Privacy Policy
Bitcan sp. z o.o.
dated July 2025

I. Introduction

1. This Privacy Policy, i.e., the policy on the processing of personal data, applies to the processing of personal data of individuals who are:
   - users of the website,
   - visitors to the website,
   - visitors to the Administrator's social media accounts.
2. This Privacy Policy sets out how, why, and on what legal basis the Administrator processes the personal data of the data subject, as well as how the right to privacy of that individual is protected.
3. The Administrator processes personal data in accordance with the applicable legal regulations, including Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: "GDPR"), the Polish Data Protection Act of 10 May 2018, as well as the Electronic Communications Law of 12 July 2024.

II. Definitions

The following definitions apply in this Privacy Policy:

- **Controller** – the entity that determines the purposes and means of the processing of personal data. In this Policy, the Controller refers to Bitcan spółka z ograniczoną odpowiedzialnością with its registered office in Poznań (60-623), at Podlaska 15 St., entered into the Register of Entrepreneurs of the National Court Register maintained by the District Court for Poznań – Nowe Miasto i Wilda in Poznań, 8th Commercial Division of the National Court Register, under KRS number: 0000808472, tax identification number (NIP): 6292495068, statistical number (REGON): 384619443, with a share capital of PLN 10,500.00.
- **Personal Data** – any information relating to an identified or identifiable natural person ("data subject"), including, but not limited to, identification, address, and contact details.
- **Third Country** – a country outside the European Union (EU) and the European Economic Area (EEA).
- **Processor** – an entity that processes personal data on behalf of and under the instructions of the Controller.
- **Website** – the website available at https://ari10.com, through which the User may: browse its contents, subscribe to a newsletter, contact the Controller using the provided contact details or contact forms available on the Website, as well as access the services offered by the Controller.

- **Services** – services offered by the Controller, consisting of the exchange between virtual currencies and fiat currencies, as well as the exchange between virtual currencies.
- **User** – a natural person who uses the services available on the Website, expresses interest in them, or visits the Website.
- **Joint Controller** – an entity that jointly determines, together with the Controller, the purposes and means of the processing of personal data – *ARI10 sp. z o.o.* with its registered office in Poznań, at ul. Jana Henryka Dąbrowskiego 77A, 60-529 Poznań, entered into the Register of Entrepreneurs of the National Court Register maintained by the District Court for Poznań – Nowe Miasto i Wilda in Poznań, 8th Commercial Division of the National Court Register, under KRS number: 0000837013, REGON: 385893198, NIP: 7831815010, with a share capital of PLN 100,050.00.

III. Contact

Contact with the Controller

You may contact the Controller using the following methods:

- by post – ul. Podlaska 15, 60-623 Poznań, Poland
- by telephone – +48 760 701 396
- by e-mail – office@ari10.com

Contact with the Data Protection Officer

You may contact the Data Protection Officer (DPO) using the following methods:

- by post – ul. Podlaska 15, 60-623 Poznań, Poland, with the annotation: "Data Protection Officer"
- by e-mail – iod@ari10.com

IV. Methods of Collecting Personal Data

1. **Personal data collected directly from data subjects**, i.e., through:
   - completion of a contact form when submitting an inquiry via the website,
   - completion of a newsletter subscription form,
   - provision of personal data for the purpose of preparing, concluding, and performing a contract using available communication channels,
   - provision of personal data as part of the user verification procedure (KYC – Know Your Customer or KYB – Know Your Business) conducted by the Controller, in accordance with the applicable provisions of the Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing,
   - provision of personal data for the purpose of transferring due funds or crypto-assets.
2. **Personal data collected from third parties**, insofar as permitted by applicable laws and regulations, including:
   - a business user to whom the data subject is connected,
   - payment service providers or other financial service providers,
   - public databases, such as the relevant Chamber of Commerce, the Central Register of Beneficial Owners / Transparency Register (or equivalent), Google searches, and

other reliable and independent sources. The Controller may also receive such public information through third-party service providers,
- publicly available transaction data from service providers.

3. **Personal data collected automatically**, for example – each time you interact with the Controller's Website. Automatically collected data includes:
   - information on how the Controller's Services are accessed and used, such as the User's IP address,
   - when and for how long the Website is visited, which subpages are accessed, which links are clicked, and technical information (e.g., browser type and operating system).

