Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

Kyvento

Thomas Jäger (Einzelunternehmen)
Schönberger Str. 29
61476 Kronberg im Taunus

(nachfolgend auch „**Auftragnehmer**“)

Der vorliegende Auftragsverarbeitungsvertrag gilt für die Verarbeitungsmaßnahmen personenbezogener Daten durch den Auftragnehmer, die gegenüber Kunden (nachfolgend „**Auftraggeber**“) in Erfüllung des Hauptvertrages erbracht werden.

Präambel

Der Auftragnehmer erbringt für den Auftraggeber Leistungen gemäß dem zwischen ihnen geschlossenen SaaS-Vertrag über die Software „Kyvento“ (im Folgenden: „**Hauptvertrag”**). Teil der Durchführung des Hauptvertrags ist die Verarbeitung von personenbezogenen Daten im Sinne der Datenschutzgrundverordnung („**DSGVO**”). Zur Erfüllung der Anforderungen der DSGVO an derartige Konstellationen schließen die Parteien den nachfolgenden Auftragsverarbeitungsvertrag (auch „**Vertrag**“), der mit Unterzeichnung bzw. Wirksamwerden des Hauptvertrages zustande kommt.

1. Gegenstand/Umfang der Beauftragung

(1) Im Rahmen der Zusammenarbeit der Parteien nach Maßgabe des Hauptvertrages hat der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers (nachfolgend „**Auftraggeberdaten**”). Diese Auftraggeberdaten verarbeitet der Auftragnehmer im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 8 und Art. 28 DSGVO.

(2) Klarstellung: „Auftraggeberdaten“ im Sinne dieses Vertrages sind alle personenbezogenen Daten, die der Auftragnehmer im Rahmen der Leistungserbringung für den Auftraggeber verarbeitet (einschließlich der Inhalte, die der Auftraggeber oder dessen Endnutzer in die Systeme des Auftragnehmers eingeben, sowie daraus generierter personenbezogener Ausgaben/Reports). Nicht als „Auftraggeberdaten“ gelten (i) rein technische Betriebs- und Sicherheitsprotokolle (z. B. System- und Zugriffsdaten), die der Auftragnehmer zur Gewährleistung der Informationssicherheit, zur Fehleranalyse und zur Stabilität des Dienstes verarbeitet, soweit diese Datenverarbeitung für die sichere Bereitstellung der Leistung erforderlich ist, sowie (ii) aggregierte, anonymisierte Statistiken ohne Personenbezug. Soweit Betriebs-/Sicherheitsprotokolle ausnahmsweise personenbezogene Daten enthalten, verarbeitet der Auftragnehmer diese ausschließlich zu den vorgenannten Zwecken und unter Anwendung angemessener Schutzmaßnahmen.

(3) Die Verarbeitung der Auftraggeberdaten durch den Auftragnehmer erfolgt in der in den Anlagen beschriebenen Art sowie in dem dort spezifizierten Umfang und Zweck. Der Kreis der von der Datenverarbeitung betroffenen Personen wird dargestellt. Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

(4) Ob die Leistungen des Auftragnehmers für die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO geeignet sind, bedarf einer Risikobewertung durch den Auftraggeber. Soweit der Auftraggeber dem Auftragnehmer besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO zur Verarbeitung überlässt oder deren Verarbeitung im Rahmen der beauftragten Leistungen erfolgt,

gilt: Die Verarbeitung erfolgt ausschließlich auf dokumentierte Weisung des Auftraggebers und nur im in diesem Vertrag sowie seinen Anlagen beschriebenen Umfang. Der Auftragnehmer wendet hierfür ein dem Risiko angemessenes, erhöhtes Schutzniveau an (insbesondere restriktive Berechtigungskonzepte/Need-to-know, Verschlüsselung bei Übertragung, Mandantentrennung, Protokollierung privilegierter Zugriffe und Maßnahmen zur Sicherstellung der Vertraulichkeit). Der Auftragnehmer unterstützt den Auftraggeber nach Maßgabe dieses Vertrages bei der Durchführung einer ggf. erforderlichen Datenschutz-Folgenabschätzung (Art. 35 DSGVO) und bei der Dokumentation der hierfür erforderlichen Informationen.

(5) Dem Auftragnehmer ist eine von den in den Anlagen genannten Verarbeitungen abweichende Verarbeitung von Auftraggeberdaten untersagt.

(6) Die Verarbeitung der Auftraggeberdaten findet grds. im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt.

(7) Eine Verarbeitung oder sonstige Übermittlung von Auftraggeberdaten in einem Drittland (außerhalb EU/EWR) oder eine Zugriffsmöglichkeit aus einem Drittland (z. B. Support/Administration) erfolgt nur mit vorheriger Zustimmung des Auftraggebers und nur unter Einhaltung der Anforderungen der Art. 44 bis 49 DSGVO.

(8) Soweit kein Angemessenheitsbeschluss einschlägig ist, vereinbaren die Parteien geeignete Garantien, insbesondere die Standardvertragsklauseln gemäß Durchführungsbeschluss (EU) 2021/914. Soweit ein Angemessenheitsbeschluss genutzt wird (z. B. EU-US Data Privacy Framework), darf sich der Auftragnehmer hierauf nur stützen, wenn der jeweilige Datenimporteur für den einschlägigen Mechanismus gültig zertifiziert/gelistet ist.

(9) Der Auftragnehmer unterstützt den Auftraggeber bei der Durchführung und Dokumentation der für Drittlandübermittlungen erforderlichen Bewertung (Transfer-Assessment) durch Bereitstellung der hierfür notwendigen Informationen (insbesondere zu Datenkategorien, Empfängern, Subunternehmerkette, Speicher-/Zugriffsorten, technischen und organisatorischen Maßnahmen). Erforderliche ergänzende Maßnahmen zur Absicherung der Übermittlung werden nach Maßgabe der EDPB-Empfehlungen zu ergänzenden Maßnahmen umgesetzt.

(10) Weiterübermittlungen (Onward Transfers) in weitere Drittländer sind nur zulässig, wenn auch hierfür die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind und der jeweilige Empfänger mindestens gleichwertige Verpflichtungen (insbesondere nach SCC oder Angemessenheitsbeschluss) übernimmt. Der Auftragnehmer dokumentiert Weiterübermittlungen in geeigneter Weise.

