Lynk

DATA PROTECTION PACK · LYNK IN YOUR OWN CLOUD ACCOUNT

Your candidate data, *clearly* accounted for.

For recruitment agencies that run Lynk in their own cloud or server account. HP Capital GmbH sets it up and does not host it. Inside: data processing agreement for our support access (Art. 28 GDPR), technical and organisational measures (Art. 32 GDPR), our sub-processors and the providers you contract yourself, plus practical notes on candidate information, retention and the EU AI Act.

TEMPLATE – review by counsel required before use

This pack is a template, not legal advice. Values in [square brackets] are filled in per agency or are a choice for counsel. Your agency is the controller; your cloud, AI, Unipile and e-mail providers are your own processors.

01
One-page summary
Where your candidate data lives and who can see it

02
Data processing agreement
Only for our access during setup, support, developer days and maintenance

03
Technical & organisational measures
Software features · our access rules · your side

04
Sub-processors & your providers
Our short list vs. the providers you contract

05
Your duties as controller
Art. 14 information, legitimate interest, retention, EU AI Act

06
Open points for review
Your decisions, our to-dos, points for counsel

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

Template v1.0 · 29 September 2026

Contents

1 Where your candidate data lives and who can see it 2

2 Data processing agreement (Art. 28 GDPR) – support access 3

Annex 2.A – Parties and contacts 6

Annex 2.B – Description of the processing 7

Annex 2.C – Technical and organisational measures 7

Annex 2.D – Authorised sub-processors 7

3 Technical and organisational measures (Art. 32 GDPR) 8

3A Security features of the software 8

3B HP Capital's measures for support access 9

3C Your side – run in your own account 10

4 Sub-processors and your providers 11

4A HP Capital's sub-processors (DPA § 8) 11

4B Your providers – contracted and paid by you 11

5 Notes for your own compliance as controller 13

5.1 Legal basis: legitimate interest 13

5.2 Informing candidates (Art. 14 GDPR) 13

5.3 Data subject requests 13

5.4 Retention and deletion 14

5.5 Impact assessment and automated decisions 14

5.6 EU AI Act – what applies to recruitment AI 14

5.7 LinkedIn usage 15

6 Open points and decisions for review 16

7 Sources 17

Status of this pack – please read first

- **Template, not legal advice.** Every legal part is a draft for review by a data-protection lawyer on both sides. Values in [square brackets] are filled in per agency or are a choice for counsel.
- **Lynk runs in your own cloud account.** HP Capital GmbH does not host Lynk. During setup we install it in a cloud or server account that you open in your own name and pay directly. Your agency is the controller for all candidate data in it.
- **Your providers are your processors.** The cloud or server provider, the AI (LLM) provider, Unipile (LinkedIn connection), the e-mail provider and your ATS/CRM are contracted and paid by you. You sign their data processing terms directly; they are not HP Capital's sub-processors.
- **When HP Capital is a processor.** Only when we access personal data in your installation during setup, support, developer days, installing updates or maintenance (remote access). The data processing agreement in Part 2 covers exactly this limited access: least privilege, logged, removed after each task.

1 Where your candidate data lives and who can see it

A one-page summary for agency owners. No legal jargon – the details follow in Parts 2 to 5.

LinkedIn
Your recruiter finds a profile and imports it

→

Your Lynk
Stored in your own cloud account, in the data centre you choose

→

Your AI provider
Reads CV text to score and draft messages

→

Your recruiter
Reviews, decides and sends – a human stays in charge

1 Where it lives

In **your own Lynk installation**, in a cloud or server account opened in **your agency's name**. You choose the data centre; for EU agencies we recommend one in the EU. You pay the provider directly. HP Capital does not host Lynk and keeps no copy of your data.

2 Who owns it

You do. Your agency is the "controller". You hold all keys and passwords after handover. We never use your candidate data for our own purposes or to train AI.

3 Who in your team can see it

Only people you invite. Roles decide what they can do: **Owner, Admin, Recruiter, Viewer**. Sign-in with password (12+ characters) or Microsoft account; each user can add two-factor codes from an authenticator app.

4 Who else can see it

- **Your providers**, contracted by you: cloud or server, AI provider, Unipile (LinkedIn connection), e-mail, your ATS/CRM. Each only gets what it needs.
- **HP Capital** – only during setup, support, developer days, updates or maintenance you ask for: personal, logged access that is removed afterwards.
- **Nobody else.** No selling, no sharing.

5 What the AI sees

To score a candidate and draft a message, Lynk sends the relevant CV/profile text and job description to **the AI provider you choose**. Pick one that processes in the EU and does not train on your data; we help you choose. The match score is an **estimate, not a hiring decision**.

6 How long it stays

You set the rules. Lynk deletes old sourced profiles and message logs automatically (standard setting: 24 months, adjustable). Single candidates can be exported or erased. The data never leaves your account when our work ends – there is nothing to hand back.

