Lynk

DATENSCHUTZ-PAKET · LYNK IM EIGENEN CLOUD-KONTO

Ihre Kandidatendaten – *nachvollziehbar* geschützt.

Für Personalvermittlungen, die Lynk im eigenen Cloud- oder Serverkonto betreiben. Die HP Capital GmbH richtet es ein und hostet es nicht. Inhalt: Auftragsverarbeitungsvertrag für unseren Support-Zugriff (Art. 28 DSGVO), technische und organisatorische Maßnahmen (Art. 32 DSGVO), unsere Unterauftragsverarbeiter und die Anbieter, die Sie selbst beauftragen, sowie praktische Hinweise zu Informationspflichten, Löschfristen und EU AI Act.

MUSTER – vor Verwendung datenschutzrechtlich prüfen lassen

Dieses Paket ist ein Muster und keine Rechtsberatung. Werte in [eckigen Klammern] werden je Agentur ausgefüllt oder sind eine Wahl für die Rechtsberatung. Ihre Agentur ist Verantwortlicher; Ihre Cloud-, KI-, Unipile- und E-Mail-Anbieter sind Ihre eigenen Auftragsverarbeiter.

01
Auf einer Seite
Wo Ihre Kandidatendaten liegen und wer sie sehen kann

02
Auftragsverarbeitungsvertrag
Nur für unseren Zugriff bei Einrichtung, Support, Entwicklertagen und Wartung

03
Technische & organisatorische Maßnahmen
Software-Funktionen · unsere Zugriffsregeln · Ihre Seite

04
Unterauftragsverarbeiter & Ihre Anbieter
Unsere kurze Liste und die Anbieter, die Sie beauftragen

05
Ihre Pflichten als Verantwortlicher
Art. 14 DSGVO, berechtigtes Interesse, Löschung, EU AI Act

06
Offene Punkte zur Prüfung
Ihre Entscheidungen, unsere Aufgaben, Punkte für die Rechtsberatung

HP Capital GmbH · Mayrwiesstraße 11 · 5300 Hallwang (Salzburg) · Österreich · FN 631120 v · UID ATU82731634

Muster v1.0 · 29. September 2026

Inhalt

1 Wo Ihre Kandidatendaten liegen und wer sie sehen kann 2

2 Auftragsverarbeitungsvertrag (Art. 28 DSGVO) – Support-Zugriff 3

Anlage 2.A – Parteien und Kontakte 6

Anlage 2.B – Beschreibung der Verarbeitung 7

Anlage 2.C – Technische und organisatorische Maßnahmen 7

Anlage 2.D – Genehmigte Unterauftragsverarbeiter 7

3 Technische und organisatorische Maßnahmen (Art. 32 DSGVO) 8

3A Sicherheitsfunktionen der Software 8

3B Maßnahmen der HP Capital für den Support-Zugriff 9

3C Ihre Seite – Betrieb im eigenen Konto 10

4 Unterauftragsverarbeiter und Ihre Anbieter 11

4A Unterauftragsverarbeiter der HP Capital (AVV § 8) 11

4B Ihre Anbieter – von Ihnen beauftragt und bezahlt 11

5 Hinweise für Ihre eigene Compliance als Verantwortlicher 13

5.1 Rechtsgrundlage: berechtigtes Interesse 13

5.2 Kandidaten informieren (Art. 14 DSGVO) 13

5.3 Betroffenenanfragen 13

5.4 Speicherdauer und Löschung 14

5.5 Folgenabschätzung und automatisierte Entscheidungen 14

5.6 EU AI Act – was für Recruiting-KI gilt 14

5.7 Nutzung von LinkedIn 15

6 Offene Punkte und Entscheidungen zur Prüfung 16

7 Quellen 17

Stand dieses Pakets – bitte zuerst lesen

- **Muster, keine Rechtsberatung.** Alle rechtlichen Teile sind Entwürfe zur Prüfung durch eine Datenschutzberatung auf beiden Seiten. Werte in **[eckigen Klammern]** werden je Agentur ausgefüllt oder sind eine Wahl für die Rechtsberatung.
- **Lynk läuft in Ihrem eigenen Cloud-Konto.** Die HP Capital GmbH hostet Lynk nicht. Bei der Einrichtung installieren wir es in einem Cloud- oder Serverkonto, das Sie im eigenen Namen eröffnen und direkt bezahlen. Ihre Agentur ist für alle Kandidatendaten darin Verantwortlicher.
- **Ihre Anbieter sind Ihre Auftragsverarbeiter.** Cloud- oder Serveranbieter, KI-Anbieter (LLM), Unipile (LinkedIn-Anbindung), E-Mail-Anbieter und Ihr ATS/CRM beauftragen und bezahlen Sie selbst. Deren Auftragsverarbeitungsbedingungen schließen Sie direkt ab; sie sind keine Unterauftragsverarbeiter der HP Capital.
- **Wann HP Capital Auftragsverarbeiter ist.** Nur wenn wir bei Einrichtung, Support, Entwicklertagen, dem Einspielen von Updates oder Wartung (Fernzugriff) auf personenbezogene Daten in Ihrer Installation zugreifen. Der Auftragsverarbeitungsvertrag in Teil 2 regelt genau diesen begrenzten Zugriff: minimale Rechte, protokolliert, nach jeder Aufgabe entfernt.

1 Wo Ihre Kandidatendaten liegen und wer sie sehen kann

Eine Seite für Agenturinhaber, ohne Juristendeutsch – die Details folgen in Teil 2 bis 5.

LinkedIn
Ihr Recruiter findet ein Profil und importiert es

→

Ihr Lynk
Gespeichert in Ihrem eigenen Cloud-Konto, im Rechenzentrum Ihrer Wahl

→

Ihr KI-Anbieter
Liest Lebenslauftext für Score und Nachrichtenentwurf

→

Ihr Recruiter
Prüft, entscheidet und sendet – ein Mensch behält die Kontrolle

1 Wo die Daten liegen

In **Ihrer eigenen Lynk-Installation**, in einem Cloud- oder Serverkonto im **Namen Ihrer Agentur**. Sie wählen das Rechenzentrum; für EU-Agenturen empfehlen wir eines in der EU. Sie bezahlen den Anbieter direkt. HP Capital hostet Lynk nicht und behält keine Kopie Ihrer Daten.

2 Wem sie gehören

Ihnen. Ihre Agentur ist „Verantwortlicher". Nach der Übergabe halten Sie alle Schlüssel und Passwörter. Wir nutzen Ihre Kandidatendaten nie für eigene Zwecke oder zum Training von KI.

3 Wer in Ihrem Team sie sieht

Nur eingeladene Personen. Rollen legen fest, was sie dürfen: **Owner, Admin, Recruiter, Viewer**. Anmeldung mit Passwort (mind. 12 Zeichen) oder Microsoft-Konto; jeder Nutzer kann Zwei-Faktor-Codes aus einer Authenticator-App einrichten.

4 Wer sie sonst sehen kann

- **Ihre Anbieter**, von Ihnen beauftragt: Cloud oder Server, KI-Anbieter, Unipile (LinkedIn-Anbindung), E-Mail, Ihr ATS/CRM. Jeder erhält nur, was er braucht.
- **HP Capital** – nur bei Einrichtung, Support, Entwicklertagen, Updates oder Wartung, um die Sie bitten: persönlicher, protokollierter Zugang, der danach entfernt wird.
- **Sonst niemand.** Kein Verkauf, keine Weitergabe.

5 Was die KI sieht

Für Score und Nachrichtenentwurf sendet Lynk den relevanten Lebenslauf-/Profiltext und die Stellenbeschreibung an **den KI-Anbieter Ihrer Wahl**. Wählen Sie einen, der in der EU verarbeitet und nicht mit Ihren Daten trainiert; wir helfen bei der Auswahl. Der Match-Score ist eine **Einschätzung, keine Einstellungsentscheidung**.