V. Scope of Processed Personal Data

1. The scope of the personal data processed is limited to what is strictly necessary:

a) Users of the Website and the Controller's Services:

- **Identification and contact details**: email address, full name, phone number, and identification number (e.g. PESEL).
- **Demographic and personal data**: date of birth, nationality, country of birth, and residency status.
- **Identity document data**: details from an identity card, passport, residence permit, or other identification document (including number, series, expiration date, place and country of issuance).
- **Additional information**: image (captured via photo or video) for the purpose of verifying the User and applying financial security measures (video verification).
- **Location and activity**: full residential address (street, building/apartment number, postal code, city, country), utility bill data, business activity information, and source of funds.
- **Login and transaction history**: data on successful and unsuccessful login attempts and transaction details related to the provided Services are recorded.
- **Security and crime prevention**: data collected for the purposes of fraud detection and anti-money laundering measures, including payment data used to verify transactions.
- **Corporate data (for business Users)**: in addition to the above, data is processed regarding the type of business activity, company name, tax identification number (NIP), registration number, REGON, country of operation, date of establishment, website address, as well as information about directors, beneficial owners, and shareholders (including ownership structure and number of shares).

b) Data of visitors to the Website – particularly the IP address, transaction data, deposit and withdrawal addresses, information about the computer or mobile device, frequency, time, operating system, browser type, device type, unique device identifier, identifying cookies, optionally form data, performance data, and third-party cookies.

c) Data of individuals interested in the Services – persons contacting the Controller provide the data included in their message, such as name, surname, and email address.

d) Data provided in contact forms or through contact details published on the Website – email address, phone number, name, and any additional data voluntarily submitted by the data subject.

e) Persons subscribing to the newsletter – name and email address.

f) Data required for the preparation, conclusion, and performance of a contract with the Controller and for the provision of Services by the Controller – name, surname, residential address, ID number, PESEL number. The provision of this personal data is a condition for the preparation, conclusion, or performance of the contract; although it is voluntary, failure to provide it may prevent the preparation, conclusion, or performance of the contract.

2. In connection with the introduction of new functionalities and Services, or changes to applicable legal provisions, the Controller may request the User to provide additional information. In such cases, a separate notice will be provided concerning the purposes, scope, and legal basis for such additional processing of personal data. Where necessary, this Privacy Policy may also be updated accordingly.

VI. Purposes of Personal Data Processing

3. The Controller processes personal data when permitted by applicable law, including for the following purposes:
    - **Preparation and performance of a contract** to which the data subject is a party, including the exercise of rights arising from such a contract (e.g. non-performance, withdrawal from the contract), the provision of Services to that person, and taking steps at the request of the data subject, such as responding to inquiries sent via electronic communication or handling correspondence received by post. This processing is carried out pursuant to Article 6(1)(b) of the GDPR – processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
    - **Compliance with legal obligations** imposed on the Controller, for example under the Act on Counteracting Money Laundering and Terrorist Financing, the Accounting Act, or the Tax Ordinance. This processing is carried out pursuant to Article 6(1)(c) of the GDPR – processing is necessary for compliance with a legal obligation to which the Controller is subject.
    - **Sending of marketing information** (including marketing of the Controller's own products and Services) electronically to the email address provided by the User. This processing is carried out on the basis of the User's consent, pursuant to Article 6(1)(a) of the GDPR and Article 398 of the Act of 12 July 2024 – Electronic Communications Law.
    - **Improving the quality of Services provided by the Controller**, tailoring services to Users' needs, responding to requests, increasing the efficiency of the Website and Services, ensuring the security of the Website, and sending newsletters. This processing is based on Article 6(1)(f) of the GDPR – processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party.
    - **Establishing, exercising, or defending legal claims** by the Controller or the data subject. This processing is based on Article 6(1)(f) of the GDPR – processing is necessary for the purposes of the legitimate interests pursued by the Controller or by the data subject.

4. The provision of personal data by Users for the purposes listed in points 1, 2, 4, and 5 above is voluntary but necessary to use the Services provided by the Controller via the Website, including the conclusion of relevant contracts. Some data is collected pursuant to separate legal provisions applicable to the Controller, particularly the Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing, for the purpose of ensuring financial security.

