

DEFINITIONS

Company	Beamloop UAB (registration address: J. Savickio g. 4-7, LT-01108 Vilnius, Lithuania; registration number: 306029168)
License(s)	
Platform	A website that is operated by the Company and available at cryptostorm.net .
Cryptostorm	Collective name that can refer to both the Platform and the Company.
Privacy Policy	This document
Customer	An individual Customer from an age of 18+ or a legal entity that has read and agreed to the Customer Agreement of Cryptostorm and uses services of the company provided through the Website Platform.
GDPR	The General Data Protection Regulation (EU) 2016/679.
KYC or Due Diligence	Documents that are requested by Cryptostorm from the Customers in order to identify the Customer and comply with applicable laws.

1. PURPOSE AND SCOPE

The Policy is meant for use by Customers of Cryptostorm.

Cryptostorm is a company registered in Lithuania that has developed and governs the Platform and the services, products and content that is accessible and offered on the Platform.

The company is compliant with the applicable Lithuanian and International laws for the Prevention of Money Laundering and Terrorist Financing, the General Data Processing Regulation as well as other legislations applicable in Lithuania.

This policy aims to provide Company's Customers with information on what type of information Company collects, how it is used and the circumstances where it could be shared with third parties.

Through this document, Customer's data may be called either "personal data" or "personal information". Company may also sometimes collectively refer to handling, collecting, protecting and storing Customer's personal data or any such action as

“processing” of such personal data. For the purposes of this policy, personal data shall mean any information relating to Customer, which identifies or may identify a Customer and which includes, for example, Customer’s name, address and identification number.

The present Privacy Statement aims to help you better understand the most recent changes to the Privacy Policy and cookie policy and how they may affect Customers. To understand the changes in full, the Customer will need to read the full Privacy Policy and cookie policy.

2. COLLECTION OF PERSONAL DATA

The Company shall collect information necessary to fulfil legal obligations for the provision of services and to improve our service to you.

Cryptostorm will gather information and documentation to identify, contact or locate Customers and may gather information from third parties and or other sources, which will help us to offer our services effectively.

3. PURPOSE OF COLLECTING AND PROCESSING OF PERSONAL DATA

According to the Lithuanian and International laws for the Prevention of Money Laundering and Terrorist Financing, as well as in order to enhance Customer support, Customer’s personal data will be used for specific, explicit and legitimate purposes.

The performance of contractual obligations

The personal data collected from Customers is used to verify Customer’s identity for Due Diligence purposes, to manage Customer’s account with the Platform, to process Customer’s transactions, to provide Customers with post-transaction information, to inform Customers of additional products and/or services relevant to Customer’s profile, to produce analysis and statistical data which will help the Company improve its products and services, and for Platform enhancement purposes.

Identity Verification purposes

The Company needs to perform its Due Diligence measures and apply the principles of KYC (Know-Your-Customer) before entering a business relationship with any Customer in order to prevent actions, such as money laundering or terrorist

financing, and to perform other duties imposed by law.

Company collects from its Customers' identity verification information (such as copies, images, scans of Customer's government issued national ID card or International Passport, or other governmental proof of identification) or other authentication information. Cryptostorm also requests its Customers to provide the Company with a recent Utility Bill in order to verify Customer's residential address. Further to this, the Company can use third parties to carry out identity checks on its behalf.

Compliance with a legal obligation

There are a number of legal obligations emanating from the relevant laws to which the Company is subject to, as well as other statutory requirements.

Such obligations and requirements impose on Cryptostorm are necessary personal data processing activities for credit checks, identity verification, compliance with court orders, tax law or other reporting obligations and anti-money laundering controls.

Purposes of safeguarding legitimate interests

Company processes personal data to safeguard the legitimate interests pursued by Cryptostorm or by a third party. A legitimate interest is when Cryptostorm has a business or commercial reason to use Customer's information. Even then, it must not unfairly go against what is right and best for the Customer.

Examples of such processing activities include:

- a. Initiating court proceedings and preparing our defence in litigation procedures,
- b. Means and processes we undertake to provide for the Company's IT and system security, preventing potential crime, asset security, admittance controls and anti-trespassing measures,
- c. Measures to manage business and for further developing products and services,
- d. The transfer, assignment (whether outright or as security for obligations) and/or sale to one or more persons and/or charge and/or encumbrance over, any or all of the Company's benefits, rights, title or interest under any agreement between the Customer and the Company.

Marketing Purposes

The Company may use Customer data, such as location or transaction history to deliver any news, analysis, research, reports, campaigns and training opportunities that may interest the Customer, to their registered email address.

Customer always has the right to change the option if he no longer wishes to receive

such information.

4. CONTROLLING AND PROCESSING CUSTOMER'S PERSONAL DATA

Cryptostorm and any agents that it engages for the purpose of collecting, storing and processing personal data and any third parties acting on Company's behalf, may collect, process and store personal data provided by the Customer.

For the purpose of processing and the storage of personal data provided by the Customer in any jurisdiction within the European Union or outside of the European Union, the company can confirm this will be done in accordance with applicable laws.

