

Privacy

We take privacy seriously, and we want to inform you about the ways that LINK processes personal data. By using our webpage it is treated as consent to our Privacy Policy, this also means that you agree with our terms. Should you not agree to our Privacy Policy, we encourage you not to engage or interact with us in any way.

SMSAPI PRIVACY STATEMENT

LINK Mobility Poland Sp. z o.o. hereinafter called “SMSAPI” is a part of Norwegian LINK Mobility Group AS (org. no 984 066 910) hereinafter called “LINK”. LINK Mobility consists of many subsidiaries, all companies that are a part of the LINK Mobility Group can be found here <https://linkmobility.com/list>.

EU/EEA headquarters of LINK is Link Mobility Group Holding ASA (reg. no. no. 920 901 336), located in Norway.

Each subsidiary is responsible for processing Personal Data in accordance with this Privacy Statement. Data Controller for this site is: LINK Mobility Poland sp. z o.o.

“SMSAPI” is responsible for processing Personal Data. SMSAPI processes Personal Data within applicable laws and regulations.

Last updated: 03.03.2026. Effective as: 03.04.2026.

Terminology

We will be using some terms that will be common within this privacy statement and which should be understood in accordance with Article 4 of the GDPR.

- A Data Subject is an identifiable natural person;
- A Data Controller is the legal person which, alone or jointly with others, that determines the purposes and means of the processing of personal data;
- A Data Processor is the legal person which processes personal data on behalf of the Data Controller;
- Personal Data is any data that directly or indirectly is linked to a natural person (Data Subject).
- Data Processing of Personal Data is any use of Personal Data, including collecting, storing, modifying, transferring or deleting.
- Traffic Data is data generated through the use of a network. As an example, when an individual is using the mobile network, information about who is sending and receiving a message or a phone call, start and end time, and the location of the mobile phone is generated. If traffic data directly or indirectly can be linked to you as an individual, these are classified as Personal Data. Traffic Data can, for example, be used for billing purposes.

- Anonymous Data is data where all identifying items have been removed making it impossible to associate the data with an individual.
- SMSAPI – LINK Mobility Poland sp. z o.o. (org. no 969-156-67-36)

Privacy Notice and processing of Personal Data at LINK Mobility

When you use LINK or SMSAPI products and services we process those general types of personal data:

- If you have already signed an agreement with us to use one or more of our services we will use your Personal Data information as a Customer or Supplier
- If you do not have already signed an agreement with us and you contact us using one of the channels – like visiting this website – we will use your data as a Potential Customer or Potential Supplier.
- Personal data of our Customers which they process using SMSAPI services are called End User Data.

Data Retention

SMSAPI will retain Personal Data for as long as it is necessary to fulfill the purposes for processing and will as a main rule retain Personal Data until termination of the agreement or until end users request deletion. Please note that legal obligations, e.g. statutory rules related to storage for accounting purposes or anti-terrorism laws may make it necessary to store Personal Data after the termination of the agreement. Continued storage may also occur where such storage is necessary for the purposes of legitimate interests pursued by SMSAPI, including, but not limited to, the establishment, exercise or defense of legal claims.

SMSAPI as a Data Controller

How SMSAPI processes Personal Data as Data Controller is defined and described in this privacy notice and if applicable the data processing agreement or the terms and conditions between SMSAPI and our customer/supplier, or it is processed due to SMSAPI's legitimate legal interest.

If applicable the data processing of your personal data is based on one or more of the following legal basis:

- your consent (ref. GDPR Art 6.1.a), in relation to the marketing of LINK services
- your (or your company of employment) agreement between LINK and you as the Customer or Supplier of LINK or as an employee, other hired personnel, consultants, or management of the Customer or Supplier (ref GDPR Art 6 1. b or GDPR Art 6.1.f); To fulfill the agreement for use of a service provided by LINK to the end-user, e.g., in relation to the management of the user profile or memberships, and to notify end-users of changes to, or respond to inquiries related to services, terms, and conditions or this privacy notice.

