 Sofern in dieser Vereinbarung nicht anders definiert, gelten die Definitionen des Vertrags bzw. der DSGVO.

1.1.3 Der Verantwortliche stimmt den Bedingungen dieser Vereinbarung im eigenen Namen und im Namen aller verbundenen Unternehmen zu, die an der Verarbeitung personenbezogener Daten im Rahmen dieser Vereinbarung beteiligt sein können.

1.2 Gegenstand der Verarbeitung, Kategorien der Daten und Betroffenen

1.2.1 Der Gegenstand des Vertrags ergibt sich aus der zwischen den Parteien abgeschlossenen Vereinbarung über die Bereitstellung von Software zum Zugriff über das Internet (SaaS) und/oder die Erbringung von Wartung, Support und/oder IT Services des Auftragsverarbeiter an den Verantwortlichen, auf die hier (folgend Hauptauftrag) verwiesen wird. Diese Vereinbarung zur Auftragsverarbeitung findet Anwendung auf alle Tätigkeiten, die mit der Auftragsverarbeitung bei der Erbringung von Leistungen gemäß Hauptvertrag in Zusammenhang stehen und bei denen der Auftragnehmer mit personenbezogenen Daten, die dem Auftragnehmer vom Auftraggeber übermittelt oder offengelegt werden, in Berührung kommen kann.

Details bezüglich der möglichen Datenverarbeitung ergeben sich aus den Ziffern 1.2.2 und 1.2.3. Der für die Verarbeitung Verantwortliche erkennt an, dass der Umfang der Datenverarbeitung im Ermessen des Verantwortlichen liegt und je nach Nutzung der Software variieren kann.

1.2.2 Folgende Datenarten/ -kategorien sind regelmäßig Gegenstand der Verarbeitung:

Personalstammdaten (insb. Name, Anschrift, Geburtsdatum, Telefonnummer, Geschlecht, Familienstand)

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

Vertragsstammdaten (insb.Eintrittsdatum Arbeitnehmer/in))

- Planungs- und Steuerungsdaten (insb., Abwesenheiten, Urlaubspläne, Krankmeldungen, Arbeitszeiten,)

Zeitstempel

1.2.3 Die Kategorien, der durch die Verarbeitung betroffenen Personen können in Bezug auf den Verantwortlichen (oder ein verbundenes Unternehmen des Verantwortlichen) regelmäßig umfassen:

Beschäftigte -, Angestellte ,Freiwillige oder Freiberufler/innen

Ehemalige beschäftigte - Angestellte , Freiwillige oder Freiberufler/innen,

Zukünftige beschäftigte , Freiwillige oder Bewerber/innen

1.2.4 Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union, einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum oder einem Staat mit angemessenem Datenschutzniveau nach Art. 45 DSGVO, welches durch die Europäische Kommission festgestellt wird, statt.

1.2.5 Der Auftragsverarbeiter darf eine internationale Übermittlung personenbezogener Daten in ein Land außerhalb des Europäischen Wirtschaftsraums nur in Übereinstimmung mit der DSGVO durchführen und muss in dem nach der DSGVO erforderlichen Umfang angemessene Schutzmaßnahmen ergreifen.

1.2.6 Der Auftragsverarbeiter darf eine internationale Übermittlung personenbezogener Daten in ein Land außerhalb des Europäischen Wirtschaftsraums nur in Übereinstimmung mit der DSGVO durchführen und muss in dem nach der DSGVO erforderlichen Umfang angemessene Schutzmaßnahmen ergreifen.

2. Vertraulichkeit

Der Auftragsverarbeiter sorgt für die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. (b), 29 und 32 Abs. 4 DSGVO. Der Auftragsverarbeiter gewährleistet, dass alle Personen, die er zur Verarbeitung personenbezogener Daten heranzieht, einer (vertraglichen oder gesetzlichen) Verschwiegenheitspflicht unterliegen.

3. Pflichten des Verantwortlichen

3.1 Der Verantwortliche ist für die Einhaltung der DSGVO in Bezug auf die Nutzung der Software (soweit zutreffend) verantwortlich.

3.2 Der Verantwortliche hat den Auftragsverarbeiter unverzüglich zu informieren, wenn er im Hinblick auf die Verarbeitung bezüglich datenschutzrechtlicher Bestimmungen Fehler oder Unregelmäßigkeiten feststellt.