Authorized Processor

The GDPR sets out what needs to be included in the contract which the company has adhered to, the below is not an exhaustive list of the obligations of all relevant parties:

- a. Such third parties must only act on the written instructions of the our company (unless required by law to act without such instructions);
- b. Ensure that people processing the data are subject to a duty of confidence;
- c. Take appropriate measures to ensure the security of processing;
- d. The rights of Customers will not be impaired in meeting with GDPR requirements;
- e. The security of processing, the notification of personal data breaches and data protection impact assessments will not be impaired;
- f. Deletion or return of all personal data as requested at the end of the contract;
- g. Such providers will provide various services as agreed with the Company.

Cryptostorm has a regulatory obligation to supervise and effectively oversee the outsourced functions and to act appropriately when it determines that the service provider is not performing the said functions effectively and in accordance with the applicable legislation.

Cryptostorm may use or disclose personal information without Customer's consent only in certain circumstances:

- h. if required by law or by order of a court, administrative agency, or other government entities;
- i. if there are reasonable grounds showing disclosure is necessary to protect the rights, privacy, property, or safety of Customers or others;

- j. if we believe the information is related to a breach of an agreement or violation of the law, that has been, is being, or is about to be committed;
- k. if it is necessary for fraud protection, risk reduction, or the establishment or collection of funds owed to us;
- l. if it is necessary to enforce or apply the Terms and Conditions and other agreements, to pursue remedies, or to limit damages to our company;
- m. for other reasons allowed or required by law;
- n. if the information is public.

When the Company is required or permitted to disclose information without consent, Company will not disclose more information than necessary to fulfil the disclosure purpose.

Cryptostorm informs all Customers to maintain confidentially and not to share with others its Customer names and private passwords or as provided by the Company. The Company bears no responsibility for any unlawful or unauthorized use of Customers' personal information due to the misuse or misplacement of Customers' access codes (i.e. passwords/credentials), negligent or malicious, however conducted.

5. HOW THE COMPANY TREATS CUSTOMER'S PERSONAL DATA FOR MARKETING ACTIVITIES

The Company may process Customer's personal data to inform Customers about products, services and offers that may be of interest to them. The personal data that Cryptostorm processes for this purpose consists of information Customers provide to the Company and data Cryptostorm collects and/or infers when Customer uses services of the Platform, such as information on Customer's transactions. Company studies all such information to form a view on what is needed or what may be of interest to Customers.

In some cases, profiling may be used. Profiling is a process when Customer's data is being automatically processed with the aim of evaluating certain personal aspects and to further provide Customers with targeted marketing information on products.

Company's site uses technologies of third-party partners to help Company recognize Customer's device and understand how Customer uses Company's site so that Cryptostorm can improve its services to reflect Customers interests and serve advertisements about the services that are likely to be of more interest to Customer. Specifically, these partners collect information about Customer's activity on Company's site to enable Company to:

- a. measure and analyze traffic and browsing activity on Company's site;
- b. show advertisements for Company's services to Customer on third-party sites;

- c. measure and analyze the performance of Company's advertising campaigns;

Company may share data, such as hashed email derived from emails or other online identifiers collected on Company's site with Company's advertising partners. This allows Company's partners to recognize and deliver ads to Customer across devices and browsers.

Cryptostorm can only use Customer's personal data to promote its products and services to Customers if Cryptostorm has Customer's explicit consent to do so – by clicking on the tick box during the account opening form – or in certain cases, if the Company considers that it is in their legitimate interest to do so.

Further, Customers have the option to choose whether they wish to receive marketing related emails (company news, information about campaigns, the company's newsletter, the company's strategic report, etc.) to Customer's provided email address by clicking the relevant tick box during the account opening form.

Company's partners may use non-cookie technologies that may not be impacted by browser settings that block cookies. Customer's browser may not permit to block such technologies. For this reason, Customer can use the following third party tools to decline the collection and use of information for the purpose of serving Customer interest based advertising:

- d. The NAI's opt-out platform: <http://www.networkadvertising.org/choices/>
- e. The EDAA's opt-out platform <http://www.youronlinechoices.com/>
- f. The DAA's opt-out platform: <http://optout.aboutads.info/?c=2&lang=EN>

Customers have the right to object at any time to the processing of Customer's personal data for marketing purposes or unsubscribe to the provision of marketing related emails by the Company, by contacting at any time Company's Customer support department via the following ways:

- g. By Email: support@cryptostorm.net
- h. Customer support via the platform

Period of keeping Customer's personal information

The Company will keep Customer's personal data for:

- i. As long as a business relationship exists with the Customer, either as an individual or in respect of our dealings with a legal entity Customer is authorized to represent or are a beneficial owner of.
- j. Once the business relationship with Customers has ended, Company is required to keep Customer's data for a period of five years to meet regulatory and legal requirements. In some cases, this period may be extended.

When Company no longer needs personal data, it will securely delete or destroy it.

