



Document Name

PRIVACY POLICY

Document version 2.1

Revision date: 09 SEPTEMBER 2024

© APIFONICA, SMARTTEL PLUS OÜ

Maakri st r. 19/1-7K, 10145 Tallinn, Estonia

+48 22 1530 003 | +372 6346 295 | +371 676 60858

SmartTel Plus OÜ, operating under Apifonica © trademark, is part of the SmartTel Plus company group which includes the entities and branches offering and providing its services in the EU market. This Privacy policy explains how our organizations being part of our group (further also referred to as “our Company”) collect, use, process and store personal information. Current document implies our better interaction with you in terms of our compliance with the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the EU General Data Protection Regulation or the GDPR).

Definitions

Personal data – any information related to living natural person (identified or identifiable), also called ‘Data Subject’. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data in this Privacy Policy means the data of general nature (name, identification number, location data, etc.) and not special or biometric data. Whenever it relates to other type of information, it is clearly marked as special or biometric data as the context may require.

Controller - means the natural or legal person, which, alone or jointly with others, determines the purposes and means of the processing of personal data. Our Company acts as a controller in respect of your personal data if it collects the data and determines the purpose of such processing such as provision or prompting of our services to you or others as disclosed in this Privacy Policy. In event when we receive and process your personal data from another controller (e.g. your employer who use our HR voicebot) we act only as a processor of your personal data.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Our Company may process the Personal Data on the basis of respective agreement with a Persona Data controller.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as

collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Legal basis for data processing

For the purposes of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, customers located in the European Union or the European Economic Area are required to give their consent for processing their personal data unless the controller relies on another legal basis for the processing (e.g. an agreement or pre-contractual communication, legitimate interests, contract on processing of the Personal Data between the controller and the processor etc.).

Depending on the circumstances, the legal basis for processing of your personal data is either your expressed consent for such processing or conclusion and/or performance of your agreement with STP (including ones by acceptance of the Terms of Service as it is placed on our website) or other actions as the steps at your request prior to entering into a contract and/or to subscribing to our services. STP may process your data as the controller or act as the processor when such processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party to extent it is allowed by the EU General Data Protection Regulation.

You may always withdraw your given consent by using following email: dpo@apifonica.com. SmartTel Plus OÜ (Maakri st r. 19/1-7K, 10145 Tallinn, Estonia) is liable for processing your personal data in the use of web-site under the link: www.apifonica.com SmartTel servers (web-servers, application-servers, databases, etc) and API services (hereinafter "Platform" or "Services").

Before using Apifonica Platform and Services you are always prompted to provide the consent for processing your personal data and to confirm that by giving the consent you act by your own will and in your own interest. Consent for processing personal data extends only to that personal data that is processed in the use of Platforms and during the performance of Terms of Service (https://www.apifonica.com/public/legal/apifonica_terms_of_service.pdf). In accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 you agree registering your personal account on the Platforms to provide the following personal data, which is not special or biometric:

name, family name, e-mail, address, VAT Number if needed, including capturing of browser cookies and our further processing of the mentioned data for the purpose of provision services to you and declared purposes of the data processing.

We request you to confirm your consent before we start processing of your data before the first processing and your consent remains valid for all next processing unless it has been revoked by you or unless the data is processed for other purposes that were declared, in this case we will request your consent again for such processing.

We also rely on our legitimate interest in respect of the personal data:

- for processing of traffic data, customer's IP-address to analyze the routing and to prevent spam, fraud and for troubleshooting and detecting problems with the network, and to ensure correct billing data, to settle interconnection payments with telecom operators and other communications providers.;
- for processing of retained records containing communications related data as stipulated in the relevant national data retention provisions regulating the law enforcement matter in order to comply with our legal obligations,
- collecting logs on your activities created during your use of our Services or processing B2B business contact for the purpose enabling us to offer you our improved services.
- to process the personal data as the processor in accordance with the respective controller's instructions and data processing agreements;
- for processing of personal data within the our group of companies.

Whenever our company acts as a processor of the Personal Data under a data processing agreement with another controller, it is controller's liability to ensure a consent to be given by the subject of the Personal Data prior to the processing or to have another a valid legitimate basis for such processing

For protection of children and minors we do not collect their data and do not offer our services to the children and minors without consent of the persons being the holders of parental responsibility over the child or the minor. We consider the declaration given in respect of the age of our present and potential customers true unless we have reasonable doubts arisen out of behavior or due to other reasons when we are entitled to request copies of documents evidencing the age of the such persons.

