

We take privacy seriously, and We want to inform you about the means by which we process personal data in LINK. By visiting our page you give consent to our Privacy Policy, which 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.

Read more about how and why we collect data and how we handle our data or download our PDF.

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”. “SMSAPI” is responsible for processing Personal Data. SMSAPI processes Personal Data within applicable laws and regulations. LINK Mobility Group consists of many subsidiaries and personal data may be shared and transferred between LINK Mobility Group and subsidiaries listed in the following list: <https://linkmobility.com/list/>. Each subsidiary is responsible for processing Personal Data in accordance with this Privacy Statement.

Terminology

We will be using some terms that will be common within this privacy statement that should be understood as in Article 4 of 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.
- LINK – LINK Mobility Group AS (org. no 984 066 910 with subsidiaries)
- 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 the end-users that our Customers share with LINK when processing is carried out using SMSAPI services are called End User Data

The nature of processing depends on the type of data you have given us.

LINK offers many products and solutions to its Customers. This document presents a general description of Personal Data Processing within LINK Mobility which may be broader or narrower depending on which specific solution LINK Customer may be using. Please consult product-specific Privacy Notices on the given products webpage or Data Processing Agreement.

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.

Business contacts, hereunder Supplier/customer or investor, representatives, and employees:

SMSAPI may obtain your data as Business contacts when, for example, you contact our sales team or our investor relations 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.

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.

SMSAPI Employees

Please refer to internal documentation.

Mobile phone owners (End Users):

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 the chosen channel by the LINK customer.

Examples of processing activities when SMSAPI acts as Data Controller

Notifying Customers/Suppliers and their representatives and employees of:

- Changes in the terms and conditions, other regulations or privacy policy,
- Changes directly related to the provision of services within the SMSAPI services, m.in. 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,

Responding to inquiries:

- or questions related to services, terms, and conditions or this privacy notice
- to the operation of the SMSAPI service.
- Information related to the quality of service:

Another usage:

- Manage End User profile and End User consents.
- Contact, or to keep visitors or our website informed of information that SMSAPI think may be of interest of the visitor (marketing) after a visitor has submitted a web form on our website or via other means (opt-in);
- Obtain an insight into the use of our website, as described below in the cookie section;
- Send messages like SMS or email from our customer (acting a Data Controller) to the end user (Data Subject).
- Customer Satisfaction Surveys
- Manage memberships Mediate information and membership offers.
- Improve and evaluate our website and services;
- Execute individual rights;
- Comply with laws and regulations.

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).
- Location Data, such as GPS, Wi-Fi location data and location data derived from Processor's network (that is not traffic data as defined below).
- 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.

Legal basis for SMSAPI processing are:

- To fulfil the agreement for use of a service provided by SMSAPI 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.
- To pursue SMSAPI legitimate interests (provided always that the interests of the data subjects do not override such interests), e.g. in relation to improve the services or the user experience, to establish, exercise or defend a legal claim, to prevent loss or damages to SMSAPI or any third parties or to prevent any actions that may compromise SMSAPI or a third party's property or the personal data of the other users of the services.
- Consent, e.g. in relation to the marketing of SMSAPI services.
- To comply with a legal obligation to which SMSAPI is subject e.g. continued storage due to statutory rules of storage for accounting purposes.

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.
- Enrich Personal Data with data from third party sources (e.g. economic and demographic data from publicly available sources) prior to anonymisation and segmentation for use in analysis for marketing and reporting purposes. Note that SMSAPI or SMSAPI's customer will not use enriched data until anonymised
- Monitor traffic to ensure message delivery and system stability.
- Manage Data Subject consents.
- Store and manage Data Subjects information on Data Controllers behalf
- Provide catalogue services.

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.
- Location Data, such as GPS, Wi-Fi location data and location data derived from Processor's network (that is not traffic data as defined below).
- 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;

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.

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.

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.

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 the personal data of Business contacts and Website visitors between all of the entities listed as subsidiaries in LINK Mobility Group. LINK also have subsidiaries that are located outside EU/EEA area. The access to the personal data from the subsidiaries is protected with EU Standard Contractual Clauses signed between 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 (website visitors) may be transferred to a third country (USA) based on your explicit content – cookie information. How does LINK ensure transfer to third countries in accordance with new requirements?

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.

How do we use cookies?

SMSAPI uses cookies and similar technologies on our websites. Cookies help us to determine the most popular parts of our websites, which pages are visited and for how long. The data is used for the development and analysis of services and targeting website advertisements in services provided by partners.

Cookies are small text files containing a string of characters that can be placed on your computer or mobile device to identify your unique browser or device. Cookies cannot damage your computer or files on your computer. Cookies just allow a site or services to know if your computer or device has visited that site or service before. Cookies can be used to help understand how a site or service is used. Also, they help you navigate between pages more efficiently, remember your preferences, and generally improve your browsing experience.

We use cookies to:

- Enable the use of services available through the service, e.g. Authenticating cookies used to log on to the site and maintain login sessions within the site.
- Adjust the content of the website to individual preferences of the user by “remembering” the user’s chosen settings and personalizing the user interface, eg. for the selected language or region.
- Create statistics that help you understand how website users use websites, which allows better customization of the website to the users ‘ needs.
- Deliver advertising content to website users more tailored to their interests.

We also use Google Analytics, a web analytics service based on our legitimate interests (i.e. interest in the analysis, optimization and economic operation of our online offer within the meaning of Article 6 (1) f) of GDPR) based on the Data Subject consent (Article 6 (1) a), after accepting the cookie banner. We only use Google Analytics with IP anonymization enabled. This means that the IP address of users is being shortened by Google within Member States of the European Union or in other Contracting States to the Agreement on the European Economic Area.

Google LLC (“Google”). Google uses cookies. The information generated by the cookie about users ‘ use of the online offer is usually transmitted to a Google server in the USA and stored there).

Google will use this information on our behalf to evaluate the users ‘ use of our online offering, to compile reports on the activities within this online offering, and to provide further information on the use of this online offer and the Internet use related services to provide us. Pseudonymous user profiles can be created from the processed data.

Only in exceptional cases will the full IP address be transmitted to a Google server in the USA and shortened there. The IP address transmitted by the user's browser will not be merged with other Google data. Users can prevent cookies from being stored by adjusting their browser software accordingly.

Users can also prevent Google from collecting the data generated by the cookie and relating to its use of the website (including its IP address) and by using that data by Google by providing it with the data available at the following link. Download and install browser plugin <http://tools.google.com/dlpage/gaoptout>.

For more information on Google's data usage, hiring and objection options, see Google's privacy policy (<https://policies.google.com/>) and the presentation settings Advertising by Google (<https://adssettings.google.com/authenticated>).

The collected data will be deleted after 12 months.

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 Wieczorkiewicz.

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.

Last update to the policy: 01.01.2021.