⟨∞⟩ LinkMCP

DATA PROCESSING ADDENDUM

Effective Date: The effective date of the applicable Terms of Service.

Document Date: 2026-10-30

This Data Processing Addendum (the "**DPA**") supplements and forms part of the Terms of Service between Third Person Systems LLC (d/b/a LinkMCP) ("**Processor**"), a limited liability company organized under the laws of Wyoming, United States, and the customer entity identified in the applicable Terms of Service ("**Controller**").

Processor's contact for data protection matters under this DPA is info@linkmcp.io.

Each of Processor and Controller is referred to herein as a "**Party**" and collectively as the "**Parties**."

1. DEFINITIONS

Capitalized terms not defined herein shall have the meanings set forth in the Terms of Service. In this DPA:

1.1 **"Applicable Data Protection Laws"** means Regulation (EU) 2016/679 ("**GDPR**"), the laws of the EEA member states implementing or supplementing it, the GDPR as incorporated into UK law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("**UK GDPR**") and the UK Data Protection Act 2018, the Swiss Federal Act on Data Protection and its implementing ordinances, the California Consumer Privacy Act of 2018, as amended, and any other applicable laws governing the Processing of Personal Data under this DPA.

1.2 **"Controller"** means the entity that determines the purposes and means of the Processing of Personal Data. Under this DPA, the Customer is the Controller.

1.3 **"Data Subject"** means an identified or identifiable natural person to whom Personal Data relates.

1.4 **"LinkedIn Data"** means any data retrieved from or submitted to LinkedIn via the Service on behalf of Controller, whether through Controller's LinkedIn session, from LinkedIn's public web pages, or from third-party LinkedIn data providers, including profile information, messages, posts, comments, connections, reactions, and related metadata.

1.5 **"Personal Data"** means any information relating to an identified or identifiable natural person that is subject to Applicable Data Protection Laws and that is provided by Controller to Processor, or otherwise collected or received by Processor on behalf of Controller, in connection with the Service.

1.6 **"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

1.7 **"Processing"** (and its grammatical variations) means any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment or combination, restriction, erasure, or destruction.

1.8 **"Processor"** means the entity that Processes Personal Data on behalf of the Controller. Under this DPA, Third Person Systems LLC (d/b/a LinkMCP) is the Processor.

1.9 **"Security Measures"** means appropriate administrative, technical, physical, and organizational safeguards designed to protect the confidentiality, integrity, availability, and resilience of Personal Data in Processor's possession or control, as described in this DPA and Exhibit B.

1.10 **"Service"** means the LinkMCP MCP server and related services provided by Processor to Controller under the Terms of Service.

1.11 **"Subprocessor"** means any third party engaged by Processor to assist in Processing Personal Data on behalf of Controller under this DPA.

1.12 **"Subprocessor List"** means Processor's then-current list of authorized Subprocessors, available at https://linkmcp.io/legal/SL-STD.pdf.

1.13 **"Terms of Service"** or **"TOS"** means the Terms of Service agreement between the Parties governing Controller's use of the Service.

2. SCOPE & APPLICATION

2.1 Incorporation

This DPA is incorporated by reference into and forms part of the Terms of Service. By agreeing to the Terms of Service, Controller also agrees to the terms of this DPA.

2.2 Applicability

This DPA applies only to the extent Processor Processes Personal Data subject to Applicable Data Protection Laws in connection with the Service.

2.3 Order of Precedence

In the event of any conflict or inconsistency between this DPA and the Terms of Service, the terms of this DPA shall prevail solely with respect to the Processing of Personal Data.

3. DATA PROCESSING

3.1 Processing on Instructions

Processor shall Process Personal Data only in accordance with Controller's documented instructions, which include the Terms of Service and this DPA, unless otherwise required by applicable law. Controller's use of the Service constitutes Controller's instructions to Processor to Process Personal Data as necessary to provide the Service. If Processor believes any instruction violates Applicable Data Protection Laws, it shall promptly inform Controller.

3.2 Nature and Purpose of Processing

The Service is an MCP server that accesses LinkedIn on behalf of Controller. Processor retrieves LinkedIn Data through Controller's LinkedIn session, from LinkedIn's public web

pages, or from third-party data providers, and retrieves contact data (such as email addresses and phone numbers) from third-party data providers. Processor caches and transmits this data as directed by Controller through API requests. The nature, purpose, duration, types of Personal Data, and categories of Data Subjects are described in Exhibit A.