3.3 Der Verantwortliche nennt dem Auftragsverarbeiter bei Bedarf den/die Ansprechpartner/in für im Rahmen diese Vereinbarung Vereinbarunganfallende Datenschutzfragen.

4. Weisungen

4.1 Der Auftragsverarbeiter darf die personenbezogenen Daten nur im Rahmen von Weisungen des Verantwortlichen verarbeiten (vorausgesetzt, diese Weisungen fallen in den Anwendungsbereich der Software) oder soweit es zur Einhaltung der DSGVO erforderlich ist. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO verstoßen könnte. Der Auftragsverarbeiter ist nicht verpflichtet, eine solche gegen die DSGVO verstoßende Anweisung zu befolgen, es sei denn, die Angelegenheit wurde von den Parteien einvernehmlich geklärt.

4.2 Der Verantwortliche benennt die ausschließlich weisungsbefugten Personen innerhalb der Software. Falls keine weisungsbefugte Person benannt wird, sind nur natürliche Personen, die zur gesetzlichen Vertretung des Verantwortlichen befugt sind, zur Erteilung von Weisungen berechtigt. Der Auftragsverarbeiter kann die Ausführung von Weisungen so lange aussetzen, bis der Verantwortliche dem Auftragsverarbeiter die Befugnis zur gesetzlichen Vertretung des Verantwortlichen nachgewiesen hat.

5. Pflichten des Auftragsverarbeiter

5.1 Allgemeine Pflichten des Auftragsverarbeiter

5.1.1 Der Auftragsverarbeiter benennt eine/n Datenschutzbeauftragte/n. Die (von Zeit zu Zeit aktualisierten) Kontaktdaten des/der Datenschutzbeauftragten werden auf der Website des Auftragsverarbeiters veröffentlicht.

5.1.2

5.1.3 Der Auftragsverarbeiter wird den Verantwortlichen unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informieren, soweit sie sich auf diese Vereinbarung beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten aus dieser Auftragsverarbeitung beim Auftragsverarbeiter ermittelt, es sei denn, der Auftragsverarbeiter ist gesetzlich oder behördlich verpflichtet, eine Mitteilung zu unterlassen.

5.2 Überprüfungen

5.2.1 Der Verantwortliche ist berechtigt, die Einhaltung der Pflichten aus dieser Vereinbarung, der technischen und organisatorischen Maßnahmen („TOM“) sowie der datenschutzrechtlichen Vorschriften nach Vereinbarung - unter Berücksichtigung eines mind. 14-tägigen Vorlaufs - mit dem Auftragsverarbeiter zu deren üblichen Geschäftszeiten selbst zu überprüfen oder durch im Einzelfall zu benennende Prüfer/innen überprüfen zu lassen. Dazu kann der Verantwortliche u.a. die maßgeblichen Gebäude und Einrichtungen des Auftragsverarbeiters besichtigen, Auskünfte einholen oder Einsicht in die eigenen Daten unter Rücksichtnahme auf die berechtigten Interessen des Auftragsverarbeiters nehmen. Für Überprüfungen, die aufgrund eines Sicherheitsvorfalles bzw. eines mehr als unwesentlichen Verstoßes gegen die Vorschriften zum Schutz personenbezogener Daten oder Festlegungen dieser Vereinbarungs erforderlich werden („anlassbezogene Vor-Ort-Prüfung“), ist die Anmeldefrist aus Satz 1 auf einen angemessenen Zeitraum verkürzt. Weiterhin unterliegen anlassbezogene Vor-Ort-Prüfungen nicht den Einschränkungen der Ziffern 5.2.3.-5.2.4. dieser Vereinbarung.

5.2.2 Der Auftragsverarbeiter darf die Zustimmung zur Prüfung davon abhängig machen, dass sich der/die Prüfende einer angemessenen Verschwiegenheitserklärung unterwirft. Sollte der/die durch den Verantwortlichen beauftragte Prüfer/in in einem Wettbewerbsverhältnis zum Auftragsverarbeiter stehen oder liegt ein anderer begründeter Fall vor, hat der Auftragsverarbeiter gegen diese/n ein Einspruchsrecht.

