# Policy for the Protection of Personal Data When Providing Trust Services

Identifier: **PL-PD-1**
Version: **1 / 01.05.2025**
Classification: **C1 / PUBLIC DOCUMENT**

# Contents

# 1. Introduction

This policy describes how personal data is collected, processed, and stored. It applies to the trust services provided by BORICA AD.

Any amendments or additions to this policy will take effect after they are published on the website: http://www.b-trust.bg.

# 2. Terms and Abbreviations

***Personal data controller*** is any natural or legal person who determines the purposes and means of processing personal data. If the purposes and means of such processing are determined by European Union or Member State law, then the controller or the criteria for its determination may be specified in that law.

***Personal data*** is any information relating to an identified or identifiable natural person ("data subject"). Identification may be direct or indirect, for example by reference to a name, identification number, location data, online identifier, or one or more factors specific to the person's physical, physiological, genetic, mental, economic, cultural, or social identity.

***Personal data processing*** refers to any operation or sets of operations performed on personal data or sets of personal data, whether by automatic means or otherwise. This includes activities such as collection, recording, use, disclosure by transmission, dissemination, arrangement, combination, restriction, erasure, or destruction.

***Pseudonymization*** is the processing of personal data in a way that prevents its association with a specific natural person, without the use of additional information. The additional information must be stored separately and be subject to the appropriate technical and organizational measures to ensure that the personal data cannot be associated with an identified or identifiable person.

***Data subjects*** are natural persons who request and/or use the trust services of BORICA AD in their personal capacity or as legal or authorized representatives of a natural or legal person. Their data is processed in connection with the provision of trust services and the conclusion of a contract (they are referred to as "clients").

***Consent of the data subject:*** any freely given, specific, informed, and unambiguous indication by which the data subject signifies agreement to the processing of personal data relating to him or her.

***Applicable laws and regulations*** include legal acts of the European Union, such as the General Data Protection Regulation (GDPR) (EU) 2016/679, the Personal Data Protection Act, and the Electronic Document and Electronic Certification Services Act. These acts apply to the processing of personal data.

***A registering authority*** is either a separate entity of BORICA AD, or an external legal entity (subcontractor) entrusted by the company with providing user registration, identification, and identity verification services.

***EGN*** stands for Bulgarian Unified Civil Number. It is a unique 10-digit number assigned to each Bulgarian citizen. It serves as a national identification number.

# 3. Personal Data Controller

BORICA AD is the personal data controller within the meaning of the applicable legislation. The company's identification data are as follows:

- UIC 201230426.
- Registered office and address: Sofia 1612, Krasno Selo District, Tsar Boris III Blvd. 41.
- Corporate website: http://www.borica.bg.
- Email: office@borica.bg.
- Contact Center: support@borica.bg
- Phone: 0700 199 10, *9910

# 4. Personal Data Processed Depending on the Method of Providing Trust Services

Depending on how trust services are requested and provided, BORICA AD processes different types of personal data, such as identification, contact, biometric, and payment information, as outlined below:

## 4.1 For services provided upon personal appearance at an office of a Registration Authority of BORICA AD

The following data are processed for identification and confirmation of identity:

- Names (according to the identity document), EGN/foreigner's personal number, date of birth (for foreigners), address, telephone number, and email address.
- Data of the authorized person (names, EGN, address, etc., as contained in the authorization document).
- Number, date of issue, and validity period of the identity document.
- Data extracted from national registers of primary data controllers when performing an official check of the identity document's validity and the individual's vital status, as well as data automatically extracted from the machine-readable part of the document.
- Data from payments made by the client for services provided, including bank account numbers and other payment information.

