Vereinbarung zur Auftragsverarbeitung

gemäß Art. 28 EU-DSGVO

Vereinbarung

zwischen dem/der Verantwortlichen

- nachstehend *Auftraggeber* genannt -

und dem/der Auftragsverarbeiter/in

Fyndery GmbH, Agnes-Pütreich-Straße 70, 93053 Regensburg

- nachstehend *Auftragnehmer* genannt -

Einbeziehung in den Hauptvertrag

Diese Vereinbarung einschließlich ihrer Anlage ist Bestandteil des Hauptvertrags zwischen dem Auftraggeber und der Fyndery GmbH. Sie wird mit Abschluss des Hauptvertrags in der dem Auftraggeber vor Vertragsschluss zur Verfügung gestellten Fassung vereinbart. Eine gesonderte Unterzeichnung dieser Vereinbarung ist nicht erforderlich. Der Abschluss kann im elektronischen Format erfolgen.

1. Gegenstand des Auftrags

(1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer: Es wird die Buchungssoftware „Fyndery Buchungstool“ zur Verfügung gestellt. Diese wird für die Kurs- und Teilnehmerverwaltung sowie für die Erstellung, Bewerbung und Abrechnung der Kurse/Angebote auf der Website des Auftraggebers sowie auf der eigenen Plattform des Auftragnehmers, dem sogenannten „Marktplatz“, genutzt. Der Auftrag beinhaltet somit die Speicherung, Aktualisierung, Übertragung und Löschung von Teilnehmerdaten, eventuell den Export von Teilnehmerdaten, die Kursverwaltung und Übertragung von Kursdaten sowie die Bearbeitung von Supportanfragen.

Der Auftragnehmer bietet darüber hinaus die Übernahme der Kundenkommunikation, wie z. B. den Newsletterversand, an. Zudem bietet der Auftragnehmer das Erstellen und Pflegen der Partner-Websites an.

Die Bearbeitung von Supportanfragen kann unter Einsatz des Dienstes Gleap einschließlich KI-gestützter Funktionen erfolgen. Soweit hierbei personenbezogene Daten im Auftrag des Auftraggebers verarbeitet werden, ist diese Verarbeitung Gegenstand dieser Vereinbarung. Sie umfasst insbesondere die Entgegennahme, Zuordnung, Speicherung und Auswertung von Supportanfragen sowie die Erstellung von Antworten.

Nicht Gegenstand dieser Vereinbarung sind Verarbeitungsvorgänge, bei denen der Auftragnehmer selbst Verantwortlicher ist, insbesondere die Verwaltung seiner eigenen Kundenbeziehungen und die Bearbeitung entsprechender Kontaktanfragen. Für diese Verarbeitung gelten die Datenschutzhinweise des Auftragnehmers.

(2) Zweck

Der Auftrag dient der Erfüllung folgender Zwecke:

- Buchungsabwicklung;
- Transaktions- und Zahlungsabwicklung;
- Teilnehmerverwaltung;
- Anbieterverwaltung;
- Auswertungen;
- Teilnehmerkommunikation einschließlich Newsletter-Anmeldungen;
- technische Unterstützung bei der Nutzung der Buchungssoftware, Untersuchung und Behebung von Fehlern sowie KI-gestützte Bearbeitung von Supportanfragen, soweit diese Tätigkeiten personenbezogene Daten im Auftrag des Auftraggebers betreffen.

(3) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung.

(4) Ort der Datenverarbeitung

Die Verarbeitung personenbezogener Daten erfolgt grundsätzlich in Deutschland sowie in Mitgliedstaaten der Europäischen Union oder in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum.

Soweit Unterauftragnehmer im Vereinigten Königreich eingesetzt werden, erfolgt die Datenverarbeitung auf Grundlage des Angemessenheitsbeschlusses der Europäischen Kommission gemäß Art. 45 DSGVO.

