

# Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Version 1.0 – Stand: 14.10.2026

zwischen

**dem Kunden** als Verantwortlichem im Sinne von Art. 4 Nr. 7 DSGVO

– nachstehend „Auftraggeber“ genannt –

und

**Marco Nitsche, codii**

Am alten Kiesberg 48, 16356 Ahrensfelde, Deutschland

als Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO

– nachstehend „Auftragnehmer“ genannt –

– gemeinsam „Parteien“, einzeln „Partei“ –

---

## Präambel

Der Auftragnehmer erbringt für den Auftraggeber Leistungen aus den Bereichen Hosting, E-Mail, Domainverwaltung, Programmierung sowie Wartung und Betreuung von IT-Systemen auf Grundlage eines gesonderten Vertrags bzw. einzelner Aufträge einschließlich der Allgemeinen Geschäftsbedingungen des Auftragnehmers (nachstehend „Hauptvertrag“). Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien, soweit der Auftragnehmer im Rahmen des Hauptvertrags personenbezogene Daten im Auftrag des Auftraggebers verarbeitet.

Dieser Vertrag gilt ausschließlich gegenüber Unternehmern im Sinne von § 14 BGB, juristischen Personen des öffentlichen Rechts und sonstigen Stellen, die als Verantwortliche im Sinne der DSGVO handeln. Begriffe werden im Sinne der Datenschutz-Grundverordnung (DSGVO) verwendet.

---

## § 1 Gegenstand, Art und Zweck der Verarbeitung

1. Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten, die der Auftraggeber dem Auftragnehmer im Rahmen des Hauptvertrags überlässt oder auf Systemen speichert, die der Auftragnehmer betreibt oder wartet (nachstehend „Auftraggeber-Daten“).
2. Die Verarbeitung umfasst je nach gebuchter Leistung insbesondere:
  - a. **Hosting:** Bereitstellung von Speicherplatz, Datenbanken und Rechenleistung für Websites und Webanwendungen des Auftraggebers auf vom Auftragnehmer betriebenen Servern;
  - b. **E-Mail:** Empfang, Speicherung, Filterung (Spam- und Virenprüfung) und Versand von E-Mails für Postfächer des Auftraggebers;
  - c. **Domainverwaltung:** Registrierung, Verwaltung und Übertragung von Domains einschließlich der Übermittlung von Inhaber- und Ansprechpartnerdaten an Registrare und Registrierungsstellen;
  - d. **Wartung und Betreuung:** Installation, Aktualisierung, Konfiguration, Überwachung, Datensicherung und Fehlerbehebung von Servern und Anwendungen (z. B. CMS, Shops), auch per Fernzugriff auf Systeme des Auftraggebers oder Dritter;
  - e. **Programmierung:** Entwicklung und Anpassung von Software und Websites, soweit dabei ein Zugriff auf Auftraggeber-Daten erfolgt oder nicht ausgeschlossen werden kann.

3. Der Auftragnehmer nimmt Auftraggeber-Daten grundsätzlich nicht gezielt zur Kenntnis. Ein Zugriff erfolgt nur, soweit er zur Erbringung der Leistung, insbesondere zur Wartung und Fehlerbehebung, erforderlich ist. Die Möglichkeit der Kenntnisnahme bei Betrieb und Wartung ist von diesem Vertrag erfasst.
4. Art der personenbezogenen Daten und Kategorien betroffener Personen ergeben sich aus **Anlage 1**.
5. Nicht Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten des Auftraggebers selbst (z. B. Ansprechpartner, Vertrags- und Abrechnungsdaten), die der Auftragnehmer zur Begründung, Durchführung und Abrechnung des Hauptvertrags in eigener Verantwortung verarbeitet.

## **§ 2 Dauer**

1. Dieser Vertrag beginnt mit seinem Abschluss und läuft auf unbestimmte Zeit. Er endet automatisch, wenn kein Hauptvertrag mehr besteht und der Auftragnehmer keine Auftraggeber-Daten mehr verarbeitet (einschließlich der Löschung nach § 11).
2. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

## **§ 3 Ort der Verarbeitung**

1. Die Verarbeitung erfolgt ausschließlich in einem Mitgliedstaat der Europäischen Union oder einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum.
2. Eine Verarbeitung in einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers in Textform und ist nur zulässig, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
3. Werden Systeme des Auftraggebers oder von ihm beauftragter Dritter gewartet, ist der Ort dieser Systeme Sache des Auftraggebers.