5.2.3 Im Rahmen dieser Ziffer ist der Auftragsverarbeiter lediglich zur Duldung und Mitwirkung bei einer anlasslosen Vor-Ort-Prüfung pro Kalenderjahr verpflichtet. Der Aufwand einer anlasslosen Vor-Ort-Prüfung ist für den Auftragsverarbeiter grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

5.2.4 Wenn und solange der Auftragsverarbeiter den Nachweis über die Erfüllung seiner Pflichten, insbesondere die Umsetzung der TOM sowie ihrer Wirksamkeit, durch geeignete Nachweise erbringt, behält er sich das Recht vor die anlasslose Vor-Ort-Prüfung dieses Abschnitts abzulehnen. Geeignete Nachweise können insbesondere genehmigte Verhaltensregeln im Sinne von Art. 40 DSGVO oder ein genehmigtes Zertifizierungsverfahren im Sinne von Art. 42 DSGVO sein. Beide Parteien einigen sich darauf, dass auch die Vorlage von Testaten oder Berichten unabhängiger Instanzen, ein schlüssiges Datensicherheitskonzept oder eine geeignete Zertifizierung durch ein IT-Sicherheits- und Datenschutzaudit als geeignete Nachweise anerkannt werden.

6. Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter hat die Sicherheit gemäß Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen. Die einzelnen Maßnahmen dokumentiert der Auftragnehmer in einem Maßnahmenkonzept sie Anhang 1..

2.2. 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.

2.3. 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.

7. Unterauftragsverhältnisse

7.1 Unterauftragsverhältnisse im Sinne dieses Vereinbarungs sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung, wie in Ziffer 1.2.1. beschrieben, aufweisen. Auf die aktuellen Unterauftragsnehmer/innen des Auftragsverarbeiters kann über die Software zugegriffen werden (derzeit in „Einstellungen" > „Support" > „Paket & Rechnung" > „Datenschutzinformationen"). Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung, die Inanspruchnahme von Telekommunikationsdienstleistungen, Benutzerservice oder Kundenbeziehungsmanagement sowie sonstige Maßnahmen zur Gewährleistung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen, sind nicht erfasst. Die Pflicht des Auftragsverarbeiters, auch in diesen Fällen für die Beachtung von Datenschutz und Datensicherheit gemäß einschlägiger Rechtsvorschriften zu sorgen, bleibt unberührt.

7.2 Die Beauftragung von Unterauftragnehmern / Unterauftragnehmerinnen bei der Verarbeitung oder Nutzung personenbezogener Daten ist grundsätzlich nur mit einer Genehmigung vom Verantwortlichen gestattet. Für die zum Zeitpunkt des Vertragsschlusses innerhalb von Personio aufgezählten Unterauftragnehmer/innen gilt diese Genehmigung als erteilt.

7.3 Der Auftragsverarbeiter kann Unterauftragnehmer/innen herausnehmen oder neue hinzufügen. Der Auftragsverarbeiter informiert den für die Verarbeitung Verantwortlichen in Textform durch aktive Benachrichtigung (E-Mail), wenn er beabsichtigt, eine/n Unterauftragnehmer/in herauszunehmen oder eine/n neue/n zu beauftragen. Erhebt der für die Verarbeitung Verantwortliche innerhalb von 14 Tagen nach Erhalt der Mitteilung keinen begründeten Einspruch aus Datenschutzgründen in Textform (einschließlich E-Mail), so gilt dies als Zustimmung zu der Änderung. Können die Parteien im Falle eines Widerspruchs keine Einigung erzielen, so kann der Auftragsverarbeiter die Vereinbarung mit sofortiger Wirkung kündigen.

7.4 Erteilt der Auftragsverarbeiter Aufträge an Unterauftragnehmer/innen, so obliegt es dem Auftragsverarbeiter, ihre datenschutzrechtlichen Pflichten aus diesem Vereinbarung auf die Unterauftragnehmer/innen zu übertragen und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 3 DSGVO mit diesen abzuschließen. Der Auftragsverarbeiter bleibt für jede Handlung oder Unterlassung seiner Unterauftragnehmer/innen verantwortlich.