## 4.2 For services provided through the B- Trust Mobile application

The following data are processed for identification and confirmation of identity:

- Names (according to the identity document), EGN, date of issuance and validity of the identity document, issuer of the identity document, gender, date of birth, nationality, address, telephone number, and email address.
- Biometric data:
  - An electronic copy (photo) of the identity document including all data automatically downloaded from its machine-readable part.
  - Video recording of the person with a text/code pronounced by him or her.
  - A photo of the person extracted from the national registers of primary data controllers.
- Data extracted from national registers of primary data controllers when performing an official check of the identity document's validity and the individual's vital status.
- Data from national registers of primary data controllers when an electronic identification service is initiated by the client or a relying party.
- A report on the verification and confirmation of the identity of a natural person during remote video identification, including the results of the correspondence between the scanned identity document, the data from the official check, and the video recording.
- Data used when signing electronic documents via B-Trust Mobile (EGN, telephone number, email address).
- Data collected during authentication in systems and applications.
- Data from payments made by the client for services provided, including bank account numbers and other payment information.

If the client uses the B-Trust Mobile application, he must go through a registration process and remote video identification. Before starting the remote identification process, the client must voluntarily provide personal data, including biometric data. This data will be processed to enable trust services through the application. By checking the box, the client confirms that he or she has accepted the terms of use of his/her personal data. This action, together with continuing the registration process, constitutes an electronic statement under the Electronic Document and Electronic Trust Services Act, indicating acceptance of and obligation to comply with the requirements of this policy.

If clients wish to use B-Trust services but do not want their biometric data processed, they can identify themselves in person at BORICA AD's Registration Authority office and request trust services that do not require a mobile application.

## 4.3 Upon remote identification via the web interface

In order to provide specific services, including the conclusion of contracts via an electronic channel, the

company collects, processes, and stores the following personal data of the client:

**1. Identification data:**

- Names according to identity document.
- EGN (or other national identification number according to the country of issuance).
- Number, date of issuance, validity period, and issuer of the identity document.
- Nationality, gender, and date of birth.
- Address, telephone number and email address.

**2. Biometric data:**

- An electronic copy (photo) of the identity document including all data automatically downloaded from its machine-readable part.
- Video and photos taken during the identification process, including spoken text/code recordings.
- A photo of the person extracted from the national registers of primary data controllers.
- Photos extracted from official national registers if connectivity is available.

**3. Data from official registers:**

- Data extracted during automated verification of identity document validity and vital status.
- Data related to verifying correspondence between the provided data and national registers, including photo matches.

**4. Identification report:**

- Result of verification and confirmation of identity, including degree of correspondence between the data provided and the data obtained from official sources.

By checking a box, the client confirms that he or she has accepted the terms of use of his/her personal data. This action, together with continuing the registration process, constitutes an electronic statement under the Electronic Document and Electronic Trust Services Act, indicating acceptance of and obligation to comply with the requirements of this policy.

# 5. Purposes of Processing

BORICA AD processes the personal data of its clients for the following purposes:

- Providing certification services and managing customer relationships.
- Obtaining preliminary information necessary for concluding a service contract.
- Identifying and confirming the identity of clients using B-Trust certification services.

- Responding to requests for information and complaints, disputes, and clarifications about services used and reports on those services.
- Protecting clients using B-Trust certification services from fraud and abuse by third parties.
- Updating personal data provided upon registration or when concluding a contract for B-Trust services and products.
- Providing technical assistance and support when using B-Trust certification services via telephone, email, or on-site.
- Fulfilling legal obligations and resolving disputes before the competent authority (court, arbitration, conciliation commission, administrative authorities, etc.) in connection with BORICA AD activities.

# 6. Grounds for Processing

BORICA AD processes personal data of its clients on the following grounds:

- **Legal obligation**

To fulfill legal obligations to identify clients and carry out identification checks in accordance with Regulation (EU) No. 910/2014 on electronic identification and trust services, the Anti-Money Laundering Act, and the Payment Services and Payment Systems Act.

- **Performance of contractual relations**

Proper identification upon conclusion of a contract and during its validity period. This processing ensures the lawful use of the agreed-upon products or services and includes notification of important changes to them.

