DATA PROTECTION POLICY

The data controller - Electrocoin d.o.o., with its registered seat at Ilica 15, Zagreb 10 000, PIN: 45841695639 (hereinafter: "EC"), is dedicated to protecting your privacy and personal data. In accordance with the General Data Protection Regulation of the European Union 2016/679 (hereinafter: "Regulation"), our Data Protection Officer - Satya Perk, available at dpo@electrocoin.eu, ensures compliance with the highest data protection standards.

1. FOCUS ON DATA PROTECTION

Your privacy is our priority. EC is committed to preserving and protecting your personal data, adhering to the highest standards required by the General Data Protection Regulation (GDPR) of the European Union.

2. PURPOSES AND TYPES OF DATA

a) Services of the electrocoin.eu platform:

When users use the services available on the electrocoin.eu platform, various data are collected to ensure the security and legality of transactions. This data includes:

Transaction Amount: Essential for recording the value of a purchase or sale.
IBAN: Used to carry out transactions.
Wallet Address : A unique address for sending or receiving cryptocurrencies.
PIN: Required to identify the natural or legal person participating in the transaction.
Name of recipient or payer: Important for recording and verifying transactions.
E-mail: Serves for communication and notifications related to the transaction.
Cookie specifications and copy ID: Used to improve user experience and security on the web.
Docusign and Onfido (identification data): Platforms for electronic signature and identity verification, increase the security and authenticity of transactions.

b) Chat channels (information or help with buying and selling cryptocurrencies and using services):

Chat channels provide a platform for communication and support for users during the process of buying and selling cryptocurrencies and using platform services. Data collected includes:

Crisp, Google & Facebook session logins: Allows users to easily log in and interact through these platforms.
Post-Session User ID: Maintains user anonymity and security, reducing the amount of personal data retained after a chat session ends.
Other chat channels (Telegram, Whatsapp, Viber, Facebook): These platforms provide additional options for communication, each with its own set of security and privacy measures.

All this data is collected for the purpose of providing services while respecting user privacy

c) E-mail notifications (informing about transactions):
When users initiate any transaction, they receive an e-mail with the details of the transaction and a confirmation of the completed transaction, if applicable. These email messages serve as official documentation and a record of the transaction, providing users with transparency and a reliable record of their cryptocurrency activities.

d) Newsletter (for the purpose of general information of respondents):
Newsletters are sent to users who have given their consent to receive such information. Consent can be revoked at any time, either through the option in the header of the received e-mail or by contacting the Data Protection Officer directly. Newsletters serve as a means of informing users about news, changes in the data protection policy, news related to cryptocurrencies and similar topics.

e) PayCek (payment with cryptocurrencies at the point of sale):
When using PayCek to pay with cryptocurrencies at points of sale, various data are collected to process transactions. This includes the Wallet Address for the transaction, the amount to be paid, a randomly generated identification string that serves as a unique identifier for the transaction, the customer's email address for communication purposes, and the payment and completion timestamps of the transaction. This data enables secure and efficient payment processing and provides a trail for possible monitoring and verification of the transaction.

f) Notification system (informing respondents about rights and obligations):
In the context of the notification system, the data collected includes the user's IP address. This is used to ensure security and protect against misuse. Also, the documentation required for the identification of the respondent is collected, which may include personal documents or other forms of identification. These procedures help establish transparent communication with users, informing them of their rights and obligations in connection with the use of services.

g) Website - cookies (for the purpose of functionality):
On websites, cookies are used to improve user experience and site functionality. Data collected through cookies may include the user's IP address, which helps identify and resolve technical issues. We also collect data about the frequency of access to the website and information about the device from which it is accessed, such as the type of device, operating system and browser. This data provides insight into how users integrate with the website, enabling optimization and adaptation of content and functionality according to user needs.

These adaptations and extensions provide more detailed insight into the types of data that are collected and their purpose, thereby increasing transparency and understanding of users about the ways in which their data is used and processed.

3. LAWFULNESS OF DATA COLLECTION AND PROCESSING
The collection and processing of data are based on a lawful basis to ensure that the handling of personal data complies with relevant legislation. These lawful grounds include:

1. Consent: In cases such as sending a newsletter (as specified under point 2.d), EC collects and processes data based on the express consent of the user. This means that users actively consent to the processing of their data for specific, clearly defined purposes.

2. Necessity for the performance of a contract or preparing for a contractual relationship: For the services provided by the platform, the use of chat channels for support, notifications about transactions via email, payments and withdrawals of cryptocurrencies or fiat currencies (mentioned under points 2.a, 2.b, 2.c, 2.e, and 2.f), data processing is necessary for the execution of the contract or for taking steps at the user's request before concluding the contract.