3.3 Caching and Retention

LinkedIn Data and contact data retrieved through the Service are cached with per-request-type time-to-live ("**TTL**") periods to improve performance and reduce API load. After the applicable TTL expires, cached entries are treated as stale and are overwritten with fresh data upon the next API request for the same resource. Cached entries are not linked to Controller's Account. Controller instructs Processor to keep LinkedIn Data and contact data in a cache that is shared by all customers of the Service, so that an entry retrieved for one customer can be used to answer the same request from another customer within the TTL. Each cached entry is deleted automatically within thirty-one (31) days after it was last fetched.

3.4 Confidentiality

Processor shall ensure that any person it authorizes to Process Personal Data is subject to a duty of confidentiality (whether contractual or statutory) and shall not Process such data except on Processor's instructions.

3.5 No Independent Use

Processor shall not sell or share Personal Data for cross-context behavioral advertising, and shall not sell, share, license, disclose, or otherwise use Personal Data for Processor's own independent purposes. Processor shall Process Personal Data only as necessary to provide, secure, support, and maintain the Service (including the shared cache described in Section **3.3**) and strictly in accordance with Controller's documented instructions, this DPA, and Applicable Data Protection Laws.

4. CUSTOMER OBLIGATIONS

4.1 Lawful Basis

Controller is responsible for ensuring that it has a valid legal basis for the Processing of Personal Data under Applicable Data Protection Laws, including for the collection and use of LinkedIn Data through the Service.

4.2 LinkedIn Terms of Service

Controller acknowledges that use of the Service involves accessing LinkedIn's platform and data. Controller is solely responsible for ensuring that its use of the Service complies with LinkedIn's applicable terms of service, user agreements, and policies. Processor makes no representations regarding the permissibility of Controller's specific use cases under LinkedIn's terms.

4.3 Accuracy of Instructions

Controller is responsible for the accuracy of the Personal Data it provides to Processor, for the lawfulness of its documented instructions, and for the secure use of the Service and systems under Controller's control, including safeguarding API keys and account credentials.

4.4 Prohibited Data

Controller shall not use the Service to Process special categories of personal data as described in Article 9 GDPR, data regarding criminal convictions or offenses, protected health information, biometric identifiers, or personal data of children under sixteen (16) years of age, unless the Parties execute a written amendment expressly authorizing such Processing.

5. SUB-PROCESSORS

5.1 Authorization for Subprocessing

Controller authorizes Processor to engage the Subprocessors identified on the Subprocessor List available at https://linkmcp.io/legal/SL-STD.pdf as authorized Subprocessors for the Service and for the purposes described therein.

5.2 Notification of Changes

Processor shall provide Controller with at least fifteen (15) business days' prior written notice (the "**Notice Period**") of any intended addition or replacement of a Subprocessor that will Process Personal Data on behalf of Controller. Such notice may be provided by email and may reference an updated Subprocessor List. Processor shall not disclose or otherwise make available Personal Data to a proposed new or replacement Subprocessor until (a) Controller has given its written approval or (b) the Notice Period has expired without Controller having raised a written objection in accordance with Section **5.3**.

5.3 Objection Right

Controller may object to the engagement of a proposed Subprocessor on reasonable, data-protection-related grounds by delivering written notice to Processor within the Notice Period. Each notice shall identify the proposed Subprocessor, its location, and the Processing activities it will perform, whether in the notice itself or in the updated Subprocessor List. Upon receipt of a timely objection, the Parties shall cooperate in good faith to resolve the objection, which may include considering an alternative Subprocessor or implementing additional safeguards. If the Parties do not reach a mutually acceptable resolution within thirty (30) calendar days after Processor receives Controller's objection, Controller may, as its sole and exclusive remedy, terminate the affected services upon written notice.

5.4 Subprocessor Obligations

Processor shall enter into a written agreement with each Subprocessor imposing data protection obligations that are substantially similar to those set forth in this DPA. Processor remains responsible for any acts or omissions of its Subprocessors that cause Processor to

breach any of its obligations under this DPA. As an exception, Anymail Finder (Section 2.6 of the Subprocessor List) keeps the email addresses that it finds or confirms for the Service, with the related name and company, in its own business contact database as an independent controller, and it can return them to its other customers. Controller authorizes Processor to use Anymail Finder for the contact discovery tools on these terms. For that use only, the agreement with Anymail Finder does not include the obligations of Section **3.5**, and Exhibit A, Section **2(c)** does not apply to it.

