# Privacy Notice and Terms

ThinkPenguin, Inc recognizes the importance of protecting the privacy of it’s PenguinVPN users.

Usage of the PenguinVPN service is subject to the terms of this Privacy Notice.

Although the servers may be located in various countries, all servers and all data collected by those servers are subject to this "Privacy Notice and Terms" and are compliant to the standards set forth by European Directives 95/46/EC ("Data Protection"), 2002/58/EC ("privacy on electronic communications"), the EU General Data Protection Regulation 2016/679 and the best practices recommended by the EU Art. 29 Working Party and the EDPS (European Data Protection Supervisor).

Some servers are operated outside of the European Union and may be operated to a higher level of privacy and data protection, but will never be operated with a lower level of privacy and data protection. ThinkPenguin, Inc will not offer service in countries which have laws which would force ThinkPenguin, Inc to violate the aforementioned European Union directives.

PenguinVPN servers and software procedures in general do not acquire personal data.

If a PenguinVPN user or customer registers an account for which a valid e-mail address is provided, such e-mail address will be protected as personal data according to the aforementioned legal framework. PenguinVPN will not treat this address to profile the user or disclose his/her identity, and will not transmit it to any third party. The identical protection is enforced by default on every other field, to protect those users who should enter in their account fields any information that could be considered personal data in spite of the fact that ThinkPenguin, Inc does NOT require accurate information.

When users connect to PenguinVPN Virtual Private Network, no cookies are stored on their system. When users access ThinkPenguin, Inc’s web site (for example to place an order) cookies are stored on systems in order to enable access to the web site. Cookies are stored only for technical reasons and can be deleted anytime by the user. Cookies are specifically meant for technical functioning. Under no circumstance does ThinkPenguin, Inc use cookies to track and/or profile users. ThinkPenguin, Inc’s web servers do not use third party add-ons or any other procedure that may lead to users profiling by any third party or by ThinkPenguin, Inc itself.

If users decide to pay for the PenguinVPN service via intermediary companies (e.g. PayPal) which process payments, any data the users give to such companies are not under ThinkPenguin, Inc’s control and are not stored or treated by ThinkPenguin, Inc, but by the payment processor companies.

Users do not need to enter any personal data to access PenguinVPN services. Users may optionally provide their e-mail addresses to receive courtesy e-mail pertaining to technical support. When they do so, e-mail addresses are stored in ThinkPenguin’s servers exclusively for assistance purposes. Technical and sales support is not outsourced. E-mail addresses are not used by ThinkPenguin, Inc to identify or collect any other information about the users, are not processed for any purpose different than providing courtesy, automated communications for technical support, and are not transmitted to any third party. A valid e-mail address is NOT required to access PenguinVPN services and/or receive technical support, so usage of a valid e-mail address remains totally optional.

Users may ask for information held to be deleted with a simple written request by e-mail to: support (at) thinkpenguin (dot) com.

Technical data which are strictly necessary for the Internet / networking connections that are specifically related to the PenguinVPN service are handled by automatic systems only in RAM and only for the time being necessary to provide the service. Activity traffic and/or traffic content and/or IP addresses of the customers or users are not inspected, logged, or stored on any permanent medias.

Security measures are taken to protect data leakage, illegal use of data, unauthorized access to data, specifically (but not limited to):

- Machines where operations which might involve personal data are protected by redundant security, including, but not limited to, responding only to private host names and rejecting connections from anything different that a tiny white list of addresses
- The database of the accounts is not stored in those PenguinVPN servers which are dedicated to provide VPN access; it is stored in servers which are not accessible from the outside
- PenguinVPN databases, according to their contextual usage, are isolated from each other
- In the users database all personal data that do not need a search index are encrypted
- Physical access to the machines keeping the users database is prevented by state of the art surveillance in top rated datacenters
- PenguinVPN uses only ciphers for which a cryptographic practical/feasible attack has not been found by the worldwide scientific community
- Different PenguinVPN servers are not allowed to communicate directly with each other. Each communication, only when strictly necessary for technical reasons (for example checking the authorization of a user in order to let him/her enter an PenguinVPN service), is performed through an intermediary application service, and is always encrypted
- Personnel take care to check daily security and vulnerability bulletins, to keep PenguinVPN server system software (including kernels) up to date and to act very expeditiously to patch any found vulnerability in any employed software