Vereinbarung zur Auftragsbearbeitung / Auftragsverarbeitung

Promptspace.ch / Naft Unique GmbH

Stand: 23. März 2026

Anbieterin und Geltungsbereich

Diese Auftragsverarbeitungvereinbarung regelt die vertraglichen Beziehungen zwischen der Naft Unique GmbH, c/o uhuhus KmG, Chamerstrasse 172, CH-6300 Zug, Schweiz, Handelsregister-Nr. CHE-181.461.693, nachfolgend „Promptspace“, und ihren Kunden betreffend die Nutzung der Leistungen von Promptspace.

zwischen

[Kunde / Firma / vollständige Anschrift]

als Verantwortliche/r im Sinne der Verordnung (EU) 2016/679 sowie, soweit anwendbar, als Verantwortliche/r im Sinne des schweizerischen Bundesgesetzes über den Datenschutz

nachfolgend „Verantwortlicher“ genannt

und

Naft Unique GmbH
c/o uhuhus KmG
Chamerstrasse 172
CH-6300 Zug
Schweiz

Handelsregister-Nr.: CHE-181.461.693

vertretungsberechtigt durch Martin Rüegsegger und Rolf Leuenberger
nachfolgend „Auftragsbearbeiter“ bzw. „Auftragsverarbeiter“ genannt
gemeinsam die „Parteien“, einzeln die „Partei“.

1. Zweck, Gegenstand und Verhältnis zum Hauptvertrag

1.1 Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit der Bearbeitung bzw. Verarbeitung personenbezogener Daten durch den Auftragsbearbeiter im Auftrag des Verantwortlichen.

1.2 Sie ergänzt den zwischen den Parteien bestehenden Hauptvertrag über die Nutzung der Leistungen von Promptspace, insbesondere Angebot, Bestellformular, Pilotvertrag, Leistungsbeschreibung, AGB oder sonstige schriftliche oder in Textform dokumentierte Vereinbarungen. Diese Vereinbarung ist integraler Bestandteil jedes Vertrags über die Nutzung der Leistungen von Promptspace. Die jeweils aktuelle Fassung kann auf der Website veröffentlicht werden. Für das konkrete Vertragsverhältnis gilt die bei Vertragsschluss einbezogene Fassung dieser Vereinbarung.

1.3 Soweit diese Vereinbarung Regelungen zur Bearbeitung bzw. Verarbeitung personenbezogener Daten enthält, gehen diese bei Widersprüchen den datenschutzbezogenen Regelungen des Hauptvertrags vor.

1.4 Diese Vereinbarung begründet keine eigenständige Leistungspflicht des Auftragsbearbeiters, sondern konkretisiert ausschliesslich die datenschutzrechtliche Ausgestaltung der im Hauptvertrag vereinbarten Leistungen.

2. Anwendbares Datenschutzrecht und Begriffe

2.1 Diese Vereinbarung ist so auszulegen, dass sie die Anforderungen von Art. 28 DSGVO sowie, soweit anwendbar, des schweizerischen Rechts zur Bearbeitung durch Auftragsbearbeiter erfüllt.

2.2 Soweit in dieser Vereinbarung der Begriff „Auftragsverarbeiter“ verwendet wird, umfasst dieser im schweizerischen Rechtskontext auch den „Auftragsbearbeiter“.

2.3 Der Verantwortliche bleibt für die Rechtmässigkeit der Datenbearbeitung, insbesondere für das Bestehen einer Rechtsgrundlage, die Erfüllung von Informationspflichten, die Wahrung von Betroffenenrechten sowie die Zulässigkeit der Beauftragung des Auftragsbearbeiters verantwortlich, soweit das anwendbare Recht nichts anderes vorsieht.

3. Gegenstand, Art, Zweck und Dauer der Bearbeitung

3.1 Gegenstand, Art, Zweck, Kategorien personenbezogener Daten, Kategorien betroffener Personen sowie Dauer der Bearbeitung ergeben sich aus Anlage 1.

3.2 Der Auftragsbearbeiter bearbeitet personenbezogene Daten ausschliesslich zur Erbringung der im Hauptvertrag vereinbarten Leistungen und nur im Rahmen dieser Vereinbarung.

3.3 Eine Bearbeitung zu eigenen Zwecken des Auftragsbearbeiters ist ausgeschlossen, soweit sie nicht gesetzlich vorgeschrieben oder vom Verantwortlichen ausdrücklich und gesondert veranlasst wurde.

