Principles of Processing Personal Data (Privacy Policy)

Effective from: 10 April 2020

1. General information

These principles of processing personal data describe how EcIdentity LLC (hereinafter referred as " EcIdentity ") as a data controller ensures the protection of personal data in accordance with applicable laws. The aim of these principles is to provide information for the subscribers on the relevant issues related to personal data processing.

These principles do not concern the storage and processing of data of legal persons or other institutions. The person representing the legal person or other institution is not considered a natural person; it is an authorized representative of the legal person or other institution whose personal data is not covered by GDPR.

Should you have any questions relating to the processing of personal data we ask you to contact us using the following contacts:

Data controller:

EcIdentity LLC
Registry code: 14638864
Address: Regati 6c, Tallinn, Estonia
Phone: +372 5811 3062
E-mail: info@ecidentity.io

Data protection officer:
E-mail: dp@ecidentity.io

2. Definitions

Subsequently, we explain the definitions and abbreviations used in the present principles.

2.1. What is GDPR?

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 (GDPR)

Personal data is processed according to GDPR, however, please note, that as trust service provider,

2.2. What are personal data and what is personal data processing?

Personal data are any data concerning an identified or identifiable natural person, regardless of the form or format in which such data exist. Processing of personal data is any act performed with personal data (incl. collection, recording, storage, alteration, granting access to, retrieval and communication, etc.) or several of the operations, regardless of the manner in which the operations are carried out or the means used.

2.3. Who is a third person?

A third person is any person (both legal and natural persons) who is not a contractual client, employee or authorized data processor of EcIdentity.

2.4. What is a data controller?

‘Data controller’ means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Within the context of this document, EcIdentity is the data controller.

2.5. What is a data processor?

'Data processor' means a natural or legal person, public authority, agency or any other body which has been contractually appointed by EcIdentity to process personal data on behalf of the data controller.

2.6. What is a certificate?

Digital data that facilitate identity verification, in which the public key relates to the natural person who owns the certificate. Certificates that enable either electronic identity verification are related to personal data.

2.7. What is an online service?

An online service is an information system, application or e-environment using services provided by EcIdentity (ecid) for authentication of persons.

2.8. What is a registration authority?

'Registration authority' is an organization responsible for the identification and authentication of persons. In addition, a registration authority may accept certificate requests, verify them and/or send them to EcIdentity.

3. EcIdentity's principles on processing personal data

Privacy and personal data protection is very important to us, therefore we have adopted necessary organizational, physical and information technology security measures to ensure the integrity, availability and confidentiality of the data.

We have mapped the personal data we need for service provision and specified the purpose, extent and period of time we need to store such data. We have laid down requirements and instructions for EcIdentity ´s employees and authorized data processors, how to process personal data in a correct way. We grant access to personal data only for trained employees and authorized data processors that have passed a relevant background check. EcIdentity ´s employees and authorized staff are aware that they have the right to process personal data only to the extent necessary for them to carry out their duties or, as is the case with authorized data processors, fulfil the contractual obligations.

We confirm that the processing of personal data is legitimate, fair, fit for purpose, minimal, safe and transparent. All our activities are guided by applicable EU and Estonian legislation, policies and principles of EcIdentity as well as the present principles of processing personal data. The policies and principles of EcIdentity are available on EcIdentity's website: ecIdentity.io/en/privacy.pdf.

4. Sources of personal data

EcIdentity obtains personal data from the following sources:

- From the person;
- Personal devices;

5. Lawfulness of personal data processing

EcIdentity processes personal data only in a fair and lawful way, either for the performance of contracts or on the basis of consent or law. EcIdentity confirms that it only collects personal data for the purposes which have been clearly established and are legitimate, and limits the collection of personal data to the minimum necessary for meeting the objectives of such processing.

6. What personal data and for what purposes we process?

Personal data may only be processed for specific purposes and processing must have a legal basis.

EcIdentity processes personal data on three legal bases: processing is necessary for the performance of an agreement, the data subject has given consent or the processing is necessary for fulfillment of an obligation arising from law.

The processing of personal data for performance of an agreement means that we need personal data to provide a high quality service. We have defined what personal data EcIdentity needs for the provision of the service and we keep the amount of personal data processed to a minimum.

