Vertrag zur Auftragsverarbeitung der unvyl GmbH

Anlage zum Vertrag mit der unvyl GmbH (Paceways) · Stand: 15. Oktober 2026 · gültig ab 1. November 2026

Diese Vereinbarung wird zwischen den Parteien als ergänzende Regelung zur Einhaltung der datenschutzrechtlichen Regelungen gemäß Art. 28 der Datenschutz-Grundverordnung (DSGVO) getroffen und konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im zwischen den Parteien geschlossenen Vertrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben.

Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i. S. d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

1. Gegenstand des Vertrages

1.1. Die Auftragnehmerin erbringt für die Auftraggeberin Leistungen, insbesondere im Bereich der Bereitstellung von Webhosting-Dienstleistungen einschließlich Backups, der Erstellung von Websites (Website-Erstellungsservice), der automatisierten Erstellung und Aktualisierung von Datenschutzerklärung und Impressum und des Betriebs eines Cookie-Banners zur Einholung, Verwaltung und Protokollierung von Einwilligungen (nachfolgend „Rechtsmodul“) sowie der Bereitstellung von Funktionen auf Basis Künstlicher Intelligenz (nachfolgend „KI-Funktionen“), auf Grundlage des diesbezüglich zwischen den Parteien geschlossenen Vertrages (nachfolgend als „Hauptvertrag“ bezeichnet). Dabei erhält die Auftragnehmerin Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung der Auftraggeberin. Der Umfang der Datenverarbeitung durch die Auftragnehmerin ergibt sich aus dem Hauptvertrag. Die Datenverarbeitung erfolgt zum Zweck der Erbringung der Leistungen nach dem Hauptvertrag, insbesondere des Betriebs der Website der Auftraggeberin. Der Auftraggeberin obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

1.2. Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Hauptvertrages vor.

1.3. Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen die Auftragnehmerin und ihre Beschäftigten oder durch die Auftragnehmerin Beauftragte mit personenbezogenen Daten in Berührung kommen, die von der Auftraggeberin stammen oder für die Auftraggeberin erhoben wurden.

1.4. Nutzt die Auftraggeberin die Leistungen als Agentur oder Freelancer für ihre eigenen Kunden, verarbeitet sie personenbezogene Daten ihrer Kunden in der Regel selbst im Auftrag. Die Auftragnehmerin ist in diesem Fall weitere Auftragsverarbeiterin im Sinne von Art. 28 Abs. 4 DSGVO. Die Auftraggeberin stellt sicher, dass ihre Kunden dem Einsatz der Auftragnehmerin und der in Anhang 2 genannten Subunternehmer zugestimmt haben, und gibt Informationen über Änderungen nach Ziff. 7.1 an ihre Kunden weiter. Weisungen der Kunden der Auftraggeberin nimmt die Auftragnehmerin ausschließlich über die Auftraggeberin entgegen.

2. Art der verarbeiteten Daten, Kreis der Betroffenen

2.1. Im Rahmen der Durchführung des Hauptvertrags erhält die Auftragnehmerin Zugriff auf personenbezogene Daten. Diese Daten umfassen:

- Kontaktdaten über Formulare
- Protokolldaten (z. B. Logfiles über Nutzungsvorgänge)
- Internetnutzungsdaten (z. B. IP-Adresse, Besuchszeit, Datum, Land)
- Einwilligungsinformationen aus dem Cookie-Banner und technische Daten zum Nachweis der Einwilligung (insbesondere IP-Adresse, Zeitstempel, User-Agent, Endgeräte- und Browserinformationen)
- Angaben der Auftraggeberin für Impressum und Datenschutzerklärung (z. B. Name oder Firma, Anschrift, Kontaktdaten, Vertretungsberechtigte)
- Namen, Adress- und Kontaktdaten nebst Bewerbungsunterlagen von Bewerbern der Auftraggeberin
- Inhalte und Eingaben, die die Auftraggeberin auf der Plattform erstellt, hochlädt oder mit den KI-Funktionen bearbeitet

- Daten aus Diensten, die die Auftraggeberin mit der Plattform verbindet, etwa aus der Google Search Console oder aus Werbekonten
- weitere Daten von Dritten, die von der Auftraggeberin verarbeitet werden

2.2. Kreis der von der Datenverarbeitung Betroffenen:

- Beschäftigte der Auftraggeberin
- Inhaber, Vertretungsberechtigte und Ansprechpartner der Auftraggeberin
- Kunden der Auftraggeberin
- Bewerber der Auftraggeberin
- Dritte wie Besucher der Website und/oder Apps der Auftraggeberin

3. Laufzeit

3.1. Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

3.2. Ein außerordentliches Kündigungsrecht jeder Partei bleibt unberührt.

4. Weisungsrecht

4.1. Die Auftragnehmerin darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen der Auftraggeberin erheben, verarbeiten oder nutzen.

