⟨∞⟩ LinkMCP

PRIVACY POLICY

Effective Date: 2026-10-30

This Privacy Policy describes how **Third Person Systems LLC** (d/b/a LinkMCP) ("**LinkMCP**," "**we**," "**us**," or "**our**") collects, uses, discloses, and protects Personal Data when you access or use our website at https://linkmcp.io or https://app.linkmcp.io (collectively, the "**Website**"), our MCP server product, APIs, and related services (collectively, the "**Service**"). By accessing or using the Service, you acknowledge that you have read and understood this Privacy Policy.

1. INTRODUCTION

LinkMCP is an MCP server that gives AI assistants direct access to LinkedIn through API endpoints. The Service operates as a self-service SaaS platform where users sign up with a one-time email code or with Google, can connect their LinkedIn account by signing in to LinkedIn on our connection page, and connect their AI assistants through OAuth or an API key. We are committed to protecting the privacy of our users and being transparent about how we handle Personal Data.

For the purposes of the EU General Data Protection Regulation ("**GDPR**"), Third Person Systems LLC is the data controller. For the purposes of the California Consumer Privacy Act ("**CCPA**"), we are the business that determines the purposes and means of processing Personal Data described in this Privacy Policy.

2. INFORMATION WE COLLECT

2.1 Account Information

When you create and use an account, we collect the following information:

a. **Sign-Up Data**. You can sign up with a one-time code sent to your email address, or with Google. With email sign-up, we collect your email address and the first name you enter. With Google sign-up, we receive your name, email address, and profile picture from Google. We do not receive or store your Google password.

b. **LinkedIn Connection**. When you connect your LinkedIn account, you sign in to LinkedIn with your LinkedIn email and password, or with session cookies from your browser. Depending on how you connect: (i) on the connection page in the Application, your sign-in details pass through our servers in a single encrypted request, and we forward them, with your IP address and browser type, to our LinkedIn connectivity provider, Unipile SAS ("**Unipile**"); or (ii) on the hosted connection page at auth.linkmcp.io, which Unipile operates for us, your sign-in details go directly to Unipile and our servers do not receive them. Unipile uses the sign-in details to sign in to LinkedIn and then maintains your LinkedIn session, and processes your LinkedIn messages so that the messaging features work. We do not store your LinkedIn password or session cookies. We store a reference to the connection and basic details of your LinkedIn profile: your name, public profile URL, LinkedIn member ID, and whether you have Sales Navigator or Recruiter.

c. **API Keys**. We generate API keys, and access tokens for AI assistants that you authorize through OAuth, that authenticate your MCP access to the Service. In our database, we store them only in hashed form.

d. **Content You Store in the Service**. If you use these features, we store: posts that you or your AI assistant save as drafts or schedule (the text, links to images, mentions, the planned time, and, after publication, the link to the post on LinkedIn), including after they are published or cancelled, so that you can see them in the Application; webhook endpoints that you set up (the URL and a signing secret) and a record of each webhook delivery, including the event data sent (for example, the name, company, position, and profile URL of a person who accepted your connection request); and connection links that you create (only in hashed form).

e. **Email Address Changes**. If you change the email address of your account, we keep a record of the previous and the new address. For ninety (90) days after the change, a sign-in with the previous address does not create a new account.

f. **Onboarding Answers and Your Profile URL**. If you choose to answer, we store what you want to use the Service for (for example, sales, recruiting, or job search), any short text you add, and the URL of your own LinkedIn profile if you enter it. We use your answer to show you the relevant features and to understand who uses the Service. We give your profile URL to the AI assistants that you connect, so that they can find your own LinkedIn profile (see Section 4(g)). You can change or remove your profile URL on the Account page of the Application.

