

PRIVACY POLICY

WIMBA.APP

I. The Controller of Personal Data

WIMBA POLAND Spółka z ograniczoną odpowiedzialnością (limited liability company incorporated under the laws of Poland) with its registered seat in Cracow, Fabryczna Str. 20A, 31-553 Cracow, entered into the entrepreneurs register of National Court Register maintained by the District Court for Krakow-Śródmieście in Krakow, XI Commercial Division of the National Court Register under the KRS number: 0000974000, NIP (Tax Identification Number): 6751765315 REGON (Statistical number): 522124301

II. Contact with the Controller of Personal Data

Contact with the Controller of Personal Data is possible:

- a) by email at: hello@wimba.vet

III. Terms and definitions

The terms used in this Privacy Policy have the same meaning as the terms indicated in §2 of the App's Terms of Service.

IV. Processing of personal data

The Controller will only collect and process Users' personal data in accordance with the provisions of this Privacy Policy. Any data provided by the User, will only be used by the Controller for:

1) Scope of processing of Personal Data

- a) First and last name of the Account or Sub-account User
- b) Place of work
- c) In the case of sole traders who are Account Users: first name, surname, company name, business address, tax identity number, email.
- d) First and last name, telephone number, email and address for services of owner of the pet, for which measurements are taken and products are ordered via App,
- e) Data processing in the form of cookies, to the extent indicated in paragraph XII of the Privacy Policy - collected in the purpose of maintain the user session and enable uninterrupted use of the App.

2) Collection of Personal Data

The User's Personal data are collected by the Controller in the moment of:

- a) setting up the Account for the Clinic employing the User,
- b) setting up the Sub-accounts for individual Users - with regard to Users who are persons using the App via the Clinic's Account,
- c) entering the pet's owner Personal Data into the App, for which pet f measurements are made and the Products are ordered via App.

3) Purposes and grounds for processing personal data

Data entered into the App shall be processed in the following purposes:

- to provide customer service and to contact the user, including for the purpose of informing the user, upon request, of details of the offer, products and services offered by the Controller of Personal Data - the legal basis for the processing of the data is Article 6(1)(b) or (f) of GDPR;
- the processing of orders for Products placed through the App - the legal basis for the processing of the data is Article 6(1)(b) and Article 6(1)(f) of GDPR;
- performance of the Contract between the Controller and the Clinic and verification of its implementation - the legal basis for the processing of the data is Article 6(1)(b) and Article 6(1)(f) of GDPR;
- processing of personal data in order to comply with legal obligations - the legal basis for processing is Article 6(1)(c) of GDPR;
- for analytical, development, improvement purposes (including to improve user experience), administration, maintenance, technical and security support of the App, which is a legitimate interest of the processing - the legal basis for the processing is Article 6(1)(f) of GDPR;
- the possible establishment, investigation or defence of claims, the enforcement or investigation of potential violations of the terms and conditions of use of the App or other actual or alleged unlawful activities, the protection of the rights, property or security of the App, users, customers and employees of the Controller and other third parties, which constitutes a legitimate interest of the Controller's processing - the legal basis for the processing is Article 6(1)(f) of GDPR;
- for the use of the contact form provided by the Controller and the App, including for the handling of queries and requests made through the contact channel provided by the User - the legal basis for the processing is Article 6(1)(f) of GDPR;

V. The Recipients of Personal Data

The User's Personal data may be made available by the Controller:

- to persons authorised by the Controller, i.e. employees and associates who need to have access to personal data in order to perform their duties;
- the Users' personal data may be transferred to partners and third parties providing services to the Controller and processed by them in order to enable them to perform the services commissioned by the Controller, including providers of IT services, hosting services,

administrative and sales system management services, postal or courier services, as well as accounting, marketing and legal services;

- to public authorities or bodies entitled to obtain data on the basis of applicable law, e.g. courts, law enforcement agencies or state institutions, when they make a request, on the basis of the applicable legal basis.

In the event of a data security breach, certain personal data may be subject to disclosure to authorities competent to protect them.

In the case of cooperation with the Controller's partners or third-party suppliers, such third-party providers may be located either within the territory of countries that are members of the EU or outside the European Economic Area (EEA).

Where our partners or suppliers are based outside the EEA, the Controller shall ensure that transfers of data outside the EEA are carried out in accordance with applicable laws. The level of data protection in countries outside the EEA may differ from that guaranteed by European law. We may transfer data to our partners outside the EEA in particular on the basis of decisions issued by the European Commission or standard data protection clauses (e.g. when the transfer occurs in connection with the Controller's use of the Digital Ocean or Salesforce tools).

All external parties are obliged to comply with the Controller's guidelines and to implement appropriate technical and organisational measures to protect Users' personal data. Recipients of data may act as our processors (in which case they are fully subject to our instructions as to the processing of personal data) or as independent controllers (in which case you should additionally familiarise yourself with the personal data processing rules applied by these entities).