4.2. Die Weisungen der Auftraggeberin werden anfänglich durch diesen Vertrag festgelegt und können von der Auftraggeberin danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Einstellungen, die die Auftraggeberin in der Plattform vornimmt, insbesondere zur Konfiguration des Cookie-Banners, gelten als Weisung.

4.3. Alle erteilten Weisungen sind sowohl von der Auftraggeberin als auch von der Auftragnehmerin zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

4.4. Ist die Auftragnehmerin der Ansicht, dass eine Weisung der Auftraggeberin gegen datenschutzrechtliche Bestimmungen verstößt, hat sie die Auftraggeberin unverzüglich darauf hinzuweisen. Die Auftragnehmerin ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch die Auftraggeberin bestätigt oder geändert wird. Die Auftragnehmerin darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

5. Allgemeine Pflichten und Schutzmaßnahmen der Auftragnehmerin, Vertraulichkeit

5.1. Die Auftragnehmerin ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich der Auftraggeberin erlangten Informationen nicht an Dritte weiterzugeben oder Dritten Zugriff darauf zu gewähren. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

5.2. Die Auftragnehmerin trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten der Auftraggeberin gem. Art. 32 DSGVO. Der Auftraggeberin sind die in Anhang 1 zu dieser Vereinbarung dargestellten technischen und organisatorischen Maßnahmen bekannt, und sie trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt der Auftragnehmerin vorbehalten, wobei sie sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

5.3. Die Auftragnehmerin ist verpflichtet, ihr Unternehmen und ihre Betriebsabläufe so zu gestalten, dass die Daten, die sie im Zusammenhang mit dem Hauptvertrag im Auftrag verarbeitet, vor der unbefugten Kenntnisnahme Dritter geschützt sind.

5.4. Die Auftragnehmerin meldet der Auftraggeberin jede Verletzung des Schutzes personenbezogener Daten, die bei ihr oder einem Unterauftragsverarbeiter eintritt, unverzüglich, spätestens innerhalb von 24 Stunden, nachdem sie selbst davon Kenntnis erlangt hat. Die Meldung enthält, soweit der Auftragnehmerin bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO, insbesondere die Art der Verletzung, die Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen

Maßnahmen. Informationen, die zum Zeitpunkt der Meldung noch nicht vorliegen, werden unverzüglich nachgereicht. Bei Störungen, Verdacht auf Verletzungen vertraglicher Verpflichtungen der Auftragnehmerin, Verdacht auf sicherheitsrelevante Vorfälle oder anderen Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten informiert die Auftragnehmerin die Auftraggeberin ebenfalls unverzüglich. Die Bewertung, ob eine Meldung an die Aufsichtsbehörde oder eine Benachrichtigung betroffener Personen erforderlich ist, obliegt der Auftraggeberin.

5.5. Die Auftragnehmerin wird ihren Pflichten aus Art. 30 Abs. 2 DSGVO zum Führen eines Verarbeitungsverzeichnisses nachkommen.

5.6. Die Auftragnehmerin unterstützt die Auftraggeberin bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten, soweit die Auftraggeberin auf die Unterstützung der Auftragnehmerin angewiesen ist.

5.7. Für Datenschutzfragen ist die Auftragnehmerin unter info@paceways.com erreichbar. Eine Pflicht zur Benennung eines Datenschutzbeauftragten besteht bei der Auftragnehmerin derzeit nicht.

5.8. Den bei der Datenverarbeitung durch die Auftragnehmerin beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Die Auftragnehmerin wird ihre Beschäftigten und durch sie Beauftragte, die von ihr mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden, entsprechend zur Vertraulichkeit verpflichten und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen.

6. Kontrollrechte der Auftraggeberin

6.1. Die Auftraggeberin hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen der Auftraggeberin durch die Auftragnehmerin jederzeit im erforderlichen Umfang zu kontrollieren.