! What stays your job

- **Tell candidates** you have their data – at the latest in your first message, with a link to your privacy notice and their right to object (Part 5.2).
- **Keep a human in charge**: a recruiter checks every shortlist and message before it counts. Recruiting AI is "high-risk" under the EU AI Act; the full duties apply from **2 December 2027** (Part 5.6).
- **Run your installation safely** with your IT partner – backups, updates, access to the cloud console (Part 3C) – and **sign** the agreement in Part 2 with us and the data processing terms of your own providers (Part 4B).

2 Data processing agreement (Art. 28 GDPR) – support access

TEMPLATE – review by counsel required before use

Scope. HP Capital does not host Lynk. This agreement covers only HP Capital's **access to personal data in the agency's own Lynk installation** during setup, support, developer days, installing updates and maintenance. The agency's cloud, AI, Unipile and e-mail providers are the agency's own processors under their own terms.

How this template is built. It follows the structure and content of the European Commission's standard contractual clauses for controller–processor contracts (Implementing Decision (EU) 2021/915, Clauses 7–10) and fills in the concrete Lynk details the EDPB expects (Guidelines 07/2020). **Choice for counsel** [Variant 1 or 2] **: Variant 1** – adopt the official wording of the standard clauses unchanged and attach Annexes 2.A–2.D; **Variant 2** – use this individual agreement. §§ 5 and 13 (access rules, AI) can be used with either variant.

between [Agency name, legal form, address, company register no.] – the **"Controller"** –

and HP Capital GmbH, Mayrwiesstraße 11, 5300 Hallwang (Salzburg), Austria, FN 631120 v, UID ATU82731634 – the **"Processor"**.

§ 1 Subject matter and relationship to the main contract

1.1 The Controller operates the Lynk recruiting software in a cloud or server account opened in its own name ("Customer Environment") under the Software Licence and Setup Agreement between the parties ("Main Contract"). The Processor does not host the software and does not store the Controller's personal data on its own systems.

1.2 Under the Main Contract and any maintenance contract, the Processor provides setup, support, developer days, installation of updates and maintenance ("Services"). When doing so it may gain access to personal data in the Customer Environment. Only to that extent does it process personal data on behalf of the Controller, and only to that extent does this agreement apply.

1.3 This agreement governs the parties' data protection obligations for that access. In case of conflict it prevails over the Main Contract as regards data protection. Details of the processing are set out in **Annex 2.B**. The Controller is solely responsible for the lawfulness of the processing in its installation, including sourcing and informing candidates, and for its own providers (see Parts 4B and 5).

§ 2 Instructions

2.1 The Processor processes personal data only on documented instructions from the Controller, including with regard to transfers to third countries, unless required to do so by Union or Member State law; in that case it informs the Controller before processing unless the law prohibits this.

2.2 The Main Contract, this agreement and each individual request or approval for a task (e.g. a support ticket, an order for developer days, an agreed update window) constitute the Controller's documented instructions. Further instructions are given in text form to **datenschutz@lynk-recruiting.com**.

2.3 The Processor informs the Controller without delay if it considers an instruction to infringe the GDPR or other data protection law, and may suspend carrying it out until it is confirmed or changed.

§ 3 Purpose limitation and duration

3.1 The Processor processes the data only to perform the task concerned. It does not use the data for its own purposes, in particular not to train, fine-tune or evaluate AI models, for benchmarking across customers or for marketing.

3.2 The Processor does not copy personal data from the Customer Environment to its own systems. If a copy is unavoidable for a task (e.g. to reproduce a fault), it is made only with the Controller's consent, pseudonymised where possible, stored encrypted and deleted as soon as the task is completed.

3.3 This agreement applies for as long as the Processor provides Services with access to personal data under the Main Contract or a maintenance contract.

§ 4 Security of processing and confidentiality

4.1 For its access, the Processor implements at least the measures in **Part 3B** of this pack (Annex 2.C). The security features of the software (Part 3A) are part of the licensed software; configuring and running the Customer Environment (Part 3C) is the Controller's responsibility.

4.2 The Processor may adapt its measures to technical progress, provided the level of protection is not reduced. Material changes are documented and notified to the Controller.

4.3 Only staff named to the Controller receive access, and only to the extent strictly necessary for the task. All persons authorised to process the data are bound to confidentiality (contractually or by law, incl. § 6 Austrian Data Protection Act, DSG).

§ 5 Rules for access to the Customer Environment

5.1 **On request only.** The Processor accesses the Customer Environment only for a task the Controller has requested or approved. During setup, access is granted for the setup period; after handover the Processor removes its administrative access (Main Contract, clause 8.1).

5.2 **Least privilege.** Access uses personal, named accounts with multi-factor authentication, never shared accounts, and only the rights the task needs. Where test or anonymised data is sufficient, the Processor does not use production data.

5.3 **Logging.** The Processor records each access (person, date and time, task, systems concerned) and provides this record to the Controller on request. Technical logs in the Customer Environment remain with the Controller.