Contact details

You can always initiate any requests relating to your Personal Data, processing and protection of your personal data, revocation of your consent, your complaint of any nature connected with processing of your Personal Data by us, if you it send to our **Data Protection Officer by using following addresses:**

email: dpo@apifonica.com for mailing: Maakri st r. 19/1-7K, 10145 Tallinn, Estonia.

Confidentiality

Our Company treats all Personal Data collected by our Company as strictly confidential. All our contracts and business arrangements entrusting to us processing of the Personal Data collected by the other controllers, always include confidentiality clauses with our commitment of confidentiality and our respective liability for our employees who have an access to such Personal Data.

How do we collect data?

You directly provide our Company with most of the data we collect.

We collect data about you in different scenarios during interaction with our products and upon obtaining clear consent from you.

You provide us with your personal data:

- during registration in our web-site: [apifonica.com](https://www.apifonica.com);
- when you send any request by e-mail to the address with @apifonica.com or contact our representative's phone numbers.

The scenarios when we collect your personal data may also involve:

- Your web-site activity (products interested, tabs visited) is stored and collected by using browser cookies. (you can find more information in our Cookies policy placed at:
https://www.apifonica.com/public/legal/apifonica_cookie_policy.pdf);
- Your subscription to our newsletters, blogs or our other email marketing communication through the webforms available on our website;

- Our existing business relationship for the purpose of business to business (B2B) marketing with our customers, suppliers and their staff), who may share data (subject to your consent or other legitimate business) collected from you or your organization when entering into an agreement or during our business relationship;
- Your answers to the questions of your recruiter or employer loaded to our voicebot a part of our automated communication services provided to such employer or recruiter who is the controller of your data while our Company only process the data;
- Contact data used for communications in automated calls and SMS including the contact data of the recipients;
- Communication records made by our customers with third parties at their own discretion using our Platform. Recording of communication will always require the customer's active action in using tools of recording while using the services. In such cases the customer shall be deemed the controller and he/she shall advise such third persons of recording and processing and shall receive their informed consent prior to further actions. The recording of calls may contain biometric data and the subject of the Personal data shall be informed of such processing and shall give a consent for this.

What Data do we collect?

We collect the following data essential for offering and provision of our services to you or to the legal entities represented by you:

- Personal identification information (Name, email address, phone numbers, domicile address, mail address for billing, VAT or other tax number if applicable, your position in respect to the represented legal entity);
- Location and traffic information related to routing (end-users numbers used for calls and SMS, e-mail address) IP-address, customer's geotags;
- Cookies, logs of your activities during your use of our services;
- Other personal information such as education and your professional experience etc., job title only if you are involved in a recruitment process using our respective services and applications directly by you or your current

or potential.

We neither collect nor process any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, data concerning health or other sensitive data or special categories of data.

We do not collect or process the information of your bank card or your account or other financial institution. Once you choose the respective option on our site for payment for our services, you are redirected to the site of the payment services provider who is responsible for further processing of data of your bank card or account. For further information about measures of technical character protection of the personal data, the available guarantees and declarations we recommend you get the information presented on the official sites of the mentioned suppliers.

How do we use and store your personal data?

We collect and process the information about you to provide cloud-based services, perform our activities for managing your Apifonica accounts, API services (if you already became our customer). This information is needed to identify you for providing you any kind of support by our service desk assistants, for performance of our services to you and billing purposes. We may collect and process the personal data for the purposes of compliance with regulatory requirements and/or to act in our legitimate interest as described above.

We may process personal data as a processor under instruction of your provider, employer or recruiter in strict compliance with instruction of the said controllers.

We may use the anonymized data (data not containing name, family name or any other information solely identifying a person) for statistical purposes processed automatically for improving the quality of our products or their marketing promotions.

Your personal data is used exclusively with the platforms of the reliable cloud technologies providers in respective functions essential for our services such as billing or interaction and support at your request for provision of our services such as Google Cloud Platform (GCP <https://cloud.google.com/privacy>), HubSpot (<https://legal.hubspot.com/privacy-policy>), Amazon (<https://aws.amazon.com/privacy/>), ElevenLabs (<https://elevenlabs.io/privacy>) who

confirm its integrity and full compliance with the GDPR and provide guaranties as stated in the GDPR. For further information about measures of technical character protection of the personal data, the available guarantees and declarations we recommend you to get the information presented on the official sites of the mentioned suppliers.