6.2. Die Auftragnehmerin verpflichtet sich, der Auftraggeberin auf deren schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle im Sinne der Ziff. 6.1 erforderlich sind. Für Unterauftragsverarbeiter kann die Auftragnehmerin die Kontrolle durch Vorlage der von diesen bereitgestellten Nachweise erfüllen.

6.3. Sollten im Einzelfall Inspektionen durch die Auftraggeberin oder einen von dieser beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Die Auftragnehmerin darf diese Kontrollen von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch die Auftraggeberin beauftragte Prüfer in einem Wettbewerbsverhältnis zu der Auftragnehmerin stehen, hat die Auftragnehmerin gegen diesen ein Einspruchsrecht.

6.4. Für die Ermöglichung der Kontrollrechte durch die Auftraggeberin kann die Auftragnehmerin einen angemessenen Vergütungsanspruch geltend machen.

6.5. Die Auftragnehmerin ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber der Auftraggeberin i. S. d. Art. 58 DSGVO i. V. m. § 40 BDSG, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten, die erforderlichen Auskünfte an die Auftraggeberin zu erteilen.

7. Unterauftragsverhältnisse

7.1. Die Auftraggeberin stimmt zu, dass die Auftragnehmerin die in Anhang 2 genannten Subunternehmer zur Erfüllung der vertraglich vereinbarten Leistungen hinzuzieht. Die Auftragnehmerin ist im Rahmen ihrer vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern befugt. Über die beabsichtigte Hinzuziehung weiterer oder die Ersetzung bisheriger Subunternehmer informiert die Auftragnehmerin die Auftraggeberin in Textform mindestens 14 Tage vor deren Wirksamwerden. Die Auftragnehmerin ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Die Auftragnehmerin hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten.

7.2. Die Auftraggeberin kann der Änderung innerhalb von 10 Tagen nach Zugang der Information aus berechtigten datenschutzrechtlichen Gründen gegenüber der Auftragnehmerin in Textform widersprechen. Erfolgt kein

Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als erteilt. Liegt ein berechtigter datenschutzrechtlicher Grund vor und ist eine einvernehmliche Lösung zwischen den Parteien nicht möglich, steht der Auftraggeberin ein Sonderkündigungsrecht für den Hauptvertrag zu.

7.3. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat die Auftragnehmerin sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist, insbesondere durch einen Angemessenheitsbeschluss der EU-Kommission, die Zertifizierung nach dem EU-US Data Privacy Framework oder den Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln und ggf. die Schaffung weiterer Garantien.

7.4. Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice, sind nicht erfasst. Die Auftragnehmerin ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten der Auftraggeberin auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

7.5. Die Auftraggeberin stimmt außerdem zu, dass die in Anhang 2 genannten Subunternehmer ihrerseits weitere Unterauftragsverarbeiter einsetzen, soweit diese den Anforderungen des Art. 28 Abs. 4 DSGVO entsprechend verpflichtet sind. Dies betrifft insbesondere den Subunternehmer des Rechtsmoduls und den Subunternehmer, über den die KI-Funktionen an Sprachmodelle verschiedener Anbieter angebunden sind. Die jeweils aktuellen Listen dieser weiteren Unterauftragsverarbeiter stellt die Auftragnehmerin der Auftraggeberin auf Anfrage zur Verfügung. Über Änderungen informiert die Auftragnehmerin die Auftraggeberin nach Ziff. 7.1, sobald sie selbst davon Kenntnis erhält.

8. Anfragen und Rechte Betroffener

8.1. Die Auftraggeberin ist für die Wahrung der Betroffenenrechte allein verantwortlich.

8.2. Die Auftragnehmerin unterstützt die Auftraggeberin nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, der Pflicht der Auftraggeberin zur Beantwortung und Erfüllung von Anfragen von Betroffenen nach den Art. 12 bis 23 DSGVO nachzukommen, soweit die Auftraggeberin insoweit auf die Unterstützung der Auftragnehmerin angewiesen ist. Wendet sich eine betroffene Person unmittelbar an die Auftragnehmerin, leitet diese das Anliegen unverzüglich an die Auftraggeberin weiter.

8.3. Auf Anforderung der Auftraggeberin stellt die Auftragnehmerin die über den Cookie-Banner protokollierten Einwilligungsnachweise zur Verfügung, soweit dies zur Erfüllung von Nachweis- oder Auskunftspflichten der Auftraggeberin erforderlich ist.