3.4 Diese Vereinbarung gilt für alle Tätigkeiten, bei denen der Auftragsbearbeiter oder von ihm eingesetzte weitere Auftragsbearbeiter personenbezogene Daten des Verantwortlichen im Rahmen des Hauptvertrags bearbeiten.

4. Weisungsbindung

4.1 Der Auftragsbearbeiter bearbeitet personenbezogene Daten ausschliesslich auf dokumentierte Weisung des Verantwortlichen, sofern er nicht durch anwendbares Recht zu einer bestimmten Bearbeitung verpflichtet ist. In einem solchen Fall informiert der Auftragsbearbeiter den Verantwortlichen vor der Bearbeitung, soweit eine solche Information rechtlich zulässig ist.

4.2 Weisungen sind mindestens in Textform zu erteilen. E-Mail genügt.

4.3 Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.

4.4 Hält der Auftragsbearbeiter eine Weisung für offensichtlich rechtswidrig, weist er den Verantwortlichen unverzüglich darauf hin. Bis zur Bestätigung oder Anpassung der Weisung ist der Auftragsbearbeiter berechtigt, deren Umsetzung auszusetzen.

4.5 Der Auftragsbearbeiter ist nicht verpflichtet, Weisungen umzusetzen, die über die im Hauptvertrag vereinbarten Leistungen hinausgehen, sofern die Parteien hierzu keine gesonderte Vereinbarung treffen.

5. Vertraulichkeit und berechtigter Zugang

5.1 Der Auftragsbearbeiter stellt sicher, dass Personen, die unter seiner Verantwortung Zugang zu personenbezogenen Daten haben, diese nur auf Weisung des Verantwortlichen bearbeiten, sofern sie nicht gesetzlich zur Bearbeitung verpflichtet sind.

5.2 Der Auftragsbearbeiter verpflichtet alle zur Bearbeitung personenbezogener Daten eingesetzten Personen in geeigneter Weise zur Vertraulichkeit oder stellt sicher, dass diese einer angemessenen gesetzlichen Geheimhaltungspflicht unterliegen.

5.3 Der Zugriff auf personenbezogene Daten ist auf diejenigen Personen zu beschränken, die ihn zur Erbringung der vertraglich geschuldeten Leistungen benötigen.

6. Technische und organisatorische Massnahmen

6.1 Der Auftragsbearbeiter trifft geeignete technische und organisatorische Massnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dabei berücksichtigt er insbesondere den Stand der Technik, die Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Bearbeitung und die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte natürlicher Personen.

6.2 Die zum Zeitpunkt des Vertragsschlusses bestehenden technischen und organisatorischen Massnahmen sind in Anlage 2 beschrieben.

6.3 Der Auftragsbearbeiter ist berechtigt, technische und organisatorische Massnahmen zu ändern oder zu ersetzen, sofern das Schutzniveau insgesamt nicht unterschritten wird.

6.4 Der Auftragsbearbeiter wird dem Verantwortlichen auf Verlangen geeignete Informationen zur Verfügung stellen, die erforderlich sind, um die Einhaltung dieser Verpflichtungen nachzuweisen.

7. Unterstützung des Verantwortlichen

7.1 Der Auftragsbearbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Bearbeitung und der ihm zur Verfügung stehenden Informationen durch geeignete technische und organisatorische Massnahmen, soweit dies erforderlich ist, damit der Verantwortliche seinen datenschutzrechtlichen Pflichten nachkommen kann.

7.2 Dies umfasst insbesondere Unterstützung bei Anfragen betroffener Personen, bei der Sicherheit der Bearbeitung, bei der Meldung und Behandlung von Verletzungen des Schutzes personenbezogener Daten, bei Datenschutz-Folgenabschätzungen sowie bei allfälligen Konsultationen von Aufsichtsbehörden, soweit die Unterstützung nach Art und Umfang der beauftragten Leistung erforderlich und zumutbar ist.

7.3 Soweit eine Unterstützung über die vertraglich geschuldeten Standardleistungen hinausgeht und erheblichen Zusatzaufwand verursacht, kann der Auftragsbearbeiter hierfür eine angemessene Vergütung verlangen, sofern dies im Hauptvertrag vorgesehen ist oder vorab vereinbart wird.

