



Auftragsverarbeitung gemäß Art. 28 DS-GVO

Vereinbarung

zwischen der

NAME

Straße

PLZ Ort

- Verantwortlicher - nachstehend Auftraggeber genannt -

und der

o-byte.com GmbH & Co. KG

Urbanstraße 12

48143 Münster

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsverarbeitungsverhältnis eingegangen. Um die sich hieraus ergebenden Rechte und Pflichten gemäß den Vorgaben der europäischen Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG - DSGVO), und des Bundesdatenschutzgesetzes (BDSG) zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

I. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Vertrages

ist der Vertrieb von EDV- und Telekommunikationsanlagen (Software, Hardware, und Services).
Sowie die Instandhaltung und Installation sowie Support der o.g. Anlagen. (Support)

ist das Hosting einer virtuellen Telekommunikationsanlage im Rechenzentrum

ist die Verwaltung, Konfiguration und Service von Telekommunikationsanlagen in einem entsprechenden Cloud-System.

ist der Vertrieb und Service zu Microsoft Produkten und deren Zusätze.

Der genaue Umfang ist der Auftragsbestätigung zu entnehmen.

(2) Dauer

Der Auftrag wird unbefristet erteilt. Er kann von beiden Parteien mit einer Frist von 2 Wochen zum Monatsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Der Auftragnehmer stellt dem Auftraggeber eine Support-, Installations- und oder Betriebsleistung zur Verfügung. Im Rahmen einer Leistungsvereinbarung (Hauptvertrag) nimmt der Auftragnehmer Zugriff auf die Systeme des Auftraggebers, um für den ordnungsgemäßen Betrieb zu unterstützen. Im Rahmen der Tätigkeiten des Auftragnehmers ist nicht ausgeschlossen, dass der Auftragnehmer Zugriff auf personenbezogenen Daten des Auftraggebers erhält.

Der Auftragnehmer stellt dem Auftraggeber eine gehostete Telefonanlage (Starface / JTel) zur Verfügung. Im Rahmen des Auftrages können weitere Dienstleistungen (z. B. Support) gemäß der Leistungsbeschreibung durchgeführt werden. Unter diesen Punkt fallen auch Cloud Telefonanlagen und Vertragsspezifische Daten im Bereich der vertriebenen Software.

Der Auftragnehmer stellt dem Auftraggeber, dem Hauptvertrag entsprechend, Hard- und Software verschiedener Hersteller zur Verfügung und führt, wenn angegeben, Installations-, Konfigurations- und Supportleistungen diesbezüglich zur Verfügung. Dabei kann es notwendig sein, auf personenbezogene Daten zuzugreifen.

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. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

Das angemessene Schutzniveau in Deutschland ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);

(2) Art der Daten

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

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail, Verbindungsdaten)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Vertragsabrechnungs- und Zahlungsdaten
- Personalisierte Lizenzdaten
- Zugangsdaten

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Geschäftspartner
- Beschäftigte
- Lieferanten
- Ansprechpartner
- Und alle anderen Arten von möglichen Nutzern einer EDV oder Kommunikations-Anlage

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 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 [Einzelheiten in Anlage I].

(3) 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

(1) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

(2) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 28 und 29 DS-GVO ausübt.

Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt. Als Datenschutzbeauftragter des Auftragnehmers ist bestellt: secom IT GmbH, vertreten durch Marc Friedrich, Nienburger Straße 9a, 27232 Sulingen, Tel.: 04271 1000 412, E-Mail: Datenschutz@secom-it.de.

- (3) Die Wahrung der Vertraulichkeit gemäß Art. 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 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.
- (4) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO [Einzelheiten in Anlage I].
- (5) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- (6) 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.
- (7) 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.
- (8) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.
- (9) 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.

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) grundsätzlich nur dann beauftragen, wenn er selbst sichergestellt hat, dass der Unterauftragnehmer die nötigen gesetzlichen Anforderungen erfüllt. Die eingesetzten Unterauftragnehmer sind in der Anlage 2 aufzuführen.

(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 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).

(4) Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen 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-Folgeabschätzung
- e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Für Unterstützungsleistungen nach 8.(1). d) und e) sowie Unterstützungsleistungen die nicht in der Leistungsbeschreibung enthalten oder 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 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 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. Sonstiges

- (1) Die Haftung der Vertragsparteien richtet sich nach den gesetzlichen Vorschriften.
- (2) Der Auftragnehmer stellt den Auftraggeber von Haftungsansprüchen Dritter frei, die ihm aus Fehlleistungen des Auftragnehmers entstehen.
- (3) Die Einrede des Zurückbehaltungsrechts wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen
- (4) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts und der Regelungen des IPR. Als Gerichtsstand wird Münster vereinbart.

