

TERMS AND CONDITIONS

PRIVACY POLICY

This Privacy Policy, together with our Terms and Conditions and IMA Agreement governs OneLife's collection, processing and use of your Personal Information. Any person, including OLN's IMAs, by accessing OneLife's website and any related websites, including those hosted by OneLife's partners including by accessing its account in our system (hereinafter referred as "accessing party") accepts and agrees to be bound by the present Privacy policy, unless otherwise declared expressly in writing by the person.

OneLife undertakes everything possible to maintain that the information is protected on the highest level.

Your personal data will be used in accordance with this Privacy Policy only. The objective of OneLife is to work actively towards increasing the confidence of its users in the field of protection of your information by taking all possible measures to increase the security and protection of your data. OneLife considers information protection as an extremely serious issue and strives to meet all the requirements of the existing data protection legislation. We consciously observe the confidentiality of our customers' information, and this Policy sets out the data processing methods used to work on the World Wide Web and Internet.

For the purpose of this policy "**Personal Information**" refers to information that identifies an individual, such as but not limited to name, address, e-mail address, transaction information, and banking details. Personal Information does not include anonymised and/or aggregated data that does not identify a specific user.

Please be advised that in connection with your registration on onelife.eu website and on the basis of the requirements of the existing Personal Data Regulations and other laws or subsidiary regulations, the company must verify the identity of its participants and for this purpose shall use various means it considers necessary and as permitted by law to verify your identity.

Collection of Your Personal information

In order to register as an Independent Marketing Associate and further to access your account in our system, you will be required to sign up/sign in with user name and password. You will be able to access your OneLife account using the user name and password chosen. Have in mind that as part of this registration process, you have to provide strong password and transaction password as well, which have to be different from the password and to keep all that credentials in strict confidentiality from any other third party.

We ask you when registering to provide personal information, such as your e-mail address, name, country, telephone number, address. We may also collect demographic information, such as your postcode, age, gender etc. For your safety we use Secure Sockets Layered (SSL) technology to ensure that your information is fully encrypted and sent across the Internet securely.

We may collect information about your visit, including the pages you view, the links you click and other actions taken in connection with OneLife system, website and related websites. We also collect certain standard information that your browser sends to every Website you visit, such as your IP address, browser type and language, access times and referring Web site addresses.

When you receive newsletters or other e-mails from OneLife, customised links or similar technologies may be used to determine whether the e-mail has been opened and which links you click, in order to provide you with more focused e-mail communications or other information in the future.

In order to offer you a more consistent and personalised experience in your interactions with OneLife, information collected through the Onelife website, and via your access to your account in our system (back office) may be combined with information obtained through other related websites, including those hosted by OneLife Network's partners.

Personal data when operating with your user account

For the creation, processing, withdrawals and payments, personal data is provided and processed in compliance with the current applicable legislation. Before the authorization of first payment, you will be asked for a copy of an official identity document (passport/ID card/ driving license) and also proof of address in accordance with the applicable KYC policy and procedures.

Personal data processed for purposes of analysis, statistics, advertising, and inquiries and complaints processing

When you contact us through one of the channels of communication - we will process those personal details you decide to share with us in connection with the particular matter you are addressing to us. If you share your sensitive personal information, such as your health, we will process this information only in order to provide you with the requested services and respond to your specific needs, complaints or inquiries.

We may process your personal data for the purposes of analyzing, statistics and improving the quality of our services, testing and enhancing your satisfaction. Submitting your personal information to third parties in the case of direct marketing, is a matter of your choice. If we have received your prior consent, we will send you information about our products and services

Data subject rights and obligation

Data Subject Consent

With the present and by accepting the OneLife T&Cs, in relation to and based on art. 4, para 11 of the GDPR, I am hereby consenting that OneLife Network Ltd can process my personal data for the following purposes:

- Verification of the individual;
- Verification of the profile/account created by the individual;
- Verification of the representation capacity of a legal entity, which profile/account is created by an individual;
- AML/CFT compliance purposes;
- marketing purposes

In addition with the present I hereby acknowledge that I have carefully read and understood all relevant documents related to the processing of my personal data processed in relation to my participation in OneLife.