8. Meldung von Datenschutzverletzungen

8.1 Der Auftragsbearbeiter informiert den Verantwortlichen unverzüglich nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten, die personenbezogene Daten des Verantwortlichen betrifft.

8.2 Die Meldung enthält zumindest die dem Auftragsbearbeiter zu diesem Zeitpunkt verfügbaren Informationen, die der Verantwortliche benötigt, um seinen gesetzlichen Melde- und Benachrichtigungspflichten nachzukommen.

8.3 Weitere Informationen werden nachgereicht, sobald sie verfügbar sind.

8.4 Der Auftragsbearbeiter trifft im Rahmen seiner Möglichkeiten unverzüglich angemessene Massnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen.

9. Weitere Auftragsbearbeiter / Unterauftragsverarbeiter

9.1 Der Verantwortliche erteilt dem Auftragsbearbeiter eine allgemeine schriftliche Genehmigung zur Beiziehung weiterer Auftragsbearbeiter, soweit diese in Anlage 3 aufgeführt sind oder nach Massgabe dieser Ziffer wirksam angekündigt werden.

9.2 Der Auftragsbearbeiter informiert den Verantwortlichen in Textform über beabsichtigte Änderungen bei der Beiziehung oder dem Ersatz weiterer Auftragsbearbeiter.

9.3 Der Verantwortliche kann einer solchen Änderung innerhalb von 14 Kalendertagen ab Zugang der Mitteilung aus wichtigem datenschutzrechtlichem Grund widersprechen.

9.4 Erfolgt kein fristgerechter Widerspruch, gilt die Änderung als genehmigt.

9.5 Im Fall eines berechtigten Widerspruchs werden die Parteien prüfen, ob die Leistung ohne den betroffenen weiteren Auftragsbearbeiter fortgesetzt werden kann. Ist dies nicht zu wirtschaftlich vertretbaren Bedingungen möglich, kann der Auftragsbearbeiter die betroffene Leistung mit angemessener Frist einstellen oder den Hauptvertrag insoweit ausserordentlich kündigen.

9.6 Der Auftragsbearbeiter verpflichtet jeden weiteren Auftragsbearbeiter vertraglich zu Datenschutzpflichten, die dem Schutzniveau dieser Vereinbarung entsprechen, soweit dies für die jeweilige Leistung erforderlich ist.

10. Datenbearbeitung in der Schweiz, im EU/EWR und in Drittstaaten

10.1 Die Bearbeitung personenbezogener Daten erfolgt grundsätzlich in der Schweiz sowie, soweit erforderlich, im EU/EWR.

10.2 Erfolgt eine Bearbeitung ausserhalb der Schweiz und ausserhalb des EU/EWR oder ein Zugriff aus einem solchen Staat, stellt der Auftragsbearbeiter sicher, dass die hierfür nach anwendbarem Datenschutzrecht erforderlichen Voraussetzungen erfüllt sind.

10.3 Soweit der Verantwortliche ausdrücklich Dienste aktiviert oder Weisungen erteilt, bei denen ein Drittstaatentransfer erfolgt oder nicht vollständig ausgeschlossen werden kann, bleibt der

Verantwortliche für die datenschutzrechtliche Zulässigkeit dieser Weisung verantwortlich, sofern der Auftragsbearbeiter ihn zuvor transparent über die Transferkonstellation informiert hat.

11. Kontrollrechte und Nachweise

11.1 Der Auftragsbearbeiter stellt dem Verantwortlichen auf Verlangen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung dieser Vereinbarung nachzuweisen.

11.2 Der Nachweis kann insbesondere durch aktuelle Zertifizierungen, Auditberichte, Prüfberichte, Sicherheitsdokumentationen, Selbstauskünfte oder andere geeignete Nachweise erbracht werden.

11.3 Vor-Ort-Prüfungen durch den Verantwortlichen oder einen unabhängigen, zur Vertraulichkeit verpflichteten Prüfer sind nur zulässig, wenn ein konkreter sachlicher Anlass besteht, die Prüfung erforderlich ist und überwiegende berechtigte Interessen des Auftragsbearbeiters oder anderer Kunden nicht entgegenstehen.

11.4 Vor-Ort-Prüfungen sind mit angemessener Frist schriftlich anzukündigen, während der üblichen Geschäftszeiten durchzuführen und so auszugestalten, dass Betriebsabläufe, Sicherheitsmassnahmen sowie Vertraulichkeitsinteressen anderer Kunden nicht unverhältnismässig beeinträchtigt werden.

