# LUP Technologies AB

# Sub-processors

Date of Last Revision: 2024-03-01

LUP Technologies AB (“LUP”, “we”, “us”, or “our”) uses certain sub-processors (including third parties, as listed below) and content delivery networks to assist it in providing the LUP Services, as described in our Terms of Service (“ToS”). Defined terms used herein shall have the same meaning as defined in the ToS.

**When does LUP act as a Data Processor vs. a Data Controller?**

- **As a Data Processor**: LUP processes personal data on behalf of customers (e.g., handling driver check-ins, managing logistics notifications).
- **As a Data Controller**: LUP determines how and why some personal data is processed (e.g., usage analytics, fraud prevention, security monitoring).

Customers using LUP’s services must ensure they have the appropriate legal basis for collecting and sharing data with us. Customers are responsible for informing their end users (e.g., drivers) that LUP processes their data as a sub-processor.

## What is a Sub-processor

A sub-processor is a third party data processor engaged by LUP, including entities from within the LUP Group, who has or potentially will have access to or process Service Data (which may contain Personal Data). LUP engages different types of sub-processors to perform various functions as explained in the tables below.

## Due Diligence & Compliance

LUP undertakes a commercially reasonable selection process to evaluate the security, privacy, and confidentiality practices of all sub-processors that may have access to or otherwise process personal data. We ensure that all sub-processors meet GDPR and other applicable data protection laws.

**Data Transfers Outside the EEA:**

Some of our sub-processors operate outside the European Economic Area (EEA). Where personal data is transferred outside the EEA, we ensure adequate safeguards such as:

- Standard Contractual Clauses (SCCs) approved by the European Commission
- Binding Corporate Rules (BCRs) where applicable
- Encryption and other technical safeguards

A full list of sub-processors, their locations, and compliance measures is provided below.

## Customer Rights Regarding Sub-Processors

Customers have the right to object to the engagement of new sub-processors if they believe it will negatively impact their compliance obligations. Customers may submit objections via email to support@lupnumber.com.

LUP will provide reasonable notice before engaging a new sub-processor. If a customer objects, LUP will work with the customer to find a resolution, which may include discontinuing the use of the service.

## List of sub-processors

LUP owns or controls access to the infrastructure that LUP uses to host and process Service Data submitted to the Services, other than as set forth herein.

Currently, the LUP production systems used for hosting Service Data for the Services are located in co-location facilities in the United States and Europe and in the infrastructure sub-processors listed below. Subscriber accounts are typically established in one of these regions based on where the Subscriber is located, but may be shifted among locations to ensure performance and availability of the Services. The following table describes the countries and legal entities engaged by LUP in the storage of Service Data. LUP also uses additional services provided by these sub-processors to process Service Data as needed to provide the Services.

| Company and Location | Data-processing | Legal references |
|---|---|---|
| Amazon Web Services, Inc., United States (Frankfurt Data Centers Used) | Server and storage hosting for cloud-based applications and data storage solutions. AWS provides infrastructure for processing and storing data securely, ensuring high availability, redundancy, and compliance with security standards such as ISO 27001, SOC 1, SOC 2, and SOC 3. AWS also implements encryption, access controls, and data residency options to comply with regulatory requirements. | AWS offers a GDPR-compliant **AWS Data Processing Addendum** (AWS DPA) that incorporates AWS's commitments as a data processor. The AWS DPA, which includes Standard Contractual Clauses, is part of the AWS Service Terms and is automatically available for all customers who require this to comply with the GDPR. |

| | | |
|---|---|---|
| 46elks AB, Sweden | We use 46elks for sending SMS notifications to drivers, enabling two-way communication, and handling automated calls. This ensures that real-time updates and alerts are reliably delivered to users in our system. All communication data is processed and transmitted in compliance with Swedish telecom regulations. | 46elks operates under the EU Directive **2002/58/EG** (implemented by Swedish law 2022:482, also called LEK), rather than GDPR. The Swedish Post and Telecom Authority (PTS) regulations, such as **PTS Föreskrift 2022:11** , govern the protection of personal data in their services. Since 46elks is classified as a telecom operator, no separate GDPR agreement is required. As part of our GDPR compliance process, we document 46elks as a data controller for SMS and telephony services, ensuring that all communication-related personal data is handled in accordance with applicable regulations. |
| Google LLC, United States | We use Google Analytics to analyze website traffic and user behavior, helping us improve our services. Google Ads is used for advertising and remarketing purposes, ensuring relevant ads are displayed based on user interactions. Google reCAPTCHA is implemented to protect our online forms and authentication flows from automated abuse and bots. | Google processes data in compliance with the **Google Ads Data Processing Terms** , which align with GDPR requirements. Google Analytics data is processed based on user consent, with IP anonymization enabled where required. Google Ads and reCAPTCHA follow the **Google Privacy Policy** and **Google Partner Sites Data Processing Policy** , ensuring compliance with applicable privacy regulations. |