6 Wie lange sie bleiben

Sie legen die Regeln fest. Lynk löscht alte gesourcte Profile und Nachrichtenprotokolle automatisch (Standard: 24 Monate, einstellbar). Einzelne Kandidaten lassen sich exportieren oder löschen. Die Daten verlassen Ihr Konto nicht, wenn unsere Arbeit endet – es gibt nichts zurückzugeben.

! Was Ihre Aufgabe bleibt

- **Kandidaten informieren**, dass Sie ihre Daten haben – spätestens in der ersten Nachricht, mit Link zu Ihrer Datenschutzinformation und dem Widerspruchsrecht (Teil 5.2).
- **Ein Mensch entscheidet**: Ein Recruiter prüft jede Shortlist und jede Nachricht. Recruiting-KI ist nach dem EU AI Act „Hochrisiko"; die vollen Pflichten gelten ab **2. Dezember 2027** (Teil 5.6).
- **Installation sicher betreiben** mit Ihrem IT-Partner – Backups, Updates, Zugang zur Cloud-Konsole (Teil 3C) – und den Vertrag in Teil 2 mit uns sowie die Auftragsverarbeitungsbedingungen Ihrer eigenen Anbieter **unterschreiben** (Teil 4B).

2 Auftragsverarbeitungsvertrag (Art. 28 DSGVO) – Support-Zugriff

MUSTER – vor Verwendung datenschutzrechtlich prüfen lassen

Umfang. HP Capital hostet Lynk nicht. Dieser Vertrag regelt nur den **Zugriff der HP Capital auf personenbezogene Daten in der eigenen Lynk-Installation der Agentur** bei Einrichtung, Support, Entwicklertagen, dem Einspielen von Updates und Wartung. Cloud-, KI-, Unipile- und E-Mail-Anbieter der Agentur sind deren eigene Auftragsverarbeiter nach eigenen Bedingungen.

Aufbau. Das Muster folgt Aufbau und Inhalt der Standardvertragsklauseln der EU-Kommission für Verantwortliche und Auftragsverarbeiter (Durchführungsbeschluss (EU) 2021/915, Klauseln 7–10) und ergänzt die konkreten Lynk-Angaben, die der EDSA statt einer bloßen Wiederholung des Gesetzes erwartet (Leitlinien 07/2020). **Wahl für die Rechtsberatung** [Variante 1 oder 2]**: Variante 1** – den amtlichen Wortlaut der Standardvertragsklauseln unverändert übernehmen und die Anlagen 2.A–2.D beifügen; **Variante 2** – diesen individuellen Vertrag verwenden. §§ 5 und 13 (Zugriffsregeln, KI) sind mit beiden Varianten nutzbar.

zwischen [Name der Agentur, Rechtsform, Anschrift, Firmenbuch-/Registernummer] – **„Verantwortlicher“** –

und HP Capital GmbH, Mayrwiesstraße 11, 5300 Hallwang (Salzburg), Österreich, FN 631120 v, UID ATU82731634 – **„Auftragsverarbeiter“**.

§ 1 Gegenstand und Verhältnis zum Hauptvertrag

1.1 Der Verantwortliche betreibt die Recruiting-Software Lynk in einem im eigenen Namen eröffneten Cloud- oder Serverkonto („Kundenumgebung“) auf Grundlage des Software-Lizenz- und Einrichtungsvertrags zwischen den Parteien („Hauptvertrag“). Der Auftragsverarbeiter hostet die Software nicht und speichert personenbezogene Daten des Verantwortlichen nicht auf eigenen Systemen.

1.2 Nach dem Hauptvertrag und einem etwaigen Wartungsvertrag erbringt der Auftragsverarbeiter Einrichtung, Support, Entwicklertage, das Einspielen von Updates und Wartung („Leistungen“). Dabei kann er Zugriff auf personenbezogene Daten in der Kundenumgebung erhalten. Nur insoweit verarbeitet er personenbezogene Daten im Auftrag des Verantwortlichen, und nur insoweit gilt dieser Vertrag.

1.3 Dieser Vertrag regelt die datenschutzrechtlichen Pflichten der Parteien für diesen Zugriff. Bei Widersprüchen geht er dem Hauptvertrag in Datenschutzfragen vor. Einzelheiten der Verarbeitung enthält **Anlage 2.B**. Der Verantwortliche ist allein für die Rechtmäßigkeit der Verarbeitung in seiner Installation verantwortlich, einschließlich Sourcing und Information der Kandidaten, sowie für seine eigenen Anbieter (siehe Teile 4B und 5).

§ 2 Weisungen

2.1 Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf Übermittlungen in Drittländer, sofern er nicht nach Unionsrecht oder mitgliedstaatlichem Recht dazu verpflichtet ist; in diesem Fall teilt er dies dem Verantwortlichen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.

2.2 Der Hauptvertrag, dieser Vertrag und jede einzelne Anfrage oder Freigabe einer Aufgabe (z. B. Support-Ticket, Abruf von Entwicklertagen, vereinbartes Update-Fenster) sind die dokumentierten Weisungen des Verantwortlichen. Weitere Weisungen erfolgen in Textform an **datenschutz@lynk-recruiting.com**.

2.3 Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er eine Weisung für einen Verstoß gegen die DSGVO oder andere Datenschutzvorschriften hält, und kann ihre Ausführung bis zur Bestätigung oder Änderung aussetzen.

§ 3 Zweckbindung und Dauer

3.1 Der Auftragsverarbeiter verarbeitet die Daten nur zur Erledigung der jeweiligen Aufgabe. Er nutzt sie nicht für eigene Zwecke, insbesondere nicht zum Training, Feintuning oder zur Bewertung von KI-Modellen, für kundenübergreifende Vergleiche oder für Marketing.

3.2 Der Auftragsverarbeiter kopiert keine personenbezogenen Daten aus der Kundenumgebung auf eigene Systeme. Ist eine Kopie für eine Aufgabe unvermeidlich (z. B. zur Nachstellung eines Fehlers), erfolgt sie nur mit Zustimmung des Verantwortlichen, möglichst pseudonymisiert, verschlüsselt gespeichert und wird gelöscht, sobald die Aufgabe erledigt ist.

3.3 Dieser Vertrag gilt, solange der Auftragsverarbeiter Leistungen mit Zugriff auf personenbezogene Daten nach dem Hauptvertrag oder einem Wartungsvertrag erbringt.

§ 4 Sicherheit der Verarbeitung und Vertraulichkeit

4.1 Für seinen Zugriff setzt der Auftragsverarbeiter mindestens die Maßnahmen in **Teil 3B** dieses Pakets (Anlage 2.C) um. Die Sicherheitsfunktionen der Software (Teil 3A) sind Teil der lizenzierten Software; Konfiguration und Betrieb der Kundenumgebung (Teil 3C) obliegen dem Verantwortlichen.

4.2 Der Auftragsverarbeiter darf seine Maßnahmen dem technischen Fortschritt anpassen, sofern das Schutzniveau nicht sinkt. Wesentliche Änderungen werden dokumentiert und dem Verantwortlichen mitgeteilt.

4.3 Zugriff erhalten nur dem Verantwortlichen benannte Personen und nur im für die Aufgabe unbedingt nötigen Umfang. Alle zur Verarbeitung befugten Personen sind zur Vertraulichkeit verpflichtet (vertraglich oder gesetzlich, u. a. § 6 DSG).

§ 5 Regeln für den Zugriff auf die Kundenumgebung

5.1 **Nur auf Anfrage.** Der Auftragsverarbeiter greift nur für eine vom Verantwortlichen angefragte oder freigegebene Aufgabe auf die Kundenumgebung zu. Während der Einrichtung besteht der Zugang für die Einrichtungsdauer; nach der Übergabe entfernt der Auftragsverarbeiter seinen administrativen Zugang (Hauptvertrag, Punkt 8.1).

5.2 **Minimale Rechte.** Der Zugriff erfolgt über persönliche, namentliche Konten mit Mehr-Faktor-Authentifizierung, nie über geteilte Konten, und nur mit den Rechten, die die Aufgabe erfordert. Wo Test- oder anonymisierte Daten genügen, nutzt der Auftragsverarbeiter keine Produktivdaten.