11.5 Der Verantwortliche trägt die Kosten der von ihm veranlassten Prüfungen selbst, sofern nicht eine wesentliche Pflichtverletzung des Auftragsbearbeiters nachgewiesen wird.

12. Betroffenenanfragen

12.1 Der Auftragsbearbeiter wird den Verantwortlichen unverzüglich informieren, wenn eine betroffene Person ihre Rechte unmittelbar gegenüber dem Auftragsbearbeiter geltend macht und die Anfrage dem Verantwortlichen zuzuordnen ist.

12.2 Ohne dokumentierte Weisung des Verantwortlichen wird der Auftragsbearbeiter eine solche Anfrage nicht eigenständig beantworten, es sei denn, er ist hierzu gesetzlich verpflichtet.

12.3 Der Auftragsbearbeiter unterstützt den Verantwortlichen angemessen bei der Bearbeitung solcher Anfragen.

13. Löschung, Rückgabe und Aufbewahrung

13.1 Nach Beendigung des Hauptvertrags wird der Auftragsbearbeiter alle personenbezogenen Daten, die er im Auftrag des Verantwortlichen bearbeitet hat, nach Wahl des Verantwortlichen löschen oder zurückgeben, sofern keine gesetzliche Pflicht zur weiteren

Aufbewahrung besteht. Erteilt der Verantwortliche bis spätestens 30 Kalendertage nach Vertragsende keine anderslautende Weisung, ist der Auftragsbearbeiter berechtigt, die betreffenden personenbezogenen Daten datenschutzkonform zu löschen.

13.2 Soweit gesetzliche Aufbewahrungspflichten bestehen, wird der Auftragsbearbeiter die betreffenden personenbezogenen Daten während der Dauer der Aufbewahrungspflicht nur noch zu diesem Zweck speichern und nach Ablauf der Frist löschen, sofern keine weitere Rechtsgrundlage besteht.

13.3 Gesetzlich oder zur Rechenschaft erforderliche Dokumentationen und Nachweise darf der Auftragsbearbeiter über das Vertragsende hinaus aufbewahren, soweit und solange erforderlich. Diese Unterlagen sind weiterhin vertraulich zu behandeln und gegen unbefugte Zugriffe zu schützen.

13.4 Der Auftragsbearbeiter bestätigt dem Verantwortlichen auf Verlangen die Löschung oder Rückgabe in angemessener Form.

14. Haftung

14.1 Die Haftung der Parteien richtet sich nach dem Hauptvertrag sowie nach den zwingenden Bestimmungen des anwendbaren Datenschutzrechts.

14.2 Vertragliche Haftungsbeschränkungen des Hauptvertrags gelten nicht, soweit zwingendes Datenschutzrecht entgegensteht.

15. Kontaktstelle für Datenschutz und Sicherheit

15.1 Der Auftragsbearbeiter benennt dem Verantwortlichen eine Kontaktstelle für Datenschutz- und Sicherheitsanfragen.

15.2 Aktuell ist dies:

Naft Unique GmbH
Kontaktstelle Datenschutz / Sicherheit:
Martin Rüegsegger, CEO; Rolf Leuenberger, CTO
E-Mail: contact@promptspace.ch

15.3 Änderungen der Kontaktstelle werden dem Verantwortlichen in Textform mitgeteilt.

16. Schlussbestimmungen

16.1 Änderungen und Ergänzungen dieser Vereinbarung bedürfen mindestens der Textform.

16.2 Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise unwirksam, undurchführbar oder lückenhaft sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien verpflichten sich, die betroffene Bestimmung durch eine wirksame Regelung zu ersetzen, die dem wirtschaftlichen und rechtlichen Zweck möglichst nahekommt.

16.3 Diese Vereinbarung untersteht materiellem schweizerischem Recht, unter Ausschluss des Kollisionsrechts, soweit dem keine zwingenden Bestimmungen des anwendbaren Datenschutzrechts entgegenstehen.