2.2 Usage Data

We automatically collect certain information when you use the Service:

a. **API Call Logs**. For each request made through the Service, we log the tool or endpoint called, the request parameters (for example, search terms, profile identifiers, or message text, each shortened to five hundred (500) characters), the timestamp, the result status, error details, and the cost of the request.

b. **IP Addresses**. We collect IP addresses and user-agent strings (the type of browser or AI client) associated with requests to the Service and Website.

c. **Browser & Device Information**. When you visit the Website, we collect browser type, operating system, referring URLs, pages viewed, and the date and time of each visit, including through Google Analytics and PostHog (see Section 10). When you sign up, we record the referring page, the landing page, and any campaign (UTM) parameters. When you are signed in to the Application, we record the pages you view and the buttons you click. PostHog also records your clicks and a replay of your interactions with the pages, with all form inputs masked (see Section 10(e)).

d. **Error Reports & Session Replays**. When an error occurs, our error-monitoring service (Sentry) records technical details of the request, such as the URL, headers, and request data. If you accept session replays in our cookie banner (see Section 10), Sentry also records, for a sample of sessions in the Application, a replay of the page interactions, with text and form inputs masked.

e. **Email Engagement**. When we send you product update emails, our own email software (it runs on our servers at DigitalOcean) records whether each email was

delivered and opened and which links in it were clicked. Amazon Web Services (Amazon SES) delivers these emails.

2.3 Cached LinkedIn Data

The Service caches the results of lookups that it obtains from LinkedIn's public web pages and from third-party data providers. We cache this data with per-request-type time-to-live ("**TTL**") values to improve performance and reduce API load. This cached data may include profile information, company information, post content, comments, reactions, and contact details (email addresses and phone numbers) returned by our contact discovery tools. After the applicable TTL expires, the cached entry is treated as stale and is overwritten with fresh data upon the next API request for the same resource. For example, post comments are cached for approximately three (3) minutes, and profile, company, and contact data for approximately twenty-four (24) hours. Cached entries are not linked to a specific Account: an entry fetched for one user can be returned to another user who makes the same request within the TTL. Cached entries are deleted automatically within thirty-one (31) days after they were last fetched.

2.4 Payment Data

Payment processing for the Service is handled by Stripe, LLC ("**Stripe**"), our third-party payment processor. When you subscribe, Stripe collects and processes your payment instrument details (e.g., credit card numbers) on our behalf. We do **not** collect, receive, or store credit card numbers or other payment instrument details. We collect and store your billing name and billing address for invoicing and tax purposes. For information about how Stripe handles your data, please refer to Stripe's privacy policy.

2.5 Information We Do Not Collect

a. **LinkedIn Passwords**. We do not store your LinkedIn password. If you enter it on the connection page in the Application, it passes through our servers once, in memory, only to be forwarded to Unipile. If you use the hosted connection page, our servers do not receive it.

b. **Credit Card Numbers**. Stripe handles all payment processing. We never see, receive, or store your credit card or other payment instrument details.

2.6 People Who Connect Through a Connection Link

A customer of the Service can send you a connection link so that you connect your LinkedIn account to that customer's workspace (for example, an agency that manages LinkedIn activity for you). When you use such a link, you sign in to LinkedIn on the hosted connection page described in Section 2.1(b)(ii), and you do not get a LinkMCP account. The customer who sent the link then decides how your LinkedIn account is used through the Service, and we process the related Personal Data on that customer's behalf. We store the same connection reference and profile details as described in Section 2.1(b). You can end the connection at any time by signing out of the session or changing your password in your LinkedIn account settings, by asking the customer to disconnect it, or by contacting us at info@linkmcp.io.

2.7 Referrals

If we offer our referral program to your workspace, its administrators can share a referral link that contains a code for the workspace. If a person opens the link and then creates a new account, we keep a referral record that links the new account, and later the workspace it creates, to the workspace that shared the link. The record also holds the status of the referral, the amount, date, and Stripe references of the first payment of the new workspace, and the amount and Stripe references of any credit that we give for the referral. It does not hold names or email addresses. We use referral records to run the referral program: to decide whether a referral earns a credit, to prevent abuse of the program, to give the credit as a balance on the Stripe customer account of the workspace that shared the link, which Stripe applies to its next invoice, and to leave referred sign-ups out of our measurements of how people find and buy the Service. To prevent abuse, we check, for example, that the new account uses a company or school email address that was not used for an earlier account, that the two workspaces do not share an email domain or a member, that the payments were not refunded or disputed, and that the same payment card did not pay for both workspaces. For the card check, we compare card fingerprints that Stripe provides, not card numbers. The administrators of the workspace that shared the link see only the number of people who signed up through it, the number of referrals that wait for a credit, and the number of credits earned, and not who signed up. If they referred only one person, these numbers can show them that this person signed up or paid.