6. DATA SECURITY

6.1 Security Measures

Processor shall implement and maintain appropriate technical and organizational Security Measures to protect Personal Data from (i) accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access, and (ii) all other unlawful forms of Processing. Such measures shall be commensurate with the risk of Processing and the nature of the Personal Data, taking into account current industry practices and the costs of implementation. A description of such measures is appended as Exhibit B.

6.2 Encryption

Processor shall encrypt Personal Data in transit using TLS 1.2 or higher and at rest using AES-256 or equivalent encryption standards.

6.3 Access Controls

Processor shall implement role-based access controls, unique user identifiers, strong password policies, and multi-factor authentication for personnel accessing systems that Process Personal Data. Administrative access shall be restricted to limited personnel with a demonstrated need-to-know.

6.4 Infrastructure Isolation

The Service is hosted on DigitalOcean virtual servers and a managed database located in Amsterdam, the Netherlands. Database backups are stored in encrypted form with Amazon

Web Services in Stockholm, Sweden. Processor shall maintain logical isolation between customers' Accounts (other than the shared cache described in Section **3.3**) and segregation of production and non-production environments.

6.5 Incident Response

Processor shall maintain a written incident response plan with defined roles, responsibilities, and procedures for escalation, investigation, remediation, and post-incident review.

7. DATA SUBJECT RIGHTS

7.1 Cooperation with Controller

Taking into account the nature of the Processing, Processor shall provide reasonable assistance to Controller in fulfilling Controller's obligations to respond to Data Subject requests to exercise their rights under Applicable Data Protection Laws, including rights of access, rectification, erasure, restriction, data portability, and objection.

7.2 Notification of Requests

Processor shall, to the extent permitted by law, promptly notify Controller if it receives a request from a Data Subject to exercise rights under Applicable Data Protection Laws. Processor shall not respond to such request except (i) to direct the Data Subject to contact Controller, or (ii) with Controller's prior written instructions.

8. DATA BREACH NOTIFICATION

8.1 Notification Obligation

Processor shall notify Controller without undue delay and, where feasible, within seventy-two (72) hours after becoming aware of a Personal Data Breach affecting Personal Data Processed on behalf of Controller.

8.2 Content of Notification

Processor shall provide reasonable information regarding:

a. the nature of the Personal Data Breach, including the categories and approximate number of Data Subjects and Personal Data records concerned;

b. the likely consequences of the Personal Data Breach;

c. the measures taken or proposed to address the Personal Data Breach, including measures to mitigate its possible adverse effects; and

d. the name and contact details of Processor's point of contact for further information.

8.3 Controller Responsibility

Controller remains responsible for determining whether to notify Data Subjects, supervisory authorities, or any other third parties, except to the extent Applicable Data Protection Laws require Processor to do so directly.

9. DATA PROTECTION IMPACT ASSESSMENTS

9.1 Assistance with DPIAs

Taking into account the nature of the Processing and the information available to Processor, Processor shall provide reasonable assistance to Controller with data protection impact assessments and prior consultations with supervisory authorities, to the extent required under Articles 35 and 36 of the GDPR or equivalent requirements under other Applicable Data Protection Laws.

10. INTERNATIONAL DATA TRANSFERS

10.1 Processing Locations

Processor is established in the United States (Wyoming). The Service infrastructure is hosted in Amsterdam, the Netherlands (DigitalOcean), and database backups are stored in

Stockholm, Sweden (Amazon Web Services). Processing under this DPA may take place in these locations and in other jurisdictions where Processor or its authorized Subprocessors perform services, in each case subject to this Section **10**.

10.2 Lawful Transfer Mechanisms

Processor shall not transfer Personal Data to a third country or international organization unless it has implemented a lawful transfer mechanism under Applicable Data Protection Laws, such as an adequacy decision, the standard contractual clauses adopted by the European Commission, the UK International Data Transfer Addendum, the Swiss supplements recognized under Swiss Data Protection Laws, or another valid transfer mechanism.