6. CUSTOMER'S RIGHTS

Customer has the right to request copies of his/hers personal data. Information must be provided without delay and at the latest within one month of receipt. The company will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we will inform Customers within one month of the receipt of the request and explain why the extension is necessary.

Cryptostorm must provide a copy of the information free of charge. However, the Company can charge a "reasonable fee" when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The fee if applied will be based on the administrative cost of providing the information and for delivery expenses, if Customer requests to deliver this information in hard copy. If at any time we refuse to respond to a request, we will explain why to the Customer, informing them of their right to complaint to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

The Geographical Area of Processing

As a general rule, the Customer data is processed within the European Union/European Economic Area (EU/EEA), but in some cases it is transferred to and processed in countries outside the EU/EEA.

The transfer and processing of Customer data outside the EU/EEA can take place provided there are appropriate safeguards in place and the actions are made based on a legal basis only.

Upon request, the Customer may receive further details on Customer data transfers to countries outside the EU/EEA.

Other related information

Cryptostorm uses appropriate technical, organizational and administrative security measures to protect any information it holds in its records from loss, misuse, and unauthorized access, disclosure, alteration and destruction. Unfortunately, no company or service can guarantee complete security. Unauthorized entry or use, hardware or software failure, and other factors, may compromise the security of Customer information at any time.

Among other practices, Customer's account is protected by a password for Customer's privacy and security. Customers must prevent unauthorised access to Customer's account and Personal Information by selecting and protecting Customer's password appropriately and limiting access to Customer's computer or device and browser by signing off after you have finished accessing Customer's account.

Transmission of information via regular email exchange is not always completely secure. The Company however exercises all possible actions to protect Customers' personal data, yet it cannot guarantee the security of Customer data that is transmitted via email; any transmission is at the Customers' own risk. Once the Company has received the Customer information it will use procedures and security features in an attempt to prevent unauthorised access.

When Customers email the Company (via the "Contact Us" page), or using the Live Chat feature, a person may be requested to provide some additional personal data, like their name or email address. Such data will be used to respond to their query and verify their identity. Emails are stored on Company's standard internal contact systems which are secure and cannot be accessed by unauthorised external parties.

7. RAISING A CONCERN

Customer has the right to be confident that Cryptostorm handles Customer's personal information responsibly and in line with good practice.

If a Customer has a concern about the way the Company is handling Customer's information, or for example if a Customer feels we may not be;

- a. keeping Customer's information secure;
- b. holds inaccurate information about you;
- c. has disclosed information about you;
- d. is keeping information about you for longer than is necessary; or
- e. has collected information for one reason and is using it for something else;

We take all concerns seriously and will work with you to resolve any such concerns.

Any concerns and/or requests can be raised to the appointed Data Protection Officer whose contact details are below:

Email: dataprivacy@cryptostorm.net

If the Customer is not satisfied with any responses provided by the Company, the Customer has a right to raise such matters with the Lithuanian Data Protection Inspectorate:

- f. E-mail address: ada@ada.lt
- g. L. Sapiegos str. 17, LT-10312 Vilnius, Lithuania
- h. Phone: +370 5 212 7532

The Customer has the right go to court or to escalate their complaint to the data protection regulator in their jurisdiction for the protection of rights, unless the applicable laws prescribe a different procedure for handling such claims.

8. CHANGES TO THIS PRIVACY STATEMENT

The Company reserves the right to modify or amend this Privacy Statement unilaterally at any time in accordance with this provision.

If any changes are made to this privacy statement, we shall notify you accordingly. The revision date shown on at the end of this page will also be amended. We do however encourage you to review this privacy statement occasionally so as to always be informed about how we are processing and protecting Customer's personal information.

9. COOKIES

Company's website uses small files known as cookies to enhance its functionality and improve Customer's experience.

A cookie is a small text file that is stored on a Customer's computer for record-keeping purposes. Company uses cookies on the Platform(s). Cryptostorm links the information it stores in cookies to any personally identifiable information Customer submits while on the Platform. Cryptostorm uses both session ID cookies and persistent cookies. A session ID cookie does not expire when Customer closes his browser. A persistent cookie remains on Customer's hard drive for an extended period of time. Customer can remove persistent cookies by following directions provided in Customer's Internet browser's "help" file.

Company sets persistent cookies for statistical purposes. Persistent cookies also enable the Company to track and target the location and interests of our Customers and to enhance the experience of Company's services on the Platform.

If Customer rejects cookies, Customer may still use the Platform.

Some of Company's business partners use cookies on the Platform. Company has no access to or control over these cookies.

10. MONITORING AND REVIEW

The Company will monitor on a regular basis the effectiveness of this Policy and, in particular, the execution quality of the procedures explained in the Policy and, where appropriate, it reserves the right to correct any deficiencies.

In addition, the Company will review the Policy at least annually. A review will also be carried out whenever a material change occurs that affects the ability of the Company to continue to the best possible result for the execution of its Customer Orders on a consistent basis using the venues included in this Policy.

The Company will inform its Customers of any material change to this Policy by posting an updated version of this Policy on its Website(s).