Auftragsverarbeitungsvertrag[1] nach Art. 28 Abs. 3 DSGVO

Nutzer

als Verantwortlicher (hier bezeichnet als „**Auftraggeber**“)

und

PENEMUE Technologies GmbH, Rathausgasse 48, 79098 Freiburg

als Auftragsverarbeiter (hier bezeichnet als „**Auftragnehmer**“)

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 2 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

In diesem Vertrag verwendete Begriffe, die in Art. 4, 9 und 10 DSGVO definiert werden, sind im Sinne der gesetzlichen Definition zu verstehen.

§ 2 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich der IT-gestützten Analyse von Beiträgen auf den zwischen den Parteien abgestimmten Social Media Accounts des Auftraggebers und der Erkennung von Hass-Kategorien (Hate Speech).

Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers, sofern der Auftragnehmer nicht durch das Recht der Union oder deutsches Recht zu einer anderen Verarbeitung verpflichtet ist. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus der **Anlage 1** zu diesem Vertrag.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden oder auf sonstige Weise in dessen Auftrag verarbeitet werden.

(4) Die Laufzeit dieses Vertrags zur kostenlosen Testnutzung beträgt 2 Wochen ab Verbindung der Social Media Accounts.

(5) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den europäischen Wirtschaftsraum (Beschluss 94/1/EG) statt. Jede Verlagerung von Teilleistungen oder

[1] Aus Gründen der besseren Lesbarkeit wird in diesem Dokument die Sprachform des generischen Maskulinums verwendet.

der gesamten Dienstleistung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers in Schriftform oder dokumentiertem elektronischen Format und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO, einschließlich aller damit einhergehenden erforderlichen Maßnahmen, erfüllt sind.

§ 3 Art der personenbezogenen Daten, Kategorien betroffener Personen

Im Rahmen der Durchführung des Auftrages gemäß § 2 erhält der Auftragnehmer Zugriff auf die in **Anlage 1** näher spezifizierten personenbezogenen Daten der ebenfalls in **Anlage 1** näher spezifizierten betroffenen Personen. Diese Daten umfassen die in **Anlage 1** aufgeführten und als solche gekennzeichneten besonderen Kategorien personenbezogener Daten.

§ 4 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Vertragsgegenstands gemäß § 2 und gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten. Dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. 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) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in dokumentiertem elektronischem Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei weitere volle Kalenderjahre aufzubewahren. Weisungen, die über die vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

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

§ 5 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) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere mindestens die in **Anlage 2** aufgeführten Maßnahmen getroffen hat. Sofern auch besondere Kategorien personenbezogener Daten verarbeitet werden, trifft der Auftragnehmer zusätzlich die sich aus § 22 Abs. 2 BDSG ergebenden

angemessenen und spezifischen Maßnahmen. Der Auftragnehmer legt auf Anforderung des Auftraggebers die näheren Umstände der Festlegung und Umsetzung der Maßnahmen offen. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Beim Auftragnehmer ist als betrieblicher Datenschutzbeauftragter benannt: UvH Datenschutzberatung UG, vertreten durch Dr. Frank Eickmeier, 040-414000-34, info@uvh-datenschutzberatung.com .

(4) Den bei der Datenverarbeitung durch den Auftragnehmer eigenen beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu nutzen oder auf sonstige Weise zu verarbeiten. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im Folgenden Beschäftigte genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und über die sich aus diesem Vertrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren sowie mit der gebotenen Sorgfalt die Einhaltung der vorgenannten Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Vertragsverhältnisses zwischen den eigenen Beschäftigten und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 6 Informationspflichten 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 personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich, spätestens jedoch innerhalb von 48 Stunden, in Schriftform oder dokumentiertem elektronischen Format informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält soweit möglich folgende Informationen:

a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
b. eine Beschreibung der wahrscheinlichen Folgen der Verletzung und
c. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Person(en), informiert hierüber den Auftraggeber und ersucht diesen um weitere Weisungen.

(3) Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Abs. 1 betroffen sind.

(4) Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Pflichten des Auftraggebers nach Art. 33 und 34 DSGVO in angemessener Weise (Art. 28 Abs. 3 S. 2 lit. f DSGVO). Meldungen für den Auftraggeber nach Art. 33 oder 34 DSGVO darf der Auftragnehmer nur nach vorheriger Weisung seitens des Auftraggebers gem. § 4 dieses Vertrags durchführen.

(5) Sollten die Daten des Auftraggebers 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 bei dem Auftraggeber als „Verantwortlichen" im Sinne der DSGVO liegt.

(6) Über wesentliche Änderungen der Sicherheitsmaßnahmen nach § 5 Abs. 2 dieses Vertrags hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(7) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten (vgl. § 5 Abs. 3 dieses Vertrags) ist dem Auftraggeber unverzüglich mitzuteilen.

(8) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

(9) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber sowie bei der Erstellung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden gem. Art. 36 DSGVO hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z.B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung (mindestens drei Kalendertage vorher) zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche, schriftliche oder elektronische Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(3) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftragnehmer stellt dem Auftraggeber auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(5) Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der eigenen Beschäftigten nach § 5 Abs. 4 dieses Vertrags auf Verlangen nach.