- **Legitimate interest**
  - To improve products and services according to clients' needs and requirements, as well as to improve customer service.
  - To prevent fraud or money laundering in order to protect the business and to comply with applicable laws.
  - Video surveillance is used to collect evidence in criminal situations and to protect clients and employees.
  - In electronic correspondence and telephone records, such as alerts, notifications of lost electronic signature certificates, and inquiries to a contact center.
  - In sending messages about products and services via SMS notifications that are not marketing related.
  - To address complaints and requests and resolve disputes related to the use of certification or payment services.

- **Client consent**

When BORICA AD processes data based on a client's explicit consent, processing is carried out only for the specified purposes and data. Consent may be withdrawn at any time without affecting the lawfulness of processing prior to withdrawal.

# 7. Storage of Personal Data

The retention period for personal data depends on the purpose for which it was collected. BORICA AD processes personal data for the periods established by the country's current legislation. Personal data for which there is no legal obligation to store is deleted once the purposes for which it was collected and processed have been achieved. However, some periods may be extended in certain circumstances, such as in cases of lawsuits, extension of a limitation period due to interruption, implementation of specific legal provisions, and/or requirements of supervisory authorities.

Data submitted in connection with an application for an electronic signature that is not implemented is stored for up to three months after submission to alert company employees of possible fraud attempts. After this period, the data is deleted.

Data used under the Electronic Document and Electronic Trust Services Act is stored for ten years.

| Data Types | Retention Period |
|---|---|
| Personal data collected and stored for provision of trust services and electronic identification | 10 years after termination of the service |
| Personal data collected in connection with the conclusion and performance of contracts | 10 years after termination of the contract |
| Personal data from the process of successful remote identification | 10 years after termination of the service |
| Personal data collected and processed from failed remote identification processes | 3 months after execution |
| Personal data collected and stored in connection with the use of the service for the qualified storage of electronically signed documents (with storage): | this data is stored until it is deleted by the client or until the relevant service is terminated, but for no longer than 10 years |
| Information from communications with clients in relation to the services. | 10 years after termination of service |
| Telephone call records | up to 5 years from the date of the call |

| | |
|---|---|
| Financial and accounting records | up to 10 years after the beginning of the year following payment |
| System logs | up to 3 years from log generation |
| Data processed on the basis of consent | consent is withdrawn |

# 8. Rights of Data Subjects

Data subjects (clients) have the following rights:

- **Right to access their personal data**

  Clients may request access to all personal data stored at BORICA AD. This is the so-called "personal access request". Access to personal data can be obtained by submitting the appropriate request as outlined below.

- **Right to rectify inaccurate or incomplete data**

  Clients may request that BORICA AD correct their personal data.

- **Right to erasure ("right to be forgotten")**

  Clients have the right to request that BORICA AD erase their personal data without undue delay, provided that the conditions of Article 17 of the EU General Data Protection Regulation 2016/679 (GDPR) are met.

- **Right to restriction of processing**

  Clients have the right to request that BORICA AD restrict the processing of their personal data, or to object to such processing.

- **Right to data portability**

  Clients have the right to data portability for their personal data, if applicable, pursuant to Article 20 of the EU General Data Protection Regulation 2016/679 (GDPR).

- **Right to lodge a complaint with a supervisory authority**

  Clients have the right to lodge a complaint with the Data Protection Commission, the supervisory authority, regarding their personal data provided to BORICA AD.

  Clients may exercise their rights by submitting their requests to BORICA AD in writing, either on paper or via email, using the following contact information:

  - Postal address: 41 Tsar Boris III Street
  - E-mail: office@borica.bg

When submitting a written request, clients must unambiguously verify their identity and ownership of the identifier with which they are registered to use the services.