8. Betroffenenrechte

8.1 Richtet sich ein/e Betroffene/r an den Auftragsverarbeiter mit einer Forderung aus Kapitel III der DSGVO im Hinblick auf die Rechte der betroffenen Personen, dann wird der Auftragnehmer die betroffene Person an den Verantwortlichen verweisen, sofern eine Zuordnung an den Verantwortlichen nach Angabe der betroffenen Personen möglich ist.

8.2 Der Verantwortliche erkennt an, dass die Software eine umfassende Selbstverwaltung seiner personenbezogenen Daten ermöglicht, um ihn bei der Erfüllung seiner Pflichten nach der DSGVO (einschließlich seiner Pflichten zur Beantwortung von Anfragen der betroffenen Personen) zu unterstützen. Soweit der Verantwortliche nicht in der Lage ist, eine Anfrage eigenständig zu bearbeiten, leistet der Auftragsverarbeiter angemessene Unterstützung.

8.3 Der Auftragnehmer haftet nicht, sofern das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird und dies einzig von diesem verschuldet ist.

9. Informations- und Mitteilungspflichten

Der Auftragsverarbeiter benachrichtigt den Verantwortlichen unverzüglich, sobald er von einer Verletzung des Schutzes personenbezogener Daten erfährt, die die personenbezogenen Daten des Verantwortlichen betrifft. Die Benachrichtigung erfolgt im Einklang mit Artikel 33 der DSGVO.

10. Herausgabe und Löschung von Daten

10.1 Mit Beendigung der Auftragsverarbeitung hat der Auftragsverarbeiter die übermittelten personenbezogenen Daten gemäß den nachfolgenden Ziffern herauszugeben. In der Regel ist die Auftragsverarbeitung mit Vertragsende des Vertrages beendet.

10.2 Der Auftragsverarbeiter ist verpflichtet, die eingebrachten personenbezogenen Daten für einen Zeitraum von 30 Tagen nach Vertragsende aufzubewahren. Der Verantwortliche ist berechtigt, jederzeit bis zum Ablauf dieser Frist in Textform die Herausgabe der personenbezogenen Daten in einem maschinenlesbaren Format oder die Löschung der gespeicherten personenbezogenen Daten zu verlangen oder, sofern möglich, die Daten direkt aus der Software herunterzuladen. Der Verantwortliche ist allein für den rechtzeitigen Export seiner Daten verantwortlich.

10.3 Erteilt der Verantwortliche dem Auftragsverarbeiter eine verbindliche Löschungsweisung in Textform, so ist der Auftragsverarbeiter berechtigt, auch vor Ablauf der Aufbewahrungsfrist gemäß Ziffer 10.2, die Datenlöschung durchzuführen. Hiervon ausgenommen sind lediglich die Daten, hinsichtlich derer der Auftragsverarbeiter gesetzlich zur Aufbewahrung verpflichtet ist.

10.4 Sollte der Verantwortliche bis zum Ablauf der Frist gemäß Ziffer 10.2 weder die herauszugebenden Daten angefordert noch die Löschung dieser verlangt haben, ist der Auftragsverarbeiter verpflichtet, diese Daten zu löschen.

11. Haftung

11.1 Beide Parteien haften gemäß Art. 82 DSGVO für Schäden, die durch einen Verstoß gegen dieses Vereinbarung oder die DSGVO verursacht werden.

11.2 Sind gemäß Art. 82 Abs. 4 DSGVO beide Parteien für Ansprüche Betroffener oder Dritter verantwortlich, so haftet der Verantwortliche allein für den Schaden, es sei denn, dass ein Teil des Gesamtschadens dem Auftragsverarbeiter zuzurechnen ist. Der Verantwortliche trägt die Beweislast dafür, dass der Schaden nicht auf Umstände zurückzuführen ist, die er zu vertreten hat.

11.3 Etwaige Haftungsbeschränkungen in diesem Vereinbarung gelten nicht bei Vorsatz oder grober Fahrlässigkeit oder bei Schäden aus der Verletzung von Leben oder Körper.