(11) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen. Gleiches gilt für alle Tätigkeiten, bei denen der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit Auftraggeberdaten in Berührung kommen.

2. Weisungsbefugnisse des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Auftraggeberdaten im Rahmen der Beauftragung und im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber hat das alleinige Recht, Weisungen über Art, Umfang, und Methode der Verarbeitungstätigkeiten zu erteilen (nachfolgend auch ”Weisungsrecht”). Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese

rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Weisungen werden vom Auftraggeber grundsätzlich schriftlich oder in elektronischer Form (E-Mail ausreichend) erteilt; mündlich erteilte Weisungen sind vom Auftragnehmer in elektronischer Form zu bestätigen.

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

3. Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Ferner wird der Auftragnehmer alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im Folgenden ”Mitarbeiter” genannt), zur Vertraulichkeit verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO). Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Verpflichtung der Mitarbeiter schriftlich oder in elektronischer Form nachweisen.

(3) Der Auftragnehmer wird seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er verpflichtet sich, alle geeigneten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Auftraggeberdaten gem. Art. 32 DSGVO, insbesondere die in Anlage 2 zu diesem Vertrag aufgeführten Maßnahmen, zu ergreifen und diese für die Dauer der Verarbeitung der Auftraggeberdaten aufrecht zu erhalten.

(4) Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(5) Auf Verlangen des Auftraggebers wird der Auftragnehmer dem Auftraggeber die Einhaltung der technischen und organisatorischen Maßnahmen nachweisen.

(6) Der Auftragnehmer und die bei oder für ihn Beschäftigten ist berechtigt, die gem. des Hauptvertrags zu erbringenden Leistungen und damit auch die Verarbeitung personenbezogenen Daten aus seiner Hauptverwaltung, seinen Betriebstätten, Niederlassungen oder aus dem Home- und Mobile-Office heraus erbringen zu lassen, sofern sichergestellt ist, dass die Schutzmaßnahmen, die in diesem Vertrag definiert werden, hierbei eingehalten werden.

4. Informations- und Unterstützungspflichten des Auftragnehmers

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der Auftraggeberdaten informiert der Auftragnehmer den Auftraggeber unverzüglich nach Bekanntwerden.

(2) Die Information erfolgt als Erstmeldung unverzüglich, in der Regel binnen 24 Stunden, mindestens mit den zu diesem Zeitpunkt verfügbaren Kerninformationen (Art des Vorfalls, betroffene Systeme/Datenkategorien, erste Einschätzung der möglichen Auswirkungen,

eingeleitete Sofortmaßnahmen, Kontaktstelle). Soweit nicht alle Angaben vollständig vorliegen, ergänzt der Auftragnehmer die Informationen ohne schuldhaftes Zögern in angemessenen Abständen (Updates), bis die Meldung vollständig ist.

(3) Dasselbe gilt für Prüfungen des Auftragnehmers durch Datenschutz-Aufsichtsbehörden, soweit rechtlich zulässig.

5. Sonstige Verpflichtungen des Auftragnehmers

(1) Der Auftragnehmer ist, sofern die Voraussetzungen des Art. 30 DSGVO auf ihn zutreffen, verpflichtet, ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung gem. Art. 30 Absatz 2 DSGVO zu führen. Das Verzeichnis ist dem Auftraggeber auf Verlangen zur Verfügung zu stellen.

(4) Der Auftragnehmer ist verpflichtet, den Auftraggeber bei der Erstellung einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und einer etwaigen vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO zu unterstützen.

(5) Der Auftragnehmer bestätigt, dass er – soweit eine gesetzliche Verpflichtung hierzu besteht – einen Datenschutzbeauftragten bestellt hat.

(6) Sollten die Auftraggeberdaten beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DSGVO liegt.

6. Subunternehmerverhältnisse

(1) Der Auftragnehmer darf die Verarbeitung personenbezogener Daten ganz oder teilweise durch weitere Auftragsverarbeiter (nachfolgend auch „**Unterauftragnehmer**“ oder „**Subunternehmen**“) erbringen lassen.

(2) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Bewachungsdienste, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

(3) Der Auftragnehmer wird mit dem Unterauftragnehmer die in diesem Vertrag getroffenen Regelungen inhaltsgleich vereinbaren. Insbesondere müssen die mit dem Unterauftragnehmer zu vereinbarenden TOM ein gleichwertiges Schutzniveau aufweisen.

(4) Der Auftragnehmer hat mit den in Anlage 1 genannten Unternehmen Subunternehmerverhältnisse begründet, denen der Auftraggeber mit Abschluss dieses Auftragsverarbeitungsvertrages zustimmt. Die in der Anlage 1 genannten Unternehmen können durch den Auftragnehmer ergänzt oder verringert werden. Sollte der Auftragnehmer einen weiteren Unterauftragnehmer hinzufügen, so fügt er diese in die Anlage 1 ein und informiert den Auftraggeber hierüber spätestens 4 Wochen vor dem beabsichtigten Einsatz des Unter-

auftragnehmers. Sollte der Auftraggeber nicht mit der Hinzufügung des weiteren Unterauftragnehmers einverstanden sein, so hat er die Möglichkeit, innerhalb von 4 Wochen nach Zufügung gegenüber dem Auftragnehmer zu widersprechen. Widerspricht der Auftraggeber der Hinzufügung des weiteren Unterauftragnehmers, so hat der Auftragnehmer das Recht den Hauptvertrag inkl. sämtlicher Anlagen innerhalb von 2 Wochen zu kündigen, sollte keine alternative Lösung zur weiteren Zusammenarbeit gefunden werden und sollte die Hinzufügung des weiteren Unterauftragnehmers für das Unternehmen des Auftragnehmers von besonderer Wichtigkeit sein.