5.3 **Protokollierung.** Der Auftragsverarbeiter dokumentiert jeden Zugriff (Person, Datum und Uhrzeit, Aufgabe, betroffene Systeme) und stellt diese Aufzeichnung dem Verantwortlichen auf Anfrage zur Verfügung. Technische Protokolle in der Kundenumgebung verbleiben beim Verantwortlichen.

5.4 **Entfernen nach der Aufgabe.** Befristete Konten, Schlüssel und Sitzungen werden nach Erledigung der Aufgabe entfernt oder deaktiviert. Der Verantwortliche kann jeden Zugang jederzeit widerrufen.

§ 6 Sensible Daten

Lebensläufe und Nachrichten können beiläufig besondere Kategorien personenbezogener Daten (z. B. Gesundheitsangaben, Religion, Gewerkschaftszugehörigkeit, Fotos) oder Daten über strafrechtliche Verurteilungen enthalten. Der Verantwortliche weist seine Nutzer an, solche Daten nur zu erfragen oder zu erfassen, wenn dies erforderlich und zulässig ist. Der Auftragsverarbeiter sieht solche Daten nicht ein, exportiert oder kopiert sie nicht, sofern eine Aufgabe dies nicht zwingend erfordert.

§ 7 Nachweise, Einhaltung und Kontrollen

7.1 Der Auftragsverarbeiter beantwortet Fragen des Verantwortlichen zur Verarbeitung zeitnah und stellt die Informationen bereit, die zum Nachweis der Einhaltung von Art. 28 DSGVO und dieses Vertrags nötig sind, insbesondere die Aufzeichnungen nach § 5.3.

7.2 Der Verantwortliche kann die Einhaltung kontrollieren, vorrangig durch Anforderung von Unterlagen. Vor-Ort-Kontrollen sind 30 Tage vorher anzukündigen, finden während der Geschäftszeiten statt, dürfen keine Daten anderer Kunden offenlegen und sind auf eine pro Jahr begrenzt, außer bei konkretem Anlass (z. B. Datenschutzverletzung). Der Prüfer muss zur Vertraulichkeit verpflichtet sein. Jede Partei trägt ihre eigenen Kosten.

7.3 Die Parteien stellen diese Informationen der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung.

§ 8 Unterauftragsverarbeiter

8.1 **Allgemeine schriftliche Genehmigung.** Der Verantwortliche genehmigt die in **Teil 4A** (Anlage 2.D) genannten Unterauftragsverarbeiter. HP Capital erbringt alle Zugriffe auf die Kundenumgebung derzeit mit eigenem Personal.

8.2 Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 30 Tage vorher in Textform über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters (Name, Ort, Leistung, betroffene Daten, Übermittlungsgrundlage). Der Verantwortliche kann binnen 14 Tagen aus berechtigten datenschutzrechtlichen Gründen widersprechen. Einigen sich die Parteien nicht, kann der Verantwortliche die betroffenen Leistungen (z. B. einen Wartungsvertrag) zum Zeitpunkt der Änderung beenden; die Lizenz bleibt unberührt.

8.3 Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter vertraglich im Wesentlichen dieselben Datenschutzpflichten wie in diesem Vertrag auf und bleibt dem Verantwortlichen für deren Erfüllung voll verantwortlich.

8.4 **Eigene Anbieter des Verantwortlichen.** Der Anbieter der Kundenumgebung und die übrigen Dienste, die der Verantwortliche selbst beauftragt (KI-Anbieter, Unipile, E-Mail, Microsoft, ATS/CRM – Teil 4B), sind **keine** Unterauftragsverarbeiter des Auftragsverarbeiters. Der Verantwortliche schließt und verwaltet die Verträge mit ihnen selbst; der Auftragsverarbeiter richtet die Anbindungen nur auf Weisung des Verantwortlichen ein.

§ 9 Internationale Übermittlungen

Der Auftragsverarbeiter greift nur aus der EU/dem EWR auf die Kundenumgebung zu. Eine Übermittlung in ein Drittland durch den Auftragsverarbeiter (einschließlich Fernzugriff aus einem Drittland) erfolgt nur auf dokumentierte Weisung des Verantwortlichen und wenn die Voraussetzungen von Kapitel V DSGVO erfüllt sind. Verarbeiten eigene Anbieter des Verantwortlichen Daten außerhalb der EU/des EWR, prüft und sichert der Verantwortliche dies selbst ab.

§ 10 Unterstützung des Verantwortlichen

10.1 **Betroffenenanfragen.** Der Auftragsverarbeiter leitet Anfragen, die ihn direkt von Betroffenen erreichen, unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht selbst. Die Software stellt die Werkzeuge bereit: Export je Person in maschinenlesbarer Form (Art. 15/20 DSGVO), Löschung je Person über den gesamten Datenbestand mit Bericht über nicht Gelöschtes und die Gründe (Art. 17) sowie eine Erläuterung, wie ein Kandidat bewertet und kontaktiert wurde. Der Administrator oder IT-Partner des Verantwortlichen führt sie in der Kundenumgebung aus; der Auftragsverarbeiter hilft im Rahmen des Supports.

10.2 Der Auftragsverarbeiter unterstützt den Verantwortlichen außerdem unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen bei Datenschutz-Folgenabschätzungen (Art. 35, 36 DSGVO), der Sicherheit (Art. 32), Meldungen von Datenschutzverletzungen (Art. 33, 34) und den Betreiberpflichten nach dem EU AI Act (§ 13).

10.3 Unterstützung über den im Hauptvertrag oder in einem Wartungsvertrag enthaltenen Support hinaus wird zum Tagessatz des Hauptvertrags abgerechnet, sofern sie nicht auf einem Verstoß des Auftragsverarbeiters beruht.

§ 11 Verletzungen des Schutzes personenbezogener Daten

11.1 Der Auftragsverarbeiter meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit seinem Zugriff (z. B. kompromittierter Zugangsschlüssel oder kompromittiertes Gerät) unverzüglich, spätestens binnen 24 Stunden nach Kenntnis, an den Kontakt in Anlage 2.A.

11.2 Die Meldung enthält mindestens: Art der Verletzung (soweit möglich Kategorien und ungefähre Zahl der Betroffenen und Datensätze), eine Anlaufstelle, die wahrscheinlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen. Noch nicht verfügbare Informationen werden schrittweise unverzüglich nachgereicht.

11.3 Der Auftragsverarbeiter ergreift die nötigen Maßnahmen zur Eindämmung, dokumentiert die Verletzung und unterstützt den Verantwortlichen bei der Meldung an die Aufsichtsbehörde (72 Stunden, Art. 33) und an Betroffene (Art. 34). Bei Vorfällen in der Kundenumgebung ohne Zusammenhang mit seinem Zugriff unterstützt er im Rahmen des Supports.

§ 12 Vertragsende und Löschung

12.1 Dieser Vertrag endet, wenn der Auftragsverarbeiter keine Leistungen mit Zugriff auf personenbezogene Daten mehr erbringt. Pflichten, die ihrer Natur nach fortbestehen (Vertraulichkeit, Löschung), gelten weiter.

12.2 Die personenbezogenen Daten bleiben durchgehend in der Kundenumgebung; eine Rückgabe ist nicht nötig. Zum Ende entfernt der Auftragsverarbeiter alle verbliebenen Zugangsdaten, löscht etwaige Kopien nach § 3.2 unverzüglich, spätestens binnen 30 Tagen, und bestätigt dies in Textform.

12.3 Eine Aufbewahrung ist nur zulässig, wenn Unionsrecht oder mitgliedstaatliches Recht den Auftragsverarbeiter zur Speicherung verpflichtet; er informiert den Verantwortlichen darüber.