3. HOW WE USE YOUR INFORMATION

We use the Personal Data we collect for the following purposes:

a. **Provide & Operate the Service**. To create and manage your account, authenticate API requests, connect your LinkedIn account, and deliver the functionality of the Service.

b. **Performance & Optimization**. To cache the results of LinkedIn data lookups, monitor API performance, and improve the speed and reliability of the Service.

c. **Usage Analytics**. To understand how users interact with the Service, measure feature adoption, and inform product development.

d. **Customer Support**. To respond to your inquiries, troubleshoot issues, and provide technical assistance.

e. **Billing & Subscription Management**. To manage your subscription, process payments via Stripe, and provide invoices and receipts.

f. **Communications**. To send messages about your account and the Service (e.g., sign-in codes, account confirmations, security alerts, usage and billing notices, emails during your free trial, and service updates) and, where you have opted in or where permitted by law, product news and other marketing communications (for example, our product update emails). You may opt out of product news and marketing communications at any time with the unsubscribe link in each such email or by contacting us at info@linkmcp.io.

g. **Security & Fraud Prevention**. To detect, investigate, and prevent unauthorized access, abuse, or other malicious activities.

h. **Legal Compliance**. To comply with applicable laws, regulations, and legal processes, and to enforce our terms and protect our rights.

Where the GDPR applies, we process Personal Data on the following legal bases: (i) performance of a contract with you (providing the Service); (ii) our legitimate interests in

operating, securing, and improving the Service, provided those interests are not overridden by your rights; (iii) your consent, where specifically requested; and (iv) compliance with legal obligations.

4. HOW WE SHARE YOUR INFORMATION

We do not sell your Personal Data. We share Personal Data only in the following circumstances:

a. **Subprocessors & Service Providers**. We engage third-party service providers who process Personal Data on our behalf to help us operate and deliver the Service. A current list of our subprocessors, including the categories of data processed and processing locations, is maintained in our Subprocessor List, available at https://linkmcp.io/legal. These providers include: DigitalOcean (hosting and databases); Amazon Web Services (encrypted database backups and delivery of product update emails); Unipile (LinkedIn connection and session management); LinkdAPI and ReverseContact (LinkedIn profile, company, and post data); LeadMagic (email and phone discovery, and email validation); Anymail Finder (email discovery when LeadMagic finds no email); Proxy Empire (proxy network used to fetch public LinkedIn pages); Twilio SendGrid (email delivery); MailerLite (product update emails); Sentry (error monitoring and session replay); PostHog (product analytics and session replay); Google (Google sign-in, Google Analytics, and our business email); Stripe (payments); and Linear and Slack (internal handling of feedback and operational notifications). We require all subprocessors to maintain appropriate security measures and to process Personal Data only as instructed by us. One exception is Anymail Finder, which keeps the email addresses that it finds, with the related name and company, in its own business contact database as an independent controller (see the Subprocessor List).

b. **Stripe (Payment Processor)**. Stripe processes your payment information on our behalf as our third-party payment processor. Stripe processes payment data in accordance with its own privacy policy and PCI-DSS requirements.

c. **LinkedIn**. When you use a feature that acts on LinkedIn as you, or that reads your own LinkedIn data, your request is sent to LinkedIn through your LinkedIn session, which Unipile maintains. LinkedIn processes that data according to its own terms and privacy policy. Lookups of profile, company, and post data may instead be sent to the data providers listed in Section 4(a), or fetched from LinkedIn's public web pages through our proxy provider.