11.4 Im Übrigen richtet sich die Haftung nach dem Vertrag.

12. Schlussbestimmungen

12.1 Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der anderen Partei auch über die Beendigung des Vertrags hinaus vertraulich zu behandeln. Dies gilt insbesondere auch für den Inhalt dieses Vereinbarungs sowie für alle im Rahmen des Datenschutzaudits zur Verfügung gestellten Unterlagen, Nachweise etc. Bestehen Zweifel, ob eine Information der Geheimhaltung unterliegt, so ist sie bis zur schriftlichen Freigabe durch die andere Partei vertraulich zu behandeln.

12.2 Änderungen und Ergänzungen dieses Vereinbarungs und aller seiner Bestandteile - einschließlich etwaiger Zusicherungen des Auftragsverarbeiters - erfolgen gemäß der DSGVO in Textform (einschließlich E-Mail), die auch in elektronischer Form erfolgen kann, und erfordern einen ausdrücklichen Hinweis darauf, dass diese Bedingungen geändert oder ergänzt wurden. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Die Parteien vereinbaren, dass Anpassungen dieses Vereinbarungs in einem elektronischen Format gemäß Art. 28 Abs. 9 DSGVO erfolgen können.

12.3 Änderungen und Ergänzungen dieses Vereinbarungs und aller seiner Bestandteile - einschließlich etwaiger Zusicherungen des Auftragsverarbeiters - erfolgen gemäß der DSGVO in Textform (einschließlich E-Mail), die auch in elektronischer Form erfolgen kann, und erfordern einen ausdrücklichen Hinweis darauf, dass diese Bedingungen geändert oder ergänzt wurden. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Die Parteien vereinbaren, dass Anpassungen dieses Vereinbarungs in einem elektronischen Format gemäß Art. 28 Abs. 9 DSGVO erfolgen können.

12.4 Es gilt das Recht der Bundesrepublik Deutschland. Das UN-Übereinkommen über Verträge über den internationalen Warenkauf (CISG) ist nicht anwendbar. Ausschließlicher Gerichtsstand für alle Streitigkeiten im Zusammenhang mit dieser VereinbarungVereinbarungist, soweit zulässig, Chemnitz.

12.5 Dieses Vereinbarung ersetzt alle vorherigen oder gleichzeitigen Zusicherungen, Absprachen, Vereinbarungen, Verträge oder Mitteilungen zwischen dem Verantwortlichen und dem Auftragsverarbeiter, ob schriftlich oder mündlich, in Bezug auf den Gegenstand dieses Vereinbarungs, es sei denn die Parteien haben vor dem 08. August 2023 einen Auftragsverarbeitungsvertrag geschlossen.

12.6 Diese Vereinbarung Vereinbarungersetzt alle vorherigen oder gleichzeitigen Zusicherungen, Absprachen, Vereinbarungen, Verträge oder Mitteilungen zwischen dem Verantwortlichen und dem Auftragsverarbeiter, ob schriftlich oder mündlich, in Bezug auf den Gegenstand dieses Vereinbarungs, es sei denn die Parteien haben vor dem xxxx einen Auftragsverarbeitungsvertrag geschlossen.

Anhang 1: TECHNISCHE-ORGANISATORISCHE MASSNAHMEN

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind. Der Auftragsverarbeiter stellt sicher, dass folgende Angaben umgesetzt werden:

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

1.1 Zutrittskontrolle

Maßnahmen, die einen unbefugten Zutritt zu Datenverarbeitungsanlagen verhindern

Schlüsselverwaltung für Mitarbeiter; geregelter Zutritt zu den Büroräumen

Regelung für Besucher und Wartungspersonal

1.2 Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungsanlagen von Unbefugten genutzt werden können

Regelung des Zugangs zu den Datenverarbeitungssystemen über ein Benutzer- und Berechtigungskonzept („Least Privilege-Prinzip“)

Vergabe von personalisierten Benutzer-Accounts mit entsprechenden Kennwort-Richtlinien (minimale Kennwort-Länge 10 Zeichen, Komplexitätsanforderungen, regelmäßige Änderung)

Sperren des Zugangs bei zehn fehlerhaften Anmelde-Versuchen

Sperren der Arbeitsstationen bei Verlassen des Arbeitsplatzes (automatisch nach 15 Minuten oder manuelles Sperren mit Reaktivierungskennwort)