(5) Der Auftragnehmer schließt mit jedem Unterauftragnehmer vor dessen Einsatz einen Vertrag ab, der die Anforderungen des Art. 28 Abs. 3 und Abs. 4 DSGVO inhaltlich abbildet und ein gleichwertiges Schutzniveau (insbesondere hinsichtlich technischer und organisatorischer Maßnahmen) sicherstellt. Mit Wirksamwerden dieses Vertrages genehmigt der Auftraggeber die in diesem Vertrag sowie dessen Anlagen genannten Unterauftragnehmer. Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Erfüllung sämtlicher Pflichten aus diesem AVV auch bei Einsatz von Unterauftragnehmern voll verantwortlich.

(6) Bestandteil der Auftragsverarbeitungsverträge mit den Unterauftragnehmern ist insbesondere auch, dass die Unterauftragnehmer sicherstellen, ihrerseits angemessene und geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO wegen der von ihnen im Auftrag durchgeführten Verarbeitungen personenbezogener Daten getroffen zu haben.

7. Kontrollrechte

(1) Der Auftraggeber ist berechtigt, die Einhaltung der Regelungen dieses Vertrages in angemessenem Umfang zu überprüfen. Der Auftragnehmer unterstützt Überprüfungen, indem er dem Auftraggeber auf Anfrage geeignete Nachweise zur Verfügung stellt (z. B. aktuelle TOM-Dokumentation, Zusammenfassungen von Prüfberichten, Zertifizierungen/Testate, soweit vorhanden) und angemessene Auskünfte erteilt.

(2) Überprüfungen erfolgen vorrangig als Remote-Audit (Dokumentenprüfung, Fragebogen, Videotermin). Vor-Ort-Inspektionen kommen nur in Betracht, wenn (i) ein Remote-Audit nicht ausreicht, (ii) ein konkreter Anlass besteht (z. B. schwerwiegender Sicherheitsvorfall) oder (iii) eine Aufsichtsbehörde dies verlangt, und sofern keine überwiegenden Geheimhaltungs- oder Sicherheitsinteressen entgegenstehen.

(3) Der Auftraggeber kündigt Vor-Ort-Inspektionen mit angemessener Frist (in der Regel mindestens 30 Kalendertage) an und berücksichtigt die Betriebsabläufe des Auftragnehmers. Inspektionen werden zu üblichen Geschäftszeiten durchgeführt. Der vom Auftraggeber beauftragte Prüfer darf nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen und ist vorab schriftlich zur Vertraulichkeit zu verpflichten.

(4) Soweit der Auftraggeber wiederkehrende Routine-Audits ohne besonderen Anlass durchführt, sind diese auf höchstens ein Audit pro Kalenderjahr beschränkt. Weitergehende Audits bleiben bei Vorliegen eines Anlasses oder bei behördlicher Anforderung zulässig.

(5) Etwaige Kostenregelungen für Audits (insbesondere Vor-Ort-Inspektionen) werden transparent vereinbart; die Parteien berücksichtigen hierbei, dass Audit- und Nachweispflichten Teil der gesetzlich vorgesehenen Zusammenarbeit nach Art. 28 Abs. 3 lit. h DSGVO sind.

8. Rechte Betroffener

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach

Art. 12 bis 22 sowie Art. 32 bis 36 DSGVO. Der Auftragnehmer stellt dem Auftraggeber die hierfür erforderlichen Informationen unverzüglich, spätestens binnen 5 Werktagen zur Verfügung, soweit der Auftraggeber nicht selbst über die entsprechenden Informationen verfügt. In dringenden Fällen (insbesondere bei drohendem Fristablauf oder behördlichen Anfragen) bearbeitet der Auftragnehmer das Ersuchen vorrangig und stellt die verfügbaren Informationen so schnell wie möglich bereit.

(2) Soweit der Auftraggeber den Auftragnehmer anweist, Auftraggeberdaten zu berichtigen, zu löschen oder die Verarbeitung einzuschränken, setzt der Auftragnehmer die Weisung unverzüglich um; die Umsetzung erfolgt spätestens binnen 5 Werktagen, soweit nicht aufgrund der technischen Ausgestaltung (z. B. Backup-/Restore-Prozesse) eine längere, sachlich erforderliche Frist notwendig ist. In diesem Fall teilt der Auftragnehmer dem Auftraggeber die Gründe und die voraussichtliche Umsetzungsfrist unverzüglich mit.

(3) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragnehmer geltend, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten und wartet dessen Weisungen ab. Ohne entsprechende Einzelweisung wird der Auftragnehmer nicht mit der betroffenen Person in Kontakt treten.

9. Laufzeit und Kündigung

Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrags. Er endet damit automatisch mit Beendigung des Hauptvertrags. Ist der Hauptvertrag ordentlich kündbar, gelten die Regelungen zur ordentlichen Kündigung für diesen Vertrag entsprechend. Sollte der Auftragnehmer vor Ablauf des Hauptvertrages keine Auftraggeberdaten mehr verarbeiten, endet dieser Vertrag ebenfalls automatisch.

10. Löschung und Rückgabe nach Vertragsende

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Verlangen alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder auf Wunsch des Auftraggebers, sofern nicht eine gesetzliche Aufbewahrungsfrist besteht, vollständig und unwiderruflich löschen. Dies gilt auch für Vervielfältigungen der Auftraggeberdaten beim Auftragnehmer, wie etwa Datensicherungen, nicht aber für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der Auftraggeberdaten dienen. Solche Dokumentationen sind vom Auftragnehmer für eine Dauer von 6 Monaten aufzubewahren und auf Verlangen an den Auftraggeber herauszugeben.

(2) Der Auftragnehmer bestätigt dem Auftraggeber die Löschung/Rückgabe in Textform („Löschbestätigung“). Die Löschbestätigung enthält mindestens: (i) Datum der Löschung/Rückgabe, (ii) Beschreibung der betroffenen Datenkategorien und Systeme/Speicherorte, (iii) Aussage, ob und in welchem Umfang Daten in Backups/Archiven enthalten sind, sowie (iv) die Frist und das Verfahren, nach dem Backups/Archive turnusmäßig überschrieben oder gelöscht werden.