10. Schlussbestimmungen

- (1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragsverarbeiters - bedürfen einer schriftlichen Vereinbarung 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.
- (2) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich die Vereinbarung als lückenhaft erweist.

Datum

Auftraggeber

Datum

Auftragnehmer

Anlage Ia – Technisch-organisatorische Maßnahmen Support

M.1 Maßnahmen zur Vertraulichkeit

M.1.1 Beschreibung der Zutrittskontrolle:

- Einsatz einer Alarmanlage
- Protokollierung der Besucher (z.B. Besucherbuch)
- Bewegungsmelder
- Biometrische Zugangssperren (z.B. Fingerabdruckleser)
- Chipkarten-/Transponder-Schließsystem
- Besucherkontrolle am Empfang
- Manuelles Schließsystem mit Schließzylinder
- Personenkontrolle beim Pförtner
- Schließsystem mit PIN Codesperre
- Schlüsselregelung mit Dokumentation der Schlüssel (z.B. Schlüsselbuch)
- Videoüberwachung der Zugänge

Erläuterungen: keine

M.1.2 Beschreibung der Zugangskontrolle:

- Authentifikation mit Benutzer + Passwort
- Benutzerberechtigungen verwalten (z.B. bei Eintritt, Änderung, Austritt)
- Einsatz von Firewalls zum Schutz des Netzwerkes
- Einsatz von Mobile Device Management
- Sorgfältige Auswahl von Reinigungspersonal und Sicherheitspersonal
- Sperren von externen Schnittstellen (z.B. USB-Anschlüsse)
- Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren (wenn technisch möglich)

Erläuterungen: keine

M.1.3 Beschreibung der Zugriffskontrolle:

- Erstellen und Einsatz eines Berechtigungskonzepts
- Sichere Löschung von Datenträgern vor deren Wiederverwendung (z.B. durch mehrfaches Überschreiben)
- Einsatz von Aktenvernichtern (min. Sicherheitsstufe 3 und Schutzklasse 2)
- Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit DIN 66399 Zertifikat)
- Passwortrichtlinie inkl. Länge und Komplexität
- Sichere Aufbewahrung von Datenträgern
- Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren (wenn technisch möglich)
- Verschlüsselung von Smartphones mit dem Stand der Technik entsprechenden Verfahren

Erläuterungen: keine

M.1.4 Beschreibung der Weitergabekontrolle:

- E-Mail-Verschlüsselung mit S/MIME oder PGP Verfahren (oder anderen, dem Stand der Technik entsprechenden Verfahren)
- Sichere Transportbehälter und -verpackungen
- Einrichtungen von VPN-Tunneln zur Einwahl ins Netzwerk von außen
- Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet

Erläuterungen: keine

M.1.5 Beschreibung des Trennungsgebots:

- Logische Mandantentrennung (softwareseitig)
- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Trennung von Produktiv- und Testsystem

Erläuterungen: keine

M.1.6 Beschreibung der Pseudonymisierung:

- Verwendung von Kennziffern für Kunden oder Personal anstatt Namen
- Trennung von Kontaktdaten und anderen Daten
- Trennung von Kundenstammdaten und Auftragsdaten

Erläuterungen: keine

M.1.7 Beschreibung der Verschlüsselung:

- Verschlüsselte Datenspeicherung (z.B. Dateiverschlüsselung nach AES256 Standard)
- Verschlüsselte Datenübertragung (z.B. VPN, verschlüsselte Internetverbindungen mittels TLS/SSL)

Erläuterungen: keine

M.2 Maßnahmen zur Integrität

M.2.1 Beschreibung der Eingabekontrolle:

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe.

