27/10/2018

PRIVACY POLICY

Telemedicine OÜ, an exempted company that is officially registered under the law of Estonia and has been given its own ID number - 14514949, legal address: Randla tn 13-201, 10315 Tallinn, info@lifepet.io ("**We**"), is committed to protecting and respecting your privacy.

This policy (together with our terms of use available at https://icopet.life ("Website") and any other documents referred to on it) sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our views and practices regarding your personal data and how we will treat it.

NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS PRIVACY POLICY, WE MAY PRESERVE OR DISCLOSE YOUR INFORMATION IF WE BELIEVE THAT IT IS REASONABLY NECESSARY TO COMPLY WITH A LAW, REGULATION, LEGAL PROCESS, OR GOVERNMENTAL REQUEST; TO PROTECT THE SAFETY OF ANY PERSON; TO ADDRESS FRAUD, SECURITY OR TECHNICAL ISSUES; OR TO PROTECT OUR OR OUR USERS' RIGHTS OR PROPERTY. HOWEVER, NOTHING IN THIS PRIVACY POLICY IS INTENDED TO LIMIT ANY LEGAL DEFENSES OR OBJECTIONS THAT YOU MAY HAVE TO A GOVERNMENT'S REQUEST FOR DISCLOSURE OF YOUR INFORMATION.
WE USE GOOGLE ANALYTICS ON OUR WEBSITE. IF YOU WANT TO KNOW MORE ABOUT GOOGLE ANALYTICS AND ITS "DO NOT TRACK" POLICY, PLEASE VISIT HTTPS://WWW.GOOGLE.COM/ANALYTICS/TERMS/US.HTML.
WE STRICTLY FOLLOW INDUSTRY BEST PRACTICES AND ADHERE TO THE RULES SET FORTH IN THE GENERAL DATA PROTECTION REGULATION, OPPA, CAN-SPAM AND COPPA.

We store and process your data on the territory of the EU and Russia Federation. Please note that we identify your jurisdiction based on your IP address.

Your data is stored through Telemedicine's data storage and databases. We store your data on a secure server behind a firewall.

The following means of protection are used to secure the virtual infrastructure of the site location and the www.icopet.life database:

- Kaspersky Anti-Virus for virtual environments 3.0
- Check Point R77.10 Firewall and Intrusion Detection System
- Secret Net Studio (the mean of data protection)
- vGate R2 (computer software of the virtualization protection)
- Wallix Admin Bastion (WAB - Access control system of internal and external IT-services providers)

Consent

Consent to the collection and processing of personal data

When you provide us with personal information we ask you to explicitly consent to our collecting it and using it for specific reason only.

If we ask for your personal information for a secondary reason, like marketing, we will either ask you directly for your expressed consent, or provide you with an opportunity to say no.

Refusal to consent to the collection and processing of personal data

If after you opt-in, you change your mind, you may withdraw your consent for us to contact you, for the continued collection, use or

disclosure of your information, at anytime, by contacting us at info@icopet.life

INFORMATION WE COLLECT FROM YOU

We will collect and process the following data about you:

- **Information you give us**. This is information about you that you give us by filling in forms on the Website (https://icopet.life) or by corresponding with us by phone, e-mail or otherwise. The information you give us may include your name, address, e-mail address and phone number, financial and credit card information, personal description and photograph
- **Information we collect about you**. With regard to each of your visits to our site we will automatically collect the following information:

  - technical information, including the Internet protocol (IP) address used to connect your computer to the Internet, your login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform;
  - information about your visit, including the full Uniform Resource Locators (URL), clickstream to, through and from our site (including date and time), products you viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), methods used to browse away from the page, and any phone number used to call our customer service number.

- **Information we receive from other sources**. We are working closely with third parties (including, for example, business partners, sub-contractors in technical, payment and delivery

services, advertising networks, analytics providers, search information providers, credit reference agencies) who may provide us information about you.

If you are a registered user of our Website or Services, you can do so in your account settings. In accordance with the GDRP, you may correct, delete, or modify the personal information you provided to us and associated with your account.

COOKIES

Our website uses cookies to distinguish you from other users of our website. This helps us to provide you with a good experience when you browse our website and also allows us to improve our site.

USES MADE OF THE INFORMATION

We use information held about you in the following ways:

Information you give to us. We will use this information:

- to carry out our obligations arising from any contracts entered into between you and us and to provide you with the information, products and services that you request from us;
- to comply with applicable laws and legislation;
- to provide you with information about other goods and services we offer that are similar to those that you have already purchased or enquired about;
- to notify you about changes to our service;
- to ensure that content from our site is presented in the most effective manner for you and for your computer.

Information we collect about you. We will use this information:

- to administer our site and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;
- to comply with applicable laws and legislation;
- to improve our site to ensure that content is presented in the most effective manner for you and for your computer;
- to allow you to participate in interactive features of our service, when you choose to do so;
- as part of our efforts to keep our site safe and secure;
- to measure or understand the effectiveness of advertising we serve to you and others, and to deliver relevant advertising to you;
- to make suggestions and recommendations to you and other users of our site about goods or services that may interest you or them.

Information we receive from other sources. We will combine this information with information you give to us and information we collect about you. We will use this information and the combined information for the purposes set out above (depending on the types of information we receive).

DISCLOSURE OF YOUR INFORMATION

You agree that we have the right to share your personal information with:

- Any member of our group, which means respective past, present and future employees, officers, directors, contractors, consultants, equity holders, suppliers, vendors, service providers, parent companies, subsidiaries, affiliates, agents, representatives, predecessors, successors, and assigns ("**Petlife Team**").