§ 13 Ergänzende Regelungen zur KI-Verarbeitung (EU AI Act)

13.1 Der Verantwortliche wählt und beauftragt den KI-Anbieter und stellt sicher, dass mit ihm Auftragsverarbeitungsbedingungen nach Art. 28 DSGVO bestehen. Der Auftragsverarbeiter empfiehlt Anbieter, die Daten in der EU/im EWR verarbeiten und Ein- und Ausgaben nicht zum Training ihrer Modelle nutzen.

13.2 Ändert ein Update die voreingestellten KI-Modelle oder die Bewertungslogik so, dass Ergebnisse beeinflusst werden können, informiert der Auftragsverarbeiter den Verantwortlichen in den Versionshinweisen mindestens 14 Tage vor Veröffentlichung des Updates und führt das Modell-Änderungsprotokoll fort. Die Software protokolliert je KI-Aufruf einen Konfigurations-Fingerabdruck.

13.3 Der Auftragsverarbeiter stellt eine Betriebsanleitung bereit. Die Software speichert Protokolle (Bewertungsereignisse, Entscheidungs- und Audit-Aufzeichnungen) in der Kundenumgebung; der Verantwortliche bewahrt sie mindestens sechs Monate auf (vgl. Art. 26 Abs. 6 KI-VO). Der Auftragsverarbeiter unterstützt Erläuterungen gegenüber Kandidaten (vgl. Art. 86 KI-VO).

13.4 Die Rollen der Parteien nach dem EU AI Act (Anbieter / Betreiber) regelt Punkt 14 des Hauptvertrags (siehe Teil 5.6).

§ 14 Haftung und Schlussbestimmungen

14.1 Die Haftung gegenüber Betroffenen richtet sich nach Art. 82 DSGVO. Zwischen den Parteien gelten die Haftungsregeln des Hauptvertrags.

14.2 Änderungen bedürfen der Textform. Ist eine Bestimmung unwirksam, bleibt der Rest wirksam; die Parteien ersetzen sie durch eine Regelung, die dem beabsichtigten Zweck im Rahmen der DSGVO am nächsten kommt.

14.3 Es gilt österreichisches Recht unter Ausschluss der Verweisungsnormen. Gerichtsstand: Salzburg, Österreich.

Ort, Datum · Verantwortlicher
[Name, Funktion]

Ort, Datum · Auftragsverarbeiter – HP Capital GmbH
Paul Hagler oder Philipp Habring, Geschäftsführer

Anlage 2.A – Parteien und Kontakte

	Verantwortlicher	Auftragsverarbeiter
Name, Anschrift	[Agentur, Anschrift]	HP Capital GmbH, Mayrwiesstraße 11, 5300 Hallwang (Salzburg), Österreich
Register / UID	[Registernummer / UID]	FN 631120 v, Landesgericht Salzburg / ATU82731634
Geschäftsführung	[Namen]	Paul Hagler, Philipp Habring
Kontakt Datenschutz	[Name, E-Mail]	datenschutz@lynk-recruiting.com. Kein Datenschutzbeauftragter bestellt (keine Pflicht nach Art. 37 DSGVO erwartet; von der Rechtsberatung zu bestätigen).

	Verantwortlicher	Auftragsverarbeiter
Meldungen von Datenschutzverletzungen an	[täglich gelesene E-Mail-Adresse]	datenschutz@lynk-recruiting.com
Personen mit Zugriff	–	Paul Hagler, Philipp Habring; weitere Personen nur nach Mitteilung in Textform

Anlage 2.B – Beschreibung der Verarbeitung

Gegenstand und Art	Fernzugriff des Auftragsverarbeiters auf die eigene Lynk-Installation des Verantwortlichen (Kundenumgebung) für: Einrichtung (Installation, Konfiguration, Anbindung der Anbieter des Verantwortlichen, Tests); Support (Analyse und Behebung von Fehlern); Entwicklertage (Umsetzung von Anpassungen); Einspielen von Updates; Wartung nach gesondertem Wartungsvertrag. Einsehen, Abfragen und – nur wenn eine Aufgabe es erfordert – Ändern oder Löschen von Daten in der Installation. Kein Hosting, keine Speicherung auf Systemen des Auftragsverarbeiters.
Zweck	Erbringung der Leistungen nach dem Hauptvertrag oder einem Wartungsvertrag.
Häufigkeit	Gelegentlich, je Aufgabe; durchgehender Zugang nur während der Einrichtung.
Betroffene	(1) potenzielle Kandidaten aus LinkedIn und anderen Quellen; (2) Bewerber und Kandidaten in Vermittlungsprozessen; (3) Ansprechpersonen bei Kunden des Verantwortlichen; (4) Nutzer des Verantwortlichen (Recruiter, Admins).
Datenkategorien	Was in der Installation gespeichert ist und bei einer Aufgabe sichtbar wird: Identitäts- und Kontaktdaten; berufliche Profildaten; Lebenslaufdokumente und deren ausgelesener Inhalt; Nachrichteninhalte und -verläufe; Antworten und Ergebnisse von Assessments; Interviewtermine; KI-Ergebnisse (Match-Scores, Entwürfe) und Entscheidungs-/Audit-Aufzeichnungen; Pipeline-Status und Notizen; Nutzerkonten, Rollen und Protokolle.
Besondere Kategorien	Nicht vorgesehen; können beiläufig in Lebensläufen oder Nachrichten vorkommen (siehe § 6).
Dauer	Einrichtungszeitraum; Support und Updates für 12 Monate nach Go-Live nach dem Hauptvertrag; danach nur mit optionalem Wartungsvertrag.
Ort der Verarbeitung	Die Kundenumgebung am vom Verantwortlichen gewählten Standort. Der Auftragsverarbeiter greift aus der EU/dem EWR (Österreich) darauf zu.

Anlage 2.C – Technische und organisatorische Maßnahmen

Siehe **Teil 3B** dieses Pakets (verbindliche Maßnahmen für den Zugriff des Auftragsverarbeiters), der Bestandteil dieses Vertrags ist. Teile 3A und 3C dienen der Information.

Anlage 2.D – Genehmigte Unterauftragsverarbeiter

Siehe **Teil 4A** dieses Pakets, der Bestandteil dieses Vertrags ist. Teil 4B nennt die eigenen Anbieter des Verantwortlichen; sie sind keine Unterauftragsverarbeiter des Auftragsverarbeiters (§ 8.4).

3 Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Drei Arten von Schutz, klar getrennt. **3A**: Sicherheitsfunktionen der Lynk-Software – mit Fundstelle im Quellcode, damit Ihre IT sie prüfen kann. **3B**: was HP Capital bei jedem Zugriff auf Ihre Installation tut – verbindlich nach dem AVV. **3C**: was Ihr IT-Partner in Ihrem eigenen Cloud-Konto einrichtet und betreibt – wir richten es mit Ihnen ein und dokumentieren es bei der Übergabe.

In der Software im Lynk-Quellcode geprüft HP Capital verbindlich für unseren Zugriff Ihre Seite Ihr Konto, Ihr IT-Partner