Erläuterungen: keine

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

M.3.1 Beschreibung der Verfügbarkeitskontrolle:

- Einsatz von Antivirensoftware zum Schutz vor Malware sofern technisch möglich
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Erstellen eines Backup- & Recoverykonzepts
- Feuer- und Rauchmeldeanlagen
- CO2 Feuerlöschgeräte in Serverräumen
- Erstellung und Anwendung von IT-Notfallplänen
- Klimaanlage in Serverräumen
- Redundante Datenhaltung (z.B. gespiegelte Festplatten, RAID 1 oder höher, gespiegelter Serverraum)
- Schutzsteckdosenleisten in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- (USV) Unterbrechungsfreie Stromversorgung

Erläuterungen: keine

M.3.2 Beschreibung der Wiederherstellbarkeit:

- Regelmäßige und dokumentierte Datenwiederherstellungen
- IT-Notfallpläne und Wiederanlaufpläne

Erläuterungen: keine

M.4 Weitere Maßnahmen

M.4.1 Beschreibung der Auftragskontrolle:

- Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO.
- Benennung eines Datenschutzbeauftragten
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Schulungen aller zugriffsberechtigten Mitarbeiter. Regelmäßig stattfindende Nachschulungen.
- Verpflichtung auf die Vertraulichkeit gem. Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO

Erläuterungen: keine

M.4.2 Beschreibung des Managementsystems:

- Durchführung regelmäßiger interner Audits
- Incident-Response-System zur Nachvollziehbarkeit von Sicherheitsverstößen und Problemen
- Managementsystem zum Datenschutz
- Managementsystem zur Informationssicherheit (z.B. in Anlehnung an ISO 27001 oder VdS 3473)
- Durchführung regelmäßiger IT-Schwachstellenanalysen (z.B. Penetrationstest)
- Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. (Art. 25 Abs. 2 DS-GVO)
- Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen (z.B. audatis MANAGER, Privacy Guard)

Erläuterungen: keine

Anlage Ib – Technisch-organisatorische Maßnahmen Hosting

M.1 Maßnahmen zur Vertraulichkeit

M.1.1 Beschreibung der Zutrittskontrolle:

- Einsatz einer Alarmanlage
- Protokollierung der Besucher (z.B. Besucherbuch)
- Bewegungsmelder
- Biometrische Zugangssperren (z.B. Fingerabdruckleser)
- Chipkarten-/Transponder-Schließsystem
- Besucherkontrolle am Empfang
- Manuelles Schließsystem mit Schließzylinder
- Personenkontrolle beim Pförtner
- Schließsystem mit PIN Codesperre
- Schlüsselregelung mit Dokumentation der Schlüssel (z.B. Schlüsselbuch)
- Videoüberwachung der Zugänge

Erläuterungen: keine

M.1.2 Beschreibung der Zugangskontrolle:

- Authentifikation mit Benutzer + Passwort
- Benutzerberechtigungen verwalten (z.B. bei Eintritt, Änderung, Austritt)
- Einsatz von Firewalls zum Schutz des Netzwerkes
- Einsatz von Mobile Device Management
- Sorgfältige Auswahl von Reinigungspersonal und Sicherheitspersonal
- Sperren von externen Schnittstellen (z.B. USB-Anschlüsse)
- Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren

Erläuterungen: keine

M.1.3 Beschreibung der Zugriffskontrolle:

- Erstellen und Einsatz eines Berechtigungskonzepts
- Sichere Löschung von Datenträgern vor deren Wiederverwendung (z.B. durch mehrfaches Überschreiben)
- Einsatz von Aktenvernichtern (min. Sicherheitsstufe 3 und Schutzklasse 2)
- Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit DIN 66399 Zertifikat)
- Passwortrichtlinie inkl. Länge, Komplexität und Wechselhäufigkeit
- Sichere Aufbewahrung von Datenträgern
- Verschlüsselung von Datenträgern mit dem Stand der Technik entsprechenden Verfahren
- Verschlüsselung von Smartphones mit dem Stand der Technik entsprechenden Verfahren

Erläuterungen: keine

M.1.4 Beschreibung der Weitergabekontrolle:

- E-Mail-Verschlüsselung mit S/MIME oder PGP Verfahren (oder anderen, dem Stand der Technik entsprechenden Verfahren)
- Sichere Transportbehälter und -verpackungen
- Einrichtungen von VPN-Tunneln zur Einwahl ins Netzwerk von außen
- Einsatz von SSL-/TLS-Verschlüsselung bei der Datenübertragung im Internet

Erläuterungen: keine

M.1.5 Beschreibung des Trennungsgebots:

- Logische Mandantentrennung (softwareseitig)
- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Trennung von Produktiv- und Testsystem

Erläuterungen: keine

M.1.6 Beschreibung der Pseudonymisierung:

- Verwendung von Kennziffern für Kunden oder Personal anstatt Namen
- Trennung von Kontaktdaten und anderen Daten
- Trennung von Kundenstammdaten und Auftragsdaten

Erläuterungen: keine

M.1.7 Beschreibung der Verschlüsselung:

- Verschlüsselte Datenspeicherung (z.B. Dateiverschlüsselung nach AES256 Standard)
- Verschlüsselte Datenübertragung (z.B. VPN, verschlüsselte Internetverbindungen mittels TLS/SSL)

Erläuterungen: keine

M.2 Maßnahmen zur Integrität

M.2.1 Beschreibung der Eingabekontrolle:

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Personenbezogene Zugriffsrechte zur Nachvollziehbarkeit der Zugriffe.

