

PRIVACY NOTICE

Use of Kriptomat devices for the purchase and sale of cryptocurrencies

In brief

This Privacy Notice ("Notice") explains how and why Bitblock d.o.o. ("Controller", "Company", "we") processes the personal data of users who use Kriptomat devices for the purchase and sale of cryptocurrencies. The Notice is intended for users of the devices.

The Company processes personal data primarily for the purpose of complying with legal obligations in the area of preventing money laundering and terrorist financing, as well as for ensuring system security and executing transactions.

Most of the processing of personal data relates to the user identification procedure, which is legally required in the context of the purchase and sale of cryptocurrencies and is not connected with marketing activities or user profiling.

The Company carries out user identification for the purpose of establishing a business relationship in all cases where an individual transaction, or several mutually connected transactions carried out by the user within a period of seven days, reaches or exceeds the amount of EUR 1,000. In certain situations, in accordance with applicable regulations, the Company may also carry out additional checks of the user's identity and the circumstances of the transaction. The identification procedure may include the entry of personal data, submission of a copy of an identification document and, in certain cases, identity verification by means of a photograph or video recording, as described in more detail in this Notice. If the user does not wish to, or is unable to, complete the identification procedure in cases where it is mandatory, the Company will not be able to execute the requested transaction.

If the Company is not required to carry out identification, only the user's telephone number is collected for the purpose of carrying out the transaction and/or fulfilling legal obligations.

More information about the controller, the types of data processed, the purposes and retention periods, and users' rights is available below in this Notice.

1. Who is the controller

The controller of personal data is:

Bitblock d.o.o.

Address: Ilica 71, 10000 Zagreb

E-mail (GDPR): osobnipodaci@bitblock.hr

2. What this Notice relates to

This Notice relates to the processing of personal data in connection with:

- the use of Kriptomat devices for the purchase and sale of cryptocurrencies,
- ensuring the security of the Company's business operations, users and property, including the implementation of video surveillance,
- sending marketing communications, if the user gives consent for this.

The Company provides the service exclusively through Kriptomat devices and, within the scope of this service, does not create user accounts, provide mobile applications or web profiles connected with the processing of users' personal data. The Company does not provide long-term custody services for crypto-assets and does not manage users' private cryptographic keys.

3. What data we process

Depending on the circumstances of using the service, the applicable legal obligations and the user's choice, the Company may process the following categories of personal data:

3.1. Identification and personal data

For the purpose of carrying out prescribed identification procedures, preventing abuse and fulfilling legal obligations, the Company may process the following personal data:

- name and surname
- date of birth
- residence address
- occupation
- data on political exposure
- data on the source of funds
- purpose of the transaction
- type, number and issuing country of the identification document
- copy of the identification document

3.2. Contact data

For the purpose of communicating with the user in connection with carrying out the transaction, fulfilling legal obligations or, if the user expressly chooses this, for marketing purposes, the Company may process:

- telephone number
- e-mail address

3.3. Transaction and crypto-address data

In the context of the purchase and sale of cryptocurrencies, the Company processes data connected with the execution of an individual transaction, including:

- type and amount of cryptocurrency
- amount in euros
- date and time of the transaction
- crypto-wallet address of the sender or recipient

3.4. Technical and biometric data related to the identification procedure

Where, in accordance with applicable regulations, it is necessary to verify the user's identity, the Company processes data generated as part of that procedure. The processing is carried out directly by the Company and/or through an authorised external identity verification service provider.

Such data may include in particular:

- a facial image or photograph of the user (selfie),
- a short video recording used exclusively to confirm that the person is a real person (so-called liveness check),
- the user's IP address, which is collected when carrying out the identification procedure through an external identity verification tool,
- technical records and logs connected with carrying out the identity verification and confirmation procedure.

These personal data are processed solely within the scope of identity verification, exclusively for the purpose of fulfilling the Company's legal obligations, i.e. for preventing fraud and abuse.

3.5. Data collected through video surveillance

At locations where Kriptomat devices are installed, the Company carries out video surveillance, whereby video recordings of persons located in the area covered by video surveillance may be collected, including users of Kriptomat devices.

Video surveillance is carried out independently of the execution of the transaction itself and is connected with presence in the premises where the device is located.

4. For what purposes we process data and on what legal basis

The Company processes the personal data described in Section 3 of this Notice solely for the purposes set out below, in accordance with applicable regulations. Personal data are not used for purposes that are not compatible with those stated in this Notice.

4.1. Carrying out user identification and fulfilling legal obligations

The Company processes personal data for the purpose of establishing a business relationship with the user and carrying out user identification and verification procedures, including risk assessment, monitoring and recording transactions, and fulfilling obligations arising from regulations on the prevention of money laundering and terrorist financing, as well as other applicable regulations.