## **§ 4 Weisungsrecht des Auftraggebers**

1. Der Auftragnehmer verarbeitet Auftraggeber-Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, zu einer Verarbeitung verpflichtet. In diesem Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 lit. a DSGVO).
2. Die Weisungen werden anfänglich durch den Hauptvertrag und diesen Vertrag festgelegt. Der Auftraggeber kann sie danach in Textform (z. B. per E-Mail an [m.nitsche@codii.de](mailto:m.nitsche@codii.de)) ändern, ergänzen oder ersetzen. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.
3. Weisungen, die über den vereinbarten Leistungsumfang hinausgehen, werden als Antrag auf Leistungsänderung behandelt.
4. Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt, weist er den Auftraggeber unverzüglich darauf hin. Er ist berechtigt, die Umsetzung der Weisung auszusetzen, bis sie vom Auftraggeber bestätigt oder geändert wird.

## **§ 5 Pflichten des Auftragnehmers**

1. Der Auftragnehmer verarbeitet Auftraggeber-Daten nicht für eigene Zwecke. Kopien und Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind Datensicherungen, soweit sie zur ordnungsgemäßen Leistungserbringung erforderlich sind (vgl. Anlage 2).
2. Der Auftragnehmer erbringt die Leistungen derzeit persönlich und beschäftigt keine Mitarbeiter. Setzt er künftig Personen ein, die Zugang zu Auftraggeber-Daten haben, verpflichtet er diese vor Aufnahme ihrer Tätigkeit zur Vertraulichkeit, sofern sie keiner angemessenen gesetzlichen

Verschwiegenheitspflicht unterliegen, und weist sie in die einschlägigen Datenschutzvorschriften ein (Art. 28 Abs. 3 lit. b, Art. 29 DSGVO). Die Vertraulichkeitspflicht gilt auch nach Beendigung dieses Vertrags fort.

3. Der Auftragnehmer ist gesetzlich nicht zur Benennung eines Datenschutzbeauftragten verpflichtet. Ansprechpartner für Datenschutzfragen ist:

**Marco Nitsche, E-Mail: [m.nitsche@codii.de](mailto:m.nitsche@codii.de)**

4. Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde sowie über Ermittlungen anderer Behörden, soweit sie sich auf diesen Auftrag beziehen und die Information nicht untersagt ist.
5. Sollten Auftraggeber-Daten beim Auftragnehmer durch Pfändung, Beschlagnahme, ein Insolvenzverfahren oder sonstige Maßnahmen Dritter gefährdet werden, informiert der Auftragnehmer den Auftraggeber unverzüglich. Er weist die Beteiligten darauf hin, dass die Verantwortung für die Daten beim Auftraggeber liegt.
6. Der Auftragnehmer erteilt Dritten oder betroffenen Personen Auskünfte über Auftraggeber-Daten nur nach vorheriger Weisung des Auftraggebers oder soweit er gesetzlich dazu verpflichtet ist.

## § 6 Technische und organisatorische Maßnahmen

1. Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste zu gewährleisten. Die Maßnahmen sind in **Anlage 2** beschrieben und Bestandteil dieses Vertrags.
2. Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragnehmer darf sie durch gleichwertige oder bessere Maßnahmen ersetzen, solange das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert und dem Auftraggeber auf Anfrage mitgeteilt.
3. Der Auftragnehmer überprüft die Wirksamkeit der Maßnahmen regelmäßig (Art. 32 Abs. 1 lit. d DSGVO).
4. Dem Auftraggeber sind die Maßnahmen bekannt. Er prüft in eigener Verantwortung, ob sie für die Risiken der von ihm verarbeiteten Daten angemessen sind. Beabsichtigt der Auftraggeber, besondere Kategorien personenbezogener Daten (Art. 9, 10 DSGVO) oder Daten mit erhöhtem Schutzbedarf verarbeiten zu lassen, teilt er dies dem Auftragnehmer vorab mit. Zusätzlich erforderliche Maßnahmen werden gesondert vereinbart.