9. Haftung

Auftraggeberin und Auftragnehmerin haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

10. Beendigung des Hauptvertrages

10.1. Die Auftragnehmerin wird der Auftraggeberin nach Beendigung des Hauptvertrags oder jederzeit auf deren Anforderung alle ihr überlassenen Unterlagen, Daten und Datenträger sowie erstellten Verarbeitungs- und Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, zurückgeben, soweit die Auftraggeberin darauf nicht selbst Zugriff nehmen kann, oder auf Wunsch der Auftraggeberin löschen, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Dies betrifft auch etwaige Datensicherungen bei der Auftragnehmerin.

10.2. Die Auftragnehmerin ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihr im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus so lange gültig, wie die Auftragnehmerin über personenbezogene Daten verfügt, die ihr von der Auftraggeberin zugeleitet wurden oder die sie für diese erhoben hat.

10.3. Die Auftragnehmerin veranlasst nach Beendigung des Hauptvertrags die Löschung der Daten auch bei ihren Unterauftragsverarbeitern, für das Rechtsmodul innerhalb von 30 Tagen nach Vertragsende, soweit keine

gesetzliche Aufbewahrungspflicht besteht. Einwilligungsnachweise kann die Auftraggeberin bis zum Vertragsende nach Ziff. 8.3 anfordern.

Anhang 1: Technische und organisatorische Maßnahmen der Auftragnehmerin gemäß Art. 32 DSGVO

Stand: 15. Oktober 2026

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Als Maßnahmen zur Zutrittskontrolle können zur Gebäude- und Raumsicherung unter anderem automatische Zutrittskontrollsysteme, Einsatz von Chipkarten und Transponder, Kontrolle des Zutritts durch Pförtnerdienste und Alarmanlagen eingesetzt werden. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken zu schützen. Darüber hinaus ist es sinnvoll, die Zutrittskontrolle auch durch organisatorische Maßnahmen (z. B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) zu stützen.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Alarmanlage	☒ Schlüsselregelung / Liste
☐ Automatisches Zugangskontrollsystem	☒ Empfang / Rezeption / Pförtner
☐ Biometrische Zugangssperren	☐ Besucherbuch / Protokoll der Besucher
☒ Chipkarten / Transpondersysteme	☐ Mitarbeiter- / Besucherausweise
☒ Manuelles Schließsystem	☐ Besucher in Begleitung durch Mitarbeiter
☒ Sicherheitsschlösser	☐ Sorgfalt bei Auswahl des Wachpersonals
☐ Schließsystem mit Codesperre	☒ Sorgfalt bei Auswahl Reinigungsdienste
☐ Schließsystem per App	
☒ Türen mit Knauf Außenseite	
☐ Klingelanlage mit Kamera	
☐ Videoüberwachung der Eingänge	

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können. Mit Zugangskontrolle ist die unbefugte Verhinderung der Nutzung von Anlagen gemeint. Möglichkeiten sind beispielsweise Bootpasswort, Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, Bildschirmschoner mit Passwort, der Einsatz von Chipkarten zur Anmeldung wie auch der Einsatz von CallBack-Verfahren. Darüber hinaus können auch organisatorische Maßnahmen notwendig sein, um beispielsweise eine unbefugte Einsichtnahme zu verhindern (z. B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Orientierungshilfen für die Anwender zur Wahl eines „guten“ Passworts).

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Login mit Benutzername + Passwort	☒ Verwalten von Benutzerberechtigungen
☒ Login mit biometrischen Daten	☒ Erstellen von Benutzerprofilen
☒ Anti-Viren-Software Server	☒ Zentrale Passwortvergabe
☒ Anti-Virus-Software Clients	☒ Richtlinie „Sicheres Passwort“
☒ Anti-Virus-Software mobile Geräte	☒ Richtlinie „Löschen / Vernichten“
☒ Firewall	☒ Richtlinie „Clean desk“
☐ Intrusion Detection Systeme	☒ Allg. Richtlinie Datenschutz und / oder Sicherheit
☐ Mobile Device Management	☐ Mobile Device Policy
☐ Einsatz VPN bei Remote-Zugriffen	☒ Anleitung „Manuelle Desktopsperre“
☒ Verschlüsselung von Datenträgern	

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Verschlüsselung Smartphones ☐ Gehäuseverriegelung ☐ BIOS Schutz (separates Passwort) ☐ Sperre externer Schnittstellen (USB) ☒ Automatische Desktopsperre ☒ Verschlüsselung von Notebooks / Tablet	