Soweit eine Verarbeitung personenbezogener Daten in den Vereinigten Staaten von Amerika oder in einem sonstigen Drittland erfolgt, stellt der Auftragnehmer sicher, dass die Voraussetzungen der Art. 44 ff. DSGVO eingehalten werden. Die Übermittlung erfolgt in diesen Fällen auf Grundlage geeigneter Garantien, insbesondere durch Abschluss von Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c DSGVO, oder auf Grundlage eines gültigen Angemessenheitsbeschlusses.

Eine darüber hinausgehende Übermittlung in Drittländer erfolgt nicht. Für den Einsatz von Gleap gelten ergänzend die Regelungen in Ziffer 5 Abs. 7.

(5) Art der Daten

Gegenstand der Verarbeitung sind folgende Datenarten beziehungsweise Datenkategorien:

- Personenstammdaten;
- Kommunikationsdaten, z. B. Telefon und E-Mail;
- Vertragsstammdaten, insbesondere Vertragsbeziehung sowie Produkt- beziehungsweise Vertragsinteresse;
- Kundenhistorie;
- Vertragsabrechnungs- und Zahlungsdaten;
- Bilddaten, insbesondere Profilbilder;
- Geschlecht und Geburtsdatum;
- Benutzerkennungen;
- Support- und Kommunikationsinhalte einschließlich Chatnachrichten, Gesprächskontexten, erzeugten Antworten und übermittelten Anhängen;
- technische Verbindungs- und Sitzungsdaten, insbesondere IP-Adressen, Browser- und Betriebssysteminformationen, Zeitangaben und Sitzungskennungen.

(6) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden;
- Interessenten;
- Ansprechpartner;
- Partner;
- Beschäftigte und sonstige berechtigte Nutzer des Auftraggebers;
- Personen, deren personenbezogene Daten zur Bearbeitung einer Supportanfrage im Auftrag des Auftraggebers verarbeitet werden.

2. 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 gemäß Art. 28 Abs. 3 lit. c sowie Art. 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO 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 DSGVO zu berücksichtigen (Anlage TOM).

(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.

3. 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) Der Auftraggeber ist selbstständig für die zeitgerechte Löschung von Daten verantwortlich.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung durch geeignete technische und organisatorische Maßnahmen dabei, dessen Pflichten zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DSGVO genannten Rechte betroffener Personen zu erfüllen. Er setzt die hierfür erforderlichen dokumentierten Weisungen des Auftraggebers um. Die gesetzlichen Unterstützungspflichten bestehen unabhängig davon, ob einzelne Unterstützungsleistungen im Hauptvertrag ausdrücklich beschrieben sind.

4. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartnerin beim Auftragnehmer wird Frau Madlen Bauer, datenschutz@fyndery.de benannt.
b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. 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.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO (Einzelheiten in Anlage TOM).
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) 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.
f) 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.
g) 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.
h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 6 dieses Vertrages.

5. 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- und 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.

Die Einordnung als Nebenleistung schließt eine Auftragsverarbeitung nicht aus. Soweit ein Dienstleister im Auftrag verarbeitete, personenbezogene Daten erhält und als weiterer Auftragsverarbeiter tätig wird, gelten die Anforderungen dieser Ziffer. Dies gilt insbesondere für die durch Gleap unterstützte Bearbeitung von Supportanfragen im Auftrag des Auftraggebers.

(2) Bei Vertragsschluss bestehen bereits die nachfolgend aufgeführten Unterauftragsverhältnisse. Mit Abschluss dieser Vereinbarung genehmigt der Auftraggeber deren Einsatz unter der Voraussetzung, dass die Anforderungen des Art. 28 Abs. 2–4 DSGVO und gegebenenfalls der Art. 44 ff. DSGVO eingehalten werden:

Firma Unterauftragnehmer	Anschrift/Land	Leistung	Betroffene Daten
PythonAnywhere LLP	2nd Floor Captains House, Watermans Court, Lotus Park, The Causeway, Staines-upon-Thames, TW18 3AG, United Kingdom	Hosting der Website des Auftragnehmers	Personenstammdaten, Kommunikationsdaten, Vertragsstammdaten, Kundenhistorie, Vertragsabrechnungs- und Zahlungsdaten, Bilddaten, Geschlecht, Geburtsdatum
BunnyWay d.o.o. (Bunny CDN)	Dunajska cesta 165 1000 Ljubljana Slowenien	Hosting im Rahmen des Baukasten-systems für Partner-Websites	Personenstammdaten, Kommunikationsdaten, Vertragsstammdaten sowie sonstige Daten, die im Rahmen der Nutzung der Partner-Websites verarbeitet werden
Stripe Payments Europe Ltd.	1 Grand Canal Street Lower Grand Canal Dock	Zahlungsabwicklung, Transaktionsverarbeitung und technische	Personenstammdaten, Kommunikationsdaten, Vertragsabrechnungs- und

	Dublin 2 Irland	Abwicklung von Online-Zahlungen	Zahlungsdaten, Transaktionsdaten
Acumbamail S.L.	C/ Santa Teresa, 1 02002 Albacete Spanien	Newsletter-Versand und Newsletter-Analyse	E-Mail-Adressen, Personenstammdaten, Kommunikationsdaten, Nutzungsdaten im Zusammenhang mit Newsletter-Kampagnen
Calendly LLC	271 17th St NW 10th Floor Atlanta, GA 30363 USA	Terminbuchung und Terminverwaltung	Personenstammdaten, Kommunikationsdaten, Termin- und Kalendereinträge
Gleap GmbH	Am Dorfplatz 3, 6858 Schwarzach, Österreich	Bereitstellung von Supportfunktionen einschließlich KI-gestützter Bearbeitung von Supportanfragen, soweit die Verarbeitung im Auftrag des Auftraggebers erfolgt	Benutzer-ID, Name, E-Mail-Adresse, Support- und Chatinhalte, Gesprächskontexte, erzeugte Antworten, übermittelte Anhänge sowie technische Verbindungs- und Sitzungsdaten

Soweit Zahlungsdienstleister personenbezogene Daten zur Erfüllung eigener gesetzlicher Verpflichtungen verarbeiten, insbesondere zur Betrugsprävention, Geldwäschebekämpfung oder aufgrund aufsichtsrechtlicher Anforderungen, handeln diese insoweit als eigenständige Verantwortliche.

(3) Der Auftraggeber erteilt die allgemeine schriftliche Genehmigung zur Hinzuziehung weiterer oder zum Austausch bestehender Unterauftragnehmer unter den folgenden Voraussetzungen:

Der Auftragnehmer informiert den Auftraggeber rechtzeitig vor der beabsichtigten Änderung in Textform, insbesondere per E-Mail. Die Information umfasst den Namen, die Anschrift und die Kontaktdaten des betreffenden Unterauftragnehmers, die vorgesehenen Leistungen, die betroffenen Datenkategorien und die Verarbeitungsländer sowie gegebenenfalls die Grundlagen und Garantien für Drittlandübermittlungen. Die Vorlaufzeit muss dem Auftraggeber eine angemessene Prüfung und die Möglichkeit zum Einspruch vor Beginn der betreffenden Verarbeitung ermöglichen.

Der Auftraggeber kann der beabsichtigten Änderung aus datenschutzrechtlichen Gründen in Textform widersprechen. Bei einem rechtzeitig erhobenen Einspruch darf die betreffende Verarbeitung durch den vorgesehenen Unterauftragnehmer erst beginnen, wenn die datenschutzrechtlichen Einwände ausgeräumt sind oder die Parteien eine zulässige Alternative vereinbart haben.

Vor Beginn der Verarbeitung muss eine Vereinbarung bestehen, die dem Unterauftragnehmer gemäß Art. 28 Abs. 4 DSGVO die gleichen Datenschutzpflichten auferlegt, die für die betreffende Verarbeitung nach dieser Vereinbarung gelten.

Eine bloße Aktualisierung einer öffentlich zugänglichen Unterauftragnehmerliste ersetzt nicht die aktive Vorabinformation des Auftraggebers.