## § 7 Unterauftragsverarbeiter

1. Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) hinzuzuziehen (Art. 28 Abs. 2 DSGVO).
2. Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in der gesondert veröffentlichten **Liste der Unterauftragsverarbeiter** in ihrer jeweils aktuellen Fassung aufgeführt. Ihr Einsatz gilt mit Abschluss dieses Vertrags als genehmigt.
3. Der Auftragnehmer informiert den Auftraggeber mindestens **vier Wochen** vor der Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters in Textform (E-Mail) und aktualisiert die Liste. Der Auftraggeber kann der Änderung innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt. Ändert ein Unterauftragsverarbeiter seinerseits kurzfristig seine Unterauftragnehmer, informiert der Auftragnehmer den Auftraggeber, sobald er davon Kenntnis erlangt.
4. Im Falle eines Widerspruchs bemühen sich die Parteien um eine einvernehmliche Lösung. Kommt diese innerhalb von vier Wochen nicht zustande, kann jede Partei die betroffenen Leistungen des Hauptvertrags mit einer Frist von vier Wochen außerordentlich kündigen.

5. Der Auftragnehmer wählt Unterauftragsverarbeiter sorgfältig aus. Er schließt mit ihnen Verträge, die den Anforderungen von Art. 28 Abs. 4 DSGVO entsprechen und im Wesentlichen ein gleichwertiges Schutzniveau wie dieser Vertrag gewährleisten. Der Auftragnehmer haftet gegenüber dem Auftraggeber für die Einhaltung der Datenschutzpflichten durch seine Unterauftragsverarbeiter.
6. Keine Unterauftragsverhältnisse im Sinne dieses Paragraphen sind:
  - a. **Registrierungsstellen (Registries)** von Top-Level-Domains (z. B. DENIC eG für .de). Sie verarbeiten Domaininhaberdaten nach eigenen Registrierungsbedingungen in eigener Verantwortung;
  - b. Nebenleistungen wie Telekommunikations-, Post- und Transportdienste sowie reine Zertifizierungsstellen (CAs), die keinen Zugriff auf Auftraggeber-Daten haben;
  - c. Systeme, Software und Dienstleister, die der Auftraggeber selbst auswählt oder beauftragt (z. B. bei der Wartung externer Systeme).

## § 8 Unterstützung bei Betroffenenrechten und Pflichten des Auftraggebers

1. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen nach Kapitel III DSGVO (Art. 28 Abs. 3 lit. e DSGVO).
2. Wendet sich eine betroffene Person direkt an den Auftragnehmer, leitet dieser das Anliegen unverzüglich an den Auftraggeber weiter, sofern eine Zuordnung möglich ist. Der Auftragnehmer beantwortet solche Anfragen nicht selbst, es sei denn, der Auftraggeber weist ihn dazu an.
3. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation).

## § 9 Verletzungen des Schutzes personenbezogener Daten

1. Der Auftragnehmer meldet dem Auftraggeber eine Verletzung des Schutzes von Auftraggeber-Daten unverzüglich, möglichst innerhalb von **48 Stunden** nach Kenntniserlangung, in Textform.
2. Die Meldung enthält, soweit bekannt, insbesondere eine Beschreibung der Art der Verletzung, der betroffenen Datenkategorien und der ungefähren Zahl der betroffenen Personen und Datensätze, der wahrscheinlichen Folgen sowie der ergriffenen oder vorgeschlagenen Maßnahmen. Informationen, die noch nicht vorliegen, werden unverzüglich nachgereicht.
3. Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen, um die Daten zu sichern und mögliche nachteilige Folgen für die betroffenen Personen zu mindern. Er stimmt sich hierzu mit dem Auftraggeber ab.
4. Die Meldung an die Aufsichtsbehörde und die Benachrichtigung betroffener Personen (Art. 33, 34 DSGVO) obliegen dem Auftraggeber.