- legal obligation/s to which LINK is subject e.g. continued storage due to statutory rules of storage for accounting purposes, Traffic Data retention for national security purposes (ref GDPR Art 6 1. c, f);
- LINK's other legitimate interests (ref GDPR Art 6.1.f). To pursue LINK legitimate interests (provided always that the interests of the data subjects do not override such interests), e.g., in relation to improving the services or the user experience, to establish, exercise, or defend a legal claim, to prevent loss or damages to LINK or any third parties or to prevent any actions that may compromise LINK or a third party's property or the personal data of the other users of the services.

Business contacts, Customers/suppliers, customer/supplier representatives, and customer/supplier employees:

SMSAPI may obtain your data as Customer when, for example, you contact our sales team, when you register on our website or sign up for our web or email services we may ask you to provide personal information. This may include your name, address/zip code/city/country, telephone number and/or e-mail address.

We may also collect and process further Personal Data or information you will provide us if you are contacting us with specific requests and/or to apply to vacancies, questions on job postings or spontaneous applications.

Develop and manage sales proposals, bids, and quotes, Manage customers' accounts	Based on GDPR Art. 6. 1. a, b, c and f Data retention during the time of validity of the agreement and after the agreement lapses by the term of reasonable inquiries (up to 6 years)	LINK processes for the purpose of signing and handling the agreement with employees, other hired personnel, consultants or management of LINK Customers Notifying Customers/Suppliers and their representatives and employees of: • Changes in the terms and conditions, payments, other regulations or privacy policy, • Changes directly related to the provision of services within the LINK services, inter alia, such as service updates, updates to technical conditions and documentation, • The state of payment for the services realized (the
--	---	--

		invoicing and the status of payments), including the discount codes for services, • Other operational matters
Manage Customer service, Investor or Supplier issues, requests, and inquiries	Based on Art. 6. 1. b, c and f GDPR Data retention during the time of validity of the agreement and after the agreement lapses by the term of reasonable inquiries (up to 12 months)	LINK contacts the customer in relation to the customer inquiries Responding to inquiries: • or questions related to services, investments, applicable terms and conditions, or this privacy notice • related to the operation of the LINK service. • related to the quality of service.
Measure customer satisfaction with customer problems, requests, and inquiries handling (NPS)	Based on Art. 6. 1. f GDPR Data retention during the time of validity of the agreement and after the agreement lapses by the term of reasonable inquiries (up to 12 months)	Customer Satisfaction Surveys.

Website visitors:

We may also collect information about your visit to this website through the use and placement of cookies. This includes, among other things, the Internet protocol address (IP address), browser type, browser version, which pages you visit within the website, the duration of the visit and the page views of your computer. We use cookies for this purpose. You can read more about Cookies below.

To protect our website and forms against spam and abuse, we use Google reCAPTCHA provided by Google Ireland Limited. As part of the operation of reCAPTCHA, technical data and information about user activity on the website may be

processed. As of April 2, 2026, Google processes data in connection with the reCAPTCHA service as a data processor under the Google Cloud Terms, including the Data Processing Addendum. The legal basis for the processing is Article 6(1)(f) of the GDPR (the legitimate interest of the Controller consisting in ensuring the security of services and preventing abuse). Detailed information regarding Google's data processing practices is available in the Google Cloud documentation. Further information regarding the terms governing Google's processing of data is available at: <https://cloud.google.com/terms/service-terms>, <https://cloud.google.com/terms/data-processing-addendum>.

By visiting our page you accept our Privacy Statement. Should you not agree to our Privacy Policy, we encourage you not to engage or interact with us in any way.

Website management Website analytics	Based on GDPR Art. 6. 1. a and f GDPR. Up to 12 months of last visit	For the purpose of website management and analytics Improve and evaluate our website and services; Obtain an insight into the use of our website, as described below in the cookie section
Manage leads/opportunities via contact from on the website	GDPR Art. 6. 1. a and f GDPR Up to 12 months from last contact	For the purpose of replying to inquiries from potential customers and customers Contact, or to keep visitors of our website informed of information that LINK think may be of interest to the visitor (marketing) after a visitor has submitted a web form on our website or via other means (opt-in);

Mobile phone owners:

LINK routes messages like SMS, various forms of OTT or email from our customer (acting a Data Controller) to the end user (Data Subject) via chosen channel by the LINK customer.