VI. Transferring personal data to third countries

1. The Controller of Personal Data uses services and technologies offered by entities such as Digital Ocean LTD or Salesforce Inc., which are based outside the European Union and consequently - under the GDPR - are treated as third country entities.
2. The GDPR provides for restrictions on the transfer of personal data to third countries. Due to the fact that European legislation does not, in principle, apply there, the protection of personal data of EU citizens may unfortunately be insufficient. Therefore, it is the responsibility of each Controller of Personal Data to establish a legal basis for such transfers.
3. Where service and technology providers are based outside the EEA (European Economic Area), the Controller shall ensure that transfers of data outside the EEA are carried out in accordance with the applicable legal provisions in this regard. The level of data protection in countries outside the EEA may differ from that guaranteed by European law. We may transfer data to providers of services and technologies used in the operation of the website based outside the EEA, in particular on the basis of decisions issued by the European Commission or standard data protection clauses (e.g. when the transfer occurs in connection with the Controller's use of hosting and cloud services provided by entities outside the EEA).
4. At any time, the Controller shall provide you with additional explanations regarding the transfer of personal data, especially if this issue raises any concerns for you.

5. At any time, you have the right to obtain a copy of personal data that has been transferred to a third country.

VII. Duration of personal data storage

The Controller shall store and process the personal data of Users and of persons whose data is entered into the Application by Users for the period of time necessary for the purposes of fulfilling the purposes of the processing indicated in Section IV of this Privacy Policy or in accordance with mandatory legal provisions, i.e., for example, until the User terminates his/her relationship with the Clinic that established his/her Sub-Account, the Customer objects to the processing of his/her data in the Application or requests the deletion of his/her data, or until the completion of the contract between the Clinic and the Controller, when the parties conclude an agreement using the functionality of the Application, or until contact is made or questions sent via the contact forms are answered.

Once the purpose of the processing has been achieved, the Controller of Personal Data will delete or anonymise the personal data and, where the Controller of Personal Data intends to process the data for analytical purposes, the Controller of Personal Data undertakes to use the data to the extent adequate and necessary for the specified purposes of the processing and, in particular, in a manner that prevents the identification and identification of the data subjects (e.g. by using pseudonymisation mechanisms).

VIII. Rights of data subjects

The persons whose data is processed in the App have the following rights in relation to the personal data processed by the Controller:

- The right of access to the personal data of the person whose personal data is processed in the App;
- The right to rectify the personal data of the person whose personal data is processed in the App if the data is inaccurate or incomplete;
- The right to erasure of the personal data;
- The right to object to the processing of personal data of the person whose personal data is processed in the App. The right to object applies when the processing of the data by the Controller is based on the Controller's legitimate interest, e.g. for profiling the data for marketing purposes. Upon receipt of an objection, the Controller shall cease to process the data for these purposes unless there are compelling legitimate grounds that override the interests, rights and freedoms of the User or the User's data are necessary for the Controller to possibly establish, assert or defend claims;
- The right to portability of the personal data of the person whose personal data is processed in the App;
- The right to restrict the processing of the personal data of the person whose personal data is processed in the App.

IX. The right to withdraw consent to the processing of personal data

The data subject may at any time withdraw consent to the processing of personal data processed on the basis of his/her consent. Withdrawal of consent does not affect the lawfulness of data processing carried out before its withdrawal.

You can exercise your rights by sending an email to the following address: hello@wimba.vet.

X. Right to lodge a complaint with a supervisory authority

The data subject who believes that his/her personal data is being processed unlawfully, may submit a complaint to the President of the Personal Data Protection Office, Stawki 2 Street, 00-193 Warsaw.

XI. The requirement to provide personal data

The provision of personal data is voluntary, but nevertheless necessary if the User wishes to order Products through the App or to send a message to the Controller through the contact form available in the App.

XII. Cookies and server logs

1. The cookies files, which are short textual information stored in your browser, are used in website for its operation.
2. When you reconnect to the App, it recognises the device on which the page is opened. The files can be read by the system used by the Controller of Personal Data, as well as by the service providers used in the creation of the website.
3. Some of the cookies are anonymised, which makes it impossible to identify the user without additional information.
4. By default, your web browser allows the use of cookies on the devices you use, so when you visit the App for the first time, a message asking you to agree to the use of cookies appears.
5. The cookies used in the operation of the Application are session cookies - cookies used to enable the user's session to be maintained until the web browser is closed.
6. In the event that you do not wish cookies to be used when browsing the Website, you should change your browser settings as follows:
 - a) completely block the automatic handling of cookies, or
 - b) request notification whenever cookies are placed on your device. You can change your settings at any time.
7. Disabling or restricting the use of cookies may result in significant difficulties in using the website, e.g. in the form of longer page loading times, restrictions on the use of functionalities, etc.

8. Certain events triggered by Users and information about them are saved in the form of logging on the server. The data stored in this way is only used for the proper administration of the operation of the App, to ensure its correct operation and the uninterrupted functioning of its various functionalities. The data stored in the form of server logs does not make it possible to identify the User and is only used for the purposes indicated in the previous sentence.

XIII. Automated decision making and profiling

The App does not use mechanisms based on profiling and automated decision-making for its operation with regard to the personal data processed in the App. The measurement technologies used do not require the processing of users' personal data.

XIV. Security measures

The Controller of Personal Data shall apply appropriate and adequate technical and organisational measures to ensure an adequate level of security and integrity of users' personal data, using proven technological standards to prevent unauthorised access to users' personal data or other threats to personal data.

XV. Final provisions

1. To the extent not covered by this Policy, the relevant generally applicable regulations shall apply, in particular the GDPR and the Act of 16 July 2004. Telecommunications Law.
2. The user will be informed of any changes made to this Policy by publishing the new text of the Policy in the App and displaying a message when logging to the App.
3. This Policy is effective as of November 15, 2022.