If clients do not agree with how their personal data is managed or used, wish to receive additional

information, or wish to report possible violations of their rights, they may submit a request, complaint, or signal through the contact channels indicated above. All requests received are processed within one calendar month.

If BORICA AD does not provide a satisfactory response, clients have the right to contact the Personal Data Protection Commission at the following address:

1592 Sofia, 2 Prof. Tsvetan Lazarov Blvd.

E-mail: kzld@cpdp.bg.
Website: www.cpdp.bg.

# 9. Personal Data Security Measures

BORICA AD takes a comprehensive approach to protecting personal data, including the following security measures:

- **Technical measures:**

  - *Encryption:* Use of encryption to protect sensitive information during storage and transmission.
  - *Antivirus software:* Applicable to servers and workstations. A regularly updated corporate version of the software is used. It is installed on servers and workstations and receives regular updates.
  - *Network protection (firewalls):* Applied at key locations in the corporate network to control incoming and outgoing traffic and prevent unauthorized access.
  - *Logical Access Control:* Strong passwords, multi-factor authentication, and adequate security policies are implemented. Access to personal data is restricted to authorized employees only.
  - *Regular software updates:* Keeping operating systems and applications up to date to prevent vulnerabilities.
  - *Business continuity:* Maintenance of data backups to quickly restore workflows and services with minimal data loss.

- **Organizational measures:**

- *Security policies:* Documented internal security rules and a personal data protection policy applicable to processing and storing personal information.
- *Employee training:* Conducting periodic training in accordance with the most effective practices within the domains of cybersecurity and personal data protection.
- *Risk assessment:* Assessment and analysis of potential risks, threats, and vulnerabilities, as well as the implementation of appropriate measures to mitigate risks.

- *Confidentiality agreements:* Requiring employees and third parties to sign confidentiality agreements.
- *Incident response plan:* Implemented and regularly tested action plan for security incidents, including data breaches, and established procedures for notifying affected individuals and authorities.

- **Physical measures**

- *Restricted physical access:* Critical systems are located in high-security areas with access control systems and video surveillance.
- *Secure data destruction:* Specialized methods are used to destroy documents and electronic media containing personal information.
- *Monitoring:* Implementation of continuous monitoring of all workspaces to ensure control over the use of portable media for storing information.

BORICA AD considers the protection of personal data a top priority. The company possesses the following internationally recognized certificates:

- ISO/IEC 27001: Information Security, Cyber Security and Privacy Protection
- ISO/IEC 20000-1: Information Technology. Service Management.
- ISO 22301: Security and Resilience. Business Continuity Management Systems.
- ISO 9001: Quality Management Systems.
- eIDAS (Regulation on Electronic Identification and Trust Services)

# 10. Disclosure of Personal Data

In accordance with Regulation (EU) 2016/679, BORICA AD may disclose personal data it possesses to the following categories of recipients:

- The data subjects themselves (natural persons).
- Third parties, including natural and legal persons, public authorities, institutions and establishments, external and internal auditors, insurance companies, supervisory and regulatory authorities, and others, when performing legal or contractual obligations, including the detection and prevention of fraud and money laundering.
- Government institutions, when lawful and explicitly required.
- Subcontractors of BORICA AD, including registration authorities, who provide sufficient guarantees for the implementation of appropriate technical and organizational measures for compliance with Regulation 2016/679.
- Other parties with the consent of the data subject.

# 11. International Transfer of Personal Data

If there is a need to transfer personal data processed by BORICA AD to countries outside the European Economic Area (EEA) or to international organizations, the provisions of EU Regulation 2016/679 shall apply, and this transfer must be documented by contractual clauses.

BORICA AD does not disclose personal data or grant access to it to countries outside the European Union (EU) or the European Economic Area (EEA).

# 12. Contacts

Data subjects may contact BORICA AD at dpo@borica.bg for instructions and assistance in exercising their rights.

This policy is periodically reviewed and updated to ensure compliance with regulatory requirements and good practices.