16.4 Ausschliesslicher Gerichtsstand ist, soweit gesetzlich zulässig, Zug, Schweiz.

Anlage 1 - Gegenstand, Art, Zweck, Datenkategorien und betroffene Personen

1. Gegenstand der Bearbeitung

Gegenstand der Bearbeitung ist die Bereitstellung und der Betrieb der Leistungen von Promptspace, insbesondere der Browser-Erweiterung, der administrativen Steuerungs- und Auditfunktionen, der Lizenzverwaltung, der Ausspielung technischer Regeln und Konfigurationen sowie der technischen Betriebsüberwachung.

2. Art der Bearbeitung

Die Bearbeitung umfasst, soweit jeweils erforderlich: Erheben, Strukturieren, Speichern, Auslesen, Übermitteln, Anzeigen, Protokollieren, Verschlüsseln und Löschen.

3. Zweck der Bearbeitung

Die Bearbeitung erfolgt ausschliesslich zu folgenden Zwecken:

Bereitstellung der vertraglich vereinbarten Promptspace-Funktionalitäten, Schutz sensibler Inhalte bei der Nutzung externer KI-Systeme, Lizenzverwaltung und Mandantenadministration, Verwaltung technischer Konfigurationen und Regeln, Bereitstellung von Audit- und Nutzungsmetadaten, technische Betriebsüberwachung, Stabilität und Sicherheit sowie Support und Fehlerbehebung.

4. Kategorien personenbezogener Daten

a) Im Backend verarbeitete Daten

Administrations- und Kontaktdaten von Kundenansprechpersonen, Login- und Authentifizierungsdaten für Dashboard-Administratoren, Lizenzdaten, Konfigurationsdaten, Audit-Metadaten, technische Betriebsdaten, verschlüsselt gespeicherte API-Keys sowie verschlüsselt gespeicherte Device-Identifikatoren.

Hierzu können insbesondere gehören: Company Keys in gehashter Form zur Lizenzvalidierung, Geräte-IDs zur Sitzplatz- und Lizenzverwaltung, Audit-Metadaten wie Aktion, Risiko-Level, Anzahl erkannter sensibler Elemente und Zeitstempel sowie Health Reports, insbesondere Fehlercodes und Systemstatus, zur technischen Überwachung, Stabilität und Sicherheit des Dienstes.

b) Lokal im Browser verarbeitete Daten

Vom Endnutzer eingegebene Texte, erkannte sensible Daten oder personenbezogene Inhalte sowie lokale Ersetzungs- und Zuordnungsinformationen zur Pseudonymisierung oder Re-Identifikation.

5. Kategorien betroffener Personen

Mitarbeitende des Verantwortlichen, Kunden, Interessenten, Klienten, Mandanten, Bewerbende, Patienten oder sonstige Dritte, deren Daten durch Endnutzer in zulässiger Weise bearbeitet werden, Kontaktpersonen beim Verantwortlichen sowie kundenseitige Dashboard-Administratoren.

6. Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogener Daten können nur betroffen sein, wenn Endnutzer des Verantwortlichen solche Daten in lokal verarbeiteten Inhalten verwenden. Ihre Erkennung und Verarbeitung erfolgt lokal im Browser des Endnutzers; eine Speicherung als Klartext im Backend des Auftragsbearbeiters erfolgt nicht.

7. Speicherorte und Abgrenzung der Verarbeitung

Die Erkennung sensibler Inhalte, die Pseudonymisierung und gegebenenfalls die Re-Identifikation erfolgen lokal im Browser des Endnutzers. Das Backend des Auftragsbearbeiters speichert keine Originaltexte, keine erkannten PII-Werte und keine lokalen Re-Identifikationszuordnungen, sondern ausschliesslich die für den Betrieb erforderlichen Lizenz-, Konfigurations-, Audit- und technischen Betriebsdaten. Die produktiven Backend-Daten werden in der Schweiz gehostet. Lokale Anonymisierungs- bzw. Re-Identifikationszuordnungen werden nur temporär im Browser verarbeitet und nicht an das Backend übermittelt.

8. Dauer der Bearbeitung

Die Dauer der Bearbeitung entspricht grundsätzlich der Laufzeit des Hauptvertrags. Ergänzend gelten, soweit im Hauptvertrag oder zwingenden Recht nichts Abweichendes vorgesehen ist, folgende Fristen: Lizenzdaten und Geräte-Identifikatoren werden für die Dauer des Vertragsverhältnisses und weitere 30 Tage aufbewahrt, Audit-Metadaten für 12 Monate und Health Reports für 90 Tage. Kundendaten werden nach Vertragsende grundsätzlich innerhalb von 30 Tagen gelöscht, soweit keine gesetzlichen Aufbewahrungspflichten, berechtigten Nachweisinteressen, technisch erforderlichen Backup-Zyklen oder im Einzelfall erforderlichen Aufbewahrungen zur Wahrung oder Durchsetzung von Rechtsansprüchen entgegenstehen.