10.3 Standard Contractual Clauses

To the extent the standard contractual clauses adopted by the European Commission ("**SCCs**") are required to lawfully transfer Personal Data from the European Economic Area to Processor, those clauses are incorporated into this DPA by reference as though fully set out herein and completed as follows:

a. Module Two (Controller to Processor) applies;

b. Clause 7 (docking clause) does not apply;

c. in Clause 9, Option 2 (general written authorization) applies and the notice period for Subprocessor changes is fifteen (15) business days;

d. Clause 11's optional language (independent dispute resolution body) does not apply;

e. in Clause 17, the governing law is the law of Ireland;

f. in Clause 18(b), the Parties submit to the courts of Ireland;

g. Annex I.A is deemed completed with the Parties' details set out in this DPA and the applicable Terms of Service;

h. Annex I.B is deemed completed with the information in Exhibit A;

i. Annex I.C is the competent supervisory authority determined in accordance with Clause 13 of the standard contractual clauses; and

j. Annex II is deemed completed with the information in Exhibit B.

10.4 UK International Data Transfer Addendum

To the extent required for transfers from the United Kingdom, the standard contractual clauses shall be deemed supplemented by the UK International Data Transfer Addendum, with Tables 1 through 3 completed using the information in this DPA, the applicable Terms of Service, and the Exhibits, and Table 4 providing that neither Party may terminate the UK International Data Transfer Addendum as permitted under Section 19 of that addendum.

10.5 Swiss Transfers

To the extent required for transfers from Switzerland, the standard contractual clauses shall be deemed supplemented by the modifications required under Swiss Data Protection Laws.

10.6 Supplementary Measures

Where required by Applicable Data Protection Laws, Processor shall conduct and document a transfer impact assessment and shall implement supplementary technical, organizational, or contractual measures as reasonably necessary to ensure an essentially equivalent level of protection for the transferred Personal Data. Supplementary measures include encryption in transit and at rest as described in Section **6.2**, strict access controls as described in Section **6.3**, and infrastructure hosting within the European Union as described in Section **6.4**. Upon Controller's reasonable written request, Processor shall provide information reasonably necessary to demonstrate compliance with this Section **10**, subject to confidentiality obligations and legal restrictions.

11. RETURN & DELETION OF DATA

11.1 Cached Data

Cached entries of LinkedIn Data and contact data are deleted automatically within thirty-one (31) days after they were last fetched, as described in Section **3.3**. Logs of Controller's API

requests, which can contain request parameters (for example, profile identifiers, search terms, or message text, each shortened to five hundred (500) characters), are deleted automatically after twenty-four (24) months. Other LinkedIn Data that Processor stores for Controller (for example, the text of posts that Controller saves as drafts or schedules, and the records and payloads of webhook notifications that Controller sets up) is deleted with Controller's account data under Section **11.2**.

11.2 Account Data on Termination

Upon expiration or termination of the Terms of Service, Processor shall delete Controller's account data, including API keys, authentication tokens, and account configuration, within thirty (30) days, unless retention is required by applicable law.

11.3 Backup Copies

Processor may retain Personal Data in routine backup copies for the period such copies are retained in the ordinary course of business, provided that such Personal Data remains protected in accordance with this DPA and is not further Processed except for backup recovery or as otherwise required by law.

12. AUDIT RIGHTS

12.1 Audit Rights

Controller, or an independent external auditor appointed by Controller and bound by written confidentiality obligations, may audit Processor's compliance with this DPA and Applicable Data Protection Laws. Processor shall make available all information reasonably necessary to demonstrate such compliance. Any audit shall be:

a. limited to once per twelve (12)-month period, unless required more frequently by law, by a competent supervisory authority, or following a Personal Data Breach;

b. conducted during Processor's normal business hours upon reasonable advance written notice of at least thirty (30) days, unless a shorter period is required by law or reasonably necessary due to a Personal Data Breach;

c. limited in scope to matters directly relevant to Processor's Processing of Personal Data for Controller and conducted in a manner that avoids unreasonable disruption to Processor's business and does not compromise the confidentiality, security, or availability of other customers' data;

d. carried out first by review of available documentation, written responses, and any then-current third-party audit reports or certifications made available by Processor, with access to relevant Processor-controlled premises, personnel, and documentation only to the extent reasonably necessary to complete the audit; and

e. subject to Controller and its auditors complying with Processor's reasonable site-security, confidentiality, and health-and-safety requirements.