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z. B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Aktenschredder (mind. Stufe 3, cross cut)	☐ Einsatz Berechtigungskonzepte
☐ Externer Aktenvernichter (DIN 32757)	☒ Minimale Anzahl an Administratoren
☒ Physische Löschung von Datenträgern	☐ Datenschutztresor
☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☒ Verwaltung Benutzerrechte durch Administratoren

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Trennung von Produktiv- und Testumgebung	☒ Steuerung über Berechtigungskonzept
☐ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☒ Festlegung von Datenbankrechten
☐ Mandantenfähigkeit relevanter Anwendungen	☐ Datensätze sind mit Zweckattributen versehen

1.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

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

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (mögl. verschlüsselt)	☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

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

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung können z. B. Verschlüsselungstechniken und Virtual Private Network eingesetzt werden. Maßnahmen beim Datenträgertransport bzw. Datenweitergabe sind Transportbehälter mit Schließvorrichtung und Regelungen für eine datenschutzgerechte Vernichtung von Datenträgern.

Technische Maßnahmen	Organisatorische Maßnahmen
☐ E-Mail-Verschlüsselung (S/MIME / PGP)	☐ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☐ E-Mail-Signatur (S/MIME / PGP)	☐ Übersicht regelmäßiger Abruf- und Übermittlungsvorgänge
☐ Einsatz von VPN	☐ Weitergabe in anonymisierter oder pseudonymisierter Form
☒ Protokollierung der Zugriffe und Abrufe	☒ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
☐ Sichere Transportbehälter	☐ Persönliche Übergabe mit Protokoll
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	
☐ Nutzung von Signaturverfahren	

2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z. B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☐ Manuelle oder automatisierte Kontrolle der Protokolle	☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	☒ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	☒ Klare Zuständigkeiten für Löschungen

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

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Feuer- und Rauchmeldeanlagen	☒ Backup & Recovery-Konzept (ausformuliert)
☒ Feuerlöscher Serverraum	☐ Kontrolle des Sicherungsvorgangs
☒ Serverraumüberwachung Temperatur und Feuchtigkeit	☐ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☒ Serverraum klimatisiert	☐ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒ USV	☐ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☐ Schutzsteckdosenleisten Serverraum	☐ Existenz eines Notfallplans (z. B. BSI IT-Grundschutz 100-4)
☐ Datenschutztresor (S60DIS, S120DIS, andere geeignete Normen mit Quelldichtung etc.)	
☐ Getrennte Partitionen für Betriebssysteme und Daten	
☐ RAID System / Festplattenspiegelung	
☐ Videoüberwachung Serverraum	
☐ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	

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

4.1 Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Software-Lösungen für Datenschutz-Management im Einsatz	☐ Interner / externer Datenschutzbeauftragter
☒ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z. B. Wiki, Intranet)	☒ Mitarbeiter geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
☐ Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	☒ Regelmäßige Sensibilisierung der Mitarbeiter, mindestens jährlich
☐ Alternatives Informationssicherheitskonzept	☐ Interner / externer Informationssicherheitsbeauftragter
☐ Anderweitiges dokumentiertes Sicherheitskonzept	☐ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
☐ Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☐ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	☐ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

4.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☐ Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
☐ Intrusion Detection System (IDS)	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen z. B. via Ticketsystem
☐ Intrusion Prevention System (IPS)	☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO); Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	
☒ Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen	

4.4 Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung. Sofern der Auftragnehmer Dienstleister im Sinne einer Auftragsverarbeitung einsetzt, sind die folgenden Punkte stets mit diesen zu regeln.

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln
	☒ Schriftliche Weisungen an den Auftragnehmer
	☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
	☐ Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen Bestellpflicht
	☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	☒ Regelung zum Einsatz weiterer Subunternehmer
	☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	☒ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Anhang 2: Genehmigte Subunternehmer

Die nachfolgenden Unternehmen sind genehmigte Unterauftragnehmer im Sinne der Ziff. 7. Die eingesetzten Fachleute aus dem Paceways-Netzwerk (Nr. 9) teilt die Auftragnehmerin der Auftraggeberin auf Anfrage mit. Jede Fachkraft wird vor dem ersten Zugriff nach Ziff. 7.1 verpflichtet.