## § 10 Nachweise und Kontrollen

1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der Pflichten aus diesem Vertrag mit geeigneten Mitteln nach und stellt ihm auf Anfrage die hierfür erforderlichen Informationen zur Verfügung (Art. 28 Abs. 3 lit. h DSGVO). Als Nachweis dienen vorrangig schriftliche Auskünfte, die Dokumentation der technischen und organisatorischen Maßnahmen sowie die Auftragsverarbeitungsverträge und Nachweise der Unterauftragsverarbeiter.
2. Reichen diese Nachweise im Einzelfall nicht aus, kann der Auftraggeber Kontrollen einschließlich Inspektionen selbst oder durch einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer durchführen. Inspektionen sind mit einer Vorlaufzeit von mindestens **vier Wochen** anzumelden, finden

zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs statt und sind grundsätzlich auf einen Termin pro Kalenderjahr begrenzt, sofern kein konkreter Anlass besteht. Ein Prüfer, der in einem Wettbewerbsverhältnis zum Auftragnehmer steht, kann vom Auftragnehmer abgelehnt werden.

3. Die Rechenzentren werden nicht vom Auftragnehmer betrieben. Kontrollen der Rechenzentren richten sich nach den Bedingungen der jeweiligen Unterauftragsverarbeiter. Der Auftragnehmer stellt dem Auftraggeber deren Nachweise und Vertragsunterlagen auf Anfrage zur Verfügung.
4. Kontrollrechte von Aufsichtsbehörden bleiben unberührt.

## **§ 11 Löschung und Rückgabe**

1. Nach Beendigung der Leistungen löscht der Auftragnehmer alle Auftraggeber-Daten. Vorher kann der Auftraggeber die Herausgabe verlangen, soweit keine gesetzliche Pflicht zur Speicherung besteht (Art. 28 Abs. 3 lit. g DSGVO). Verlangt der Auftraggeber die Herausgabe nicht, löscht der Auftragnehmer die Daten innerhalb von **30 Tagen** nach Beendigung der Leistungen.
2. Die Herausgabe erfolgt in einem gängigen Format (z. B. Datei- und Datenbankexport, E-Mail-Postfächer im Standardformat) per sicherem Download oder auf einem sonstigen vereinbarten Weg.
3. Datensicherungen (Snapshots) werden im Rahmen der regulären Rotation überschrieben bzw. gelöscht, spätestens jedoch innerhalb von 30 Tagen nach Beendigung der Leistungen.
4. Der Auftraggeber kann die Löschung oder Herausgabe einzelner Daten jederzeit auch während der Vertragslaufzeit verlangen, soweit dies technisch möglich ist und vom Leistungsumfang umfasst ist.
5. Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, bewahrt der Auftragnehmer entsprechend den gesetzlichen Aufbewahrungsfristen auf.

## **§ 12 Pflichten des Auftraggebers**

1. Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung, insbesondere für die Zulässigkeit der Übermittlung der Daten an den Auftragnehmer, sowie für die Wahrung der Rechte betroffener Personen allein verantwortlich.
2. Der Auftraggeber informiert den Auftragnehmer unverzüglich und vollständig, wenn er Fehler oder Unregelmäßigkeiten in Bezug auf datenschutzrechtliche Bestimmungen feststellt.
3. Der Auftraggeber nennt dem Auftragnehmer einen Ansprechpartner für Datenschutzfragen und teilt Änderungen unverzüglich mit.
4. Soweit der Auftraggeber eigene Zugänge zu Systemen erhält (z. B. CMS, FTP, Postfächer), ist er für die sichere Verwahrung seiner Zugangsdaten und für die von ihm selbst vorgenommenen Verarbeitungen verantwortlich.

## **§ 13 Vergütung von Unterstützungsleistungen**

Unterstützungsleistungen nach § 8, § 9 Abs. 3, § 10 und § 11 Abs. 2 und 4, die über den Leistungsumfang des Hauptvertrags hinausgehen, vergütet der Auftraggeber nach dem jeweils gültigen Stundensatz des Auftragnehmers. Das gilt nicht, soweit der Aufwand auf einer Pflichtverletzung des Auftragnehmers oder seiner Unterauftragsverarbeiter beruht.