d. **Professional Advisors**. Lawyers, auditors, or insurers when necessary for legitimate business purposes.

e. **Legal & Safety**. Competent authorities or other parties when required to comply with law, respond to lawful requests, protect rights, or prevent harm.

f. **Business Transfers**. In connection with a merger, acquisition, financing, or sale of assets involving Third Person Systems LLC, subject to confidentiality protections. In such event, your Personal Data may be among the assets transferred.

g. **Services You Choose**. When you connect an AI assistant (for example, Claude, ChatGPT, or Cursor) or an automation tool to the Service, we send the results of your requests to that assistant or tool. When you set up a webhook, we send the event data to the URL that you choose. These services process the data under their own terms and privacy policies.

h. **Referrals**. If you sign up through a referral link, the administrators of the workspace that shared the link can see, as numbers, that a person signed up through it, that the referral waits for a credit, or that a credit was earned, but not your name, email address, or other details (see Section 2.7).

5. DATA CACHING & RETENTION

5.1 Cached Data

LinkedIn data and contact data are cached with per-request-type TTLs, as described in Section 2.3. After the applicable TTL expires, the cached entry is treated as stale and is overwritten with fresh data upon the next API request for the same resource. Cached entries

are not linked to an Account, so they are not deleted when an Account is deleted. Instead, each cached entry is deleted automatically within thirty-one (31) days after it was last fetched.

5.2 Account Data

We retain your account information (name, email, profile picture, LinkedIn connection reference and profile details, and hashed API keys and access tokens), your onboarding answers and the LinkedIn profile URL you entered, the content you store in the Service (see Section 2.1(d)), and a record of security and billing events in your account (such as sign-ins, changes of your email address, and purchases) for as long as your account remains active. If you ask us to close your account, we will delete or anonymize your account data within thirty (30) days, unless retention is required to comply with legal obligations (for example, billing and tax records), resolve disputes, enforce our agreements, or protect the security of the Service.

5.3 Usage Logs

API call logs, the cost records of each request, and the in-app page views and clicks described in Section 10(d) are retained for twenty-four (24) months for billing, analytics, security monitoring, and debugging purposes, and are then deleted automatically. We keep a record of the onboarding steps you completed (for example, connecting your first AI assistant and making your first request) for as long as your account remains active. You can ask us to delete or anonymize the logs linked to you before then by contacting us at info@linkmcp.io.

5.4 Backups

We keep backups of our database so that we can restore the Service after a failure. Data that we delete can remain in these backups for up to thirty (30) days, after which the backups are deleted automatically. We use backups only to restore the Service.

5.5 Referral Records

We keep each referral record (see Section 2.7) for as long as the accounts and workspaces in it exist. When a workspace is deleted, we delete its referral code. When an account or a

workspace is deleted, we remove it from the referral records. The rest of each record stays, without it: the code that was used, the status of the referral, and, where there was a payment or a credit, its amount, date, and Stripe references, which we keep as billing records (see Section 5.2). We also record the steps of each referral (for example, the sign-up, the first payment, and the credit) in our audit trail with the other billing events of the accounts involved. These audit records stay after an account or a workspace is deleted, as part of our billing records (see Section 5.2).

6. INTERNATIONAL DATA TRANSFERS

Third Person Systems LLC is a United States company incorporated in Wyoming. Our infrastructure is hosted on DigitalOcean, with servers located in Amsterdam, the Netherlands, and our database backups are stored with Amazon Web Services in Stockholm, Sweden. Depending on your location, your Personal Data may be transferred to and processed in the United States, the European Union, or other countries where we or our service providers operate.

Where Applicable Privacy Laws require cross-border transfer safeguards, we rely on an adequacy decision, Standard Contractual Clauses ("**SCCs**"), or another valid transfer mechanism recognized under applicable law. If you are located in the European Economic Area ("**EEA**"), the United Kingdom, or Switzerland, your Personal Data will be transferred in accordance with GDPR requirements.