Messaging (SMS/OTT) - monitoring of traffic	GDPR Art. 6 . 1 c,f GDPR The content of messages is retained for a period of up to 3	To send and route messages like SMS, OTT from our customer (acting a
---	--	---

(investigation, error searching)	months. Data relating to message transmission (e.g., recipient number, date and delivery status) is retained for up to 12 months. After the above retention periods expire, the data is deleted.	Data Controller) to the end user (Data Subject). Comply with laws and regulations.
----------------------------------	--	---

SMSAPI Employees

Please refer to internal documentation.

Categories of Personal Data

Depending on the service and the Customers use of the service in question, we may as Data Controller process Personal Data within the following categories

- Basic Personal Data (such as name), contact details (such as email, phone number, etc).
- Traffic Data: Personal Data processed in relation to the conveyance of a communication on an electronic communications network or billing thereof.
- Data related to the content of the communication, such as e-mails, voice mails, SMS/MMS, browsing data, etc.
- Information about visits to this website through the use and placement of cookies.

In some cases, SMSAPI will be able to link Personal Data collected by several different services, as long as the data is collected for the same purpose.

Your data will not be used in an automated decision-making system, including profiling.

Data Subjects can at any time:

- Withdraw consent to processing activities based on consent.
- Access or Amend Personal Data.
- Request export or deletion of Personal Data.
- Request restriction of, or object to, processing.
- Terminate the agreement.

Right to lodge a complaint with a supervisory authority

If you believe that SMSAPI processing of personal data infringes relevant data protection regulations, you are entitled to lodge a complaint with the supervisory

authority of your habitual residence, place of work or place of the alleged infringement, or other relevant supervisory authority.

SMSAPI as a Data Processor

How do SMSAPI process Personal Data as a Data Processor is defined and described in the agreement between SMSAPI and our Customer, the Data Controller, and in the description of the respective services. The data about an individual (Data Subject) that we process as a Data Processor depends on which of our services are used by Customer.

SMSAPI processing of Personal Data on behalf of the Customer is governed by a Data Processing Agreement (DPA), and SMSAPI will only process Personal Data to provide our services to the customer, and in accordance with the DPA and the customer's instructions. Upon termination of the agreement or instructions from the customer, we will delete or return the Personal Data processed under the agreement, unless otherwise required by mandatory law.

Examples of processing activities

- Sharing tools to help you send or route SMS and OTT messages (such as Number Database and receiving numbers)
- Produce message logs, statistics, and reports.
- Monitor traffic to ensure message delivery and system stability.
- Manage Data Subject consents.
- Store and manage Data Subjects information on Data Controllers behalf

Depending on the service and the customer's use of the service in question, we may as Data Processor process Personal Data within the following categories

- Basic Personal Data (such as name), contact details (such as email, phone number, etc).
- Special categories of Personal Data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or health data.
- Traffic Data: Personal Data processed in relation to the conveyance of a communication on an electronic communications network or billing thereof.
- Data related to the use of our customers' services, such as transaction history or messaging events.
- Data related to the content of the communication, such as e-mails, voice mails, SMS/MMS, browsing data, etc.

Legal basis for processing:

- Data Protection Agreement with Customer;

How do we protect Personal Data?

Safeguarding Personal Data is of the utmost importance to SMSAPI. We therefore continuously work to protect Personal Data. Our information security policy and personal data protection policy embraces protection for personnel, data, IT infrastructure, internal and public networks, as well as office buildings and technical facilities. Specific Technical and Organizational Measures can be found in our Data Processing Agreement. Special attention is given to information such as Personal Data.