(4) Die Weitergabe der im Auftrag verarbeiteten personenbezogenen Daten des Auftraggebers an einen Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst zulässig, wenn sämtliche Voraussetzungen für die Unterbeauftragung vorliegen.

(5) Erbringt ein Unterauftragnehmer die vereinbarte Leistung außerhalb der EU beziehungsweise des EWR, stellt der Auftragnehmer die Einhaltung der Voraussetzungen der Art. 44 ff. DSGVO sicher. Dies gilt entsprechend für weitere Unterauftragsverarbeiter und für eingesetzte Nebenleistungen, soweit dabei im Auftrag verarbeitete personenbezogene Daten betroffen sind.

Eine Weisung oder ein ausdrücklicher Wunsch des Auftraggebers entbindet den Auftragnehmer nicht von seinen eigenen gesetzlichen Pflichten.

(6) Eine weitere Auslagerung durch den Unterauftragnehmer ist nur unter den in Abs. 3 genannten Bedingungen gestattet. Den weiteren Unterauftragnehmern sind die gleichen Datenschutzpflichten aufzuerlegen, die für die betreffende Verarbeitung nach dieser Vereinbarung gelten. Die Verantwortlichkeit des Auftragnehmers gemäß Art. 28 Abs. 4 DSGVO bleibt unberührt.

(7) Ergänzende Regelungen zum Einsatz von Gleap

Für die Nutzung von Gleap ist die Hostingregion Europa (Frankfurt am Main) gewählt. Diese Einstellung betrifft das regionale Hosting der Kundendaten und schließt eine Verarbeitung durch weitere Dienstleister außerhalb dieser Region nicht aus.

Zur Bereitstellung der KI-Funktionen können unterschiedliche KI-Dienstleister einschließlich automatisch ausgewählter Ausweichmodelle eingesetzt werden. Dabei können die erforderlichen Nachrichteninhalte und Gesprächskontexte außerhalb der EU beziehungsweise des EWR verarbeitet werden, insbesondere in den USA und abhängig vom eingesetzten Anbieter und Verarbeitungsweg in China.

Der Einsatz dieser weiteren Unterauftragsverarbeiter setzt die Einhaltung der Genehmigungs-, Informations- und Einspruchsregelungen dieser Vereinbarung voraus. Dies gilt auch für Änderungen der durch Gleap eingesetzten Dienstleister. Die automatische Modellauswahl darf diese Anforderungen nicht umgehen.

Eine Verarbeitung in Drittländern ist nur unter Einhaltung der Art. 44 ff. DSGVO zulässig. Die hierfür geltenden Übermittlungsgrundlagen und gegebenenfalls erforderlichen ergänzenden Schutzmaßnahmen sind vor Beginn der betreffenden Verarbeitung sicherzustellen und zu dokumentieren.

Der Auftragnehmer stellt dem Auftraggeber vor der betreffenden Verarbeitung die für die Genehmigung erforderlichen Angaben zu den eingesetzten weiteren Unterauftragsverarbeitern, deren Aufgaben und Verarbeitungsorten zur Verfügung. Die veröffentlichte Übersicht unter https://www.gleap.ai/trust/subprocessors dient der ergänzenden Information und ersetzt nicht die vertraglich erforderliche Vorabinformation.

Die im Auftrag verarbeiteten personenbezogenen Daten dürfen durch Gleap und dessen weitere Unterauftragsverarbeiter nicht zum Training eigener oder fremder KI-Modelle verwendet werden.

Die Pflichten zur Berichtigung, Einschränkung, Rückgabe und Löschung nach dieser Vereinbarung sind auch gegenüber Gleap und dessen weiteren Unterauftragsverarbeitern sicherzustellen. Für die im Auftrag verarbeiteten Daten gelten die Weisungen des Auftraggebers sowie die Regelungen der Ziffern 3 und 9 dieser Vereinbarung.

6. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, die Einhaltung dieser Vereinbarung und der Anforderungen des Art. 28 DSGVO selbst oder durch einen von ihm beauftragten Prüfer zu überprüfen. Dies umfasst auch Inspektionen beim Auftragnehmer. Der Auftragnehmer ermöglicht diese Überprüfungen und trägt zu ihrer Durchführung bei. Ein konkreter Verdacht oder ein besonderer Anlass ist hierfür nicht erforderlich.

Überprüfungen sind grundsätzlich mit angemessener Vorankündigung und unter Berücksichtigung des Geschäftsbetriebs, der Datensicherheit sowie der Rechte anderer Kunden durchzuführen. Bei konkreten Anhaltspunkten für erhebliche Datenschutzverstöße oder sonstiger besonderer Dringlichkeit sind entsprechend kurzfristige Überprüfungen zu ermöglichen. Die organisatorischen Bedingungen dürfen die wirksame Ausübung der Kontrollrechte nicht verhindern oder unangemessen erschweren.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO 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 allgemeiner Maßnahmen sowie solcher, welche den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder

eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

7. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO 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-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

(2) Im Falle einer Unterstützungsleistung werden die Parteien eine angemessene Vergütung der Tätigkeiten des Auftragnehmers vereinbaren.

8. Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers im Sinne des Art. 28 DSGVO. Weisungen können in Textform, insbesondere per E-Mail, erfolgen.

(2) Mündliche Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen.

(3) Weisungsberechtigt sind die vertretungsberechtigten Personen des Auftraggebers sowie von diesem ausdrücklich benannte Personen. Weisungen sind an die vom Auftragnehmer benannte Kontaktadresse zu richten.

(4) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt. Er ist berechtigt, die Durchführung der betreffenden Weisung bis zur Klärung auszusetzen. Eine rechtswidrige Weisung darf auch dann nicht ausgeführt werden, wenn der Auftraggeber sie bestätigt. Die Parteien wirken auf eine rechtmäßige Anpassung der Weisung hin.

9. 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) Eine Anonymisierung der im Auftrag verarbeiteten personenbezogenen Daten erfolgt nur auf dokumentierte Weisung des Auftraggebers. Sie muss nach dem Stand der Technik so durchgeführt werden, dass eine Identifizierung betroffener Personen unter Berücksichtigung aller vernünftigerweise einsetzbaren Mittel nicht mehr möglich ist. Diese Vereinbarung begründet keine eigenständige Befugnis des Auftragnehmers, personenbezogene Daten für eigene Auswertungszwecke zu anonymisieren. Eine vom Auftraggeber verlangte Rückgabe darf durch die Anonymisierung nicht vereitelt werden.

(3) Nach Abschluss der Verarbeitungsleistungen hat der Auftragnehmer sämtliche im Auftrag verarbeiteten personenbezogenen Daten einschließlich vorhandener Kopien nach Wahl des Auftraggebers zurückzugeben oder datenschutzgerecht zu löschen. Dies gilt entsprechend bei einer früheren dokumentierten Weisung des Auftraggebers, soweit diese die betreffenden Daten erfasst. Die Abwicklung ist rechtzeitig vor Beendigung der Leistungsvereinbarung abzustimmen.

Bei einer Rückgabe sind anschließend die beim Auftragnehmer verbleibenden Kopien zu löschen. Die Pflichten erstrecken sich auch auf die eingesetzten Unterauftragnehmer und weiteren Unterauftragsverarbeiter. Auf Anforderung ist dem Auftraggeber die Durchführung der Löschung nachzuweisen.

Soweit Unionsrecht oder das Recht eines Mitgliedstaats eine weitere Speicherung vorschreibt, bleiben ausschließlich die hiervon betroffenen Daten für die gesetzlich vorgeschriebene Dauer gespeichert. Der Auftragnehmer informiert den Auftraggeber über die Rechtsgrundlage, die betroffenen Daten und die vorgesehene Speicherdauer, soweit dies rechtlich zulässig ist. Die Daten dürfen während dieser Aufbewahrung nur für den gesetzlich vorgeschriebenen Zweck verarbeitet werden.

(4) 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.

Stand der Vereinbarung zur Auftragsverarbeitung : Oktober 2026