Anlage 2 - Technische und organisatorische Massnahmen

Die nachfolgenden technischen und organisatorischen Massnahmen beschreiben den aktuellen Stand zum Datum dieser Vereinbarung. Der Auftragsbearbeiter ist berechtigt, diese weiterzuentwickeln, sofern das Schutzniveau insgesamt nicht unterschritten wird.

1. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Promptspace ist so ausgelegt, dass sensible Inhalte des Endnutzers lokal im Browser erkannt und verarbeitet werden. Originaltexte, erkannte PII-Werte und lokale Re-Identifikationszuordnungen verbleiben lokal und werden nicht im Backend gespeichert. Im Backend werden nur die für Betrieb, Lizenzierung, Konfiguration, Audit und technische Stabilität erforderlichen Daten verarbeitet.

Zur datenschutzfreundlichen Voreinstellung gehört zudem ein Fail-Closed-Ansatz: Ist eine sicherheitskritische Schutzkomponente für Erkennung, Pseudonymisierung oder Schutzlogik nicht verfügbar, wird die Übermittlung von Inhalten blockiert.

2. Zutritts- und Zugangskontrolle

Administrative Zugänge zu produktionsrelevanten Systemen sind durch Multi-Faktor-Authentisierung geschützt. SSH-Zugänge sind nur schlüsselbasiert zulässig. Dashboard-Administrationszugänge auf Kundenseite sind durch E-Mail/Passwort und TOTP-basierte Multi-Faktor-Authentisierung geschützt. Administrative Berechtigungen werden nach dem Need-to-know-Prinzip vergeben.

3. Zugriffskontrolle und Berechtigungskonzept

Der technische Zugriff auf produktive Systeme ist auf ausdrücklich autorisierte Personen beschränkt. Der technische Produktivzugriff auf Anbieter-Seite ist derzeit auf den CTO beschränkt. Der CEO hat keinen Server- oder Datenbankzugriff. Kundenseitige Administratoren erhalten ausschliesslich Zugriff auf die ihrer Organisation zugeordneten mandantenbezogenen Verwaltungsfunktionen. Die Mandantentrennung stellt sicher, dass jeder kundenseitige Administrator nur Daten seiner eigenen Organisation einsehen kann. Rollen und Berechtigungen werden nach dem Need-to-know-Prinzip vergeben und bei Bedarf angepasst.

4. Weitergabe- und Übertragungskontrolle

Verbindungen zwischen Browser-Erweiterung, Backend und weiteren technischen Komponenten sind TLS-verschlüsselt. Daten werden nur im zur Vertragserfüllung erforderlichen Umfang übermittelt. Inhalte der lokalen PII-Verarbeitung werden nicht an das Backend des Auftragsbearbeiters übermittelt, soweit sie nicht Teil der vorgesehenen Produktfunktion sind.

5. Speichersicherheit und Verschlüsselung

Soweit im Backend sensible technische Betriebs-, Lizenz-, Konfigurations- oder Auditdaten gespeichert werden, erfolgt dies nach dem Stand der Technik unter Einsatz angemessener Verschlüsselungs- und Schutzmechanismen. Company Keys werden nicht im Klartext, sondern ausschliesslich in gehashter Form gespeichert. Sensible Datenfelder und technische Identifikatoren werden verschlüsselt oder in vergleichbar geschützter Form gespeichert. Inhalte aus der lokalen PII-Verarbeitung des Endnutzers werden konstruktionsbedingt nicht im Backend gespeichert.

6. Eingabekontrolle und Nachvollziehbarkeit

Administrative und systembezogene Vorgänge werden im erforderlichen Umfang protokolliert. Für Kunden werden Audit-Metadaten und technische Nutzungsinformationen bereitgestellt, nicht jedoch die lokal verarbeiteten Klartextinhalte.

