Centralny Punkt Rejestracji Cencert
tel. 22 720 79 55 | 666 028 044
ul. Jagiellońska 78 03-301 Warszawa, II piętro, pok. 345

Cencert Privacy Policy

1. Data Controller

Cencert is a product brand of Enigma Systemy Ochrony Informacji Sp. z o.o.
The data controller within the meaning of the 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 – General Data Protection Regulation) is Enigma Systemy Ochrony Informacji Sp. z o.o., 116 Jutrzenki Street, 02-230 Warsaw, NIP (Tax ID) 5261029614, KRS (National Court Register) entry number: 0000160395.
We have appointed a Data Protection Officer, who can be contacted at iod@enigma.com.pl or, in traditional form, at 116 Jutrzenki Street, 02-230 Warsaw.

2. Purpose and Legal Basis of Processing

We process your data for the following purposes:

1. To fulfil our legal obligations related to the provision of qualified trust services, arising from Article 17 of the Act of 5 September 2016 on Trust Services and Electronic Identification, as well as legal obligations related to tax regulations (legal basis: Article 6(1)(c) GDPR);
2. To prepare or perform a contract for the provision of a trust service of which you are a party (legal basis: Article 6(1)(b) GDPR);
3. To prepare or perform a contract for the provision of a trust service entered into by a third party for your benefit, based on our legitimate interest (legal basis: Article 6(1)(f) GDPR);
4. To handle complaints submitted by you (depending on the circumstances of the complaint – legal basis: Article 6(1)(b), (c), or (f) GDPR);
5. To provide you (at your request) with assistance regarding the services we provide or the products we offer, including technical support (legal basis: Article 6(1)(b), (c), or (f) GDPR);
6. To establish, pursue, or defend against claims, which constitutes the exercise of our legitimate interest (legal basis: Article 6(1)(f) GDPR);
7. For analytical purposes (better tailoring of services to our customers' needs, general optimisation of our products, optimisation of customer service

processes, building knowledge about our customers, financial analysis of our company, etc.), which constitutes the exercise of our legitimate interest (legal basis: Article 6(1)(f) GDPR);

8. To conduct customer satisfaction surveys, which constitutes the exercise of our legitimate interest in determining the quality of our service and the level of customer satisfaction with our products and services (legal basis: Article 6(1)(f) GDPR);
9. To offer you our products and services directly (direct marketing), including tailoring them to your needs (profiling), which constitutes the exercise of our legitimate interest in this respect (legal basis: Article 6(1)(f) GDPR).

3. Right to Object

You have the right to object at any time to the processing of your personal data as described above. We will cease processing your data for these purposes unless we are able to demonstrate compelling legitimate grounds for the processing that override your interests, rights, and freedoms, or grounds for establishing, pursuing, or defending claims.
You also have the right to object at any time to the processing of your data for direct marketing purposes. If you exercise this right, we will stop processing your data for this purpose.

4. Data Retention Period

Your data processed in connection with the fulfilment of the obligation under Article 17 of the Act of 5 September 2016 on Trust Services and Electronic Identification (legal basis: Article 6(1)(c) GDPR) will be retained for the period indicated therein, i.e. for 20 years from the moment the data is generated, and additionally for the time necessary to remove archival copies, not exceeding 2 years.
Your data processed for the purpose of preparing or performing a contract for the provision of a trust service will be retained until the preparation of the contract is completed, and if the contract is concluded – depending on its type – until the contract expires or is fully performed, and additionally for the period of operation of the system delivering the given trust service (e.g. the specific certification authority issuing your certificate).
With respect to personal data processed in connection with the provision of the qualified validation service for electronic signatures and seals, the following rules apply:

- Data contained in signed documents, submitted to our website portal providing the validation service, for the purpose of performing this service, are processed exclusively in an automated process in the server's operating memory in order to perform the necessary calculations for the execution of the validation service, after which they are immediately deleted from memory. This does not apply when the validation service is provided through a "gateway" located in the client's infrastructure – in such case, the data contained in the validated documents are not processed on our servers at all.
- Data contained in reports generated in connection with the provision of the qualified validation service for signatures and seals are retained:
    - on the central servers of the validation service, for 30 days from the generation of the given validation report, and additionally for the backup retention period of up to 6 months, and additionally
    - on the servers operating the website portal providing the validation service (not applicable to the configuration with a "gateway" located at the client's premises), until the report is deleted by the service client, but not longer than 120 days from the generation of the report, and additionally for the backup retention period of up to 6 months.