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

YOUR RIGHTS

You have the right to ask us not to process your personal data for marketing purposes. You can also exercise the right at any time by contacting us at info@icopet.life

Our site may, from time to time, contain links to and from the websites of our partner networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

CHANGES TO OUR PRIVACY POLICY

Any changes we make to our privacy policy in the future will be posted on this page. Please check back frequently to see any updates or changes to our privacy policy.

CONTACT

Questions, comments and requests regarding this privacy policy are welcomed and should be addressed to info@icopet.life

ANNEX A

Know Your Customer (KYC) & Anti-Money Laundering (AML) Policy

The purpose of this KYC and AML policy (the "KYC/AML Policy") is to inform you of how Telemedicine OÜ, an exempted company that is officially registered under the law of Estonia and has been given its own ID number - 14514949, legal address: Randla tn 13-201, 10315 Tallinn, info@lifepet.io ("**Company**") protects itself from involvement in money laundering or suspicious activity. This KYC/AML Policy shall form part of our Privacy policy and terms and conditions (the "Agreement"). Each term starting with a capital letter shall have the meaning ascribed to it in the terms of services of the Agreement.

The KYC/AML Policy shall consist in the following:

- Performing an enterprise-wide risk assessment to determine the risk profile of the Company
- Establishing AML policies and procedures
- Implementing internal controls throughout its operations that are designed to mitigate risks of money laundering
- Performing KYC procedures on all users
- Designating a Compliance Officer with full responsibility for the AML Program
- Conducting an annual AML audit
- Providing AML training to all employees

Policies and procedures

This KYC/AML Policy will be provided to all employees of the Company. Each employee will acknowledge the KYC/AML Policy in writing. All policies and procedures will be reviewed and updated or revised as needed, but no less often than annually.

Internal controls

The Company has developed and implemented internal controls for the purpose of ensuring that all of its operations comply with all AML legal requirements and that all required reports are made on a timely basis.

Training

All of the officers and employees of the Company are required to receive AML training at least annually. New employees will receive appropriate AML training within 30 days of their hire date. Training for all employees will include not only the legal elements of AML laws and regulations but will also cover job specific applications of these laws. Ongoing training will be provided and updated regularly to reflect current developments and changes to laws and regulations.

Customer identification

It is the Company's policy to ensure that it has reasonably identified each customer who uses the Company's Platform. Users may be identified using a variety of methods.

Proof of identification

Individual

- Name
- Date and place of birth
- Residence address and mailing address if different (PO Box alone will not be acceptable)

- Official issued identification number (e.g., passport number, social security number, employee identification number or individual taxpayer identification number)
- Copy of valid photo identification of the principal(s) involved with the Petlife Account (e.g., driver's license, passport, alien identification card)

Verification

Documents used in opening an account relationship must be verified prior to establishing the Petlife Account. Verification of identity will require multi-factor authentication, layered security and other controls to ensure a meaningful user identity confirmation process based on Petlife Account size or other factors.

The following are examples of verification methods the Company may use:

- Obtaining proof of address, such as a copy of a utility bill or bank statement from the Petlife Account holder;
- Comparing the identifying information with information available from a trusted third party source, such as a credit report from a consumer-reporting agency, Veratad, Lexisnexis Instant ID;
- Analyzing whether there is logical consistency between the identifying information provided, such as the customer's name, street address, ZIP code, telephone number, date of birth, and social security number (logical verification);
- Utilizing knowledge-based challenge questions;
- Utilizing complex device identification (such as "digital fingerprints" or geolocation checks);
- Obtaining a notarized copy of an individual's birth certificate for valid identification; or

When the type of Petlife Account increases the risk that the Company will not be able to verify the true identity of the customer through documents is confirmed the Petlife Account will be closed.

Suspicious transaction and activity reports

The Company will diligently monitor transactions for suspicious activity. Transactions that are unusual will be carefully reviewed to determine if it appears that they make no apparent sense or appear to be for an unlawful purpose. Internal controls will be implemented so that an ongoing monitoring system is in place to detect such activity as it occurs. When such suspicious activity is detected, the Company will determine whether a filing with any law enforcement authority is necessary.

Suspicious activity can include more than just suspected money laundering attempts. Activity may be suspicious, and the Company may wish to make a filing with a law enforcement authority, even if no money is lost as a result of the transaction.

The Company will initially make the decision of whether a transaction is potentially suspicious. Once the Company has finished the review of the transaction details, he or she will consult with the Company's senior management to make the decision as to whether the transaction meets the definition of suspicious transaction or activity and whether any filings with law enforcement authorities should be filed.

The Company will maintain a copy of the filing as well as all backup documentation. The fact that a filing has been made is confidential. No one, other than those involved in the investigation and reporting should be told of its existence. In no event should the parties involved in the suspicious activity be told of the filing. The Company may

inform the Company's Board of the filing and the underlying transaction.

Reporting requirement

Reasonable procedures for maintaining records of the information used to verify a person's name; address and other identifying information are required under this Policy. The following are required steps in the record keeping process:

- The Company is required to maintain a record of identifying information provided by the customer;
- Where the Company relies upon a document to verify identity, the Company must maintain a copy of the document that the Company relied on that clearly evidences the type of document and any identifying information it may contain;
- The Company must also record the methods and result of any additional measures undertaken to verify the identity of the customer;
- The Company must record the resolution of any discrepancy in the identifying information obtained;
- All transaction and identification records will be maintained for a minimum period of five years.

AML audit

The Company is responsible for directing the annual AML audit of the Company's operations. The independent audit will be conducted by an independent third party or by Company personnel. The Company will develop corrective action plans for all issues that are raised in the audit and will provide the audit report and all corrective action plans to the Company's senior management for review. Reports of the corrective action will continue until all are resolved.