Within the scope of this processing, the Company keeps legally prescribed records, collects and stores prescribed documentation, links the user's identity with transactions carried out by the user through Kriptomat devices and, where necessary, carries out additional checks in cases of increased or high risk.

Personal data are also processed for the purpose of responding to requests from competent authorities.

Legal basis: the processing is necessary for compliance with the Company's legal obligations.

4.2. Execution of transactions and provision of the service through Kriptomat devices

The Company processes personal data for the purpose of enabling the purchase and sale of cryptocurrencies through Kriptomat devices, the technical execution of individual transactions, recording their course and results, and communicating with the user in connection with the provision of the specific service.

Without processing personal data to this extent, the Company would not be able to execute the transaction initiated by the user through a Kriptomat device.

Legal basis: the processing is necessary for the performance of a contract to which the user is a party, or in order to take steps at the request of the user prior to entering into a contract.

4.3. System security, prevention of abuse and protection of persons and business operations

The Company processes personal data for the purpose of ensuring the secure functioning of Kriptomat devices and connected IT systems, preventing abuse, fraud and unauthorised actions, protecting persons and property, and establishing facts in the event of security incidents or disputes.

For this purpose, the Company implements appropriate technical and organisational security measures, including the processing of technical records and system security logs, monitoring and analysing unusual activities and, where appropriate, processing video recordings collected through video surveillance at locations where Kriptomat devices are installed.

This processing does not relate to personal data processed for the purpose of user identification or to data necessary for the execution of the transaction itself.

Legal basis: the processing is necessary for the purposes of the legitimate interests pursued by the Company, whereby the Company ensures that those interests do not override the rights and freedoms of data subjects.

4.4. Marketing communication (based on consent)

If the user voluntarily gives consent, the Company may process the user's contact data for the purpose of sending notices about the Company's services, news and other marketing content.

Giving consent for marketing communication is not a condition for using Kriptomat devices, and refusing or withdrawing such consent does not affect the ability to use the service.

Legal basis: the data are processed on the basis of the user's consent. The user may withdraw consent for marketing communication at any time, whereby the withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

5. With whom we share data

The Company does not sell users' personal data, does not disclose them to third parties for marketing purposes and does not enable access to personal data to persons who do not have a lawful basis for such access. However, depending on the purpose of processing, users' personal data may be available to the following categories of recipients, solely to the extent necessary to carry out the purposes of processing:

5.1. External service providers (processing of personal data on behalf of the Company)

For the purpose of providing the service, the Company uses the services of external service providers who process personal data on behalf of the Company and exclusively in accordance with its instructions, including:

- providers of user identification and verification services, who carry out identity verification and regulatory compliance procedures on behalf of the Company;
- providers of compliance and risk assessment services, who provide the Company with professional or technical support in fulfilling legal obligations and analysing transactions;
- IT and technical service providers, including providers of IT infrastructure, system maintenance, hosting and technical support, to the extent that their access to personal data is necessary for the functioning of Kriptomat devices and connected systems;
- the Company's professional advisers, where access to personal data is necessary for the provision of advisory services or the protection of the Company's legal interests.

All external service providers who process personal data on behalf of the Company are contractually obliged to treat personal data as confidential, apply appropriate technical and organisational protection measures and not use personal data for their own purposes.

5.2. Competent public authorities

Personal data may be provided to competent public authorities where this is prescribed by applicable regulations or on the basis of a lawful and binding request from such authorities. This may include, for example, the provision of data in the context of supervisory proceedings, criminal or misdemeanour proceedings, procedures for the prevention of money laundering or other procedures prescribed by law.

In such cases, the Company provides only those personal data that are necessary for fulfilling a legal obligation or a lawful request.

5.3. Technical participants in transactions and public blockchain networks

In the context of executing transactions through Kriptomat devices, certain data, such as the crypto-wallet address, become technically visible to other participants in the transaction or publicly available within the blockchain network, in accordance with the rules of distributed ledger technology.

The Company has no influence over the further processing of such data by independent participants in decentralised networks and does not act as a controller in relation to such further processing.

6. Where personal data are processed

As a rule, users' personal data are processed within the European Economic Area (EEA), within the IT systems of the Company and its contractual service providers.

Considering the use of modern IT solutions and external service providers, especially in the area of identity verification and compliance with regulations on the prevention of money laundering, in certain cases personal data may be processed or access to personal data may be enabled outside the EEA as well.

If personal data are processed or transferred to third countries or international organisations that do not ensure an adequate level of personal data protection within the meaning of the GDPR, the Company will ensure the application of appropriate safeguards in accordance with applicable regulations, such as the European Commission's standard contractual clauses or other permitted transfer mechanisms.

7. How long we retain data

The Company retains personal data only for as long as is necessary to achieve the purposes for which the data are processed, or in accordance with applicable legal obligations.