With respect to personal data that may be contained in documents submitted for signing by Cencert on your behalf, processed in connection with the provision of the qualified remote signature service in the "one-time signature" mode, the following rules apply: data contained in signed documents are processed solely for the purpose of providing the one-time signature service and are deleted from the servers, without retaining copies, after 60 minutes from signing and no later than 120 minutes from the moment the documents were transmitted to the Cencert server.
Your data processed for the purpose of establishing, pursuing, or defending claims will be retained for the period during which claims related to the given contract may arise, i.e. for 4 years from the end of the year in which the contract expired, including 3 years as the maximum limitation period for claims, with an additional year in case of claims lodged at the last moment or delivery issues, with the calculation from the end of the year serving to set a uniform deletion date for contracts ending in the same year.
Data processed for the purpose of providing you with assistance regarding our products and services, including technical support, will be processed for 6 months from the date of generation of such data and additionally for the backup retention period of up to 6 months, except for telephone call recordings, which

are processed for 30 days from their generation and additionally for the backup retention period of up to 6 months.
Data processed in connection with our legal obligations will be retained until such obligations are fulfilled.
Data processed for analytical purposes, customer satisfaction surveys, and offering you our products and services may be processed until you object to such processing, withdraw your consent to be contacted via specific communication channels, or we determine that the data have become outdated.

5. Data Recipients

We may share your data with:

- entities commissioning us to provide specific services on your behalf:
    - data such as reports and summaries concerning services provided in a given period,
    - in the case of certificate issuance services containing your personal data, financed by such an entity (e.g. your employer) – also reports and summaries containing the data included in these certificates and related to the issuance process (such as first name(s), surname, email address, phone number, PESEL number or identity document number, if included in the certificate),
    - in the case of remote certificate issuance or the one-time signature service – if you were redirected to our server from the system of an intermediary entity in the purchase process (e.g. an entity operating a document workflow system requiring a certificate or one-time signature) – the data contained in the signature certificate (first name(s), surname, and possibly PESEL) are provided to such intermediary entity,
- postal and courier companies – for the purpose of delivering shipments,
- electronic payment operators, to the extent necessary to prevent fraud related to payment services, maintain the payment system, and investigate and detect such fraud by competent authorities in accordance with the Payment Services Act,
- Google Ireland Limited – analytical data related to the use of our website, collected through the Google Analytics service, which you may disable,
- entities authorised under generally applicable law.

Your data may also be accessed by entities providing us with various services related to our operations (processors):

- our partners in the provision of trust services, in particular the partners listed at https://www.cencert.pl/punkty-rejestracji/
- IT companies providing maintenance and development of our IT systems,
- telecommunications companies and marketing agencies, providing communication on our behalf via email, SMS (including advertising campaigns), as well as call centre services,
- marketing agencies conducting research or analyses for us,
- companies providing paper document archiving services.

6. Rights of Data Subjects

In accordance with the GDPR, you are entitled to:

- the right to access your data and receive a copy thereof;
- the right to rectify (correct) your data;
- the right to erasure of data, restriction of processing;
- the right to object to data processing;
- the right to data portability;
- the right to lodge a complaint with a supervisory authority.

7. Information on the Requirement/Voluntariness of Data Provision

Providing data is voluntary, but necessary for the performance of certain services.

8. Source of Data

We usually obtain data directly from the data subjects.
We may also receive data necessary for the provision of trust services from entities commissioning us to provide such services for the benefit of the data subjects.
In the case of the qualified validation service for signatures and seals, the data of persons affixing electronic signatures subject to validation are provided to us by the entities commissioning the validation service.

9. Automated Decision-Making

Not applicable.

10. How Do We Protect Personal Data?

We apply technical and organisational measures ensuring the protection of processed personal data as referred to in Article 32 GDPR, in particular by: encrypting personal data during Internet transmission, ensuring the confidentiality, integrity, availability, and resilience of processing systems and services, as well as the ability to quickly restore the availability of and access to personal data in the event of a physical or technical incident.
The technical and organisational protection measures we apply are regularly audited within our Information Security Management System, certified by Dekra Certification Sp. z o.o. (see www.cencert.pl/certyfikaty) for compliance with ISO 27001.

Approved:

Warsaw, 26 September 2025
Director of the Cencert Division
Enigma Systemy Ochrony Informacji Sp. z o.o.