I am also aware that the following related documents/forms are available upon request sent to compliance@onelife.eu :

1. Data subject withdrawal form;
2. Data subject access request form;
3. Data subject disclosure form;

The Right to be forgotten

As a data subject you are entitled to receive confirmation and/or detailed information, incl. a copy of the personal data processed for you (access right). Everyone has the right to be forgotten. This can be executed by email to compliance@onelife.eu and filling in the provided: Withdrawal consent form. Your right to erasure applies in the following cases (not an exhaustive list):

- where the personal data are no longer necessary to achieve the purposes for which they are collected or processed (*think about those essential processing principles*),
- where a data subject has withdrawn his or her consent (*obviously also the mentioned explicit consent*),
- where a data subject objects to the processing of his/her personal data (*the right to object is another data subject right*),
- where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet,
- where the processing of personal data does not otherwise comply with the GDPR.

The grounds upon which a data subject can exercise the right to be forgotten

- The personal data is not necessary in the context of the purpose of collection and/or processing. Consent to process is withdrawn by the data subject AND there is no other legal processing basis. This goes both for consent overall as for explicit consent.
- The right to object is exercised, in general and in the context of direct marketing IF there are no other legal processing grounds.
- The processing of the personal data has been done in an unlawful way.

When the right to erasure does not apply?

- In the scope of the right of freedom of expression and information
- When compliance with another law requires the data controller to process those data
- To carry out a task in the public interest in general
- When the data controller needs to process the data in the context of the previously mentioned 'vested authority'

- In the scope of healthcare, social care and public health

In the context of public interest, specifically public health (e.g. preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, the management of health or social care systems, protecting against serious cross-border threats to health and more),

Disclosure of personal information. Categories of recipients

We may provide a part of the above mentioned data to Governmental Authorities due to legal obligations as well as to our trusted partners (as far as it is necessary for the services we use, such as technical support services on our site, call center management services and help desks, chat platforms for contacting us, etc.), for which we have ensured that they meet the highest standards of information security and its privacy.

We have contractual relations with all these companies, which ensure that the personal data transmitted are processed only as strictly necessary to provide us with these services.

Also, for reasons of public interest or by law, we disclose certain information to other governmental authorities, courts and prosecutor offices if required by law, by the State or by another regulatory body.

Please be advised that in some cases your personal information may be shared with third non-EU/EEA member countries in accordance with the applicable law and in accordance with this Privacy Policy. If we disclose your personal information to non-EU/EEA third parties, we will ensure that our contractual relations with such third non-EU/EEA member countries include adequate protection measures to protect your personal information. We enter into contractual relations with such third parties only if they can guarantee a comparable standard of data protection such as the standard in EU/EEA countries.

How do we protect your privacy and personal data?

We process your personal data only in conformity with the above-mentioned purposes, grounds and deadlines. Data access is only available to a limited number of persons who have prior training and instructions on how to work with personal data.

In connection with the entry into force of new European Data Protection Rules, the Company has undertaken a detailed analysis and audit of all our processes related to the personal data processing. As part of this analysis, we check our partners, revise our procedures and rules, train our employees, and use experienced information security consultants to ensure that we meet the highest standards of privacy and security of your information.

We use the best modern encryption methods for a username and password, and any other confidential information sent by and to the client or our servers, and thus protecting the data and our company from third party manipulations. IMA should not violate or circumvent established security rules or should not attempt to gain unauthorized access to the Software as this will cause immediate termination of access - blocking their accounts and informing the authorities concerned.

In case you suspect unauthorized access and/or use of your account, please take

measures by changing your password or contact us using the following contact details for further assistance.

Compliance@onelife.eu

To ask questions about your rights or if you wish to exercise one of them, please contact us at the contacts listed in this Policy compliance@onelife.eu. We will respond to any of your requests without undue delay within 30 days of receipt of the request. If we are unable to do so for reasons beyond our control, we will notify you in good time, indicating also the reasons for the delay.

Changes in the current policy

Any changes in this policy will be announced . In the event of a substantial change of information, we will further inform you by sending an email.

Date: 08.02.2019