7. DATA SECURITY

We employ administrative, technical, and organizational measures designed to protect Personal Data from unauthorized access, alteration, disclosure, or destruction. These measures include encryption of data in transit, access controls, storage of API keys and access tokens in hashed form, and regular security reviews. Despite our efforts, no method of transmission over the internet or method of electronic storage is one hundred percent (100%) secure, and we cannot guarantee absolute security.

8. YOUR RIGHTS UNDER GDPR

If you are located in the EEA, the United Kingdom, or Switzerland, you have the following rights under the GDPR (or equivalent local law) with respect to your Personal Data:

a. **Right of Access**. You have the right to request confirmation of whether we process your Personal Data and, if so, to obtain a copy of that data.

b. **Right to Rectification**. You have the right to request correction of inaccurate Personal Data or completion of incomplete Personal Data.

c. **Right to Erasure**. You have the right to request deletion of your Personal Data, subject to certain legal exceptions (e.g., compliance with legal obligations).

d. **Right to Data Portability**. You have the right to receive your Personal Data in a structured, commonly used, and machine-readable format and to transmit it to another controller.

e. **Right to Restriction of Processing**. You have the right to request that we restrict processing of your Personal Data in certain circumstances, such as when you contest the accuracy of the data.

f. **Right to Object**. You have the right to object to processing based on our legitimate interests. We will cease processing unless we demonstrate compelling legitimate grounds that override your interests. You may object to direct marketing at any time.

g. **Right to Withdraw Consent**. Where we process your Personal Data based on consent, you may withdraw that consent at any time without affecting the lawfulness of processing prior to withdrawal.

h. **Right to Lodge a Complaint**. You have the right to lodge a complaint with your local data protection supervisory authority if you believe our processing of your Personal Data violates applicable law.

To exercise any of these rights, please contact us at info@linkmcp.io. We will verify your identity before fulfilling your request and respond within the timelines required by applicable law.

9. YOUR RIGHTS UNDER CCPA

If you are a California resident, you have the following rights under the CCPA:

a. **Right to Know**. You have the right to request disclosure of the categories and specific pieces of Personal Data we have collected about you, the categories of sources, the business purposes for collection, and the categories of third parties with whom we share it.

b. **Right to Delete**. You have the right to request deletion of Personal Data we have collected from you, subject to certain exceptions.

c. **Right to Opt Out**. You have the right to opt out of the "sale" or "sharing" of your Personal Data. We do not sell Personal Data in the traditional sense of exchanging it for monetary consideration. To the extent any disclosure of Personal Data to third parties constitutes a "sale" or "sharing" under the CCPA, you may exercise your right to opt out by contacting us at info@linkmcp.io.

d. **Right to Non-Discrimination**. We will not discriminate against you for exercising any of your CCPA rights. We will not deny you the Service, charge you different prices, or provide a different level of quality based on your exercise of privacy rights.

To exercise any of these rights, please contact us at info@linkmcp.io. We will verify your identity before fulfilling your request and respond within forty-five (45) days, or as otherwise required by applicable law.

10. COOKIES & TRACKING

The Website and the Application use essential cookies and similar browser storage that are strictly necessary for the Website and Service to function properly. These include cookies for

session management, authentication, security, and interface settings, and a record of your cookie choices. Other than the analytics and session replay technologies described below, we do not use non-essential cookies, and we do not use advertising or marketing cookies.

a. **Your Choices**. We show a cookie banner on the Website. Wherever you are, Google Analytics loads only after you accept analytics cookies in the banner. Wherever you are, Sentry records session replays only after you accept them in the banner. PostHog (see Section 10(e)) does not wait for your choice: it starts on your first page and stops when you click "Reject". You can change or withdraw your choice at any time through the cookie settings link on the Website.

b. **Google Analytics**. We use Google Analytics 4, a web analytics service provided by Google, to measure visits, sign-ups, and purchases on the Website and in the Application. We use Google Consent Mode, which tells Google Analytics whether you have accepted analytics cookies. When analytics cookies are on, Google Analytics sets its own cookies (for example, "_ga") and receives your IP address, information about your browser and device, and the pages you visit. When they are off, the Google tag does not load, and Google Analytics receives no information about your visit. You can turn them off through the cookie settings link on the Website or with Google's opt-out browser add-on at https://tools.google.com/dlpage/gaoptout.