## **§ 14 Haftung**

1. Gegenüber betroffenen Personen haften die Parteien nach Art. 82 DSGVO.
2. Im Innenverhältnis gelten die Haftungsregelungen des Hauptvertrags bzw. der Allgemeinen Geschäftsbedingungen des Auftragnehmers, soweit Art. 82 DSGVO nicht zwingend etwas anderes bestimmt.

## § 15 Abschluss und Änderungen dieses Vertrags

1. Dieser Vertrag kommt in elektronischem Format im Sinne von Art. 28 Abs. 9 DSGVO zustande, indem der Auftraggeber ihm in Textform (z. B. per E-Mail) oder im Rahmen der Beauftragung unter Einbeziehung der Allgemeinen Geschäftsbedingungen des Auftragnehmers zustimmt. Eine Unterschrift ist nicht erforderlich. Der Auftragnehmer dokumentiert den Zeitpunkt der Zustimmung und die zugestimmte Version.
2. Änderungen dieses Vertrags teilt der Auftragnehmer dem Auftraggeber mindestens **sechs Wochen** vor ihrem Inkrafttreten in Textform mit. Widerspricht der Auftraggeber nicht innerhalb dieser Frist in Textform, gelten die Änderungen als genehmigt. Der Auftragnehmer weist in der Mitteilung gesondert auf die Bedeutung des Schweigens und auf die Widerspruchsfrist hin. Im Falle eines Widerspruchs gilt der Vertrag in der bisherigen Fassung fort. Jede Partei kann die betroffenen Leistungen des Hauptvertrags dann mit einer Frist von vier Wochen kündigen. Änderungen der Liste der Unterauftragsverarbeiter richten sich ausschließlich nach § 7.
3. Änderungen, die aufgrund zwingender gesetzlicher Vorgaben oder behördlicher Entscheidungen erforderlich werden, setzen die Parteien gemeinsam um.

## § 16 Schlussbestimmungen

1. Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrags vor, soweit sie den Datenschutz betreffen.
2. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt eine Regelung, die den Anforderungen von Art. 28 DSGVO entspricht und dem Gewollten am nächsten kommt.
3. Es gilt das Recht der Bundesrepublik Deutschland.
4. Ist der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen, ist ausschließlicher Gerichtsstand der Sitz des Auftragnehmers.

### Anlagen

- Anlage 1 – Art der Daten und Kategorien betroffener Personen
- Anlage 2 – Technische und organisatorische Maßnahmen (TOMs)
- Gesondert veröffentlicht: Liste der Unterauftragsverarbeiter (jeweils aktuelle Fassung)

---

## Anlage 1 – Art der Daten und Kategorien betroffener Personen

Gegenstand der Verarbeitung sind alle personenbezogenen Daten, die der Auftraggeber auf den vom Auftragnehmer betriebenen oder gewarteten Systemen speichert oder dem Auftragnehmer zur Leistungserbringung überlässt. Je nach Leistung sind dies insbesondere:

### Arten personenbezogener Daten

| Leistung                          | Typische Daten                                                                                                                                                                                                                        |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hosting, Websites, Webanwendungen | Inhalte der Website, Daten aus Kontakt- und Bestellformularen, Benutzerkonten (Name, E-Mail-Adresse, Passwort-Hashes), Kunden-, Bestell- und Vertragsdaten (z. B. in Shops), Kommentare, hochgeladene Dateien, Bild- und Videodateien |
| Server- und Protokolldaten        | IP-Adressen, Zeitstempel, aufgerufene URLs, Browser-/User-Agent-Informationen, Fehler- und Zugriffsprotokolle                                                                                                                         |

| Leistung                | Typische Daten                                                                                                                                                                  |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| E-Mail                  | Inhalte und Anhänge von E-Mails, Metadaten (Absender, Empfänger, Betreff, Zeitstempel, IP-Adressen), Adressbücher und Kalender, soweit gespeichert, Zugangsdaten für Postfächer |
| Domainverwaltung        | Name, Anschrift, E-Mail-Adresse und Telefonnummer von Domaininhabern sowie administrativen und technischen Ansprechpartnern                                                     |
| Wartung, Programmierung | alle Daten, die in den gewarteten oder entwickelten Systemen gespeichert sind und dabei zur Kenntnis gelangen können                                                            |

Besondere Kategorien personenbezogener Daten (Art. 9, 10 DSGVO) werden nur verarbeitet, wenn der Auftraggeber sie auf den Systemen speichert. In diesem Fall gilt § 6 Abs. 4.