3. Fulfillment of EC's legal obligations: In certain cases, EC must process certain data in order to fulfill its legal obligations. This includes compliance with regulatory requirements, tax laws and other legal regulations.

4. Notification system and website - cookies: As stated under points 2f and 2g, the processing of data such as IP addresses and information about the access device is necessary for the functionality of the website and the notification system, and for informing respondents about their rights and obligations.

Each of these lawful bases ensures that EC handles personal data in a transparent and accountable manner, protecting the rights and interests of data subjects in accordance with applicable data protection laws.

4. STORAGE PERIOD

In accordance with the data protection policy, EC determines the retention period of personal data based on several key factors:

1. Duration of the contractual relationship or performance of the service: EC retains personal data for the duration of the contractual relationship with users or as long as it is necessary to provide services. This means that the data will be kept as long as the contract is active or until the services are fully performed.

2. Legal obligations: After the expiration of the contractual relationship or the performance of the service, the data is stored until the expiration of all legal storage obligations. This ensures that EC complies with relevant regulatory requirements.

3. Consent: When data is collected based on the consent of the user, EC will act in accordance with the current status of that consent. If the user withdraws his consent, EC will stop processing and storing the related data.

4. Storage period for Transaction Data: Specifically for transaction-related data, EC adheres to a statutory retention period of 11 years. This is in accordance with legal requirements to keep records of financial transactions.

5. Data about the device and access to the service: Information related to the user's device and access to the service (such as data collected through the SessionID cookie) is deleted after the expiration of the SessionID cookie. This helps preserve user privacy and ensures that data is not retained longer than necessary.

EC strictly follows these data storage guidelines, ensuring that users' personal data is retained only as necessary and in accordance with legal requirements and privacy best practices.

5. RIGHTS OF THE DATA SUBJECT

EC recognizes and respects the following rights of data subjects in relation to their personal data. These rights can be exercised by contacting the Data Protection Officer, and the EC is obliged to respond to the data subject's request within 30 days. In exceptional cases, this term can be extended to 60 days, but only with prior written notification to the respondent.

1. Access to personal data: Subjects have the right to receive confirmation of whether their personal data is being processed and to access this data.

2. Rectification: In case of inaccuracy of data, subjects have the right to request correction of this data.

3. Deletion ("right to be forgotten"): Subjects may request the deletion of their personal data in certain circumstances.

4. Restriction of processing: Subjects have the right to request restriction of the processing of their data, which means that EC will be able to store the data, but not continue to process it.

5. Transfer of personal data: Subjects have the right to transfer their data to another controller ("right to data portability").

6. Objection to processing: Data subjects may object to the processing of their data when the processing is based on the legitimate interest of EC, including objections to direct marketing.

7. Objection to automated profiling: Data subjects have the right not to be the subject of a decision based solely on automated processing, including profiling, which produces legal effects relating to them.

8. Withdrawal of consent: If the processing is based on consent, data subjects have the right to withdraw their consent for data processing at any time.

9. The right to file a complaint with the supervisory authority: Subjects have the right to file a complaint with the supervisory authority if they believe that the processing of their data violates data protection regulations.

EC undertakes to ensure that all these rights are easily accessible and clearly communicated to its users, and that requests for the realization of these rights are processed quickly and efficiently.

6. THIRD PARTIES AND DATA PROTECTION

In the context of ECa's business operations, handling of personal data and interaction with third parties is regulated through partnership relations and cooperation agreements. Key points of this policy include:

1. Cooperation agreements: EC maintains partnership relations with various entities, which it formalizes through cooperation agreements. These agreements are the basis for any exchange of data between EC and its partners.

2. Section on data protection in contracts: Every cooperation contract includes a special section dedicated to data protection. This part of the agreement ensures that all EC partners handle personal data in accordance with applicable data protection laws and regulations.

3. Non-transfer of data to third parties: EC undertakes not to forward personal data to third parties that are not covered by the cooperation agreement. This means that the user's personal data will not be shared with external entities without a clear legal basis or the necessary consent of the subject.

4. Protection of the rights and privacy of users: This policy ensures the protection of the rights and privacy of EC users. EC assumes responsibility for all data shared with partners to be protected and processed with the same level of security and confidentiality as within the organization itself.

EC thereby demonstrates its commitment to the protection of personal data and transparency in its operations, ensuring that all data are used exclusively for the purpose for which they are intended and in accordance with the highest standards of data protection.

7. SECURITY OF DATA PROCESSING

EC implements strict security measures to ensure the protection of personal data during its collection and processing. Key aspects of this policy include:

1. Principle of integrated data protection: EC applies the principle of integrated data protection, which means that security measures are built into all data collection and processing processes from the very beginning. This ensures that data protection is not considered an afterthought, but an integral part of all data processing operations.