Based on your consent we process your biometric data (facial image) for automatic biometric verification. If you send us a query that contains your personal data, then by sending a query, you give EcIdentity your consent for processing.

Compliance with obligations arising from law is the processing of personal data that we are required to perform as a service provider by law. For example, we process personal data to respond to legally justified queries from investigation authorities.

Below we explain the purpose for processing, legal basis and list of personal data for each action that, where personal data is processed.

Action	Purpose for processing	Legal basis	What personal data is processed?
Issuance and/or servicing certificates	Provision of service	Processing is necessary to fulfill the agreement; Biometric personal data is processed based on consent	1. Person's given name and surname; 2. Personal identification number (also the country that issued the personal identification code); 3. Document number; validity period for the document; document type; e-mail address; 4. A copy of the identity document used for applying the certificate; 5. Selfie which is transmitted to EcIdentity
Queries containing personal data	Responding to query	Consent	Data which is transmitted to EcIdentity
Queries from investigation authority	Responding to query	Law	Data which is demanded by investigation authority

If you use the certificate issued by the EcIdentity for authentication in the online service, we will transfer your personal data to the online service for the purpose of providing the service. We will only transfer your personal information to the online service with your consent, that means, only if you have initiated the authentication transaction by entering the corresponding pin code.

7. Right to obtain information and complaint submission

According to GDPR, a person has the right to access his/her personal data, request rectification, erasure, restriction and data portability.

Information about the operations performed by you with ecid can be obtained via ecIdentity.io. You can get information about your ecid accounts and ecid actions via ecIdentity.io. In addition, you may submit a corresponding request to EcIdentity.

The prerequisite for exercising the rights listed above, is that the person is uniquely identifiable. Therefore, we kindly ask that you submit a corresponding request in electronically signed form to the following e-mail address info@ecIdentity.io. We will respond to the request within 30 days.

We emphasize that the request cannot be met in the following cases:

- the identity of the applicant cannot be identified;

- the applicant is not legally connected with the data;
- this would be contrary to the requirements of special laws;
- this would be in conflict with EcIdentity's legal obligations;
- it may harm the rights and freedoms of another person;
- this may hinder the provision of the service or failure to provide the service;
- this may hinder the work of law enforcement agencies;
- it's not technically possible.

8. Use of data via an authorized data processor

EcIdentity has the right, under the contract, to authorize another person (i.e. both natural and legal persons) to process personal data. Authorized processors are, for example, EcIdentity s partners in issuing and servicing of certificates and solving client issues. EcIdentity as the controller of data provides the authorized processor with necessary instructions for data processing. EcIdentity is responsible for the authorized data processor's compliance with the personal data processing requirements. An authorized data processor may process personal data only for attaining the purpose. EcIdentity confirms that a contract for protection of confidential information and data protection agreements will be concluded with all authorized data processors.

An e-service that requests your personal data from EcIdentity on the basis of authentication initiated by you, is not the authorized processor of EcIdentity under the GDPR.

9. Disclosure or communication of personal data to third persons

EcIdentity does not disclose or issue personal data to third persons unless following cases:

1. Such an obligation arises from applicable legislation or measures adopted there under (e.g. transmission to investigation authority);
2. Such persons are involved in providing the services;
3. EcIdentity has the right for the purposes of performing a contract or ensuring contract performance to disclose the data to third persons, including credit information and debt collection companies and other persons handling debt claims, also to legal advisers and bailiffs if the person has failed to comply with the contract;
4. The person concerned gives his/her written consent to disclose the information to other third persons.

EcIdentity confirms that it will only disclose personal data to third persons to the extent necessary for the purposes for which the personal data are processed.

11. Period of storage of personal data

EcIdentity processes personal data only as long as necessary for fulfilling the purposes for which the personal data was collected or for fulfilling the obligations arising from applicable legislation. Please note that in order to provide trust services, we are guided by Estonian Electronic Identification and Trust Services for Electronic Transactions Act for the storage of personal data. Retention of data and evidence is required under law and verified by independent auditors and supervisory bodies.

12. Amending the principles of processing personal data

EcIdentity has the right to unilaterally alter these principles of processing personal data in accordance with the requirements laid down in applicable legislation. The amendments will be published on EcIdentity 's website ecIdentity.io and will immediately enter into force.