(3) Soweit eine sofortige Löschung aus technischen Gründen in Backups/Archiven nicht möglich ist, stellt der Auftragnehmer sicher, dass die Daten bis zur endgültigen Löschung nicht produktiv wiederhergestellt oder anderweitig genutzt werden, es sei denn, dies ist zur Störungsbeseitigung zwingend erforderlich; in diesem Fall erfolgt eine Wiederherstellung nur unter kontrollierten Bedingungen und dokumentiert.

(4) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm

im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln.

11. Haftung

(1) Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Eine Haftung des Auftragnehmers gegenüber dem Auftraggeber wegen Verletzung von Pflichten aus diesem Vertrag oder dem Hauptvertrag bleibt hiervon unberührt.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist. Dies gilt im Falle einer gegen eine Partei verhängte Geldbuße entsprechend, wobei die Freistellung in dem Umfang erfolgt, in dem die jeweils andere Partei Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

12. Vertraulichkeit & Datengeheimnis

(1) Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen.

(2) Es besteht eine Verschwiegenheitspflicht für die Mitarbeiter des Auftragnehmers und durch ihn beauftragte Dritte. Der Auftragnehmer hat die bei der Verarbeitung von Auftraggeberdaten beschäftigten Personen gemäß Art. 28 Abs. 3 lit. b DSGVO schriftlich auf die Vertraulichkeit zu verpflichten. Dies ist nicht erforderlich, wenn die beschäftigten Personen bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Auftragnehmer wird die in dieser Ziffer niedergelegte Verpflichtung schriftlich dokumentieren und sie auf Verlangen des Auftraggebers diesem vorlegen.

(3) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und er diese auf die Einhaltung der geltenden Datenschutzvorschriften zu verpflichten. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(4) Diese in dieser Ziffer geregelten Verschwiegenheitspflichten besteht auch nach der Beendigung des Vertragsverhältnisses fort.

(5) Darüber hinaus ist der Auftragnehmer neben den jeweils geltenden gesetzlichen Bestimmungen (insbesondere § 3 TDDDG, § 203 StGB, §§ 4, 23 GeschGehG sowie ggf. besondere berufsständische Verschwiegenheitspflichten) auch verpflichtet, alle Informationen und Daten, die ihm im Rahmen der vertraglich vereinbarten Leistungen zur Kenntnis gelangen, geheim zu halten und nicht an Dritte weiterzugeben (vertrauliche Informationen). Vertrauliche Informationen sind insbesondere Geschäfts- und Betriebsgeheimnisse, Vertragsschlüsse, technische oder kaufmännische Informationen jedweder Art bzw. anderweitige Angaben, die als vertraulich bezeichnet oder ihrer Natur nach als vertraulich anzusehen sind. Dies gilt insbesondere auch für:
Namen, Anschriften sowie die persönlichen, rechtlichen und wirtschaftlichen Verhältnisse aller Kunden vom Auftraggeber und die persönlichen, rechtlichen und wirtschaftlichen Verhältnisse vom Auftraggeber und aller anderen für Auftraggeber tätigen Personen.
Eine Information ist nicht als vertraulich anzusehen, wenn sie zu der Zeit, zu der der Auftragnehmer von der Information Kenntnis erlangt hat, bereits öffentlich bekannt gewesen ist. Ebenso als nicht vertraulich sind solche Informationen anzusehen, die zeitlich später

mit Zustimmung des Auftraggebers öffentlich bekannt geworden sind bzw. bekannt gemacht wurden.

(6) Der Auftragnehmer verpflichtet sich, sämtliche Mitarbeiter, die im Rahmen der Tätigkeit für Auftraggeber Kenntnis von vorgenannten vertraulichen Informationen von Auftraggeber erlangen, ebenso wie sich selbst zu verpflichten.

(7) Beauftragt der Auftragnehmer Dritte, hat er dafür Sorge zu tragen, dass die Forderungen der Absätze 1 bis 6 entsprechend umgesetzt werden.

13. Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer iSd § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der elektronischen Form.

(3) Die Regelungen dieses Vertrags gehen im Zweifel den Regelungen des Hauptvertrags vor. Sollten sich einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise als unwirksam oder undurchführbar erweisen oder infolge Änderungen einer Gesetzgebung nach Vertragsabschluss unwirksam oder undurchführbar werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll die wirksame und durchführbare Bestimmung treten, die dem Sinn und Zweck der nichtigen Bestimmung möglichst nahekommt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist der Sitz des Auftragnehmers.

Anlagen

Anlage 1 Festlegungen zum Vertrag

Anlage 2 Technische und organisatorische Maßnahmen des Auftragnehmers (Art. 32 DSGVO)

Anlage 1 - Festlegungen zum Vertrag

Gegenstand und Dauer des Auftrages
Übersicht der Anforderungen und Festlegungen

Hauptvertrag	SaaS-Vertrag über die Software Kyvento
Gegenstand des Auftrages	„Kyvento“ ist eine moderne Subscription-Management-Software für B2B-Softwareunternehmen im DACH-Raum mit wiederkehrenden Umsätzen
Zweck der Datenerhebung, Datenverarbeitung oder Datennutzung	Zur Erfüllung der Pflichten des Auftragnehmers aus dem Hauptvertrag werden personenbezogene Daten aus dem Herrschaftsbereich des Auftraggebers durch den Auftragnehmer vollumfänglich i.S.d. Art. 4 Nr. 2 DSGVO verarbeitet, insbesondere soweit jeweils erforderlich erhoben, gespeichert, verändert, ausgelesen, abgefragt, verwendet, offengelegt, abgeglichen, verknüpft und gelöscht. Der Zweck der Verarbeitung hängt damit von dem jeweils im Hauptvertrag beschriebenen Auftrag ab.