12.2 Third-Party Certifications

Processor may satisfy routine audit requests in whole or in part by providing current third-party audit reports, certifications, or completed security questionnaires, but the provision of such materials does not limit Controller's rights under Section **12.1** where a more specific audit is reasonably necessary.

12.3 Costs and Confidentiality

Controller shall bear any costs of the audit unless the audit reveals a material breach of this DPA by Processor, in which case Processor shall bear its own costs. Controller shall treat any information disclosed during the audit as Processor's confidential information.

13. TERM & TERMINATION

13.1 Term

This DPA shall become effective on the date Controller agrees to the Terms of Service and shall remain in effect for the duration of the Terms of Service. This DPA shall automatically terminate upon termination or expiration of the Terms of Service, subject to Section **11** (Return & Deletion of Data).

13.2 Survival

Sections **1** (Definitions), **8** (Data Breach Notification), **11** (Return & Deletion of Data), **12** (Audit Rights), and **14** (General Provisions) shall survive termination or expiration of this DPA to the extent necessary to give effect to their terms.

14. GENERAL PROVISIONS

14.1 Liability

EXCEPT TO THE EXTENT LIABILITY CANNOT BE LIMITED UNDER APPLICABLE DATA PROTECTION LAWS OR ANY APPLICABLE TRANSFER MECHANISM, THE LIABILITY OF EACH PARTY UNDER OR IN CONNECTION WITH THIS DPA (INCLUDING ITS EXHIBITS) IS SUBJECT TO THE LIMITATIONS OF LIABILITY SET FORTH IN THE TERMS OF SERVICE. IF THE TERMS OF SERVICE DO NOT LIMIT LIABILITY, THEN EACH PARTY'S AGGREGATE LIABILITY UNDER THIS DPA SHALL NOT EXCEED THE AMOUNTS PAID OR PAYABLE BY CONTROLLER TO PROCESSOR UNDER THE TERMS OF SERVICE IN THE TWELVE (12) MONTHS PRECEDING THE EVENT GIVING RISE TO THE LIABILITY.

14.2 Third-Party Beneficiaries

Except for Data Subjects to the extent they may invoke rights under Applicable Data Protection Laws or any applicable transfer mechanism incorporated into this DPA, there are no third-party beneficiaries to this DPA.

14.3 Entire Agreement; Amendments

This DPA, including any exhibits, and the Terms of Service constitute the entire agreement between the Parties relating to the Processing of Personal Data and supersede all prior agreements or understandings with respect to such subject matter. Any change or modification to this DPA must be made in a written amendment agreed by the Parties.

14.4 Severability

If any provision of this DPA is deemed invalid or unenforceable by a court of competent jurisdiction, the remainder of this DPA shall remain valid and in effect, and the Parties shall promptly amend the invalid provision so that it becomes valid and enforceable while preserving the Parties' original intent.

14.5 Governing Law

This DPA and any non-contractual obligations arising out of or in connection with it shall be governed by the laws of the State of Wyoming, excluding its conflict-of-laws rules, except to the extent that a different governing law is mandated by Applicable Data Protection Laws or the standard contractual clauses incorporated herein.

14.6 Venue

Any dispute arising out of or in connection with this DPA shall be submitted to the exclusive jurisdiction of the state and federal courts in Wyoming, except to the extent that a different jurisdiction is mandated by Applicable Data Protection Laws or the standard contractual clauses incorporated herein.

14.7 Electronic Assent

This DPA may be accepted by incorporation into the Terms of Service, including through an online order process, click acceptance, or other valid electronic assent, each of which will be deemed effective to form a binding agreement.

⟨∞⟩ LinkMCP

EXHIBIT A

DETAILS OF PROCESSING

1. Subject Matter and Duration

a. **Subject Matter:** The Processing of Personal Data as described in the Terms of Service and this DPA, for purposes of providing the LinkMCP Service, which enables Controller's AI assistants to access LinkedIn via the Model Context Protocol.

b. **Duration:** For the term of the Terms of Service. Cached entries of LinkedIn Data and contact data are deleted within thirty-one (31) days after they were last fetched. Logs of Controller's API requests are deleted after twenty-four (24) months. Content that Controller stores in the Service (such as post drafts, scheduled posts, and webhook records) is kept until Controller's account data is deleted under Section **11.2**. Account data is deleted within thirty (30) days of termination.