3A Sicherheitsfunktionen der Software

Funktion	Status	Nachweis / Hinweis
Eigene Installation. Lynk wird je Agentur einmal im eigenen Konto der Agentur installiert; kein gemeinsames System mit anderen Agenturen.	In der Software Ihre Seite	Bereitstellung über Docker-Images und Helm-Chart aus dem Repository, installiert in Ihrem Konto.
Workspace-Trennung: Jede Abfrage wird zentral auf den Workspace des Nutzers gefiltert; automatisierte Mandantentrennungs-Tests in der CI.	In der Software	`api: src/common/tenancy.py · SECURITY.md · docs/security/tenancy-audit-20260823.md`
Rollenbasierte Rechte (Owner, Admin, Recruiter, Viewer); Export und Mitgliederverwaltung nur für Admins.	In der Software	`api: security/rbac.py, security/rbac_enforce.py`
Passwörter: mindestens 12 Zeichen mit Komplexitätsregeln; nur als gesalzene Hashes gespeichert. **Schutz vor Passwort-Raten**: 5 Anmeldeversuche je 15 Min. und IP, Sperre nach wiederholten Fehlversuchen.	In der Software	`api: src/common/password_utils.py · src/rate_limit.py · src/modules/user/login_attempts.py`
Sitzungen: kurzlebige Zugriffstoken (Standard 60 Min.), Refresh-Token in Secure/HttpOnly-Cookie, serverseitiger Widerruf bei Abmeldung.	In der Software	`api: src/common/jwt.py · src/common/cookie_security.py`
Microsoft-Anmeldung (SSO); dann gelten die Entra-ID-Richtlinien der Agentur (MFA, bedingter Zugriff). **Zwei-Faktor-Codes (TOTP-App)**: Einrichtung und Prüfung eingebaut, Geheimnis verschlüsselt gespeichert; eine Pflicht zur Nutzung bei der Anmeldung für alle Nutzer ist noch nicht eingebaut – MFA-Pflicht über SSO-Richtlinien durchsetzen.	In der Software Ihre Seite	`web: src/App.tsx (MSAL) · api: auth/mfa.py · docs/security/mfa-enforcement-decision-20260829.md`
Feldverschlüsselung besonders sensibler Felder (Telefonnummern, Tokens verbundener Konten, MFA-Geheimnisse) mit authentifizierter Verschlüsselung und Schlüsselrotation; der Schlüssel wird bei der Einrichtung in Ihrem Konto gesetzt.	In der Software	`api: security/field_crypto.py, security/encrypted_fields.py`
Transportsicherheit: nur HTTPS; HSTS und Sicherheits-Header durch die Anwendung. **Lebensläufe privat**: keine öffentlichen Links. **Log-Bereinigung** von Tokens, Passwörtern und E-Mail-Adressen.	In der Software	`api: security/headers.py · src/common/s3_upload.py · security/log_redaction.py`
Audit- und Entscheidungsprotokoll: Export und Löschung, KI-gestützte Entscheidungen, Erläuterung je Kandidat zu Scores und Herkunft von Nachrichten. **KI-Nachvollziehbarkeit**: Konfigurations-Fingerabdruck je Aufruf, Modell-Änderungsprotokoll.	In der Software	`api: src/common/audit.py · src/modules/decision_log · src/common/llm_config_fingerprint.py · MODEL_CHANGELOG.md`

Funktion	Status	Nachweis / Hinweis
Schutz vor manipulierten Anfragen: Größenlimits, Schutz vor Server-Side Request Forgery, authentifizierte Webhooks des LinkedIn-Connectors; **Ratenbegrenzung** (Standard 300 Anfragen/Min. je Konto); KI-Nutzung je Aufruf gemessen.	In der Software	`api: src/common/body_limit.py, src/common/ssrf_guard.py, src/rate_limit.py, src/common/llm_metering.py`
Menschliche Prüfung: Recruiter prüfen und senden KI-Entwürfe; Match-Score als „automatisierte Einschätzung, keine Einstellungsentscheidung“ gekennzeichnet; optionaler KI-Hinweis an Kandidaten.	In der Software Ihre Seite	`Produktverhalten · api: src/common/ai_disclosure.py (Teil 5.6)`
Lösch- und Exportwerkzeuge: Export und Löschung je Person mit Bericht; monatliche automatische Löschung gesourcter Profile und Nachrichtenprotokolle (Standard 24 Monate, Einstellung `PII_RETENTION_MONTHS`).	In der Software	`api: src/modules/gdpr · deploy/gdpr/retention-cronjob.yaml · docs/gdpr.md`
Betriebswerkzeuge im Code: verschlüsselter Datenbank-Backup-Job (AES-256, Public Key) mit Wiederherstellungsprobe, Netzwerkrichtlinien (Default-Deny), gehärtete Container, Monitoring- und Alarmregeln, Vorlagen für einen Secrets-Manager.	In der Software Ihre Seite	`deploy/backup/* · DR-RUNBOOK.md · infra/security/* · infra/monitoring · infra/secrets/*`
Sichere Entwicklung: statische Code-Analyse (Semgrep), Secret-Scanning (Gitleaks), Container- und Abhängigkeitsprüfung (Trivy, Dependabot), Software-Stückliste; rund 10.000 automatisierte Tests; privater Meldeweg für Schwachstellen (Bestätigung binnen 3 Werktagen).	In der Software	`.github/workflows/w6_semgrep.yml, w7_gitleaks.yml, trivy-scan.yml, sbom.yml · SECURITY.md`

3B Maßnahmen der HP Capital für den Support-Zugriff

Maßnahme	Status	Detail
Zugriff nur auf Anfrage für eine benannte Aufgabe (Einrichtung, Support-Ticket, Entwicklertage, Update, Wartung).	HP Capital	AVV § 5.1; Aufgabenbezug in der Zugriffsaufzeichnung.
Persönliche, namentliche Konten mit MFA; keine geteilten Konten; Zugangsdaten nur über einen verschlüsselten Passwort-Manager, nie per unverschlüsselter E-Mail.	HP Capital	AVV § 5.2.
Minimale Rechte: nur die für die Aufgabe nötigen Rechte; Test- oder anonymisierte Daten, wo immer sie genügen.	HP Capital	AVV § 5.2.
Zugriffsaufzeichnung: Person, Datum und Uhrzeit, Aufgabe und Systeme für jeden Zugriff; auf Anfrage für Sie einsehbar.	HP Capital	AVV § 5.3.
Entfernen nach der Aufgabe: befristete Konten, Schlüssel und Sitzungen werden entfernt; der Einrichtungszugang wird bei der Übergabe entfernt.	HP Capital	AVV § 5.4; Lizenzvertrag Punkt 8.1.
Keine Kopien auf Systemen der HP Capital; unvermeidliche Kopien nur mit Zustimmung, verschlüsselt, nach der Aufgabe gelöscht.	HP Capital	AVV § 3.2.
Sichere Geräte: Festplattenverschlüsselung, aktuelle Sicherheitsupdates, Bildschirmsperre; Zugriff nur aus der EU/dem EWR.	HP Capital	AVV § 9.

Maßnahme	Status	Detail
Vertraulichkeit und Schulung: schriftliche Verpflichtung auf das Datengeheimnis (§ 6 DSG), jährliche Datenschutzschulung für alle mit Zugriff.	HP Capital	AVV § 4.3.
Ablauf bei Datenschutzverletzungen: erkennen, eindämmen, Sie binnen 24 Stunden informieren, dokumentieren.	HP Capital	AVV § 11.
Sicherheitsupdates: sicherheitsrelevante Updates werden unverzüglich bereitgestellt und angekündigt.	HP Capital	Lizenzvertrag Punkt 9.1.

3C Ihre Seite – Betrieb im eigenen Konto

Maßnahme	Status	Wie wir helfen
Sicherheit des Cloud-Kontos: MFA für alle mit Zugang zur Cloud-Konsole, wenige Administratoren, getrennte Konten für Ihren IT-Partner und für HP Capital.	Ihre Seite	Checkliste bei der Einrichtung.
Rechenzentrum und physische Sicherheit: Anbieter und Region Ihrer Wahl (EU empfohlen), zertifiziert z. B. nach ISO/IEC 27001.	Ihre Seite	Wir empfehlen passende Anbieter.
Verschlüsselung ruhender Daten für Datenbank-Volumes und Dateispeicher; Datei-Bucket privat.	Ihre Seite	Bei der Einrichtung konfiguriert.
TLS-Zertifikat am Eingang, Netzwerkregeln, auf Wunsch Web Application Firewall.	Ihre Seite	Bei der Einrichtung aus den mitgelieferten Vorlagen konfiguriert.
Backups und Wiederherstellung: tägliches verschlüsseltes Backup in getrennten Speicher, privater Schlüssel offline, regelmäßiger Wiederherstellungstest; Ihre Ziele für Datenverlust (RPO) und Wiederherstellungszeit (RTO).	Ihre Seite	Backup-Job eingerichtet und eine Wiederherstellung vor Go-Live mit Ihrer IT getestet.
Patches und Überwachung: Updates von Betriebssystem, Datenbank und Containern; Einspielen von Lynk-Updates; Alarme.	Ihre Seite	Übergabe an Ihren IT-Partner; in den 12 Update-Monaten unterstützen wir.
Nutzerverwaltung: Nutzer einladen und entfernen, Rollen vergeben, MFA über SSO durchsetzen.	Ihre Seite	Schulung.