§ 8 Einsatz von Sub-Unternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 3** genannten Sub-Unternehmer durchgeführt. Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Sub-Unternehmern („Sub-Unternehmerverhältnis“) befugt, soweit er den Auftraggeber hiervon vorab in Kenntnis setzt und dieser der Beauftragung des Sub-Unternehmers vorab schriftlich oder in dokumentiertem elektronischem Format zugestimmt hat. Der Auftragnehmer ist verpflichtet, Sub-Unternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Sub-Unternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) wahrnehmen kann. Sofern eine Einbeziehung von Sub-Unternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Sub-Unternehmer ein angemessenes Datenschutzniveau gewährleistet ist. Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Sub-Unternehmern nachweisen.

(2) Ein Sub-Unternehmerverhältnis 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, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt, sowie Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Sub-Unternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 9 Anfragen und Rechte betroffener Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32-36 DSGVO.

(2) Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist die betroffene Person unverzüglich an den Auftraggeber und wartet weitere Weisungen ab.

§ 10 Haftung

(1) Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung. Der Auftragnehmer stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Auftraggeber ab.

(2) Der Auftragnehmer stellt den Auftraggeber auf erstes Anfordern von sämtlichen Ansprüchen frei, die betroffene Personen gegen den Auftraggeber wegen der Verletzung einer dem Auftragnehmer durch die DSGVO auferlegten Pflicht oder der Nichtbeachtung oder Verletzung einer vom Auftraggeber in dieser AV-Vereinbarung oder einer gesondert erteilten Anweisung geltend machen.

(3) Die Parteien stellen sich jeweils von der Haftung frei, wenn / soweit eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Abs. 5 DSGVO.

§ 11 Schlussbestimmungen

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

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder eines dokumentierten elektronischen Formats. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Freiburg im Breisgau.

Anlagen:

Anlage 1: Beschreibung der betroffenen Personen / Betroffenengruppen sowie der Daten / Datenkategorien und Zwecke der Verarbeitung

Anlage 2: Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 3: Genehmigte Sub-Unternehmer

Anlage 4: Weisungsempfänger beim Auftragnehmer

<u>Anlage 1</u>: Beschreibung der betroffenen Personen / Betroffenengruppen sowie der Daten / Datenkategorien und Zwecke der Verarbeitung

A. Betroffene Personen / Betroffenengruppen

- Beschäftigte des Auftraggebers (User des Penemue Tools [Seats]);
- Nutzer von sozialen Netzwerken, die Beiträge / Posts mit Bezugnahme auf den Auftraggeber im entsprechenden sozialen Netzwerk in den vom Auftraggeber ausgewählten Social Media Kanälen veröffentlichen.
- Nutzer von sozialen Netzwerken, die Beiträge des Auftraggebers im entsprechenden sozialen Netzwerk kommentieren.

B. Daten / Datenkategorien

Die von dem Auftragnehmer verarbeiteten personenbezogenen Daten können jeweils einer oder mehreren der folgenden Datenkategorien zugeordnet werden:

1. Personenbezogene Daten (Art. 4 Nr. 1 DSGVO):

- Stammdaten (Username bei sozialem Netzwerk, ggf. Name, Vorname, Profilbild);
- Inhaltsdaten, d.h. personenbezogene Inhalte, die von der betroffenen Person im Rahmen des sozialen Netzwerks gemacht werden:
  - Beiträge / Posts bei sozialem Netzwerk [inkl. URL, Datum, Uhrzeit von zu nennenden Usern/Accounts];
  - Kommentare / Replies von Nutzern zu einem Beitrag [inkl. Datum, Uhrzeit, ID, Username];
  - Direktnachrichten an Social Media Kanäle des Auftraggebers sofern von diesem gesondert beauftragt.

2. Besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO):

- ggf. Inhaltsdaten, d.h. sensible Informationen, die von der betroffenen Person im Rahmen des sozialen Netzwerks angegeben werden.

C. Zwecke der Verarbeitung

- Erkennung und Kategorisierung von (möglicherweise) strafrechtlich relevanter Hatespeech in sozialen Netzwerken, die in Zusammenhang mit dem Auftraggeber steht. Die Analyse erfolgt mittels Einsatzes von sog. „künstlicher Intelligenz“;
- Erbringung von Service- und Supportleistungen.

Anlage 2: Technische und organisatorische Maßnahmen des Auftragnehmers

Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

der Organisation
Penemue
Technologies
GmbH
Stand
01.11.2026

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.

Die og. Organisation erfüllt diesen Anspruch durch folgende Maßnahmen:

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. 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
☐ Absicherung der Gebäudeschächte	
☒ Türen mit Knauf Außenseite	
☐ Klingelanlage mit Kamera	

☐ Videoüberwachung der Eingänge	

Wir haben keine physischen Server (Datenverarbeitungsanlagen), die wir selbst in eigenen Räumen verwalten. Wir nutzen externe Dienstleister für unsere Server, die die Zutrittskontrolle gewährleisten.

