



PRIVACY POLICY

Document version 1.2

Revision date: 12 March 2019

© APIFONICA

J. Vilmsi street 47, Tallinn Estonia

Phone +48 12 446 52 44 | +31 20 369 06 28 | +358 942 704184

This privacy policy explains how SmartTel Plus OÜ (Dzinga and Apifonica) collect, use, process and store any personal information. Current document implies to 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). The GDPR, present Policy and the contract for our services offered to you, your consent to process jointly represent the legal basis for processing of your personal data.

Definitions

Personal Data – any information related to living natural person (identified or identifiable), also called 'Data Subject'. Personal data includes, but not limited, name, identification number, location data, or other specific types of data like genetic, mental, social, economic, cultural identity.

Data processing legal basis

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 when using services provided under trademarks Dzinga/Apifonica or similar service providers.

SmartTel Plus OÜ (Dzinga, office J. Vilmsi str. 47, Tallinn, Estonia, 10126) is liable for processing your personal data in the use of web-site under the link: www.dzinga.com, www.apifonica.com, SmartTel servers (web-servers, application-servers, databases, etc) and API services (hereinafter "Platform" or "Services").

Before using of Dzinga/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 with Apifonica or Dzinga. 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 for us valid Dzinga/Apifonica 2018 for all next processing unless the data is processed for other purposes that declared, in this case we will request your consent again 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.

How do we collect data?

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

The scenarios when we collect your personal data:

- during registration in our web-sites: apifonica.com and dzinga.com;
- when requesting a callback from our sales managers in our web-sites: apifonica.com and dzinga.com;
- when requesting any assistance by using our online chat in our web-site: dzinga.com;
- when using our authorized mobile applications (iOS, Android).

Your web-site activity (products interested, tabs visited) is stored and collected by using browser cookies.

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, biometric 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 guaranties and declarations we recommend you to get the information presented on the official sites of the mentioned suppliers.

How do we use your personal data?

We collect the information about you to provide cloud-based services, perform our activities for managing your Dzinga or/and 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 use the anonymized data (data not containing name, family name Dzinga/Apifonica 2018 or any other information solely identifying a person) for statistic purpose 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 Amazon (<https://aws.amazon.com>), Salesforce (<https://www.salesforce.com/eu>), Mailchimp (<https://mailchimp.com/>), Leadfeeder (<https://www.leadfeeder.com/>), Power BI (<https://powerbi.microsoft.com/>), 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 guaranties 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.

Your consent for processing personal data is valid from the moment you are giving this consent and to the expiration of storage period or for periods in which the information should be stored for the purpose of processing in accordance with laws of the European Union.

The duration of processing your personal data is five years after the termination of the contract, e.g. your data will be stored only within the limitation period as stated by the law.

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 to each our client.

If any changes in our policies occurred?

We are trying to do our best in keeping this policy up-to-day 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 policy was issued on March 12, 2019.

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, Dzinga/Apifonica 2018 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 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.

To initiate the requests mentioned above, please contact our Data Protection Officer by using following

emails: dpo@dzinga.com, dpo@apifonica.com, info@apifonica.com.

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.

You have 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.

Which measures are taken to protect your data?

During the processing of personal data, Dzinga/Apifonica 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. Dzinga/Apifonica also assume the duty to provide the confidentiality of the personal data of User.

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 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 Security Team. Thus, the access to User's personal data is granted only to our employees whose job description 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 Dzinga/Apifonica 2018 all possible risks of any processing incompatible with the present Policy, GDPR and the purpose of the processing consented by you.
- As reliability measures – server 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.