5.4 **Removal after the task.** Temporary accounts, keys and sessions are removed or deactivated when the task is completed. The Controller may revoke any access at any time.

§ 6 Sensitive data

CVs and messages may incidentally contain special categories of data (e.g. health information, religion, trade union membership, photos) or data on criminal convictions. The Controller instructs its users not to request or record such data unless required and lawful. The Processor does not view, export or copy such data unless a task strictly requires it.

§ 7 Documentation, compliance and audits

7.1 The Processor responds promptly to the Controller's questions about the processing and makes available the information necessary to demonstrate compliance with Art. 28 GDPR and this agreement, in particular the access records under § 5.3.

7.2 The Controller may audit compliance, primarily by requesting documentation. On-site audits require 30 days' notice, take place during business hours, must not reveal other customers' data and are limited to one per year unless there is a specific reason (e.g. a data breach). The auditor must be bound to confidentiality. Each party bears its own costs.

7.3 The parties make this information available to the competent supervisory authority on request.

§ 8 Sub-processors

8.1 **General written authorisation.** The Controller authorises the sub-processors listed in **Part 4A** (Annex 2.D). HP Capital currently performs all access to the Customer Environment with its own staff.

8.2 The Processor informs the Controller in text form at least 30 days in advance of any intended addition or replacement of a sub-processor (name, location, service, data concerned, transfer mechanism). The Controller may object on reasonable data-protection grounds within 14 days. If the parties cannot agree, the Controller may terminate the affected Services (e.g. a maintenance contract) with effect from the change; the licence remains unaffected.

8.3 The Processor imposes on each sub-processor, by contract, essentially the same data protection obligations as in this agreement and remains fully responsible to the Controller for their performance.

8.4 **The Controller's own providers.** The provider of the Customer Environment and the other services the Controller contracts itself (AI provider, Unipile, e-mail, Microsoft, ATS/CRM – Part 4B) are **not** sub-processors of the Processor. The Controller concludes and manages its own agreements with them; the Processor only configures the connections on the Controller's instruction.

§ 9 International transfers

The Processor accesses the Customer Environment only from the EU/EEA. A transfer to a third country by the Processor (including remote access from a third country) only takes place on documented instruction of the Controller and if the requirements of Chapter V GDPR are met. Where the Controller's own providers process data outside the EU/EEA, the Controller assesses and secures this itself.

§ 10 Assistance to the Controller

10.1 **Data subject requests.** The Processor informs the Controller without delay of any request it receives directly from a data subject and does not answer it itself. The software provides the tools: a per-person export in machine-readable form (Art. 15/20 GDPR), per-person erasure across the data inventory with a report of what could not be erased and why (Art. 17), and an explanation record of how a candidate was scored and contacted. The Controller's administrator or IT partner runs them in the Customer Environment; the Processor helps as part of support.

10.2 The Processor also assists the Controller, taking into account the nature of the processing and the information available to it, with data protection impact assessments (Art. 35, 36 GDPR), security (Art. 32), breach notifications (Art. 33, 34) and the deployer obligations under the EU AI Act (§ 13).

10.3 Assistance beyond the support included in the Main Contract or a maintenance contract is charged at the day rate of the Main Contract, unless it is caused by a breach by the Processor.

§ 11 Personal data breaches

11.1 The Processor notifies the Controller without undue delay, and in any case within 24 hours, after becoming aware of a personal data breach connected with its access (e.g. a compromised access key or device), to the contact in Annex 2.A.

11.2 The notification contains at least: the nature of the breach (where possible categories and approximate number of data subjects and records), a contact point, the likely consequences and the measures taken or proposed. Information not yet available is provided in phases without undue delay.

11.3 The Processor takes the necessary measures to contain the breach, documents it and supports the Controller in its notification to the supervisory authority (72 hours, Art. 33) and to data subjects (Art. 34). For incidents in the Customer Environment not connected with its access, it supports the Controller as part of support.

§ 12 End of the agreement and deletion

12.1 This agreement ends when the Processor no longer provides Services with access to personal data. Obligations that by nature continue (confidentiality, deletion) survive.

12.2 The personal data stays in the Customer Environment throughout; no return is needed. At the end, the Processor removes all its remaining access credentials, deletes any copies under § 3.2 without undue delay and at the latest within 30 days, and confirms this in text form.

12.3 Retention is permitted only if Union or Member State law requires the Processor to store the data; the Processor informs the Controller of this.

§ 13 Additional provisions on AI processing (EU AI Act)

13.1 The Controller chooses and contracts the AI provider and ensures that it has signed data processing terms under Art. 28 GDPR. The Processor recommends providers that process data in the EU/EEA and do not use inputs or outputs to train their models.

13.2 If an update changes the default AI models or the scoring logic in a way that can affect results, the Processor informs the Controller in the release notes at least 14 days before the update is released, and keeps the model changelog up to date. The software logs a configuration fingerprint per AI call.