Gegenstand und Dauer des Auftrages

Übersicht der Anforderungen und Festlegungen

Art der Daten	Die von der Verarbeitung betroffenen Kategorien personenbezogener Daten hängen von der Nutzung der Leistungen des Auftragnehmers durch den Auftraggeber ab. Als Gegenstand der Verarbeitung in Betracht kommende Kategorien von Daten sind möglich • Stammdaten (z.B. Namen, Anschriften, Geburtsdaten), • Kontaktdaten (z.B. E-Mail-Adressen, Telefonnummern), • Inhaltsdaten (z.B. Fotografien, Videos, Inhalte von Dokumenten), • Vertragsdaten (z.B. Vertragsgegenstand, Laufzeiten, Kunden), • Zahlungsdaten (z.B. Bankverbindungen, Zahlungsdienstleister), • Nutzungsdaten (z.B. Verlauf Web-Dienste, Zugriffszeiten), • Verbindungsdaten (z.B. Geräte-ID, IP-Adressen, URL-Referrer), • Standortdaten (z.B. GPS-Daten, IP-Geolokalisierung),
Kreis der Betroffenen	Die von der Verarbeitung betroffenen Kategorien betroffener Personen hängen von der Nutzung der Leistungen des Auftragnehmers durch den Auftraggeber ab. Als Kategorien betroffener Personen kommen dabei in Betracht: • Kunden / Interessenten • Lieferanten und Dienstleister • Geschäftspartner

Unterauftragnehmer

Nr.	Unterauftragnehmer Anschrift / Land	Gegenstand der Leistung	Speicher-/Verarbeitungsort (EU/EWR/Drittland)	Transfermechanismus (Angemessenheitsbeschluss / DPF oder SCC 2021/914)	Verarbeitete personenbezogene Daten
1	Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Hosting der gesamten Plattform inkl. Datenbank/Backups Versendung transaktionaler Mails	EU	entfällt	Siehe oben „Art der Daten“

Nr.	Unterauftragnehmer Anschrift / Land	Gegenstand der Leistung	Speicher-/Verarbeitungsort (EU/EWR/Drittland)	Transfermechanismus (Angemessenheitsbeschluss / DPF oder SCC 2021/914)	Verarbeitete personenbezogene Daten
2	Stripe Payments Europe Ltd., 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Irland	Einzug der Kyvento-Nutzungsentgelte per Kreditkarte/SEPA-Lastschrift	EU	DPF	Vertragsdaten & Zahlungsdaten
3	Binect GmbH, Brunnenweg 17, 64331 Weiterstadt	physischer Briefversand	EU	entfällt	Siehe oben „Art der Daten“

Anlage 2 - Technische und organisatorische Maßnahmen

Verantwortliche für die Datenverarbeitung sind gem. Art. 32 DSGVO verpflichtet, technische und organisatorische Maßnahmen zu treffen, durch die die Sicherheit der Verarbeitung personenbezogener Daten gewährleistet wird. Maßnahmen müssen dabei so gewählt sein, dass durch sie in der Summe ein angemessenes Schutzniveau sichergestellt wird. Diese Übersicht erläutert vor diesem Hintergrund, welche konkreten Maßnahmen durch den Auftragnehmer im Hinblick auf die Verarbeitung personenbezogener Daten im konkreten Fall getroffen sind.

Weisungen zu technischen und organisatorischen Maßnahmen

1. Organisation der Informationssicherheit

Es sind Richtlinien, Prozesse und Verantwortlichkeiten festzulegen, mit denen die Informationssicherheit implementiert und kontrolliert werden kann.
Maßnahmen:

- ☒ Festlegung der Rollen und Verantwortlichkeiten für Betrieb von Anwendungen und System, Datenschutz und Informationssicherheit.

Weitere umgesetzte Maßnahmen / Erläuterungen: Einzelunternehmen ohne Mitarbeitende: Verpflichtung auf das Datengeheimnis und regelmäßige Schulungen greifen mit der ersten Einstellung. Laufende externe fachliche Begleitung durch spezialisierte IT-/Datenschutz-Kanzlei.

2. Privacy by Design

Privacy by Design beinhaltet den Gedanken, dass Systeme so konzipiert und konstruiert sein sollten, dass der Umfang der verarbeiteten personenbezogenen Daten minimiert wird. Wesentliche Elemente der Datensparsamkeit sind die Trennung personenbezogener Identifizierungsmerkmale und der Inhaltsdaten, die Verwendung von Pseudonymen und die Anonymisierung. Außerdem muss das Löschen von personenbezogenen Daten gemäß einer konfigurierbaren Aufbewahrungsfrist realisiert sein.

Maßnahmen:

- ☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.
- ☒ Prozess zur Sicherstellung von Privacy by Design bei Einführung oder Änderung von Systemen und Anwendungen.
- ☒ Die Verarbeitungen und Systeme sind so konzipiert, dass Sie ein DSGVO konformes Löschen der verarbeiteten personenbezogenen Daten ermöglichen und sicherstellen.

Weitere umgesetzte Maßnahmen / Erläuterungen: Datenminimierung u. a.: keine Speicherung vollständiger Kartennummern (nur Token und letzte vier Stellen);
Lösch-/Anonymisierungs-Workflows inkl. PSP-Token-Löschung; Retention-Regeln (gesetzliche Aufbewahrung vs. Löschung).

3. Privacy by Default

Privacy by Default bezieht sich auf die datenschutzfreundlichen Voreinstellungen / Standardeinstellungen. Inwieweit wurden diese von Ihnen vorgenommen? Beispiel: Bei einem Besuch einer Webseite kann der Besucher erwarten, dass alle Programme zunächst deaktiviert sind, die personenbezogene Daten erheben.

Maßnahmen:

- ☒ Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen.
- ☒ Trackingfunktionen, die den Betroffenen überwachen, sind standardmäßig deaktiviert.
- ☒ Sämtliche Vorbelegungen von Auswahlmöglichkeiten erfüllen die Anforderungen der DSGVO in Bezug auf datenschutzfreundliche Voreinstellungen (z.B. keine Vorbelegungen von Opt-ins).

Weitere umgesetzte Maßnahmen / Erläuterungen: Kein Marketing-Tracking; Web-Analyse ausschließlich cookieless und self-hosted (Plausible).

4. Zugriffskontrolle und Zugangskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten bzw. schutzbedürftigen Informationen und Daten zugreifen können (Beschreibung von systemimmanenten Sicherungsmechanismen, Verschlüsslungsverfahren entsprechend dem Stand der Technik. Bei Online-Zugriffen ist klarzustellen, welche Seite für die Ausgabe und Verwaltung von Zugriffssicherungscodes verantwortlich ist.). Der Auftragnehmer gewährleistet, dass die zur Benutzung von IT-Infrastruktur berechtigten Nutzer ausschließlich auf Inhalte zugreifen können, für welche sie berechtigt sind, und dass personenbezogene Daten bei der Verarbeitung und nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden können.