VII. Recipients of Personal Data

1. The Controller may disclose and share necessary personal data with third parties based on written data processing agreements. Such data processors may include, in particular: IT service providers, audit firms, accounting offices, law firms, employee outsourcing providers, providers of user service software, providers of email and data collection, analysis, and archiving services, and server hosting service providers. These processors are contractually obligated to implement appropriate technical and organizational security measures to protect Users' personal data and to process such data in accordance with the Controller's instructions.
2. As part of one of its Services, where the Controller enables payments by converting crypto-assets into fiat currency in e-commerce stores, the Controller cooperates with *Moneda sp. z o.o.*. For this product, the Controller shares personal data of the User and individuals associated with the third party implementing this product with Moneda. Moneda gains access to the above-mentioned personal data in connection with the IT solution provided to the Controller. Under this cooperation, Moneda acts as a data processor.
3. The Controller may also share personal data with third parties that process such data for their own purposes (and are therefore not classified as processors, but as "Other Controllers") in strictly defined circumstances:
    - The Controller shares personal data with a Joint Controller who owns and provides the IT system of the group and enables the Controller to use the Services. The Joint Controllers are jointly responsible for the processing of personal data and jointly determine the purposes of such processing.
    - The Controller may share personal data if required, and to the extent required, for compliance with applicable (European or Polish) laws and regulations, including in support of the Polish Financial Supervision Authority (UKNF) or other relevant supervisory authorities, law enforcement agencies, and, where necessary, to assist in combating fraud and other types of abuse, to the extent provided for by law.
    - The Controller is legally obliged to include certain personal data of the User in financial administration records, which must be made available to the national tax authority. The tax authority will process this personal data in accordance with its own privacy policy.
    - When a card payment is made, the Controller is required to share personal data, including the name, address, and card number, with financial institutions such as Mastercard or Visa.
    - If the Controller becomes subject to a sale, merger, or other transaction, it may also share personal data with the entity with which it intends to conclude the relevant agreement.

- If the Controller is required or chooses to conduct an audit, it may share personal data with professional auditors.
- In complex legal matters, the Controller may refer the case to external lawyers or law firms and may also share personal data with their professional legal advisors.

4. Additionally, the Controller shares personal data if required, and to the extent required, to comply with applicable (European or Polish) laws and regulations, including in support of the Polish Financial Supervision Authority (UKNF), other relevant supervisory authorities, law enforcement agencies, and tax authorities, and, if necessary, to assist in combating fraud and other types of abuse, as provided by law.

VIII. Profiling and Automated Decision-Making

1. Profiling refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict the User's economic situation, reliability, behaviour, location, or movements.
2. Personal data will not be subject to profiling or automated decision-making.

IX. Retention Period for Personal Data

1. The Controller processes personal data for no longer than is necessary for the fulfilment of the processing purposes and as permitted by applicable legal regulations. Once the processing purpose has been fulfilled, the personal data will be deleted or irreversibly anonymised, unless otherwise required by law. The retention period depends on the legal basis and the purpose for which the personal data was collected.
2. The retention period is determined by the specific purpose of processing. Below is an illustrative (non-exhaustive) list of data retention periods:

- **Conclusion and performance of a service agreement** – for the period necessary to document the performance of the contract, i.e. **5 years** from the end of the calendar year in which the tax payment deadline expired, pursuant to Article 112 of the Act of 11 March 2004 on Value Added Tax, in conjunction with Article 70 of the Tax Ordinance Act of 29 August 1997.
- **Information collected during the user verification process (KYC – Know Your Customer or KYB – Know Your Business)** – for as long as the User remains contractually associated with the Controller and for an additional **5 years**, in accordance with the requirements of the Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing.
- **Sending commercial information electronically (newsletter)** and/or account registration on the Website – until the consent is withdrawn, without affecting the lawfulness of processing based on consent before its withdrawal.
- **For the purpose of responding to inquiries submitted via the contact form or by phone** – for the period necessary to provide a response, but no longer than **6 months**, unless the person decides to enter into a contract with the Controller.
- **For the purpose of pursuing claims**, based on Article 118 of the Act of 23 April 1964 – Civil Code. Unless a specific provision states otherwise, the limitation period is **six years**, and for claims for periodic performance and those related to business activity – **three years**.