#	Name	Betreibergesellschaft	Anschrift	Ort der Verarbeitung	Einsatzbereich
1	Amazon Web Services (AWS)	Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855 Luxemburg	USA und Rechenzentrum Deutschland	E-Mail-Versand
2	Plausible	Plausible Insights OÜ	Västriku tn 2, 50403 Tartu, Estland	EU	Webanalysedienst
3	OpenRouter	OpenRouter, Inc.	USA (Kontakt: privacy@openrouter.ai)	USA	Anbindung von Sprachmodellen verschiedener Anbieter (u. a. OpenAI, Anthropic, Google) für die KI-Funktionen der Plattform
3a	OpenAI	OpenAI Ireland Ltd.	1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Irland	USA	Direkte Nutzung von Sprachmodellen im Rahmen des Website-Erstellungsservice
3b	Anthropic	Anthropic Ireland, Limited	Dublin, Irland	USA	Direkte Nutzung von Sprachmodellen im Rahmen des Website-Erstellungsservice
4	PrivacyBee	PrivacyBee AG	c/o Domenig & Partner Rechtsanwälte, Laupenstrasse 1, 3008 Bern, Schweiz	EU (Hosting über Heroku in der EU-Region), Impressum-Generierung in den USA (OpenAI), siehe Tabelle unten	Erstellung und Aktualisierung von Datenschutzerklärung und Impressum, Einholung, Verwaltung und Protokollierung von Einwilligungen (Cookie-Banner)
5	netcup	netcup GmbH	Daimlerstraße 25, 76185 Karlsruhe, Deutschland	Deutschland	Hosting der unvyl Plattform
6	InterNetX	InterNetX GmbH	Johanna-Dachs-Str. 55, 93055 Regensburg, Deutschland	Deutschland	Domainanbieter
7	Microsoft	Microsoft Ireland Operations Limited	One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	EU und USA	E-Mail und Bürokommunikation (Microsoft 365)
8	Backblaze	Backblaze, Inc.	201 Baldwin Ave, San Mateo, CA 94401, USA	USA und Rechenzentrum Niederlande	Backup
9	Fachleute aus dem Paceways-Netzwerk	Einzelne freiberufliche Fachleute	Liste auf Anfrage	EU	Erstellung und Bearbeitung von Websites im Rahmen des Website-Erstellungsservice und weiterer Dienstleistungen, mit Zugriff auf das Nutzerkonto der Auftraggeberin

Unterauftragsverarbeiter von PrivacyBee (Ziff. 7.5)

Nach dem Verarbeitungsverzeichnis von PrivacyBee verarbeiten die folgenden weiteren Unterauftragsverarbeiter Daten aus den Websites der Auftraggeberin oder können im Support damit in Berührung kommen.

Anbieter	Sitz / Serverstandort	Zweck	Betroffene Daten der Auftraggeberin	Drittlandtransfer
Heroku Inc. (Salesforce)	USA / EU (EU-Region von PrivacyBee bestätigt)	Hosting der PrivacyBee-Applikation	Alle Daten des Rechtsmoduls nach Ziff. 2.1, insbesondere Einwilligungsnachweise der Websitebesucher	EU-US Data Privacy Framework (Salesforce), Standardvertragsklauseln
OpenAI L.L.C.	USA / USA, kein EU-Hosting	Generierung von Texten, Extraktion von Impressumsdaten aus öffentlichen Website-Inhalten	Firmenname, Website-URL, Land, Impressumsangaben (Name, Adresse, E-Mail, Telefon)	Kein Data Privacy Framework. Standardvertragsklauseln 2021/914 Modul 2, Transfer Impact Assessment TIA-2026-001-OpenAI
Freshworks Inc. (Freshdesk)	USA / EU	Support-Ticketsystem	Daten in Supportfällen, die unvyl an PrivacyBee weitergibt	EU-US Data Privacy Framework, Standardvertragsklauseln
Microsoft Corporation (Microsoft 365)	USA / EU	Interner Arbeitsbereich von PrivacyBee	Daten in E-Mails und Dokumenten zu Supportfällen	EU-US Data Privacy Framework, Standardvertragsklauseln

Anbieter	Sitz / Serverstandort	Zweck	Betroffene Daten der Auftraggeberin	Drittlandtransfer
Slack Technologies LLC (Salesforce)	USA / USA und EU	Interne Kommunikation von PrivacyBee	Daten, die intern zu Supportfällen besprochen werden	EU-US Data Privacy Framework, Standardvertragsklauseln

Die vollständige und jeweils aktuelle Liste stellt die Auftragnehmerin auf Anfrage zur Verfügung (Ziff. 7.5).