2. Nature and Purpose of Processing

a. Processor retrieves, caches, transmits, and temporarily stores LinkedIn Data on behalf of Controller as directed through API requests made via MCP-compatible AI assistants. Processing includes searching for profiles and companies, retrieving posts, comments, reactions, and connections, sending and receiving messages, creating posts and comments, saving posts as drafts and publishing them at a scheduled time, sending event notifications to webhook endpoints that Controller sets up, and discovering contact information. Processor also logs each request, including its parameters, for billing, security, support, and debugging purposes.

b. The purpose of Processing is to enable Controller's AI assistants to interact with LinkedIn in real time on Controller's behalf. Actions taken as Controller on LinkedIn, and access to Controller's own LinkedIn data (such as messages and connections), use a LinkedIn account that Controller, a member of Controller's workspace, or another person authorized by Controller (for example, through a connection link) has connected to Controller's Account, through a LinkedIn session that a Subprocessor maintains. Lookups of profile, company, and post data may instead be answered

from the shared cache described in Section **3.3**, from LinkedIn's public web pages, or by third-party data providers.

c. Neither Processor nor its Subprocessors shall use Personal Data to train, fine-tune, or otherwise improve any generalized machine-learning model or service made available to persons other than Controller, except for the business contact database of Anymail Finder described in Section **5.4**.

3. Types of Personal Data

Depending on Controller's usage of the Service, Personal Data Processed may include:

a. LinkedIn profile data (e.g., names, job titles, employer names, profile URLs, profile photographs, work history, education, skills, endorsements)

b. Contact discovery data (e.g., email addresses, mobile phone numbers)

c. LinkedIn messaging data (e.g., message content, conversation metadata, timestamps, sender and recipient identifiers)

d. LinkedIn post and engagement data (e.g., post content, comments, reactions, authorship information)

e. LinkedIn connection data (e.g., connection lists, connection request details, mutual connections)

f. LinkedIn search results (e.g., people search results, Sales Navigator search results, company search results)

g. Controller's account data (e.g., names and email addresses of Controller's users, hashed API keys and access tokens, the reference to Controller's LinkedIn connection with basic LinkedIn profile details, and account configuration)

h. Request logs (e.g., the tool called, request parameters shortened to five hundred (500) characters, IP addresses, user agents, timestamps, result status, and cost)

i. LinkedIn sign-in details (email address and password, or session cookies) that Controller's users enter to connect a LinkedIn account. On the connection page in

the Application, Processor forwards them once, in memory, to the LinkedIn connectivity Subprocessor and does not store them. On the hosted connection page, they go directly to that Subprocessor. On the connection page in the Application, the user's IP address and browser type are also forwarded to that Subprocessor.

j. Content that Controller stores in the Service (e.g., the text, image links, and mentions of post drafts and scheduled posts, webhook endpoint URLs and delivery records with the event data sent, and connection links in hashed form)

4. Categories of Data Subjects

a. LinkedIn users whose profiles, posts, or other content are accessed by Controller through the Service

b. LinkedIn users with whom Controller communicates or connects through the Service

c. Controller's employees, contractors, or authorized users who access the Service

d. Other individuals whose Personal Data may appear in LinkedIn content accessed through the Service

e. Persons who connect their LinkedIn account to Controller's Account through a connection link that Controller sends them

5. Frequency of Transfer

Ongoing and on demand throughout the duration of the Terms of Service, as determined by Controller's API requests through MCP-compatible AI assistants.

6. Obligations and Rights of Controller

a. Controller is responsible for ensuring that it has a valid legal basis for the Processing of Personal Data, for providing any required notices to Data Subjects, for the accuracy of the Personal Data it provides to Processor, for compliance with LinkedIn's terms of service and policies, and for issuing lawful documented instructions to Processor.

b. Processor is responsible for Processing Personal Data only on Controller's documented instructions, implementing and maintaining the Security Measures described in this DPA, assisting Controller as required by Applicable Data Protection Laws, and ensuring that any onward transfer by Processor or its Subprocessors complies with Section **10** of this DPA.

c. Each Party is responsible for the security of the systems, credentials, personnel, and environments under its own control.