X. **Transfers of Personal Data Outside the European Economic Area (EEA)**

1. In certain cases, the Controller uses the services of various IT providers, business partners, consultants, etc. from third countries, who may be granted access to personal data if necessary, even though such data is generally not stored in those third countries. In such cases, IT providers, partners, etc., are subject to data processing or data sharing agreements that require them to process personal data solely in accordance with the GDPR and data protection laws applicable within EU Member States. The Controller primarily selects providers/partners who process personal data in EU/EEA countries, secondly those located in countries included in the European Commission's list of countries ensuring an adequate level of data protection (so-called "adequate countries"), and only if necessary, providers from other third countries.
2. If the Controller transfers personal data to parties in countries that have been recognized by the European Commission as providing an adequate level of protection, the Controller relies on the Commission's adequacy decision in accordance with Article 45 of the GDPR.
3. If the Controller transfers personal data to parties located in the United States, it may rely on entities certified under the EU-U.S. Data Privacy Framework, in accordance with Article 45 of the GDPR.
4. If personal data is transferred to other third countries, the Controller may rely on the European Commission's Standard Contractual Clauses (SCCs) or the business partner's Binding Corporate Rules (BCRs), accompanied by the implementation of appropriate supplementary safeguards, or it may assess local laws to ensure that personal data receives a level of protection essentially equivalent to that guaranteed within the EU/EEA. Where such transfers are necessary, the legal basis for the transfer is Article 46 of the GDPR.
5. The Controller may also transfer personal data to recipients outside the EU/EEA based on specific derogations provided under Article 49 of the GDPR – for example, Article 49(1)(e) of the GDPR, where the transfer is necessary for the establishment, exercise, or defence of legal claims.

XI. **Security Measures**

1. The Controller stores and protects personal data in accordance with the principles set out in applicable legal regulations. The Controller takes appropriate measures to:
    - ensure the protection of personal data against loss, unauthorised access, use, destruction, modification, or disclosure;
    - implement appropriate technical and organisational safeguards;
    - protect personal data in accordance with the level of risk and the nature of the data, including special categories of personal data.
2. Taking into account the state of the art, implementation costs, nature, scope, context, and purposes of the processing, as well as the rights and freedoms of natural persons, these measures include, in particular: pseudonymisation and encryption of personal data; measures ensuring the ongoing confidentiality, integrity, availability, and resilience of processing systems and services; measures enabling the restoration of access to personal data in the event of a physical or technical incident; and procedures for regularly testing, assessing, and evaluating the effectiveness of security measures.

XII. Rights of Data Subjects

1. Data subjects have the following rights:
    - the **right of access** to their personal data, including the right to obtain the first copy of the personal data free of charge;
    - the **right to rectification** of personal data that is inaccurate, incorrect, or has changed;
    - the **right to erasure** of personal data, unless legal provisions require the Controller to retain such data for a specified period;
    - the **right to data portability**;
    - the **right to withdraw consent** to the processing of personal data where such processing is based on consent. Withdrawal of consent does not affect the lawfulness of processing carried out before its withdrawal;
    - the **right to object** to the processing of personal data on grounds relating to their particular situation, where the processing is based on Article 6(1)(e) or (f) of the GDPR, as well as the right to restrict processing;
    - the **right to obtain information** about the processing of their personal data, including the identity of the Controller, the purpose, scope, and method of processing, the content of the data, the source of the data, and the recipients or categories of recipients to whom the data is disclosed.
2. To exercise the right to information, access, rectification, or any other rights, the data subject may contact the Controller using the contact details provided in this Privacy Policy.
3. The data subject also has the right to lodge a complaint with the **Polish Data Protection Authority (UODO)** if the processing of their personal data violates the provisions of the GDPR. Complaints may be submitted electronically or in writing to the following address: **President of the Personal Data Protection Office**, ul. Stawki 2, 00-193 Warsaw, Poland.
4. If the data subject's place of residence or the location of the alleged violation is in a Member State other than Poland or is otherwise connected to another Member State, the complaint may also be submitted to the data protection authority in that Member State. The data subject also has the right to bring a case before a court of law.

XIII. Personal Data of Individuals Under the Age of 18

The Controller's Services are not intended for individuals under the age of eighteen (18). If you are under 18 years of age, you may not use the Controller's Services or provide us with your personal data. If the Controller becomes aware that personal data of an individual under the age of 18 is being processed, such data will be deleted without delay. If there is any suspicion that the Controller is in possession of such data, please contact the Controller immediately.

XIV. Final Provisions

In the event of any changes to this Privacy Policy, particularly if required by implemented technical solutions or amendments to data protection laws, the Controller will introduce appropriate

modifications to this Privacy Policy (GDPR). Such modifications will become effective **14 days after their publication on the Website**.

If the changes in the processing of personal data have an **individual and significant impact** on a data subject, the Controller will take appropriate steps to inform the individual about such changes in order to allow them to exercise their rights.