7. Verfügbarkeitskontrolle, Backup und Wiederherstellung

Von den produktiv gespeicherten Backend-Daten werden täglich automatisierte Sicherungskopien erstellt. Die Sicherungen werden für 30 Tage aufbewahrt. Die Backup-Speicherung erfolgt getrennt vom Primärsystem in einem separaten Schweizer Rechenzentrumsumfeld. Das Backup-Ziel ist dreifach repliziert. Ein erster dokumentierter Wiederherstellungstest erfolgt vor Go-Live. Danach werden Wiederherstellungstests periodisch, derzeit monatlich, durchgeführt. Der Zielwert für die Wiederherstellungszeit beträgt 24 Stunden. Der Zielwert für den maximalen Datenverlust beträgt 6 Stunden.

8. Trennungsgebot

Kundendaten verschiedener Organisationen werden logisch getrennt verarbeitet. Kundenseitige Dashboard-Zugriffe sind mandantenbezogen beschränkt. Die Trennung zwischen lokaler Browser-Verarbeitung und serverseitiger Verarbeitung technischer Backend-Daten ist systemseitig vorgesehen.

9. Datenschutzfreundlich Voreinstellungen und Schutzlogik

Der Auftragsbearbeiter setzt datenschutzfreundliche Voreinstellungen um und beschränkt die Bearbeitung personenbezogener Daten auf das für den jeweiligen Zweck erforderliche Mass. Die Lösung enthält Schutzmechanismen, die bei Ausfall sicherheitskritischer Komponenten ein unkontrolliertes Weiterverarbeiten oder Übermitteln von Inhalten verhindern. Ist eine wesentliche Schutzfunktion nicht verfügbar, wird die Übermittlung blockiert, bis diese wieder ordnungsgemäss bereitsteht.

10. Incident Management

Für Sicherheits- und Datenschutzvorfälle besteht ein dokumentierter Incident-Handling-Prozess. Vorfälle werden in die Stufen niedrig, mittel und kritisch klassifiziert. Jeder Vorfall wird in einem Incident-Log dokumentiert. Kritische Vorfälle werden unverzüglich eingedämmt, analysiert und hinsichtlich einer erforderlichen Kundeninformation bewertet. Datenschutzrelevante Vorfälle mit möglicher Auswirkung auf Kundendaten werden unverzüglich an die betroffenen Kunden eskaliert. Nach relevanten Vorfällen erfolgt eine dokumentierte Nachbearbeitung in Form einer Lessons-Learned-Notiz.

11. Organisationsmassnahmen

Zuständige zentrale Kontaktpersonen für technische Sicherheits- und Incident-Themen sind CEO und CTO. Administrative Rechte sind auf wenige ausdrücklich autorisierte Personen beschränkt. Der Zugang zu produktiven Systemen folgt dem Need-to-know-Prinzip. Änderungen an den technischen und organisatorischen Massnahmen werden nach Massgabe des Betriebsmodells dokumentiert und bei Bedarf angepasst.

Anlage 3 - Genehmigte weitere Auftragsbearbeiter / Unterauftragsverarbeiter

Die folgende Liste umfasst diejenigen weiteren Auftragsbearbeiter, die personenbezogene Daten des Verantwortlichen im Rahmen der Leistungserbringung für Promptspace verarbeiten.

Dienstleister	Adresse	Leistung	Datenkategorien	Ort	AVV / DPA
Infomaniak Network SA	Rue Eugène-Marziano 25, 1227 Les Acacias, Schweiz	Hosting, Server-Infrastruktur, Backup-Speicherung	Lizenzdaten, Konfigurationsdaten, Audit-Metadaten, technische Betriebsdaten	CH	Abgeschlossen

Reine Distributionsplattformen für Browser-Erweiterungen, über die lediglich der Extension-Code ausgeliefert wird, ohne Verarbeitung personenbezogener Kundendaten im Auftrag des Verantwortlichen, gelten im Rahmen dieser Vereinbarung nicht als weitere Auftragsbearbeiter.

Anlage 4 - Kontakt- und Ansprechpersonen

1. Weisungsberechtigte Personen beim Verantwortlichen

Name: [eintragen]
Funktion: [eintragen]
E-Mail: [eintragen]

2. Empfangsberechtigte Personen beim Auftragsbearbeiter

Naft Unique GmbH
Name: Martin Rüegsegger
Funktion: CEO
E-Mail: contact@promptspace.ch

Naft Unique GmbH
Name: Rolf Leuenberger
Funktion: CTO
E-Mail: contact@promptspace.ch