4 Unterauftragsverarbeiter und Ihre Anbieter

Zwei verschiedene Listen. **4A** ist die eigene Liste der HP Capital für den AVV – bewusst kurz, weil wir Ihre Daten nicht hosten. **4B** nennt die Anbieter, die Ihre Lynk-Installation nutzt: Sie wählen, beauftragen und bezahlen sie direkt, und sie arbeiten für Sie.

4A Unterauftragsverarbeiter der HP Capital (AVV § 8)

Leistung	Anbieter	Betroffene Daten	Standort
Zugriff auf Ihre Installation	Keiner – durch eigenes Personal der HP Capital	Bei einer Aufgabe sichtbare Daten (Anlage 2.B)	Österreich / EU
Support-E-Mail (hello@ und datenschutz@lynk-recruiting.com)	[Postfach-Anbieter von lynk-recruiting.com – von HP Capital vor dem ersten Zugriff zu benennen]	Nur was Sie uns per E-Mail senden. Bitte keine Kandidatendaten per E-Mail senden – wir sehen sie uns in Ihrer Installation an.	[EU]
Integrationsdienst für die ATS-/CRM-Anbindung (nur falls genutzt)	Nur wenn für Ihre Anbindung ein Integrationsdienst genutzt wird; er wird Ihnen **vor Vertragsschluss** namentlich benannt. Wird keiner genutzt, entfällt diese Zeile.	Daten, die zwischen Ihrem ATS/CRM und Lynk übertragen werden (z. B. Stellen, Bewerbungen, Kandidatenprofile)	Wird mit dem Dienst benannt – EU bevorzugt

Zieht HP Capital jemals ein weiteres Unternehmen oder einen freien Entwickler mit Zugriff auf Ihre Installation hinzu, wird es hier mit 30 Tagen Vorlauf ergänzt, und Sie können widersprechen (AVV § 8.2).

4B Ihre Anbieter – von Ihnen beauftragt und bezahlt

Leistung	Anbieter	Betroffene Daten	Standort	Ihr Vertrag
Cloud oder Server (Server, Datenbank, Dateispeicher, Backups)	Ihre Wahl; Richtwert ≈ 50–150 €/Monat	Alle Daten Ihrer Installation	Ihre Wahl – EU empfohlen	Standardbedingungen des Anbieters inkl. Auftragsverarbeitung
KI / LLM (Lebenslauf-Auslesung, Match-Score, Nachrichtenentwürfe)	Ihre Wahl – jede OpenAI-kompatible Schnittstelle; ≈ 200–300 €/Monat bei 10 Recruitern	Lebenslauf- und Profiltext, Stellenbeschreibung, Kontext für einen Entwurf	EU-Verarbeitung wählen	Auftragsverarbeitung inkl. kein Training mit Ihren Daten
LinkedIn-Anbindung (Suche, Import, Nachrichten je Recruiter)	Unipile SAS, 168 Rue de la Rotonde, 42153 Riorges, Frankreich; ≈ 5 € je Recruiter/Monat	LinkedIn-Sitzung des Recruiters; angesehene/importierte Profile; Nachrichten	EU (Frankreich) laut Unipile	Unipile-Bedingungen; AVV auf Anfrage bei Unipile
E-Mail-Versand (Benachrichtigungen, Assessment- und Termin-E-Mails)	Ihr SMTP-Anbieter; geringe Kosten	Empfängeradresse, E-Mail-Inhalt	EU wählen	Auftragsverarbeitungsbedingungen des Anbieters

Leistung	Anbieter	Betroffene Daten	Standort	Ihr Vertrag
Microsoft (optional: Anmeldung, Outlook-Kalender)	Microsoft Ireland Operations Ltd., Dublin	Nutzeridentität; Kalenderverfügbarkeit und Termine	EU-Datengrenze laut Ihrem Vertrag	Ihre Microsoft-365-Bedingungen
ATS/CRM (Ihr bestehendes System; eine Anbindung im 8-Wochen-Programm enthalten)	Ihr Anbieter – Sie verbinden Lynk mit Ihrem eigenen Konto	Stellen, Bewerbungen, Kandidatendaten; ggf. Rückschreiben, je nach System und Tarif	Laut Ihrem Vertrag	Ihr bestehender Vertrag mit dem Anbieter

Gut zu wissen

- **Das sind Ihre Auftragsverarbeiter.** Mit jedem brauchen Sie einen Auftragsverarbeitungsvertrag (meist Teil der Standardbedingungen des Anbieters). Wir helfen bei Auswahl und Einrichtung, sind aber nicht Vertragspartei.
- **LinkedIn** selbst ist kein Auftragsverarbeiter. Ihre Recruiter nutzen ihre eigenen LinkedIn-Konten nach den LinkedIn-Bedingungen. Die Automatisierung von LinkedIn mit Drittsoftware kann der LinkedIn-Nutzervereinbarung widersprechen und zu Kontoeinschränkungen führen – Lynk setzt Versandlimits je Konto, das Risiko lässt sich aber nicht ausschließen (Teil 5.7).
- **Übermittlungen außerhalb der EU** hängen von den gewählten Anbietern ab. Mit EU-Anbietern sind keine nötig; sonst prüfen Sie die Übermittlungsgrundlage (z. B. EU-US Data Privacy Framework oder Standardvertragsklauseln).
- Preise sind grobe Richtwerte zum Stand dieses Pakets; sie werden von den Anbietern festgelegt.

Stand beider Listen: 1. Oktober 2026. Aktuelle Fassung auf Anfrage an datenschutz@lynk-recruiting.com.

5 Hinweise für Ihre eigene Compliance als Verantwortlicher

Sie als Agentur entscheiden, warum und wie Kandidatendaten genutzt werden – und Sie betreiben das System im eigenen Konto –, daher sind die folgenden Pflichten Ihre. Es handelt sich um praktische, unverbindliche Hinweise zur Abstimmung mit Ihrer Datenschutzberatung, nicht um Rechtsberatung.

5.1 Rechtsgrundlage: berechtigtes Interesse

Active Sourcing in beruflichen Netzwerken stützt sich in der Regel auf das **berechtigte Interesse** (Art. 6 Abs. 1 lit. f DSGVO): Ihr Interesse, Kundenpositionen zu besetzen, und das mögliche Interesse der Kandidaten an beruflichen Chancen, abgewogen gegen deren Privatsphäre. Aufsichtsbehörden haben Active Sourcing als zulässig angesehen, wenn die Daten im beruflichen Kontext veröffentlicht wurden und die Informationspflichten erfüllt sind (z. B. Hessischer Datenschutzbeauftragter, 51. Tätigkeitsbericht, Fall eines Personaldienstleisters).

- **Interessenabwägung dokumentieren** – einmal für Ihren Sourcing-Prozess.
- **Nur berufliche Daten**: nutzen Sie, was Kandidaten zu beruflichen Zwecken veröffentlicht haben (LinkedIn-Profil, zugesandter Lebenslauf). Keine privaten Social-Media-Profile durchsuchen, keine besonderen Kategorien erheben.
- **Relevanz**: für konkrete Positionen oder klar definierte Talent-Pools sourcen, nicht wahllos.
- **Längerfristiger Talent-Pool**: Sobald ein Kandidat antwortet, holen Sie eine **Einwilligung** (Art. 6 Abs. 1 lit. a) für künftige Positionen ein – oder speichern nur so lange, wie der aktuelle Prozess es erfordert.
- **Kundenkontakte** (Hiring Manager): berechtigtes Interesse / Vertrag; für E-Mail-Werbung an Unternehmen gelten eigene Regeln (Österreich: § 174 TKG 2021; Deutschland: § 7 UWG).