⟨∞⟩ LinkMCP

EXHIBIT B

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

1. Organization of Information Security

a. Designated personnel responsible for information security and data protection.

b. Documented internal security policies and procedures, reviewed periodically and updated as appropriate to Processor's size, services, and risk profile.

c. Risk-based review of security controls and incidents, with remediation tracked by responsible personnel.

2. Infrastructure Security

a. **Server Isolation.** The Service runs on DigitalOcean virtual servers and a DigitalOcean managed database in Amsterdam, the Netherlands. The servers are used only for the Service, and its workloads run in separate containers. The database accepts connections only from these servers, and only over TLS. Production and non-production environments are logically segregated.

b. **Cloud Provider Controls.** DigitalOcean maintains industry-standard physical security controls for its data centers, including controlled access, 24/7 on-site security, surveillance, and intrusion detection.

c. **No On-Premises Storage.** Processor does not store Personal Data on local servers or in paper form. All production data resides within the managed cloud infrastructure. Database backups are stored in encrypted form with Amazon Web Services in Stockholm, Sweden, and are deleted after thirty (30) days.

3. Data Encryption

a. Encryption of Personal Data in transit using TLS 1.2 or higher.

b. Encryption at rest using AES-256 or equivalent for stored Personal Data, including cached LinkedIn Data.

c. Securing encryption keys with industry-standard key management processes.

4. Logical Access Controls

a. Role-based access control for all systems Processing Personal Data.

b. Unique user identifiers, strong password policies, and multi-factor authentication where feasible.

c. Restricted administrative access to limited personnel with a need-to-know.

d. API key or OAuth authentication for Controller access to the Service, with API keys revocable at any time.

5. Network Security

a. Use of network security controls such as a cloud firewall that blocks all incoming connections other than web traffic (HTTP and HTTPS) and administrative access from approved addresses, a reverse proxy that serves the Service over TLS, database access limited to the servers of the Service, and infrastructure-provider protections.

b. Segregation of production and non-production environments.

6. Data Minimization & Cache Management

a. LinkedIn Data is cached with per-request-type TTLs. After TTL expiry, cached entries are treated as stale and overwritten upon the next request. Cached entries are deleted automatically within thirty-one (31) days after they were last fetched.

b. Cached LinkedIn Data is not independently queryable and is used solely to serve subsequent API requests, from any customer of the Service, during the TTL window.

c. Account data retained only for the duration of the active subscription plus the deletion period specified in Section **11.2** of the DPA.

d. Logs of API requests are deleted automatically after twenty-four (24) months.

e. LinkedIn sign-in details entered on the connection page in the Application are forwarded to the LinkedIn connectivity Subprocessor in memory and are not stored. Error reports sent to the error-monitoring Subprocessor exclude the request bodies of sign-in and LinkedIn connection requests, and filter passwords, tokens, cookies, and similar fields.

7. Operational Security

a. Maintenance of audit logs for key systems, with regular review for anomalies.

b. Formal change management procedures, including patching and updates for software dependencies.

c. Application monitoring via Sentry for error tracking and performance monitoring.

8. Personnel Security

a. Personnel screening, reference checks, or equivalent vetting measures where appropriate for the role and permitted by law.

b. Mandatory confidentiality commitments and security awareness training for personnel with access to Personal Data.

9. Endpoint Security

a. Employee devices are password-protected, encrypted, and subject to Processor's acceptable use and security policies.

b. Access to production systems from endpoints requires multi-factor authentication.

10. Incident Response

a. Written incident response plan, with defined roles and responsibilities.

b. Procedures for escalation, investigation, remediation, and post-incident reviews.

c. Notification to Controller within seventy-two (72) hours of becoming aware of a Personal Data Breach, as described in Section **8** of the DPA.

11. Business Continuity & Disaster Recovery

a. Backup and recovery procedures for production data and critical systems, appropriate to Processor's hosting environment and risk profile.

b. Periodic verification that backups can be restored and that recovery procedures remain effective.

12. Testing & Auditing

a. Periodic vulnerability review, dependency monitoring, and security testing appropriate to Processor's size and risk profile.

b. Independent assessments, customer diligence responses, or third-party audit materials may be provided where available.

(Processor reserves the right to modify these Security Measures at any time, provided such modifications do not materially reduce the overall level of protection.)