c. **Error Monitoring & Session Replays**. We use Sentry to record errors in the Website and the Application. Error reports contain technical details, such as the page address, your browser type, and details of the error. Error monitoring does not use cookies. If you accept session replays, Sentry records, for a sample of sessions in the Application and for sessions in which an error occurs, a replay of your interactions with the pages, with all text and form inputs masked. For this, Sentry keeps an identifier in your browser's session storage.

d. **Product Analytics**. When you are signed in, we record the pages you view, the buttons you click (with the button label), and your browser's time zone in the Application on our own servers, to understand how the Service is used. PostHog also records page views and clicks in the Application (see Section 10(e)). For this, we keep a random session identifier in your browser's session storage. When you visit

the Website, we also store the referring page, the landing page, any campaign (UTM) parameters, and the code of any referral link that you opened (see Section 2.7) in your browser's local storage, and if you sign up within thirty (30) days, we save them with your Account. These first-party records do not depend on your cookie banner choice.

e. **PostHog**. We use PostHog, a product analytics service of PostHog, Inc. in the United States, to understand how visitors and users use the Website and the Application. PostHog records the pages you view, your clicks, scrolling, and mouse movements, and a replay of your interactions with the pages, with all form inputs masked and email addresses and access keys removed. Pages that show your content, such as your LinkedIn accounts, your team, your scheduled posts, and your activity log, are recorded with all text masked, and pages with access keys and webhook secrets are not recorded. PostHog also receives your browser and device type, the referring page, any campaign (UTM) parameters, and an approximate location (such as country and city) that it derives from your IP address. It does not store your IP address. When you are signed in, PostHog links these records to your user ID and account details (workspace ID, plan, trial dates, sign-up date, and whether a LinkedIn account is connected). We do not give PostHog your name or email address. Our servers also send PostHog events about your Account, such as your sign-up, the start and end of your trial, your first AI assistant connection and first request (with the name of the AI assistant and of the tool), the connection of a LinkedIn account, and your purchases. These events do not contain the content of your requests, LinkedIn data, names, or email addresses. PostHog does not set cookies or store anything in your browser. It starts without waiting for your choice in the cookie banner. If you click "Reject", PostHog stops in your browser and receives nothing more from it until you click "Accept". The events that our servers send do not depend on your choice. PostHog deletes session replays after ninety (90) days at the latest, and we keep the other PostHog records for as long as we need them to understand how the Service is used.

If we introduce other non-essential cookies or tracking technologies in the future, we will update this Privacy Policy and, where required by law, obtain your consent before deploying them.

You can configure your browser to block or delete cookies. Note that blocking essential cookies may impair the functionality of the Website and Service.

11. CHILDREN'S PRIVACY

The Service is not directed to children under sixteen (16) years of age, and we do not knowingly collect Personal Data from children under sixteen (16). If we learn that we have collected Personal Data from a child under sixteen (16), we will delete that data without undue delay. If you believe a child has provided us with Personal Data, please contact us at info@linkmcp.io.

12. THIRD-PARTY LINKS

The Website and Service may contain links to third-party websites or services, including LinkedIn, Stripe, and others. We are not responsible for the privacy practices or content of those third parties. Your interactions with third-party websites and services are governed by their own privacy policies. We encourage you to review the privacy policy of any third-party site you visit.

13. CHANGES TO THIS POLICY

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or other factors. If we make material changes, we will post the revised Privacy Policy on the Website and update the Effective Date above. We encourage you to review this Privacy Policy periodically. Your continued use of the Service after the revised Privacy Policy becomes effective constitutes your acknowledgment of the changes.

14. CONTACT US

If you have questions, concerns, or requests regarding this Privacy Policy or our privacy practices, please contact us:

Third Person Systems LLC (d/b/a LinkMCP)

Email: info@linkmcp.io

Website: https://linkmcp.io