### Kategorien betroffener Personen

- Besucher und Nutzer der Websites und Anwendungen des Auftraggebers
- Kunden, Interessenten und Geschäftspartner des Auftraggebers
- Beschäftigte, Mitglieder und Beauftragte des Auftraggebers
- Kommunikationspartner im E-Mail-Verkehr
- Domaininhaber und Ansprechpartner
- sonstige Personen, deren Daten der Auftraggeber auf den Systemen verarbeitet

## Anlage 2 – Technische und organisatorische Maßnahmen (TOMs) nach Art. 32 DSGVO

### Vorbemerkung zur Struktur der Verarbeitung

Der Auftragnehmer ist ein Einzelunternehmen ohne Mitarbeiter. Die Leistungen werden ausschließlich vom Inhaber persönlich erbracht. Die Hosting- und E-Mail-Dienste laufen auf einem virtuellen Server (VPS), den der Auftragnehmer bei einem Unterauftragsverarbeiter in einem Rechenzentrum in der EU angemietet hat. Physische Rechenzentrumssicherheit, Hardware, Stromversorgung und Netzanbindung verantwortet der Rechenzentrumsbetreiber nach dessen eigenen technischen und organisatorischen Maßnahmen, die Bestandteil seines Auftragsverarbeitungsvertrags mit dem Auftragnehmer sind. Betriebssystem, Dienste, Konfiguration und Datensicherung des VPS verantwortet der Auftragnehmer.

### 1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

#### 1.1 Zutrittskontrolle

- Rechenzentrum: Zutrittskontrolle durch den Rechenzentrumsbetreiber (u. a. elektronische Zutrittskontrolle, Videoüberwachung, Besucherregelung) gemäß dessen TOMs
- Arbeitsplatz des Auftragnehmers: Büro in privaten Räumlichkeiten, Zutritt nur für den Inhaber; keine Kundendaten in Papierform am Arbeitsplatz außer Abrechnungsunterlagen

#### 1.2 Zugangskontrolle

- Administrativer Zugang zum Server ausschließlich per SSH mit Passwort und zusätzlichem Einmalpasswort (OTP, Zwei-Faktor-Authentifizierung)
- Kunden-Zugänge per SFTP bzw. SSH mit Passwort; Anmeldung per SSH-Schlüssel ist auf Wunsch des Kunden möglich

- Zugang zum Kundenportal des Rechenzentrumsbetreibers und zu den Registrar-Konten mit starken, individuellen Passwörtern und Zwei-Faktor-Authentifizierung, soweit angeboten
- Zwei-Faktor-Codes (TOTP) für Admin-Zugänge werden auf einem durch Gerätesperre und Geräteverschlüsselung geschützten Smartphone verwaltet
- Bildschirmsperre an allen Arbeitsgeräten
- Firewall auf dem Server; nur die für die Dienste erforderlichen Ports sind erreichbar
- Automatischer Schutz gegen Brute-Force-Angriffe (Sperrung nach wiederholten Fehlversuchen)

### **1.3 Zugriffskontrolle**

- Ausschließlich der Inhaber verfügt über administrative Rechte
- Getrennte Zugänge pro Kunde (z. B. eigene Datenbank- und FTP-/SFTP-Benutzer, eigene Postfächer), Berechtigungen nach dem Minimalprinzip
- Zugangsdaten für Kunden werden auf getrenntem Weg bzw. verschlüsselt übermittelt
- Zugriff auf Kundendaten erfolgt nur, soweit er zur Wartung oder Fehlerbehebung erforderlich ist
- Bei der Wartung externer Systeme: Nutzung der vom Auftraggeber bereitgestellten Zugänge, Zugriff nur über verschlüsselte Verbindungen