2. Education of employees: EC implements regular education programs for its employees with the aim of ensuring high awareness and understanding of the importance of data protection. This training includes familiarization with the rules and procedures of data processing, as well as with possible risks and methods for their prevention.

3. Compliance with the Regulation: EC has harmonized its services and processes with the measures prescribed by the relevant Regulation). This includes the application of appropriate technical and organizational measures to ensure the integrity and confidentiality of personal data.
4. Continuous improvement of security measures: EC continuously monitors and evaluates its security procedures and measures to ensure that they comply with the latest security standards and practices. This includes regular audits, vulnerability testing and upgrades to security systems.

5. Records of data collection and processing activities: EC keeps detailed records of all data collection and processing activities. This record is available to the supervisory authority, which ensures transparency and enables supervision of the handling of personal data.

6. Protective measures for devices: Devices used for data collection and processing are equipped with appropriate security measures. These measures include antivirus software, firewalls, regular security updates and other technological controls.

7. Physical protection of sensitive documentation: Sensitive documentation is stored in secure, locked and monitored locations. Access to these documents is limited to authorized persons.

8. Records of access to the server (Log System): Every access to EC servers is recorded in the log system. This system provides a detailed record of all activity, including unauthorized access attempts.

9. Additional security measures: Using a VPN (Virtual Private Network) ensures secure communication and data transfer. The use of a firewall additionally protects the network from external threats and unauthorized access. Data encryption is carried out in accordance with the prescribed instructions, which means that all sensitive data are encoded to prevent their reading or modification by unauthorized persons.

These measures ensure that the processing of personal data in EC is secure, transparent and in accordance with the highest standards of data protection, thereby protecting the rights and privacy of users.

8. IMPLEMENTATION OF THE GENERAL DATA PROTECTION REGULATION
EC actively implements and aligns its data collection and processing procedures with the General Data Protection Regulation and adheres to the following key principles:

1. Minimum Data Volume:

- Data collection is limited to what is strictly necessary to achieve the defined purposes.
- This practice ensures that no more data is collected than necessary.

2. Compliance with the Prescribed Purposes:
- Any data collection is done with clearly defined and lawful purposes, in accordance with the Regulation and this Policy.

3. Compliance with the Principles of the Regulation:
- EC adheres to all the principles prescribed by the Regulation, including legality, transparency, expediency, accuracy, storage limitation, integrity and confidentiality.

4. Territorial Integrity:
- Data collection and processing takes place within defined territorial boundaries - EU, ensuring compliance with local laws and regulations.

5. Integrated Data Protection:
- Measures have been implemented to ensure the full scope of data protection, from system design to its operational functioning.

6. Pseudonymization:
- Parts of the system are subject to pseudonymization in order to further protect the identity of the respondents and ensure a higher level of privacy.

7. Access to Information and Rights of Respondents:
- The data protection officer enables respondents to exercise their rights, including access to their own data, their correction, deletion and other rights prescribed by the Regulation.
- Respondents can request monthly reports, a summary of the Data Protection Impact Assessment, as well as any assistance or clarification regarding rights and details of the Data Protection Policy.

With this practice, EC not only fulfills legal obligations, but also demonstrates its commitment to high standards of protection and respect for the privacy of personal data of its users.

9. COOKIE SPECIFICATIONS

EC uses various cookies on its website to improve user experience, security and functionality. Here is a detailed overview of the cookies used and their specifications:

1. _cfduid (CloudFlare)
- Purpose: Security
- Duration: 30 minutes
- Function: Used to protect a website from DDOS attacks by identifying individual clients behind a common IP address.

2. crisp-session (Crisp)
- Purpose: Chat
- Duration: Until the end of use
- Feature: Allows users to use chat functionality for help and support.

3. _ga, _gid (Google)
- Purpose: Analytics
- Duration: 2 years
- Function: These cookies create anonymous visit statistics, helping to understand how users use the website.

4. onfido-js-sdk-woopra (Onfido)
- Purpose: Checking the document
- Duration: 2 years
- Function: Used to enable document verification within the Onfido platform.

5. cookieconsent_status (Internal)
- Purpose: Functionality
- Duration: 72 hours
- Function: Saves information about the user's consent status for the use of cookies.

6. cookie test (Internal)
- Purpose: Functionality
- Duration: 72 hours
- Function: Checks the user's ability to accept cookies on the device.

7. csrftoken (Internal)
- Purpose: Security
- Duration: 72 hours
- Feature: Helps prevent CSRF (Cross-Site Request Forgery) attacks on a website.

8. sessionid (Internal)
- Purpose: Functionality
- Duration: 90 days
- Function: Used to maintain a user's session within the system, allowing them to remain logged in.

EC uses these cookies to ensure an optimal browsing experience, improve website security and provide users with relevant functionality. Users have the ability to manage their cookie settings and can withdraw their consent at any time.