5.2 Kandidaten informieren (Art. 14 DSGVO)

Wenn Sie ein Profil aus LinkedIn importieren, haben Sie Daten **nicht beim Kandidaten selbst** erhoben. Dann verlangt Art. 14 DSGVO, dass Sie ihn informieren:

- **Wann:** spätestens mit Ihrer **ersten Nachricht** (Art. 14 Abs. 3 lit. b); kontaktieren Sie ihn nicht, innerhalb einer angemessenen Frist, spätestens **einen Monat** nach dem Import (Art. 14 Abs. 3 lit. a). Importierte, aber nie kontaktierte Profile sollten daher rasch gelöscht oder informiert werden.
- **Was:** wer Sie sind und wie man Sie erreicht (ggf. Ihr Datenschutzbeauftragter); Zwecke und Rechtsgrundlage; Ihr berechtigtes Interesse; Datenkategorien; **die Quelle (z. B. „Ihr öffentliches LinkedIn-Profil“)**; Empfänger (z. B. Kunden – nur mit Zustimmung zur Vorstellung; IT-Dienstleister); Speicherdauer; Rechte (Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch, Datenübertragbarkeit); Beschwerderecht bei der Aufsichtsbehörde (Österreich: Datenschutzbehörde; Deutschland: zuständige Landesbehörde).
- **Widerspruchsrecht** (Art. 21 Abs. 4): muss ausdrücklich und getrennt von anderen Informationen spätestens bei der ersten Kommunikation genannt werden.
- **KI-Einsatz**: Erwähnen Sie, dass Sie KI-gestützte Werkzeuge zur Suche, Vorauswahl und für Nachrichtenentwürfe einsetzen und ein Recruiter entscheidet (siehe 5.6).

Formulierungsbeispiel für das Ende einer ersten LinkedIn-Nachricht [mit Rechtsberatung anpassen]

„Ich bin über Ihr öffentliches LinkedIn-Profil auf Sie aufmerksam geworden und habe Ihre beruflichen Angaben gespeichert, um Sie zu dieser Position zu kontaktieren. Für die Vorauswahl nutzen wir KI-gestützte Werkzeuge; alle Entscheidungen trifft ein Recruiter. Sie können jederzeit widersprechen – antworten Sie einfach mit ‚Nein‘, dann löschen wir Ihre Daten. Details: [Kurzlink zur Datenschutzinformation]“

Lynk unterstützt das mit Nachrichtenvorlagen und Platzhaltern; ein eingebauter KI-Hinweis für generierte Nachrichten kann für Ihre Installation eingeschaltet werden.

5.3 Betroffenenanfragen

- Beantworten Sie Anfragen auf Auskunft, Löschung oder Widerspruch binnen **eines Monats** (Art. 12 Abs. 3).

- Lynk kann alle Daten zu einer Person maschinenlesbar exportieren und über alle gespeicherten Sammlungen löschen, mit Bericht über nicht Löschbares und die Gründe. Ihr Administrator oder IT-Partner führt diese Funktionen in Ihrer Installation aus (siehe Dokumentation); wir helfen im Rahmen des Supports.
- Führen Sie eine Widerspruchsliste (nur Name/Profil-ID), damit Personen, die widersprochen haben, nicht erneut importiert werden.

5.4 Speicherdauer und Löschung

Situation	Vorgeschlagene Frist (Ihre Entscheidung)	Begründung
Profil importiert, Kandidat nie kontaktiert	1 Monat	Art. 14 Abs. 3 lit. a – sonst ist ohnehin zu informieren.
Kontaktiert, keine Antwort oder kein Interesse	3–6 Monate nach letztem Kontakt	Datenminimierung; nur Widerspruchsliste behalten.
Kandidat im Vermittlungsprozess, nicht vermittelt	Prozessende + **7 Monate** (Österreich)	Die österreichische Datenschutzbehörde akzeptiert 7 Monate für Bewerberdaten wegen der 6-monatigen Anspruchsfristen nach dem Gleichbehandlungsgesetz (GlBG) plus einem Monat. Deutschland: üblich ca. 6 Monate (§ 15 Abs. 4 AGG, § 61b ArbGG).
Talent-Pool mit Einwilligung	24 Monate, dann Einwilligung erneuern	Einwilligungsbasiert; jederzeit widerrufbar.
Vermittelte Kandidaten, Rechnungen	Gesetzliche Aufbewahrung (z. B. 7 Jahre für Buchhaltungsunterlagen in Österreich, § 132 BAO)	Nur die für die Buchhaltung nötigen Unterlagen.

Was Lynk automatisch tut: Ein monatlicher Job löscht gesourcte LinkedIn-Profile und Nachrichtenprotokolle, die älter als ein einstellbarer Zeitraum sind (Standard 24 Monate ab Erstellung). Er unterscheidet nicht nach Pipeline-Status – kürzere Fristen für die obigen Situationen setzen Sie über die Einstellung oder eine regelmäßige Bereinigung durch Ihr Team um.

5.5 Folgenabschätzung und automatisierte Entscheidungen

- **DSFA (Art. 35 DSGVO):** Die KI-gestützte Bewertung von Kandidaten in größerem Umfang erfordert voraussichtlich eine Datenschutz-Folgenabschätzung. Prüfen Sie anhand der österreichischen DSFA-V bzw. der DSK-Liste in Deutschland. Wir liefern Systembeschreibung, Datenflüsse und TOMs als Grundlage.
- **Keine automatisierten Absagen (Art. 22 DSGVO):** Der Match-Score von Lynk ist eine Schätzung zur Unterstützung eines Recruiters; er entscheidet nicht. Nutzen Sie ihn nicht, um Personen ohne menschliche Prüfung automatisch abzulehnen oder auszuschließen.
- **Verarbeitungsverzeichnis (Art. 30):** Nehmen Sie Lynk, Ihren Cloud-Anbieter und Ihre übrigen Lynk-Anbieter (Teil 4B) in Ihr Verzeichnis der Verarbeitungstätigkeiten auf.

5.6 EU AI Act – was für Recruiting-KI gilt

KI-Systeme, die für die **Einstellung oder Auswahl von Personen** eingesetzt werden – insbesondere für gezielte Stellenanzeigen, das Analysieren und Filtern von Bewerbungen und die Bewertung von Kandidaten –, sind nach Anhang III Nr. 4 lit. a der KI-Verordnung (Verordnung (EU) 2024/1689) **Hochrisiko-KI**. Als Agentur, die Lynk nutzt, sind Sie **Betreiber**.

Seit / ab	Was gilt
2. Februar 2025	Verbotene Praktiken (z. B. Emotionserkennung am Arbeitsplatz – nutzt Lynk nicht). KI-Kompetenz (Art. 4): Maßnahmen, damit Ihr Team das Werkzeug versteht – durch den Digital Omnibus (VO (EU) 2026/1744) auf „Förderung" der KI-Kompetenz abgeschwächt, gilt aber weiter.
2. August 2026	Transparenz (Art. 50): Personen sind zu informieren, wenn sie mit einem KI-System interagieren (z. B. automatisierte Chat-Antwort), sofern nicht offensichtlich.
2. Dezember 2027	Volle Hochrisiko-Pflichten für Anhang-III-Systeme, durch den Digital Omnibus zur KI (in Kraft seit 27. Juli 2026) vom 2. August 2026 verschoben.