| | | |
|---|---|---|
| Loopia AB, Sweden | We use Loopia for domain name system (DNS) and nameserver hosting, ensuring reliable domain resolution and secure management of our web services. Loopia provides redundancy and security measures to prevent DNS hijacking and service interruptions. | Loopia operates under Swedish and EU data protection laws. Their **General Terms and Conditions** include compliance with GDPR and industry best practices for DNS and hosting security. Personal data related to domain registration and DNS services is processed in accordance with applicable regulations, ensuring the integrity and confidentiality of our domain infrastructure. |
| Microsoft Corporation, United States | We use Microsoft Clarity for website analytics, session recording, and heatmaps to better understand user behavior and improve our website's usability. Clarity provides anonymized insights, helping us enhance the user experience without collecting personally identifiable information (PII). | Microsoft Clarity complies with GDPR and other data protection laws. Data processing details are outlined in the **Microsoft Clarity Security and Privacy FAQs** . The service operates under **Microsoft Clarity Terms of Use** , ensuring that user data is processed securely and lawfully. Clarity does not collect sensitive data, and users can opt out via standard browser privacy controls. |
| LinkedIn Corporation, United States | We use LinkedIn for business networking, advertising, and analytics to engage with industry professionals and potential customers. LinkedIn Ads helps us target relevant audiences, while LinkedIn Insights provides analytics on ad performance and engagement. | LinkedIn processes data in compliance with GDPR and other applicable regulations. Their data processing terms are outlined in the **LinkedIn Data Processing Agreement** . LinkedIn Ads and analytics services operate under **LinkedIn's Privacy Policy** , ensuring lawful and secure data processing. Users can manage their privacy settings and opt-out of targeted advertising via LinkedIn's settings. |

| | | |
|---|---|---|
| HubSpot, Inc., United States (Data processed and stored on EU servers) | We use HubSpot for customer relationship management (CRM), marketing automation, email campaigns, and analytics. HubSpot enables us to manage customer interactions, track engagement, and optimize our marketing efforts while ensuring secure data handling. | HubSpot processes data in compliance with GDPR and other relevant privacy laws. Their data processing terms are outlined in the **HubSpot Data Processing Agreement (DPA)** . Additional details on data privacy and compliance are available in **HubSpot's Privacy Policy** . HubSpot provides tools for managing data privacy, including consent tracking, data export, and deletion options. |
| 365id AB, Sweden | We use 365id for identity verification and document scanning to ensure secure and efficient check-ins for drivers. The service helps verify identification documents, reducing fraud risk and improving compliance with site access controls. 365id processes personal identification data securely and in accordance with industry standards. | 365id processes data in compliance with GDPR and other applicable regulations. Their data protection policies ensure secure handling of identity documents and verification data. More details on their data privacy practices can be found in **365id's Privacy Policy** . 365id ensures encrypted transmission and storage of personal data, with options for data minimization and retention policies aligned with regulatory requirements. |
| Meta Platforms, Inc. (Facebook), United States | We use Facebook for advertising, remarketing, and audience engagement. Facebook Ads allows us to target relevant audiences, while Facebook Pixel helps track ad performance and optimize campaigns based on user interactions with our website. | Meta processes data in compliance with GDPR and other applicable regulations. Their data processing terms are outlined in the **Meta Data Processing Terms** . Facebook Ads and tracking services operate under **Facebook's Privacy Policy** . Users can manage their data preferences, including ad personalization and tracking, via **Facebook Ad Preferences** . |

| | | |
|---|---|---|
| Gartner, Inc., United States | We use Gartner for industry research, market analysis, and benchmarking to stay informed about trends in logistics, technology, and business strategy. Gartner provides insights that support our decision-making and competitive positioning. | Gartner processes data in compliance with GDPR and other applicable privacy regulations. Their data protection policies are outlined in the **Gartner Privacy Policy** . Gartner ensures that customer and research data are handled securely and offers options for data access, correction, and deletion in accordance with legal requirements. |

## Content Delivery Networks

As explained above, our Services may use content delivery networks (“CDNs”) to provide the Services, for security purposes, and to optimize content delivery. CDNs do not have access to Service Data but are commonly used systems of distributed services that deliver content based on the geographic location of the individual accessing the content and the origin of the content provider. Website content served to website visitors and domain name information may be stored with a CDN to expedite transmission, and information transmitted across a CDN may be accessed by that CDN to enable its functions.

## Changes

These Terms will remain in effect except with respect to any changes in its provisions in the future, which will be in effect immediately after being posted on our website.

If you have any questions about these Terms, please contact us at support@lupnumber.com