3. Privacy by Default

Privacy by Default bezieht sich auf die datenschutzfreundlichen Voreinstellungen / Standardeinstellungen. Inwieweit wurden diese von Ihnen vorgenommen? Beispiel: Bei einem Besuch einer Webseite kann der Besucher erwarten, dass alle Programme zunächst deaktiviert sind, die personenbezogene Daten erheben.

Maßnahmen:

- ☒ Berechtigungskonzepte dokumentiert.
- ☒ Vermeidung von Gruppenusern.
- ☒ Zugriff auf Daten ist eingeschränkt und nur für Berechtigte möglich.
- ☒ Sperrung des Benutzerkontos bei Fehlversuchen / Inaktivität.
- ☒ Sperrung des Endgerätes bei Verlassen des Arbeitsplatzes oder Inaktivität.
- ☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert.
- ☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten.
- ☒ Umsetzen eines Prozesses zur Berechtigungsvergabe.
- ☒ Regelmäßige Überprüfung der Berechtigungen.
- ☒ Passwortrichtlinie, Implementierung komplexer Passwörter.
- ☒ Einsatz starker Authentifizierung mit mindestens 2 Faktoren aus Wissen, Besitz, Eigenschaften (Pin, Token, Smartcard, biometrische Verfahren).

Weitere umgesetzte Maßnahmen / Erläuterungen: Passwörter ausschließlich als bcrypt-Hash (Cost-Faktor 12); administrativer Serverzugriff nur per SSH-Schlüssel (Passwort-Login deaktiviert); mandantenbezogene Zugriffsbeschränkung auf Datenbankebene (Row-Level Security). Dokumentierter Berechtigungsvergabe- und Offboarding-Prozess mit Zugangs-Inventar und halbjährlichem Review (Prüfvermerk).

5. Kryptographie und / oder Pseudonymisierung

Einsatz von Verschlüsselungsverfahren für die Sicherstellung des ordnungsgemäßen und wirksamen Schutzes der Vertraulichkeit, Authentizität oder Integrität von personenbezogenen Daten bzw. schutzbedürftigen Informationen.
Maßnahmen, die geeignet sind, eine Identifikation des Betroffenen zu erschweren.

Maßnahmen:

- ☒ Verschlüsselung von Datenträgern (z.B. mobile Festplatten, USB-Sticks etc.).
- ☒ Verschlüsselung von Datensicherungsmedien (z.B. Bänder, Festplatten etc.).
- ☒ Verschlüsselung von Zugängen zum Netzwerkzugängen und -verbindungen.
- ☒ Einsatz von Pseudonymen, Verfahren zur Pseudonymisierung von Daten.
- ☒ Einsatz Verfahren zur Anonymisierung von Daten.

Weitere umgesetzte Maßnahmen / Erläuterungen: Backups AES-256-verschlüsselt (pgBackRest/restic, off-site); sämtliche Übertragungen ausschließlich TLS/HTTPS; verschlüsselte Speicherung sensibler Zugangs-Tokens; Anonymisierung z. B. bei Newsletter-Abmeldung (SHA-256-Hash) und PII-Scrubbing in Suchindizes. Backup-Medium (separates Medium gem. Sicherungskonzept) verschlüsselt; mobile Endgeräte (Laptops, Smartphone) verschlüsselt, die stationäre Workstation folgt kurzfristig (FileVault). Datenträger-Verschlüsselung der Server (LUKS) als Nachrüstung geplant.

6. Schutz von Gebäuden

Verhinderung des unautorisierten physischen Zugriffs auf die Informationen und informationsverarbeitende Einrichtungen der Organisation sowie deren Beschädigung und Beeinträchtigung. Der Auftragnehmer trifft Maßnahmen, um zu verhindern, dass unbefugte Personen Zutritt (räumlich zu verstehen) zu Datenverarbeitungsanlagen erhalten mit denen personenbezogene Daten verarbeitet werden.

Die Maßnahmen dieser Ziffer werden durch unsere Rechenzentrums-Dienstleister umgesetzt; Nachweise (z. B. ISO/IEC-27001-Zertifizierung, TOM des Dienstleisters) stellen wir auf Anfrage bereit. Betrieb ausschließlich in ISO/IEC-27001-zertifizierten Rechenzentren der Hetzner Online GmbH; kein Eigenbetrieb von Servern.

7. Schutz von Betriebsmitteln / Informationswerten

Vorbeugung von Verlust, Beschädigung, Diebstahl oder Beeinträchtigung von Werten und Unterbrechungen der Betriebstätigkeit der Organisation.

Die Maßnahmen dieser Ziffer werden durch unsere Rechenzentrums-Dienstleister umgesetzt; Nachweise (z. B. ISO/IEC-27001-Zertifizierung, TOM des Dienstleisters) stellen wir auf Anfrage bereit. Verarbeitung ausschließlich in Rechenzentren der Dienstleister (siehe Ziff. 6); keine eigenen Server- oder Aktenbestände.

8. Betriebsverfahren und Zuständigkeiten

Sicherstellung des ordnungsgemäßen und sicheren Betriebes von Systemen sowie Verfahren zur Verarbeitung von Informationen.

Maßnahmen:

- ☒ Dokumentierte Systemkonfigurationen und Betriebsverfahren, Betriebsführunghandbücher.
- ☒ Klare Zuordnung von Verantwortlichkeiten für die System- und Anwendungsbetreuung.
- ☒ Trennung der Verarbeitung von Daten der einzelnen Mandanten.
- ☒ Trennung von Entwicklungs-, Test- und Produktivsystemen.
- ☒ Überwachung des Systembetriebs und der Anlagen.

Weitere umgesetzte Maßnahmen / Erläuterungen: Mandantentrennung mittels Row-Level Security auf Datenbankebene; Produktiv- und Test-/Entwicklungsumgebung auf physisch getrennten Servern; Systemüberwachung über self-hosted Fehler-Monitoring (Sentry) und technische Logs; Infrastruktur-Wartung durch den Rechenzentrums-Dienstleister.