Erläuterungen: keine

M.3 Maßnahmen zur Verfügbarkeit und Belastbarkeit

M.3.1 Beschreibung der Verfügbarkeitskontrolle:

- Einsatz von Antivirensoftware zum Schutz vor Malware
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Erstellen eines Backup- & Recoverykonzepts
- Feuer- und Rauchmeldeanlagen
- CO2 Feuerlöschgeräte in Serverräumen
- Erstellung und Anwendung von IT-Notfallplänen
- Klimaanlage in Serverräumen
- Redundante Datenhaltung (z.B. gespiegelte Festplatten, RAID 1 oder höher, gespiegelter Serverraum)
- Schutzsteckdosenleisten in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- (USV) Unterbrechungsfreie Stromversorgung

Erläuterungen: keine

M.3.2 Beschreibung der Wiederherstellbarkeit:

- Regelmäßige und dokumentierte Datenwiederherstellungen
- IT-Notfallpläne und Wiederanlaufpläne

Erläuterungen: keine

M.4 Weitere Maßnahmen

M.4.1 Beschreibung der Auftragskontrolle:

- Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Abschluss einer Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO.
- Benennung eines Datenschutzbeauftragten
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Schulungen aller zugriffsberechtigten Mitarbeiter. Regelmäßig stattfindende Nachschulungen.
- Verpflichtung auf die Vertraulichkeit gem. Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO

Erläuterungen: keine

M.4.2 Beschreibung des Managementsystems:

- Durchführung regelmäßiger interner Audits
- Incident-Response-System zur Nachvollziehbarkeit von Sicherheitsverstößen und Problemen
- Managementsystem zum Datenschutz
- Managementsystem zur Informationssicherheit (z.B. in Anlehnung an ISO 27001 oder VdS 3473)
- Durchführung regelmäßiger IT-Schwachstellenanalysen (z.B. Penetrationstest)
- Einsatz von Software mit datenschutzfreundlichen Voreinstellungen gem. (Art. 25 Abs. 2 DS-GVO)
- Einsatz softwaregestützter Tools zur Einhaltung der datenschutzrechtlichen Anforderungen (z.B. audatis MANAGER, Privacy Guard)

Erläuterungen: Keine

Anlage 2 Unterauftragsverhältnisse

| Firma Unterauftragnehmer | Anschrift/Land | Leistung |
|------------------------------|--|---|
| kzm GmbH | Kemperallee 15 40668 Meerbusch Deutschland | Support-Dienstleistungen |
| STARFACE GmbH | Adlerstraße 61 76137 Karlsruhe Deutschland | Support-Dienstleistungen Cloud-Dienstleister |
| jtel GmbH | Valentin-Linhof-Straße 2 81829 München Deutschland | Support-Dienstleistungen Cloud-Dienstleister |
| Gamma Communications GmbH | Ziegeleistraße 2 95145 Oberkotzau Deutschland | Support-Dienstleistungen Cloud-Dienstleister |
| Microsoft Corporation | One Microsoft Way Redmond, WA 98052- 6399 USA | Support-Dienstleistungen Cloud-Dienstleister |

Anlage 3 Ansprechpartner

Datenschutzbeauftragter/-ansprechpartner des Auftragnehmers

Name: secom IT GmbH, vertreten durch Herrn Marc Friedrich

Tel.: 04271/9473 800

Email: datenschutz@secom-it.de

Adresse: Nienburger Straße 9d, 27232 Sulingen

Datenschutzbeauftragter/-ansprechpartner des Auftraggebers

Name: _____

Tel.: _____

Email: _____

Wenn abweichend, Adresse: _____

Weisungsbefugte des Auftraggebers

Name: _____

Funktion: _____

Tel.: _____

Email: _____

Name: _____

Funktion: _____

Tel.: _____

Email: _____