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

Weitere Maßnahmen: -

Für den Login nutzen wir Multi-Faktor Authentifizierungen, also die Kombination aus mehreren Sicherheitsschritten.

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
☐	☐
☐	☐

Weitere Maßnahmen: -

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

Weitere Maßnahmen: Jeder Nutzende muss sich mit einem Account anmelden und erhält nur Zugriff auf seine/ihre eigenen Daten.

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 entsprechende technischen und organisatorischen Maßnahmen unterliegen;

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

Weitere Maßnahmen:

Nutzende werden über interne IDs identifiziert.

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
☒ Email-Verschlüsselung	☒ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☒ Einsatz von VPN	☒ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☒ Protokollierung der Zugriffe und Abrufe	☒ Weitergabe in anonymisierter oder pseudonymisierter Form
☒ Sichere Transportbehälter	☒ Sorgfalt bei Auswahl von Transport-, Personal und Fahrzeugen
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	☒ Persönliche Übergabe mit Protokoll
☐ Nutzung von Signaturverfahren	☐
☐	☐
☐	☐

Weitere Maßnahmen: -

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

Weitere Maßnahmen: -

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	☐
☐	☐
☐	☐
☐	☐

Weitere Maßnahmen:
Daten werden bei unseren externen Server-Anbietern auf mehreren Servern in Deutschland verteilt aufbewahrt, um die Verfügbarkeit zu gewährleisten.

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	☒ Externer Datenschutzbeauftragter: Dr. Frank Eickmeier, UNVERZAGT Rechtsanwälte Partnerschaftsgesellschaft mbB
☒ Zentrale Dokumentation aller Verfahrens-weisen 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
☒ Anderweitiges dokumentiertes Sicherheitskonzept	☒ Interner Informationssicherheits-beauftragter: Marlon Lückert, CTO, Penemue
☒ Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☒ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
☐	☒ Die Organisation kommt den Informations-pflichten nach Art. 13 und 14 DSGVO nach
☐	☒ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
☐	☐
☐	☐

Weitere Maßnahmen: -

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

Weitere Maßnahmen:

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 Widerrufrechts des Betroffenen durch technische Maß- nahmen	☐
☐	☐
☐	☐

Weitere 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 Standard-Vertragsklauseln
☐	☒ Schriftliche Weisungen an den Auftragnehmer
☐	☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
☐	☒ Verpflichtung zur Bestellung eines Daten-schutzbeauftragten 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

Anlage 3: Genehmigte Sub-Unternehmer

Die nachfolgenden Unternehmen sind genehmigte Sub-Unternehmer im Sinne des § 8 dieses Vertrags:

Sub-Unternehmer	**Leistung**	**Nähere Angaben zu Bestimmungen aus Art. 44 ff. DSGVO** (wenn Verarbeitung in Drittland)
Amazon Web Services Germany GmbH Krausenstr. 38 10117 Berlin	Datenbank (AWS RDS), Datei Speicher (AWS S3), Server für Background Jobs (AWS EC2)	Keine Übertragung außerhalb der EU
Microsoft Deutschland GmbH Walter-Gropius-Straße 5 80807 München	DB Hosting/Infrastruktur	Keine Übertragung außerhalb der EU
Vercel GmbH Friedrichstr. 88 10117 Berlin Deutschland	Frontend/Backend Hosting	Keine Übertragung außerhalb der EU
Google Cloud EMEA Limited, 70 Sir John Rogerson's Quay, Dublin 2, Irland	Cloud-Infrastruktur und AI-Services	Keine Übertragung außerhalb der EU (Server-Standort: Niederlande / EU-Multiregion)
PostHog, San Francisco, 2261 Market St #4008, San Francisco	Product Analytics	Keine Übertragung außerhalb der EU (Serverstandort Frankfurt)
Sendinblue GmbH (Brevo) Köpenicker Straße 126 10179 Berlin	E-Mail-Server	Keine Übertragung außerhalb der EU
TikTok Technology Limited, The Sorting Office, Ropemaker Place, Dublin 2, Dublin, D02 HD23, Ireland	API für Zugang zu Social Media Daten	Keine Übertragung außerhalb der EU
Google Ireland Limited Gordon House, Barrow Street Dublin 4 Ireland	API für Zugang zu Social Media Daten	Keine Übertragung außerhalb der EU
Meta Platforms Technologies Ireland Limited Merrion Road DUBLIN D04 X2K5 CO Dublin	API für Zugang zu Social Media Daten	Keine Übertragung außerhalb der EU

Anlage 4: Weisungsberechtigte Personen und Kommunikationsweg zur Weisung

A. Der Auftraggeber definiert eigenständig weisungsberechtigte Personen und stellt sicher, dass nur berechtigte Personen Zugriff auf die Anwendung bekommen.

B. Weisungsempfänger beim Auftragnehmer sind:

- Sara Egetemeyr, COO und Co-Geschäftsführung, sara@penemue.ai, +49-178-7184727,
- Jonas Navid Al-Nemri, CEO und Co-Geschäftsführer, jonas@penemue.ai, +49-151-15638643
- Marlon Lückert, CTO, marlon@penemue.ai, +49-1749824531