9. Datensicherungen

Maßnahmen, die gewährleisten, dass personenbezogene Daten bzw. schutzbedürftige Informationen und Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen:

- ☒ Datensicherungskonzept mit regelmäßigen Backups.
- ☒ Auslagerung der Backup in andere Brandzonen.
- ☒ Auslagerung der Backups in andere Gebäude.
- ☒ Regelmäßige Tests der Datensicherung und Wiederherstellung von Daten, Anwendungen und Systemen.

Weitere umgesetzte Maßnahmen / Erläuterungen: Verschlüsselte Backups (AES-256) off-site in räumlich getrenntem Rechenzentrum (anderes Land, EU/EWR); Datenbank mit kontinuierlicher Transaktionslog-Archivierung (Point-in-Time-Recovery); dokumentierte, regelmäßige Restore-Drills.

10. Schutz vor Malware und Patchmanagement

Verhinderung einer Ausnutzung technischer Schwachstellen durch den Einsatz von aktueller Virenschutzsoftware und die Implementierung eines Patchmanagements.

Maßnahmen:

- ☒ Regelmäßige Überwachung des Status von Sicherheitsupdates und Systemschwachstellen.
- ☒ Einsatz von Anti-Malware-Software.
- ☒ Regelmäßige Einspielen von Sicherheitspatches und Updates.

Weitere umgesetzte Maßnahmen / Erläuterungen: Automatisierte Überwachung von Dependency-/Sicherheitsupdates; Datei-Uploads werden per Virenscanner (ClamAV) geprüft.

11. Protokollierung und Überwachung

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in IT-Systeme eingegeben, verändert oder entfernt worden sind.

Maßnahmen:

- ☒ Protokollierung von Aktivitäten der Systemadministratoren.
- ☒ Überwachung der Systemnutzung.
- ☒ Protokollierung von Zugängen.
- ☒ Protokollierung von Zugriffen.
- ☒ Auswertung von Log-Dateien.

Weitere umgesetzte Maßnahmen / Erläuterungen: Audit-Trail für sicherheits- und abrechnungsrelevante Vorgänge (auch zur GoBD-Nachvollziehbarkeit); technische Logs; Auswertung über self-hosted Monitoring. Aufbewahrung gemäß Löschkonzept.

12. Netzwerksicherheitsmanagement

Es muss ein angemessener Schutz für das Netzwerk implementiert werden, so dass die Informationen und die Infrastrukturkomponenten geschützt werden.

Maßnahmen:

- ☒ Einsatz von Firewallsystemen.
- ☒ Einsatz von Intrusion Detection / Intrusion Prevention Systemen.
- ☒ Benutzerauthentifizierung und Verschlüsselung von externen Zugriffen.

Weitere umgesetzte Maßnahmen / Erläuterungen: Infrastruktur- und hostbasierte Firewalls; administrative Zugriffe ausschließlich per SSH-Schlüssel über verschlüsselte Verbindungen. Host-basierte Intrusion Prevention (fail2ban) auf allen Servern mit automatischer, bei Wiederholung eskalierender Sperrung auffälliger Zugriffe (SSH; auf Staging zusätzlich Web-Ebene).

13. Informationsübertragung

Maßnahmen, die gewährleisten, dass personenbezogene Daten bzw. schutzbedürftige Informationen und Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft sowie festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten bzw. schutzbedürftiger Informationen sowie Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
(Beschreibung der verwendeten Einrichtungen und Übermittlungsprotokolle, z.B. Identifizierung und Authentifizierung, Verschlüsselung entsprechend dem Stand der Technik, automatischer Rückruf, u.a.)

Maßnahmen:

- ☒ Regelungen für den Austausch sensibler Informationen und Beschränkung des zur Übermittlung befugten Personenkreises.
- ☒ Weitergabe von Daten an Dritte nur nach Prüfung der Rechtsgrundlage.
- ☒ Sichere Datenübertragung zwischen Client und Server.
- ☒ Angemessener Schutz von Emails, die sensible Informationen / Daten beinhalten.

Weitere umgesetzte Maßnahmen / Erläuterungen: Keine Übermittlungen in Drittländer (Verarbeitung ausschließlich EU/EWR); kein physischer Datenträgeraustausch.
E-Mail-Versand mit SPF/DKIM-Prüfung; optional vom Kunden eingebundene externe Skripte werden per SRI-Integrity-Hash abgesichert.

14. Netztrennung

Gruppen von Informationsdiensten, Mandanten, Benutzern und Informationssystemen sollten in Netzwerken voneinander getrennt gehalten werden.

Maßnahmen:

- ☒ Logische Mandantentrennung.

Weitere umgesetzte Maßnahmen / Erläuterungen: Logische Mandantentrennung auf Datenbankebene mittels Row-Level Security — jeder Mandant kann ausschließlich auf seine eigenen Daten zugreifen.

15. Anschaffung, Entwicklung und Instandhaltung von Systemen

Maßnahmen, die sicherstellen, dass Informationssicherheit ein fester Bestandteil über den Lebenszyklus von Informationssystemen ist.

Maßnahmen:

- ☒ Festlegung von Regelungen für die Entwicklung und Anpassung von Software und Systemen.
- ☒ Leitlinien zur sicheren Systementwicklung.
- ☒ Schutz von Testdaten.

Weitere umgesetzte Maßnahmen / Erläuterungen: Keine ausgelagerte Entwicklung (Entwicklung ausschließlich durch den Inhaber); getrennte Entwicklungs-, Test- und Produktivumgebungen (siehe Ziff. 8). Dokumentierte Sicherheitsregeln für die Entwicklung: verpflichtende Code-Reviews, CI mit blockierenden Test- und Statik-Analyse-Stufen, Secrets-Handling, ausschließlich synthetische Testdaten (keine Produktivdaten in Dev/Test), Dependency-Audits.

16. Lieferantenbeziehungen

Maßnahmen betreffend die Informationssicherheit zur Verringerung von Risiken im Zusammenhang mit dem Zugriff von Lieferanten auf die Werte des Unternehmens, sollten mit Sublieferanten / Subunternehmern vereinbart und dokumentiert werden.