Betreiberpflichten (Art. 26 KI-VO) – und wie Lynk unterstützt

- **Verwendung gemäß Betriebsanleitung** – von HP Capital mit der Übergabe bereitgestellt.
- **Menschliche Aufsicht** durch geschulte, kompetente Personen mit Befugnis zum Eingreifen (Art. 26 Abs. 2) – Lynk: Entwürfe werden von Recruitern geprüft und gesendet; Score als Schätzung gekennzeichnet; Freigabe-Warteschlange für Nachrichten.
- **Relevante Eingabedaten**, soweit unter Ihrer Kontrolle (Art. 26 Abs. 4) – z. B. klare, diskriminierungsfreie Stellenanforderungen.
- **Betrieb überwachen** und schwerwiegende Vorfälle oder Risiken dem Anbieter melden (Art. 26 Abs. 5).
- **Automatisch erzeugte Protokolle** mindestens sechs Monate aufbewahren (Art. 26 Abs. 6) – Lynk: Entscheidungsprotokoll und Audit-Export, gespeichert in Ihrer Installation.
- **Kandidaten informieren**, dass ein Hochrisiko-KI-System bei Entscheidungen über sie eingesetzt wird (Art. 26 Abs. 11), und auf Anfrage eine **Erläuterung** geben (Art. 86) – Lynk: Erläuterung je Kandidat, KI-Hinweis in Nachrichten.
- **Eigene Mitarbeiter**: Wenn Sie Lynk für die Einstellung eigener Mitarbeiter nutzen, informieren Sie vorher die Arbeitnehmervertretung (Art. 26 Abs. 7).
- Anbieterinformationen für Ihre **DSFA** nutzen (Art. 26 Abs. 9).

Anbieter oder Betreiber? Ein Punkt für die Rechtsberatung

Lynk wird mit vollständigem Quellcode lizenziert, läuft im eigenen Konto der Agentur und wird unter deren eigener Marke eingerichtet. Nach Art. 25 Abs. 1 KI-VO kann ein Betreiber, der ein Hochrisiko-System mit **eigenem Namen oder eigener Marke** versieht oder **wesentlich verändert**, selbst zum **Anbieter** werden – mit deutlich weitergehenden Pflichten (Konformitätsbewertung, technische Dokumentation, Registrierung). Der Lizenzvertrag (Punkt 14) regelt die Rollen; die Rechtsberatung sollte bestätigen, dass diese Zuordnung trägt.

5.7 Nutzung von LinkedIn

Die LinkedIn-Nutzervereinbarung schränkt den Einsatz von Drittsoftware zur Automatisierung ein. Lynk verbindet das eigene Konto jedes Recruiters über Unipile und setzt Versandlimits je Konto; LinkedIn kann Konten dennoch einschränken. Das ist ein vertragliches Risiko gegenüber LinkedIn, getrennt vom Datenschutz; das Safe-LinkedIn-Playbook in Ihrer Schulung enthält empfohlene Limits.

6 Offene Punkte und Entscheidungen zur Prüfung

Was vor dem ersten Zugriff auf Ihre Installation noch zu entscheiden ist – von Ihnen, von uns und von der Rechtsberatung.

6.1 Ihre Entscheidungen vor dem Go-Live

Punkt	Zu entscheiden
Cloud- oder Serveranbieter	Anbieter, EU-Region, Zertifizierung (z. B. ISO 27001), Auftragsverarbeitungsbedingungen akzeptiert.
KI-Anbieter (LLM)	Anbieter, EU-Verarbeitung, Ausschluss des Trainings, Auftragsverarbeitungsvertrag unterschrieben.
Unipile und E-Mail-Anbieter	Konten im eigenen Namen eröffnet; Auftragsverarbeitungsbedingungen unterschrieben.
IT-Partner	Wer nach der Übergabe Backups, Updates und Überwachung übernimmt (wir können einen empfehlen).
Zugangs- und MFA-Regeln	Wer das Cloud-Konto verwaltet; MFA für alle Nutzer (über Microsoft-SSO oder Authenticator-App).
Löschfristen	Ihre Fristen je Situation (Teil 5.4) und die Einstellung der automatischen Löschung (Standard 24 Monate).
Information der Kandidaten	Datenschutzinformation, Formulierung der ersten Nachricht, KI-Hinweis ein oder aus (Teile 5.2, 5.6).

6.2 Aufgaben der HP Capital

Punkt	Stand
Schriftliches Zugriffsverfahren (Teil 3B)	Vor dem ersten Kundenzugriff intern zu dokumentieren.
Postfach-Anbieter (Teil 4A)	In der Liste der Unterauftragsverarbeiter zu benennen.
MFA-Pflicht in der Software	Einrichtung vorhanden; Pflicht bei der Anmeldung für alle Nutzer noch nicht eingebaut – bis dahin über SSO durchsetzen.

6.3 In diesem Muster gesetzte Vertragswerte – von der Rechtsberatung zu bestätigen

Regelung	Wert
Grundlage	[Variante 1 oder 2] – amtlicher Wortlaut SCC 2021/915 + Anlagen oder dieser Vertrag
§ 3.2 / § 12.2	Keine Kopien; unvermeidliche Kopien nach der Aufgabe gelöscht, spätestens 30 Tage nach Ende
§ 7.2	Ankündigung von Kontrollen 30 Tage; einmal pro Jahr; jede Partei trägt ihre Kosten
§ 8.2	Ankündigung neuer Unterauftragsverarbeiter 30 Tage; Widerspruch binnen 14 Tagen
§ 11.1	Meldung von Datenschutzverletzungen binnen 24 Stunden
§ 13	Ankündigung von Modelländerungen 14 Tage; Protokolle mindestens 6 Monate

Regelung	Wert
§ 14	Haftung nach dem Lizenzvertrag; Gerichtsstand Salzburg

6.4 Punkte, die am meisten eine Datenschutzberatung brauchen

1. **Rollenverteilung ohne Hosting**: HP Capital als Auftragsverarbeiter nur für gelegentlichen Support-Zugriff – genügt der begrenzte AVV, und muss er vor dem ersten Einrichtungszugriff unterschrieben sein?
2. **Rolle nach AI Act**: Macht White-Labeling, Quellcode-Eigentum und der Betrieb im eigenen Konto der Agentur diese zum Anbieter (Art. 25)? Was schuldet HP Capital als Anbieterin der ausgelieferten Fassung (bis 2. Dezember 2027)?
3. **Eigene Anbieterkette der Agentur**: Cloud, KI, Unipile und E-Mail als Auftragsverarbeiter der Agentur – was die Agentur prüfen muss (Übermittlungen, Trainingsausschluss).
4. **Grundlage für Active Sourcing**: Interessenabwägung, Zeitpunkt und Wortlaut nach Art. 14, Umgang mit Widersprüchen, Löschfristen für Österreich und Deutschland.
5. **DSFA**: Pflicht und Vorlage für Agenturen.
6. **LinkedIn-Bedingungen**: vertragliches Risiko automatisierter Aktivität über Unipile.

7 Quellen

- Verordnung (EU) 2016/679 (DSGVO), Art. 6, 12–14, 21, 22, 28, 30, 32–37; § 6 DSG (Datengeheimnis).
- Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern (Art. 28 Abs. 7 DSGVO) – eur-lex.europa.eu/eli/dec_impl/2021/915/oj.
- EDSA-Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ (v2.1); EDSA-Stellungnahme 22/2024 zu Pflichten beim Einsatz von Auftrags- und Unterauftragsverarbeitern.
- Verordnung (EU) 2024/1689 (KI-Verordnung), Art. 4, 25, 26, 50, 86, Anhang III Nr. 4; Verordnung (EU) 2026/1744 (Digital Omnibus zur KI), ABl. vom 24. Juli 2026, in Kraft seit 27. Juli 2026.
- Hessischer Beauftragter für Datenschutz und Informationsfreiheit (HBDI), 51. Tätigkeitsbericht (2022) – Active Sourcing durch einen Personaldienstleister.
- Österreichische Datenschutzbehörde (DSB), Entscheidung 2018 zur Aufbewahrung von Bewerberdaten für 7 Monate (u. a. berichtet von dataprotect.at, 18.10.2018); §§ 15, 29 GlBG.
- Unipile SAS – französisches Unternehmensregister (annuaire-entreprises.data.gouv.fr, SIREN 885 265 595); Seite „Security & Compliance“ von Unipile (unipile.com/security-compliance) – Angaben nicht unabhängig geprüft.
- Lynk-Quellcode (Repository lynk-edits-1), Dateien wie in Teil 3A referenziert; Stand 29. September 2026.