13.3 The Processor provides instructions for use. The software keeps logs (scoring events, decision and audit records) in the Customer Environment; the Controller retains them for at least six months (cf. Art. 26(6) AI Act). The Processor supports explanations to candidates (cf. Art. 86 AI Act).

13.4 The roles of the parties under the EU AI Act (provider / deployer) are governed by clause 14 of the Main Contract (see Part 5.6).

§ 14 Liability and final provisions

14.1 Liability towards data subjects is governed by Art. 82 GDPR. Between the parties, the liability provisions of the Main Contract apply.

14.2 Amendments must be in text form. Should a provision be invalid, the remainder remains valid; the parties replace it with a provision that comes closest to the intended purpose within the GDPR.

14.3 Austrian law applies, excluding conflict-of-law rules. Place of jurisdiction: Salzburg, Austria.

Place, date · Controller
[name, function]

Place, date · Processor – HP Capital GmbH
Paul Hagler or Philipp Habring, managing director

Annex 2.A – Parties and contacts

	Controller	Processor
Name, address	[Agency, address]	HP Capital GmbH, Mayrwiesstraße 11, 5300 Hallwang (Salzburg), Austria
Register / VAT	[register no. / VAT ID]	FN 631120 v, Regional Court of Salzburg / ATU82731634
Managing directors	[names]	Paul Hagler, Philipp Habring
Contact for data protection	[name, e-mail]	datenschutz@lynk-recruiting.com. No data protection officer designated (no obligation under Art. 37 GDPR expected; counsel to confirm).

	Controller	Processor
Breach notifications to	[e-mail monitored daily]	datenschutz@lynk-recruiting.com
Staff with access	–	Paul Hagler, Philipp Habring; further staff only after notice in text form

Annex 2.B – Description of the processing

Subject matter and nature	Remote access by the Processor to the Controller's own Lynk installation (Customer Environment) for: setup (installation, configuration, connecting the Controller's providers, tests); support (analysing and fixing faults); developer days (implementing changes); installing updates; maintenance under a separate maintenance contract. Viewing, querying and – only where a task requires it – changing or deleting data within the installation. No hosting, no storage on the Processor's systems.
Purpose	Performing the Services under the Main Contract or a maintenance contract.
Frequency	Occasional, per task; continuous access only during the setup period.
Data subjects	(1) potential candidates sourced from LinkedIn and other sources; (2) applicants and candidates in placement processes; (3) contact persons at the Controller's clients; (4) the Controller's users (recruiters, admins).
Categories of data	Whatever is stored in the installation and becomes visible during a task: identity and contact data; professional profile data; CV documents and their extracted content; message content and history; assessment answers and results; interview appointments; AI outputs (match scores, drafts) and decision/audit records; pipeline status and notes; user account data, roles and logs.
Special categories	Not intended; may occur incidentally in CVs or messages (see § 6).
Duration	Setup period; support and updates for 12 months after go-live under the Main Contract; afterwards only under an optional maintenance contract.
Place of processing	The Customer Environment, in the location chosen by the Controller. The Processor accesses it from the EU/EEA (Austria).

Annex 2.C – Technical and organisational measures

See **Part 3B** of this pack (binding measures for the Processor's access), which forms part of this agreement. Parts 3A and 3C are provided for information.

Annex 2.D – Authorised sub-processors

See **Part 4A** of this pack, which forms part of this agreement. Part 4B lists the Controller's own providers; they are not sub-processors of the Processor (§ 8.4).

3 Technical and organisational measures (Art. 32 GDPR)

Three kinds of protection, clearly separated. **3A**: security features built into the Lynk software – we name the place in the source code so your IT can check it. **3B**: what HP Capital does whenever it accesses your installation – binding under the DPA. **3C**: what your IT partner sets up and runs in your own cloud account – we set it up with you and document it at handover.

In the software checked in the Lynk source code HP Capital binding for our access