Based on information stored in our assets you may receive electronic messages (emails) to inform you about any crucial updates in our products and services (you always have an option to opt-out from these notifications). Also, we use email messages to handle our interaction with you, such as Policy updates, payments reminders, based on legal agreements.

The duration of processing your personal data depends on the type of the data. The maximum period for the personal data with information identifying you as our client and information used in billing for our services is limited to seven years after the expiration of the financial year when the termination of the contract took place.

The traffic data related to routing (including the end user's telephone number or email address, as well as the customer's IP address) will be kept during 7 years after elapsing of the year when the communication happened.

The period of storage of the Personal Data entrusted to us for further processing by your entity being the controller of your Personal Data is determined by the respective data processing agreement and may vary from a month to one year upon termination of the respective data processing agreement.

The customer's communications (including customer's records shall be stored during 2 years after the end of the months when the communication was established. All other personal data shall be stored during to 2 years after its loading by the customer to the system.

In case of any litigation, law enforcement requests or government investigations urging us to preserve records with personal information, we will delete the impacted records when we are no longer legally obligated to retain them.

We never take any decision concerning interaction with you as our current or potential customer on the basis of automatic processing of your personal data. Please be assured that in any case all issues are considered by our authorized staff

personally and individually toward each of our clients. Please note that this does not refer to processing of the data made by us as the processor, when all decisions are taken by the controller and not by us.

Group Transfers and Sub-processors

The Data Processing shall be done in strict accordance with requirements of the GDPR by STP company, branch or subsidiary located in the EU (STP Group of Companies) provided that such processing excludes any transfer of the Personal Data outside of the EU.

When the performance under the Service contract concluded between STP and the Customer specifically requires involvement of any subcontractor acting under the control and at STP's responsibility, STP shall ensure that such subcontractor will act as a sub-processor under STP's control and within the Customer's (or STP's when STP is a controller) general and specific instruction in respect of such data processing. Further STP shall ensure that any other processor it engages on STP's side (i.e. sub-processor) assumes the same data protection obligations as STP by a written contract, whenever it is practical or provides sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements under the GDPR.

STP Services are based on Google cloud-services provided subject to consent with publicly announced terms of the Data Processing which include all information regarding processing, protection and complaints/disputes procedures as published on the web-resources Google <https://cloud.google.com/terms/data-processing-addendum> and related documents as may be updated by Google. By entering to the Agreement the Customer consents with processing of the entrusted personal data in Google cloud facilities and confirms that the guarantees, technical and organizational measures on the side of these cloud provider are accepted by the Customer as sufficient for the purpose of such sub-processing of the Customer's personal data and STP responsibility shall be limited to its assistance on the Customer side whenever it is practical and advisable in addition to direct rights of the subject of the personal data and/or the Customer acting through respective tools and mechanisms of such cloud services.

For certain specific services activating by the Customer at his discretion, the data of the sub-processors as may be amended from time to time can be located in the located here:

https://www.apifonica.com/public/legal/apifonica_terms_of_service.pdf in
ADDENDUM TO THE TERMS AND AGREEMENTS APIFONICA SERVICES paragraph 4.4
List of Sub-processors. Whenever there is made available the link to respective
respective webpages of the said sub-processors we urge you to read carefully the
respective information on the sub-processors side and decide if the assurances and
guaranties provided by these sub-processors sufficient for your purpose of use of
the services realized with the said additional functionality. If you start or continue
use of our services with the said additional functionality, your consent for such
subprocessing is supposed for granted and STP obligation to receive your consent
in respect of the said sub-processors, shall be deemed performed.

If any changes in our policies occurred?

We are trying to do our best in keeping this policy up-to-date and under constant, regular review, thus the latest version of the policy is available on our web-site. In case of any crucial updates, we will inform you by using email as well. Current version of the policy was issued on Aug 02, 2023.

Please note that our Company website contains links to other websites. Our privacy policy applies only to our website, so if you click on a link to another website, you should read their privacy policy.

Your access to your personal information

You always have a legal right to request an electronic copy of the data which is stored in our assets, applications. The extract will be provided in computer readable file which will include the asset name, personal data stored, geographical location for data storage, etc.