Dokumentation und sichere Aufbewahrung der Administrator-Zugänge

Protokollierung der An- und Abmeldevorgänge

Einsatz von Firewall (inkl. Intrusion Prevention System), Spamfilter und Antivirus-Software

Verschlüsselung mobiler Datenträger/Smartphones

1.3 Zugriffskontrolle

Maßnahmen, die unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems verhindern

Vergabe von Zugriffsrechten nach Benutzergruppen

Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte („Least Privilege-Prinzip“)

Jährliche Überprüfung der Zugriffskontrollen

Vernichtung nicht mehr benötigter, schriftlicher Unterlagen nach DIN 66399 Sicherheitsstufe P3 (Papier)

Nicht-reversible Löschung/Vernichtung elektronischer Datenträger nach Ausmusterung

1.4 Trennungskontrolle

Maßnahmen für die getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

Mandantenfähige IT-Systeme

Trennung von Entwicklungs- und Produktionsumgebung

Zugriffsberechtigungen nach funktioneller Zuständigkeit

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen

Nicht auftragsrelevant

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

2.1 Weitergabekontrolle

Maßnahmen, die unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport verhindern

Weitergabe der Daten auf elektronischem Weg entsprechend den Möglichkeiten des Auftraggebers

Fernwartungskonzept

Protokollierung von Datenübertragung oder Datentransport

Verschlüsselte Datenverbindungen (VPN, SFTP, HTTPS)

2.2 Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

Regelung organisatorischer Zuständigkeiten

Systemseitige Protokollierung

Regelung der Zugriffsbefugnisse auf Protokolldaten

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

3.1 Verfügbarkeitskontrolle

Maßnahmen zum Schutz vor zufälliger oder mutwilliger Zerstörung bzw. Verlust

Redundante Datenspeicherung (z.B. RAID)

Backup-Internetanbindung

Unterbrechungsfreie Stromversorgung (USV)

Feuerlöscher/Feuermelder

Backup-Strategie

Gesicherte Aufbewahrung für Sicherungsmedien (z.B. feuerfester/einbruchsicherer Tresor)

Regelmäßige Installation von Sicherheitsupdates

Klimatisierter Serverraum

Meldewege und Notfallpläne

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Cloud-Services

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

4.1 Datenschutz-Management

Maßnahmen, die gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist

Richtlinien/Anweisungen zur Gewährleistung von technisch-organisatorischen Maßnahmen zur Datensicherheit

Bestellung eines Datenschutzbeauftragten

Verpflichtung zur Vertraulichkeit der Mitarbeiter (Datengeheimnis)

Hinreichende Schulung der Mitarbeiter in Datenschutzangelegenheiten

Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DS-GVO)

Durchführen von Datenschutzfolgeabschätzungen, soweit erforderlich (Art. 35 DS-GVO)

Periodische Prüfung durch Datenschutzbeauftragten

4.2 Incident-Response-Management

Maßnahmen, die gewährleisten, dass im Fall von Datenschutzverstößen ein Meldeprozess ausgelöst wird

Meldeprozess für Vertrags- und Datenschutzverletzungen gegenüber dem Auftraggeber nach Art. 28 Abs. 3 Satz 3 sowie Art. 33 und Art. 34 DS-GVO

Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DS-GVO gegenüber den Aufsichtsbehörden

Unterstützung für Auftraggeber im Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DS-GVO gegenüber den Aufsichtsbehörden (Art 33 DS-GVO)

4.3 Datenschutzfreundliche Voreinstellungen

Maßnahmen, die sicherstellen, dass von vornherein möglichst wenig Daten erhoben, gespeichert und geteilt werden

Datenschutzfreundliche Technikgestaltung („Privacy by design“)

Datenschutzfreundliche Voreinstellungen („Privacy by default“)

4.4 Auftragskontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten nur entsprechend der Weisungen des Auftraggebers verarbeitet werden

Subunternehmen mit schriftlichen Datenschutzvereinbarungen nach Art. 28 DS-GVO

Vereinbarung zur Auftragsverarbeitung mit Regelungen zu Rechten und Pflichten des Auftragnehmers und Auftraggebers

Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern

Verpflichtung der Mitarbeiter auf das Datengeheimnis

Formalisiertes Auftragsmanagement

Standardisiertes Vertragsmanagement zur Kontrolle von Dienstleistern