Your side your account, your IT partner

3A Security features of the software

Feature	Status	Evidence / note
Your own installation. Lynk is installed once per agency in the agency's own account; no shared system with other agencies.	In the software Your side	Deployment model: Docker images and Helm chart in the repository, installed in your account.
Workspace isolation: every query is filtered centrally to the user's workspace; automated tenant-isolation tests in CI.	In the software	`api: src/common/tenancy.py · SECURITY.md · docs/security/tenancy-audit-20260823.md`
Role-based permissions (Owner, Admin, Recruiter, Viewer); export and member management reserved to admins.	In the software	`api: security/rbac.py, security/rbac_enforce.py`
Passwords: minimum 12 characters with complexity rules; stored only as salted hashes. **Brute-force protection**: 5 sign-in attempts per 15 min per IP, lock-out after repeated failures.	In the software	`api: src/common/password_utils.py · src/rate_limit.py · src/modules/user/login_attempts.py`
Sessions: short-lived access tokens (default 60 min), refresh token in a Secure/HttpOnly cookie, server-side revocation on sign-out.	In the software	`api: src/common/jwt.py · src/common/cookie_security.py`
Microsoft sign-in (SSO); the agency's own Entra ID policies (MFA, conditional access) then apply. **Two-factor codes (TOTP app)**: enrolment and verification built in, secret stored encrypted; enforcement at sign-in for all users is not yet built in – use SSO policies to enforce MFA.	In the software Your side	`web: src/App.tsx (MSAL) · api: auth/mfa.py · docs/security/mfa-enforcement-decision-20260829.md`
Field-level encryption of particularly sensitive fields (phone numbers, connected-account tokens, MFA secrets) with authenticated encryption and key rotation; the key is set in your account during setup.	In the software	`api: security/field_crypto.py, security/encrypted_fields.py`
Transport security: HTTPS only; HSTS and security headers set by the application. **CV files private**: no public links. **Log redaction** of tokens, passwords and e-mail addresses.	In the software	`api: security/headers.py · src/common/s3_upload.py · security/log_redaction.py`
Audit and decision log: export and erasure, AI-assisted decisions, per-candidate explanation of scores and message origin. **AI traceability**: model configuration fingerprint per call, model changelog.	In the software	`api: src/common/audit.py · src/modules/decision_log · src/common/llm_config_fingerprint.py · MODEL_CHANGELOG.md`

Feature	Status	Evidence / note
Protection against manipulated requests: size limits, server-side request forgery guard, authenticated webhooks from the LinkedIn connector; **rate limiting** (default 300 requests/min per account); AI usage metered per call.	In the software	`api: src/common/body_limit.py, src/common/ssrf_guard.py, src/rate_limit.py, src/common/llm_metering.py`
Human review: recruiters review and send AI drafts; match score labelled "automated estimate, not a hiring decision"; optional AI notice to candidates.	In the software Your side	`product behaviour · api: src/common/ai_disclosure.py (Part 5.6)`
Deletion and export tools: per-person export and erasure with a report; monthly automatic deletion of sourced profiles and message logs (default 24 months, setting `PII_RETENTION_MONTHS`).	In the software	`api: src/modules/gdpr · deploy/gdpr/retention-cronjob.yaml · docs/gdpr.md`
Operations tooling shipped with the code: encrypted database backup job (AES-256, public key) with restore drill, network policies (default deny), hardened containers, monitoring and alert rules, secrets-manager templates.	In the software Your side	`deploy/backup/* · DR-RUNBOOK.md · infra/security/* · infra/monitoring · infra/secrets/*`
Secure development: static analysis (Semgrep), secret scanning (Gitleaks), container and dependency scanning (Trivy, Dependabot), software bill of materials; around 10,000 automated tests; private vulnerability reporting (acknowledgement within 3 business days).	In the software	`.github/workflows/w6_semgrep.yml, w7_gitleaks.yml, trivy-scan.yml, sbom.yml · SECURITY.md`

3B HP Capital's measures for support access

Measure	Status	Detail
Access only on request for a named task (setup, support ticket, developer days, update, maintenance).	HP Capital	DPA § 5.1; task reference kept in the access record.
Personal, named accounts with MFA; no shared accounts; credentials exchanged only via an encrypted password manager, never by plain e-mail.	HP Capital	DPA § 5.2.
Least privilege: only the rights the task needs; test or anonymised data wherever sufficient.	HP Capital	DPA § 5.2.
Access record: person, date and time, task and systems for every access; available to you on request.	HP Capital	DPA § 5.3.
Removal after the task: temporary accounts, keys and sessions removed; setup admin access removed at handover.	HP Capital	DPA § 5.4; licence agreement clause 8.1.
No copies on HP Capital systems; unavoidable copies only with consent, encrypted, deleted after the task.	HP Capital	DPA § 3.2.

Measure	Status	Detail
Secure devices: full-disk encryption, current security updates, screen lock; access only from the EU/EEA.	HP Capital	DPA § 9.
Confidentiality and training: written confidentiality undertakings (§ 6 DSG), annual data-protection training for everyone with access.	HP Capital	DPA § 4.3.
Breach procedure: detect, contain, notify you within 24 hours, document.	HP Capital	DPA § 11.
Security updates: security-relevant updates released without delay and announced to you.	HP Capital	Licence agreement clause 9.1.

3C Your side – run in your own account

Measure	Status	How we help
Cloud account security: MFA for everyone with access to the cloud console, few admins, separate accounts for your IT partner and for HP Capital.	Your side	Checklist at setup.
Data centre and physical security: provider and region of your choice (EU recommended), certified e.g. to ISO/IEC 27001.	Your side	We recommend suitable providers.
Encryption at rest of database volumes and file storage; file bucket private.	Your side	Configured during setup.
TLS certificate at the entry point, network rules, web application firewall if wanted.	Your side	Configured during setup from the shipped templates.
Backups and restore: daily encrypted backup to separate storage, private key kept offline, regular restore test; your targets for data loss (RPO) and restore time (RTO).	Your side	Backup job set up and one restore tested with your IT before go-live.
Patching and monitoring: operating system, database and container updates; installing Lynk updates; alerts.	Your side	Handover to your IT partner; during the 12 update months we support.
User administration: invite and remove users, assign roles, enforce MFA via SSO.	Your side	Training.