### **1.4 Trennungskontrolle**

- Logische Trennung der Kundendaten auf dem Server (getrennte Verzeichnisse, Datenbanken, Benutzer und Postfächer)
- Entwicklung und Tests erfolgen grundsätzlich ohne Echtdaten bzw. mit Testdaten. Ist der Einsatz von Echtdaten ausnahmsweise erforderlich, geschieht dies nur nach Abstimmung mit dem Auftraggeber
- Abrechnungsdaten der eigenen Kunden werden getrennt von den Auftraggeber-Daten verarbeitet

### **1.5 Pseudonymisierung und Verschlüsselung**

- Die Pseudonymisierung von Daten innerhalb der Anwendungen des Auftraggebers obliegt dem Auftraggeber
- Verschlüsselung siehe Ziffer 2.1

## **2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)**

### **2.1 Weitergabekontrolle**

- Websites werden über HTTPS (TLS) ausgeliefert
- E-Mail-Abruf und -Einlieferung durch Nutzer (IMAP, POP3, SMTP-Submission) nur über TLS-verschlüsselte Verbindungen; Server-zu-Server-Übertragung per TLS, sofern die Gegenstelle dies unterstützt
- Administrative Zugriffe ausschließlich über verschlüsselte Verbindungen (SSH/SFTP, HTTPS)
- Keine Weitergabe von Auftraggeber-Daten an Dritte außer an genehmigte Unterauftragsverarbeiter oder auf Weisung des Auftraggebers

### **2.2 Eingabekontrolle**

- Protokollierung von Anmeldungen und administrativen Zugriffen auf dem Server (System- und Dienstprotokolle)
- Da ausschließlich der Inhaber administrativ tätig ist, sind Änderungen eindeutig zuordenbar

## **3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)**

- Physische Verfügbarkeit (Stromversorgung/USV, Klimatisierung, Brandschutz, redundante Netzanbindung) durch den Rechenzentrumsbetreiber gemäß dessen TOMs

- Regelmäßige Sicherung des gesamten Servers durch Snapshots beim Rechenzentrumsbetreiber; Wiederherstellung des Serverzustands aus einem Snapshot möglich
- Spam- und Virenfilter für E-Mails direkt auf dem Server
- Zeitnahes Einspielen von Sicherheitsupdates für Betriebssystem und Serverdienste
- Überwachung der Dienste und Ressourcen auf Verfügbarkeit
- Die Datensicherung von Inhalten, die der Auftraggeber selbst verwaltet, obliegt zusätzlich dem Auftraggeber, sofern im Hauptvertrag nichts anderes vereinbart ist

#### **4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)**

- Regelmäßige Überprüfung der Serverkonfiguration, der Zugänge und Berechtigungen; Entfernung nicht mehr benötigter Zugänge
- Verfolgung von Sicherheitshinweisen der eingesetzten Software und Reaktion auf bekannt gewordene Schwachstellen
- Auftragskontrolle: Abschluss von Auftragsverarbeitungsverträgen mit allen Unterauftragsverarbeitern; Datenverarbeitung ausschließlich in der EU/im EWR
- Dokumentation von Datenschutzvorfällen und der ergriffenen Maßnahmen

#### **5. Datensicherung und Verwahrung von Zugangsmitteln beim Auftragnehmer**

- Zwei-Faktor-Codes und Abrechnungsdaten der eigenen Kunden werden zusätzlich auf einem lokalen NAS gesichert, das nicht aus dem Internet erreichbar ist
- Auftraggeber-Daten aus Hosting und E-Mail werden nicht auf lokalen Geräten des Auftragnehmers gespeichert, außer vorübergehend, wenn dies im Einzelfall für Wartung, Migration oder Fehlerbehebung erforderlich ist. Solche Kopien werden nach Abschluss der Arbeiten gelöscht

#### **6. Löschung und Vernichtung**

- Löschung der Kundendaten auf dem Server nach Vertragsende gemäß § 11 des Vertrags
- Löschung bzw. Überschreiben von Snapshots im Rahmen der Rotation
- Defekte oder ausgesonderte Datenträger beim Rechenzentrumsbetreiber werden gemäß dessen TOMs vernichtet; eigene Datenträger des Auftragnehmers werden vor der Entsorgung sicher gelöscht oder physisch zerstört