The following general rules apply to the retention of personal data of device users:

- Personal data processed for the purpose of user identification, monitoring of the business relationship and transactions, and fulfilling obligations arising from regulations on the prevention of money laundering and terrorist financing are retained for ten (10) years from the termination of the business relationship with the user, or from the execution of an individual transaction, in accordance with applicable regulations. During this period, data connected with the execution of transactions are also retained to the extent necessary to prove their execution or to fulfil legal obligations.
- Personal data processed for the purpose of ensuring system security, preventing abuse and protecting persons and business operations are retained for a shorter period, depending on the nature of the data and the purpose of processing. Technical records and system security logs are retained for as long as is necessary to detect, analyse and resolve security incidents, after which they are deleted or anonymised.
- Video recordings collected through video surveillance at locations where Kriptomat devices are installed are retained for a maximum of seven (7) days, unless a particular recording has been set aside for the purpose of conducting proceedings or responding to a request from competent authorities, in which case it is retained until the completion of such proceedings.
- Personal data processed on the basis of the user's consent for marketing purposes are retained until the consent is withdrawn, unless the purpose of processing has been achieved earlier or the law provides otherwise.

Upon expiry of the applicable retention periods, personal data are deleted, anonymised or access to them is further restricted, in accordance with the Company's internal rules and applicable regulations.

8. Automated checks and profiling

For the purpose of fulfilling legal obligations and ensuring the security of systems and transactions, the Company uses automated tools and procedures for the processing of personal data, especially for the purposes of verifying users' identity, analysing transactions and assessing risk.

Such procedures may include automated analysis of certain personal data in order to determine characteristics relevant for risk assessment, such as the manner of using the service or patterns of carrying out transactions, which constitutes a limited form of profiling.

Profiling is carried out exclusively for the purpose of fulfilling the Company's legal obligations, preventing fraud and abuse, and ensuring system security. It is not used for marketing purposes or for making decisions that would be based on users' personal preferences.

The results of automated checks and profiling are used as an auxiliary tool and are subject to human assessment and supervision, especially in cases where increased or high risk is identified. The Company does not make decisions that would produce legal effects concerning the user or similarly significantly affect the user solely on the basis of automated processing of personal data or profiling.

9. Security of personal data processing

The Company applies appropriate technical and organisational measures for the protection of personal data in order to ensure their security, confidentiality and integrity and to prevent unauthorised access, loss, abuse or unauthorised disclosure of personal data. The protection measures are designed taking into account the nature, scope and purposes of the processing of personal data, as well as risks of varying likelihood and severity for the rights and freedoms of users, and are regularly reviewed and, where necessary, improved.

10. Your rights under the GDPR

The user has certain rights in connection with the processing of their personal data, in accordance with applicable personal data protection regulations.

The exercise of certain rights may be limited to the extent that the processing of personal data is necessary for the fulfilment of the Company's legal obligations, especially obligations arising from regulations on the prevention of money laundering and terrorist financing.

The user has the following rights:

- **Right of access** - the right to request confirmation as to whether personal data are being processed and, if they are being processed, access to such data and basic information about the processing;
- **Right to rectification** - the right to request the correction of inaccurate personal data and completion of incomplete data;
- **Right to erasure** - the right to request the deletion of personal data in cases provided for by regulations, except where the Company is obliged to retain the data in order to fulfil legal obligations;

- **Right to restriction of processing** - the right to request that the processing of personal data be temporarily restricted in cases provided for by regulations, for example if the user contests the accuracy of the personal data or the lawfulness of their processing;
- **Right to data portability** - the right to receive personal data in a structured, commonly used and machine-readable format, to the extent that the processing is based on a contract or consent and is carried out by automated means;
- **Right to object** - the right to object to the processing of personal data based on the Company's legitimate interests;
- **Right to withdraw consent** - if the processing of personal data is based on consent, the user may withdraw the consent given at any time, whereby the withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

To exercise their rights, the user may contact the Company using the contact details set out in Section 1 of this Notice. The Company may request additional information in order to confirm the identity of the applicant (to prevent unauthorised disclosure of data).

The Company will respond to requests concerning the exercise of rights without undue delay and, at the latest, within the time limits prescribed by applicable regulations. In certain cases, especially where prescribed by law, the exercise of certain rights may be limited, of which the Company will inform the user in an appropriate manner.

The user has the right to lodge a complaint with the competent supervisory authority for personal data protection if the user believes that their personal data are being processed contrary to applicable regulations. In the Republic of Croatia, the supervisory authority is the Croatian Personal Data Protection Agency (AZOP).

11. Changes to the Notice

The Company may periodically update this Notice in order to align it with changes in processes, technology or regulations.

The updated version will be made available to users before and during the use of the devices.

Date of last update: 01.07.2026.