4 Sub-processors and your providers

Two different lists. **4A** is HP Capital's own list for the DPA – deliberately short, because we do not host your data. **4B** lists the providers your Lynk installation uses: you choose, contract and pay them directly, and they work for you.

4A HP Capital's sub-processors (DPA § 8)

Service	Provider	Data concerned	Location
Access to your installation	None – performed by HP Capital's own staff	Data visible during a task (Annex 2.B)	Austria / EU
Support e-mail (hello@ and datenschutz@lynk-recruiting.com)	[mailbox provider of lynk-recruiting.com – HP Capital to name before first access]	Only what you send us by e-mail. Please do not send candidate data by e-mail – we look at it in your installation instead.	[EU]
Integration service for the ATS/CRM connection (only if used)	Only if an integration service is used for your connection; it is named to you **before the contract**. If none is used, this row does not apply.	Data passed between your ATS/CRM and Lynk (e.g. jobs, applications, candidate profiles)	Named with the service – EU preferred

If HP Capital ever involves a further company or freelance developer with access to your installation, it is added here with 30 days' notice and you can object (DPA § 8.2).

4B Your providers – contracted and paid by you

Service	Provider	Data concerned	Location	Your contract
Cloud or server (servers, database, file storage, backups)	Your choice; guide price ≈ €/$ 50–150/month	All data of your installation	Your choice – EU recommended	Provider's standard terms incl. data processing terms
AI / LLM (CV extraction, match scoring, message drafts)	Your choice – any OpenAI-compatible API; ≈ €/$ 200–300/month for 10 recruiters	CV and profile text, job description, context for a draft	Choose EU processing	Data processing terms incl. no training on your data
LinkedIn connection (search, import, messaging per recruiter)	Unipile SAS, 168 Rue de la Rotonde, 42153 Riorges, France; ≈ €/$ 5 per recruiter/month	Recruiter's LinkedIn session; profiles viewed/imported; messages	EU (France) per Unipile	Unipile terms; DPA available from Unipile on request
E-mail sending (notifications, assessment and booking e-mails)	Your SMTP provider; small cost	Recipient address, e-mail content	Choose EU	Provider's data processing terms

Service	Provider	Data concerned	Location	Your contract
Microsoft (optional: sign-in, Outlook calendar)	Microsoft Ireland Operations Ltd., Dublin	User identity; calendar availability and appointments	EU Data Boundary per your contract	Your Microsoft 365 terms
ATS/CRM (your existing system; one connection included in the 8-Week Program)	Your vendor – you connect Lynk with your own account	Jobs, applications, candidate data; write-back where agreed, depending on system and plan	Per your contract	Your existing contract with the vendor

Good to know

- **These are your processors.** You need a data processing agreement with each (usually part of the provider's standard terms). We help you choose and set them up, but we are not a party to these contracts.
- **LinkedIn** itself is not a processor. Your recruiters use their own LinkedIn accounts under LinkedIn's terms. Automating LinkedIn with third-party tools can conflict with LinkedIn's User Agreement and lead to account restrictions – Lynk applies per-account sending limits, but the risk cannot be excluded (Part 5.7).
- **Transfers outside the EU** depend on the providers you choose. With EU providers none are needed; otherwise you check the transfer basis (e.g. EU–US Data Privacy Framework or standard contractual clauses).
- Prices are rough guides at the date of this pack; the providers set them.

Status of both lists: 1 October 2026. Current version on request at datenschutz@lynk-recruiting.com.

5 Notes for your own compliance as controller

You, the agency, decide why and how candidate data is used – and you run the system in your own account – so the following duties are yours. These are practical, non-binding notes to discuss with your data-protection advisor, not legal advice.

5.1 Legal basis: legitimate interest

Sourcing candidates from professional networks is usually based on **legitimate interest** (Art. 6(1)(f) GDPR): your interest in filling client roles, and the candidate's potential interest in career opportunities, weighed against their privacy. Supervisory authorities have accepted active sourcing as permissible when the data was published in a professional context and the information duties are met (e.g. Hessian DPA, 51st activity report, case of a personnel service provider).

- **Document a balancing test** (legitimate interest assessment) once for your sourcing process.
- **Only professional data**: use what the candidate published for professional purposes (LinkedIn profile, CV they send). Do not search private social media or collect special-category data.
- **Relevance**: source for concrete roles or clearly defined talent pools, not indiscriminately.
- **Longer-term talent pool**: once a candidate has responded, ask for **consent** (Art. 6(1)(a)) to keep them for future roles, or keep only as long as the current process requires.
- **Client contacts** (hiring managers): legitimate interest / contract; B2B e-mail marketing has its own rules (Austria: § 174 TKG 2021; Germany: § 7 UWG).