Our security work aims to balance risk exposure, business value, available technology, vulnerabilities, and threats in order to comply with applicable laws, regulations as well as with contractual demands.

SMSAPI strives to implement security measures by setting appropriate levels of protection for Personal Data and by so preventing disclosure of Personal Data to unauthorized parties, externally and internally.

With whom do we share data?

SMSAPI may disclose personal data to third party vendors and hosting partners who perform services for SMSAPI, in order to be able to deliver the services. The list of subprocessors is available [here](#), in the "LINK Poland" file.

These third party vendors will only use the Personal Data for the purposes they were collected and in order to perform their services towards SMSAPI. The relationship to such third party vendors will be governed by a Data Processing Agreement.

LINK may disclose personal data of business contacts and visitors to the Site between all entities listed as subsidiaries in the LINK Mobility Group. LINK also has subsidiaries that are located outside the EU/EEA. Access to personal data from subsidiaries is protected by standard contractual clauses signed by LINK Mobility Group and all subsidiaries.

The disclosure of Personal Data to public bodies may occur if and to the extent required by law and current regulations.

Your personal data may be transferred to third countries, including the United States, on the basis of your consent (in the case of cookies) or subject to appropriate legal safeguards, such as an adequacy decision (EU–US Data Privacy Framework) or the Standard Contractual Clauses (SCC) approved by the European Commission. Detailed information can be found in the “Cookie Information” section.

How does LINK ensure transfer to third countries in accordance with requirements coming from 01/2020 Recommendations by the EDBP?

Following the judgement of the Court of Justice of the European Union (“CJEU”) of 16 July 2020 Data Protection Commissioner v. Facebook Ireland LTD, Maximillian Schrems, C-311/18 (“Schrems II”), and in the Recommendations 01/2020 from the European Data Protection Board (“EDPB”) adopted on 10 November 2020, the measures required in order for transfer of personal data outside the European Economic Area (“EEA”) require a higher level of specification and care on the side of the entities responsible for such transfers to comply with the GDPR.

LINK mobility implements the specified requirements in accordance with the steps below:

- Step 1: In LINK Mobility we know our transfers

LINK Mobility ensures through its contracts with third parties and its internal processes that transfers to countries outside the EEA do not take place without LINK Mobility’s knowledge and documentation of such transfer.

- Step 2: In LINK Mobility we verify the safeguard our transfer relies on

LINK Mobility does not rely on legacy safeguards for transfer (Privacy Shield and Safe Harbor). If any transfer is required, only European Commission adequacy decisions, and the current safeguards as listed under GDPR Article 46 are chosen.

- Step 3: Transfer under the law of the country in question

Transfer is performed only if the laws of the country in question, including any supplementary measures in place, do not prevent processing in compliance with the requirements for the applicable transfer.

Social networking

SMSAPI may collect information about you in connection with social networking sites in several ways

- When you choose to join (or “like”) a SMSAPI page on a social networking site (such as the SMSAPI page on Facebook). In these situations, the social networking site may make some information about you available to SMSAPI. Please see the privacy policy for the social networking site to learn more.
- When you interact with a SMSAPI social networking page or content, we may use cookies to learn which links you clicked.
- When you make information publicly available on your social networking page, we may collect that information.
- When you make use of the Social Sign-In feature to access content in lieu of submitting a web form. The Social Sign-In feature allows Web form visitors the opportunity to connect to your online programs using their social network identity. Visitors can use their existing social networking site such as Facebook, LinkedIn, Twitter, or Salesforce to bypass a registration or sign-up Web form.

Social Sign-In captures visitors' current contact information and stores the information directly into the database.

To learn more about the privacy practices of a social networking site on which you interact with SMSAPI, please refer to the privacy policy for that social networking site.

Information about cookies

SMSAPI uses cookies and similar technologies on our websites. We use them to ensure the proper functioning of the site and delivery of services, to provide a better user experience, to keep statistics, and to measure the effectiveness of marketing activities.