You always have a legal right to keep your data up-to-date, to request rectification or erasure of your personal data or to restrict it's processing, however please note that we will not be able to continue provision of our services onward your request for deletion of your personal data required for billing purposes or for restriction of its processing. Please also note that for our legitimate purpose to secure information evidencing the facts of the performance of your agreement with us we are allowed to keep the data within the term as stated in respective regulation.

You have the right to lodge a complaint with a supervisory authority when you

reasonably find any infringement of your rights including the right to request rectification or erasure of your personal data.

We are trying our best in order to make the mentioned procedures simple and comfortable to you and we recommend you to get acquainted with technical details in respective sections of our site. If there is no undue delay, we will process your request as soon as possible, however the process may take up to 30 calendar days.

To initiate the requests mentioned above, please contact our Data Protection Officer by using the following email: dpo@apifonica.com.

Which measures are taken to protect your data?

Privacy of our current and potential customers, web-site visitors and the contacts of our estimated clients always remains our top priority. During the processing of personal data, we take legal, organizational and technical measures or ensures that they are taken in order to protect personal data from illegal or coincidental access to them, destruction, alteration, blocking, copying, provision, transmission and other illegal acts involving personal data. We are developing our policies, business processes and products in compliance with the requirements for ISO certification and we intend to demonstrate it by respective certificates confirming our compliance to the ISO standards in respect of safety and integrity of the processing of personal data. Our company also assumes the duty to provide the confidentiality of the personal data of users.

Security Procedures and Policies. The services are operated in accordance with the following policies:

- Customer passwords are stored using a salted hash.
- User login attempts are logged in system security logs, containing time, date, user id.
- Data server access logs, system infrastructure logs, and application logs are kept for 60 days.
- Passwords are not logged.
- Changes to administrative entities data (user profiles, roles, permissions) are sent as notifications to responsible personnel.

Data Servers Security. The data storage process is secured by using the next measures:

- Access to database servers is restricted on the network level based on

Internal Policies and can be granted only upon request and after appropriate approval of the Security Team.

- Employees credentials for accessing data storing applications (Billing System, database sub-modules) can be obtained only as per internal policies upon request and after appropriate approval of the Security Team. Thus, the access to personal data is granted only to our employees and agents duties as stated in a respective job description or contract directly involves access to and processing of the personal data of the user with strong liability for keeping the data confidential and for strict rules for such processing diminishing all eventual risks of any processing incompatible with the present Policy, GDPR and the purpose of the processing consented by you.
- As reliability measures – strict monitoring is used to track all the physical resources of data storages to prevent failures, spikes.
- Data backup is performed on a daily basis to prevent unexpected data losses.

WHAT ARE YOUR DATA PROTECTION RIGHTS?

Our Company would like to make sure you are fully aware of your data protection rights. Every user is entitled to the following:

The right to access – you have the right to request our Company for copies of your personal data. We may charge you a small fee for this service.

The right to rectification – You have the rights to request Company to correct any information you believe inaccurate. You also have the right to request our Company to complete information you believe incomplete.

The right to erasure – You have the right to request erasure of your personal data by our Company, under certain conditions.

The right to restrict processing– You have the right to request that our Company restrict processing of your personal data, under certain conditions.

The right to object to processing– You have the right to object to our Company's processing of your personal data, under certain conditions.

The right to data portability erasure – You have the right to request that our Company transfer the data we have collected to another organization, or directly to you, under **certain conditions**.

If you have a request, we have one month to respond you. If you would like to exercise any of this rights, please contact us at; dpo@apifonica.com.

The right to log a complaint to the appropriate authority - Should you wish to report or if you feel that our Company has not addressed your concern in satisfactory manner, you may contact the national data protection supervisor in the following offices:

in Estonia:

Estonian Data Protection Inspectorate

39 Tatari St., 10134 Tallinn

telephone (from abroad add +372) 627 4135

e-mail info@aki.ee

in Latvia

Data State Inspectorate (DSI)

Elijas iela 17, LV-1050, Riga, Latvia

Webpage: dvi.gov.lv

E-mail: info@dvi.gov.lv

Tel. +371 6722 3131

in Poland:

Personal Data Protection Office (UODO)

ul. Stawki 2, 00-193 Warszawa, Poland

Webpage: uodo.gov.pl

e-mail kancelaria@uodo.gov.pl

tel. +48 22 531 03 00