5.2 Informing candidates (Art. 14 GDPR)

When you import a profile from LinkedIn, you have collected data **not from the candidate**. Art. 14 GDPR then requires you to inform them:

- **When:** at the latest with your **first message** (Art. 14(3)(b)); if you do not contact them, within a reasonable period and at the latest **one month** after import (Art. 14(3)(a)). Profiles you import but never contact should therefore be deleted quickly or informed.
- **What:** who you are and how to contact you (and your DPO if any); purposes and legal basis; your legitimate interest; categories of data; **the source (e.g. "your public LinkedIn profile")**; recipients (e.g. clients, only with consent to be presented; IT service providers); retention period; rights (access, rectification, erasure, restriction, objection, portability); right to complain to the supervisory authority (Austria: Datenschutzbehörde; Germany: the Land authority).
- **Right to object** (Art. 21(4)): must be pointed out explicitly and separately from other information, at the latest in the first communication.
- **AI use**: say that you use AI-assisted tools to find and pre-assess profiles and draft messages, and that a recruiter decides (see 5.6).

Example wording for the end of a first LinkedIn message [adapt with counsel]

"I found your public LinkedIn profile and saved your professional details to contact you about this role. We use AI-assisted tools to pre-select profiles; a recruiter makes all decisions. You can object at any time – just reply 'no' and we will delete your data. Details: [short link to your privacy notice]"

Lynk supports this with message templates and placeholders; a built-in AI notice for generated messages can be switched on for your installation.

5.3 Data subject requests

- Answer requests for access, erasure or objection within **one month** (Art. 12(3)).

- Lynk can export all data about a person in machine-readable form and erase it across all stored collections, with a report of anything that cannot be erased and why. Your administrator or IT partner runs these functions in your installation (see the documentation); we help as part of support.
- Keep an objection list (name/profile ID only) so that people who objected are not imported again.

5.4 Retention and deletion

Situation	Suggested period (your decision)	Reasoning
Profile imported, candidate never contacted	1 month	Art. 14(3)(a) – otherwise you must inform them anyway.
Contacted, no reply or not interested	3–6 months after last contact	Data minimisation; keep objection list only.
Candidate in a placement process, not placed	End of process + **7 months** (Austria)	Austrian DSB accepts 7 months for applicant data because of the 6-month claim periods under the Equal Treatment Act (GlBG) plus one month. Germany: commonly ~6 months (AGG § 15(4), § 61b ArbGG).
Talent pool with consent	24 months, then renew consent	Consent-based; withdrawal possible at any time.
Placed candidates, invoices	Statutory retention (e.g. 7 years for accounting records in Austria, § 132 BAO)	Only the records needed for accounting.

What Lynk does automatically: a monthly job deletes sourced LinkedIn profiles and message logs older than a configurable period (default 24 months, counted from creation). It does not distinguish by pipeline status – shorter periods for the situations above are handled via the setting or a regular clean-up by your team.

5.5 Impact assessment and automated decisions

- **DPIA (Art. 35 GDPR):** AI-supported evaluation of candidates at scale is likely to require a data protection impact assessment. Check against the Austrian DPIA list (DSFA-V) or the German DSK list. We provide system descriptions, data flows and the TOMs as input.
- **No automated rejections (Art. 22 GDPR):** Lynk's match score is an estimate that supports a recruiter; it does not decide. Do not use it to automatically reject or exclude people without a human review.
- **Records of processing (Art. 30):** add Lynk, your cloud provider and your other Lynk providers (Part 4B) to your record of processing activities.

5.6 EU AI Act – what applies to recruitment AI

AI systems used to **recruit or select people** – in particular to place targeted job ads, analyse and filter applications and evaluate candidates – are **high-risk** under Annex III point 4(a) of the AI Act (Regulation (EU) 2024/1689). As an agency using Lynk you are a **deployer**.

Since / from	What applies
2 February 2025	Prohibited practices (e.g. emotion recognition at the workplace – not used by Lynk). AI literacy (Art. 4): take measures so your staff understand the tool – softened by the Digital Omnibus (Reg. (EU) 2026/1744) to "support" AI literacy, but still applies.

Since / from	What applies
2 August 2026	Transparency (Art. 50): people must be informed when they interact with an AI system (e.g. an automated chat reply), unless obvious.
2 December 2027	Full high-risk obligations for Annex III systems, postponed from 2 August 2026 by the Digital Omnibus on AI (in force since 27 July 2026).

Deployer duties (Art. 26 AI Act) – and how Lynk supports them

- **Use according to the instructions for use** – provided by HP Capital with the handover.
- **Human oversight** by trained, competent staff with authority to override (Art. 26(2)) – Lynk: drafts are reviewed and sent by recruiters; score labelled as estimate; approval queue for messages.
- **Relevant input data** under your control (Art. 26(4)) – e.g. clear, non-discriminatory job requirements.
- **Monitor operation** and report serious incidents or risks to the provider (Art. 26(5)).
- **Keep automatically generated logs** for at least six months (Art. 26(6)) – Lynk: decision log and audit export, stored in your installation.
- **Inform candidates** that a high-risk AI system is used in decisions about them (Art. 26(11)), and give an **explanation** on request (Art. 86) – Lynk: explanation record per candidate, AI notice in messages.
- **Employees**: if you use Lynk for hiring your own staff, inform workers' representatives first (Art. 26(7)).
- Use the provider information for your **DPIA** (Art. 26(9)).