Maßnahmen:

- ☒ Auswahl des Subunternehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit).
- ☒ Schriftliche Weisungen an den Subunternehmer (z.B. durch Auftragsverarbeitungsvertrag) i.S.d. DSGVO
- ☒ Wirksame Kontrollrechte gegenüber dem Subunternehmer vereinbart.
- ☒ Vorherige Prüfung und Dokumentation der beim Subunternehmer getroffenen Sicherheitsmaßnahmen.
- ☒ Verpflichtung der Mitarbeiter des Subunternehmers auf das Datengeheimnis.
- ☒ Laufende Überprüfung des Subunternehmers und seiner Tätigkeiten.
- ☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags.

Weitere umgesetzte Maßnahmen / Erläuterungen: AVV/DPA mit sämtlichen Unterauftragnehmern (Hetzner Online GmbH liegt vor; weitere vor Aktivierung); Dokumentation der Nachweise in interner Compliance-Übersicht. Jährlicher Subprozessoren-Review (DPA-Gültigkeit, Zertifizierungen, Drittland-Status, Abgleich Liste vs. Einsatz) mit dokumentiertem Prüfvermerk.

17. Management von Informationssicherheitsvorfällen

Es sind konsistente und wirksame Maßnahmen für das Management von Informationssicherheitsvorfällen (Diebstahl, Systemausfall etc.) zu implementieren.

Maßnahmen:

- ☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- ☒ Sofortige Information des Auftraggebers bei Datenschutzvorfällen.
- ☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen.

17. Management von Informationssicherheitsvorfällen

Es sind konsistente und wirksame Maßnahmen für das Management von Informationssicherheitsvorfällen (Diebstahl, Systemausfall etc.) zu implementieren.

Weitere umgesetzte Maßnahmen / Erläuterungen: Meldung an den Auftraggeber unverzüglich gemäß Ziff. 4 dieses Vertrages. Dokumentiertes Incident-Response-Playbook (Severity-Stufen, Eskalation, Meldewege nach Art. 33/34 DSGVO, 24-h-Kundenmeldung mit Vorlagen-Texten, Post-Mortem-Pflicht); ein Datenschutzbeauftragter ist nicht bestellt (nicht erforderlich, Einzelunternehmen).

18. Informationssicherheitsaspekte des Business Continuity Management / Notfallmanagements

Die Aufrechterhaltung der Systemverfügbarkeit in schwierigen Situationen, wie Krisen- oder Schadensfälle.
Ein Notfallmanagement muss dieses sicherstellen. Die Anforderungen bezüglich der Informationssicherheit sollten bei den Planungen zur Betriebskontinuität und Notfallwiederherstellung festgelegt werden.

Maßnahmen:

- ☒ Dokumentierte Notfallpläne.
- ☒ Regelmäßige Tests bzgl. der Wirksamkeit der Notfallmaßnahmen.
- ☒ Frühzeitige Information des Auftraggebers bei Notfällen.

Weitere umgesetzte Maßnahmen / Erläuterungen: Infrastruktur-Redundanz durch den Rechenzentrums-Dienstleister (Nachweise auf Anfrage); verschlüsselte Off-site-Backups mit Point-in-Time-Recovery und dokumentierten, regelmäßig getesteten Wiederherstellungsprozessen. Dokumentierte Notfall-Runbooks (u. a. Notfall-Restore und Disaster-Recovery-Szenario in zweiter Region); monatliche Restore-Drills mit RTO-/RPO-Protokollierung.

19. Einhaltung gesetzlicher und vertraglicher Anforderungen

Implementierung von Maßnahmen zur Vermeidung von Verstößen gegen gesetzliche, amtliche oder vertragliche Verpflichtungen sowie gegen jegliche Sicherheitsanforderungen.

Maßnahmen:

- ☒ Sicherstellung der Einhaltung der gesetzlichen Verpflichtungen im Rahmen der Zusammenarbeit.
- ☒ Rückgabe sämtlicher Daten, Betriebsmittel und Informationswerte an den Auftraggeber bei Vertragsende.
- ☒ Einrichtung eines Lizenzmanagements.
- ☒ Geheimhaltungsverpflichtungen mit Mitarbeitern sowie Sublieferanten und Dienstleistern.

Weitere umgesetzte Maßnahmen / Erläuterungen: Datenrückgabe/-export als Self-Service-Funktion im Produkt; GoBD-konforme Aufbewahrung über Retention-Regeln.

20. Datenschutzanforderungen und Datenschutzmanagement

Die Privatsphäre sowie der Schutz von personenbezogenen Daten sollte entsprechend den Anforderungen der einschlägigen gesetzlichen Regelungen, anderen Vorschriften sowie Vertragsbestimmungen sichergestellt werden.

Maßnahmen:

- ☒ Einrichtung einer Datenschutzorganisation.
- ☒ Durchführung von Datenschutzschulungen.

Weitere umgesetzte Maßnahmen / Erläuterungen: Verzeichnis der Verarbeitungstätigkeiten in Erstellung; Datenschutzbeauftragter nicht erforderlich (Einzelunternehmen ohne Mitarbeitende, keine Verarbeitung besonderer Kategorien als Kerntätigkeit); Datenschutz-Kompetenz über laufende externe anwaltliche Beratung; Betroffenenrechte technisch umgesetzt (Datenexport-Self-Service, Lösch-/Anonymisierungs-Workflows).

21. Informationssicherheitsüberprüfungen

Es muss regelmäßig überprüft werden, ob die Informationsverarbeitung entsprechend der definierten Sicherheitsmaßnahmen durchgeführt wird. Hierfür wird der Auftragnehmer regelmäßige Prüfungen durchführen. Der Auftragnehmer räumt dem Auftraggeber das Recht ein, regelmäßige Audits / Überprüfungen bei ihm durchzuführen.

Weitere umgesetzte Maßnahmen / Erläuterungen: Dokumentierte Restore- und Prozess-Drills; formale interne Audits und Penetrationstests sind mit wachsendem Betrieb geplant.