Cookies are small text files containing a string of characters that can be placed on a computer or mobile device to identify a unique browser or device. Cookies cannot harm your computer or files on your computer. They only let the site or service know if your computer or device has visited the site or service before. Cookies can be used to understand how a site or service is used. They also help you navigate between pages more efficiently, remember your preferences, and improve your browsing experience.

Categories of cookies

Categories of cookies used on SMSAPI websites:

- **Essential** - enable essential platform and website functions such as browsing, navigation, access to secure areas, and use of features available through the service. These include, for example, authentication cookies used to log in to the site and maintain login sessions on the site. The site cannot function properly without these cookies. This category may also include technologies used to ensure the security of the website and forms (e.g., anti-spam mechanisms such as reCAPTCHA).
- **Preferential** - files that customize the website's content to the individual user's preferences by storing the settings selected by the user and personalizing the user interface, such as for a selected language or region.
- **Statistical** - allow the creation of statistics and analysis of data sets that help understand how site users use the site. They enable the site to be better tailored to users' needs.
- **Marketing** - files that allow you to deliver advertising content tailored to users' interests and measure the effectiveness of your marketing activities.

By law, we require user consent for the use of certain cookies. SMSAPI uses preferential, marketing, and statistical cookies on our site with informed, specific, voluntary, and unambiguous consent given during the user's first visit using the Cookiebot tool. The consent can be withdrawn or modified at any time using the shortcut in the screen's lower-left corner. Necessary cookies are placed by default because they are responsible for the site's correct operation.

It is also possible to manage and control cookies using the user's browser or private browsing mode (incognito), which deletes the files when the browser is closed.

Declaration of cookies

The table below shows the declaration of cookies used on the site by type: essential, statistical, preferential, and marketing. The declaration includes such information as:

- Cookie name
- Supplier
- Purpose of processing
- Expiration date (fixed, until the session ends, or specified over time)
- Type (cookie, local storage)

Cookies in the Marketing category

Of particular note are cookies placed by third-party advertising systems. They are used to analyze website traffic after contact with ads in the advertising environment of Google Ads, Meta Ads, LinkedIn Ads, and Microsoft Ads and, more accurately, adjust the content and placement of ads. They also allow the creation of audience groups and user segments based on the information provided on the website.

For information on the use of data by third-party advertising systems, see the following pages:

Supplier	Link to privacy policy
Google LLC / Google Ireland Ltd	https://policies.google.com
Microsoft Ireland Ltd	https://privacy.microsoft.com/en-gb/privacystatement
Meta Platforms Ireland Limited	https://www.facebook.com/privacy/policy/
LinkedIn Ireland Unlimited Company	https://www.linkedin.com/legal/privacy-policy

Advanced matching methods

When you consent to cookies and other technologies in the Marketing category, we collect the information you provide in the forms on the SMSAPI pages. Enhanced Conversions (Google) and Advanced Matching (Meta) mechanisms use this data in

advertising systems to create precise matches and increase the accuracy of measuring marketing activities. The data sent to the systems supplements the site's conversion information in encrypted form to protect privacy.

Contact information

If you are a direct customer of SMSAPI, please contact our Customer Support: <https://www.smsapi.com/en/contact>

Our Customer Support can also assist you in getting in touch with LINK Data Protection Officer (DPO) – Jan Wiczorkiewicz.

If you are an end user of a SMSAPI customer, please contact the relevant SMSAPI customer directly.

If you are not a direct client of SMSAPI, and you have received a message via SMSAPI systems, we would kindly inform you that this has could only happen only on behalf of one of our Customers. In this case, you must contact the sender of the message directly. Each SMSAPI client declares that it has the right to process the personal data of the customers to whom the message is sent.

Modification of this Privacy Statement

SMSAPI reserves the right to modify this privacy statement. The most recent revision shall supersede any earlier versions. The current version of the privacy notice will be available at SMSAPI website or at request at all times. We advise that you check the privacy notice from time to time, to keep up to date with the current notice. We will notify you of any changes to the privacy notice that you are entitled to receive information about or which requires your consent.