Provider or deployer? A point for counsel

Lynk is licensed with full source code, runs in the agency's own account and is set up under the agency's own brand. Under Art. 25(1) AI Act, a deployer that **puts its own name or trademark** on a high-risk system or **makes a substantial modification** can itself become the **provider**, with much heavier duties (conformity assessment, technical documentation, registration). The licence agreement (clause 14) allocates the roles; counsel should confirm that this allocation holds.

5.7 LinkedIn usage

LinkedIn's User Agreement restricts the use of third-party software to automate activity. Lynk connects each recruiter's own account via Unipile and applies per-account sending limits, but LinkedIn may still restrict accounts. This is a contractual risk with LinkedIn, separate from data protection; the safe-LinkedIn playbook in your training covers recommended limits.

6 Open points and decisions for review

What still has to be decided – by you, by us and by counsel – before the first access to your installation.

6.1 Your decisions before go-live

Item	Decision needed
Cloud or server provider	Provider, EU region, certification (e.g. ISO 27001), data processing terms accepted.
AI (LLM) provider	Provider, EU processing, no-training clause, data processing terms signed.
Unipile and e-mail provider	Accounts opened in your name; data processing terms signed.
IT partner	Who runs backups, updates and monitoring after handover (we can recommend one).
Access and MFA policy	Who administers the cloud account; MFA for all users (via Microsoft SSO or authenticator app).
Retention periods	Your periods per situation (Part 5.4) and the automatic deletion setting (default 24 months).
Candidate information	Privacy notice, first-message wording, AI notice on or off (Parts 5.2, 5.6).

6.2 HP Capital to-dos

Item	Status
Written access procedure (Part 3B)	To be documented internally before the first customer access.
Mailbox provider (Part 4A)	To be named in the sub-processor list.
MFA enforcement in the software	Enrolment exists; enforcement at sign-in for all users not yet built – until then enforce via SSO.

6.3 Contract values set in this template – for counsel to confirm

Clause	Value
Template basis	[Variant 1 or 2] – official SCC 2021/915 wording + annexes, or this agreement
§ 3.2 / § 12.2	No copies; unavoidable copies deleted after the task, at the latest 30 days after the end
§ 7.2	Audit notice 30 days; once a year; each party bears its own costs
§ 8.2	Sub-processor notice 30 days; objection within 14 days
§ 11.1	Breach notification within 24 hours
§ 13	Model-change notice 14 days; log retention at least 6 months
§ 14	Liability per the licence agreement; jurisdiction Salzburg

6.4 Points that most need a data-protection lawyer

1. **Role allocation without hosting**: HP Capital as processor only for occasional support access – is the limited DPA sufficient, and must it be signed before the first setup access?
2. **AI Act role**: does white-labelling, source-code ownership and running the system in the agency's own account make the agency a provider (Art. 25)? What does HP Capital owe as provider of the delivered version (by 2 Dec 2027)?
3. **Agency's own provider chain**: cloud, AI, Unipile and e-mail as the agency's processors – what the agency must check (transfers, no-training clauses).
4. **Active sourcing basis**: legitimate-interest assessment, Art. 14 timing and wording, objection handling, retention periods for Austria and Germany.
5. **DPIA** requirement and template for agencies.
6. **LinkedIn terms**: contractual risk of automated activity via Unipile.

7 Sources

- Regulation (EU) 2016/679 (GDPR), Art. 6, 12–14, 21, 22, 28, 30, 32–37.
- Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors (Art. 28(7) GDPR) – eur-lex.europa.eu/eli/dec_impl/2021/915/oj.
- EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR (v2.1); EDPB Opinion 22/2024 on obligations following from reliance on processors and sub-processors.
- Regulation (EU) 2024/1689 (AI Act), Art. 4, 25, 26, 50, 86, Annex III point 4; Regulation (EU) 2026/1744 (Digital Omnibus on AI), published OJ 24 July 2026, in force 27 July 2026.
- Hessian Commissioner for Data Protection (HBDI), 51st activity report (2022) – active sourcing by a personnel service provider.
- Austrian Data Protection Authority (DSB), decision of 2018 on retention of applicant data for 7 months (reported e.g. by dataprotect.at, 18 Oct 2018); §§ 15, 29 GlBG.
- Unipile SAS – French company register (annuaire-entreprises.data.gouv.fr, SIREN 885 265 595); Unipile security & compliance page (unipile.com/security-compliance) – statements not independently verified.
- Lynk source code (repository lynk-edits-1), files as referenced in Part 3A; state of 29 September 2026.