



General Terms and Conditions

For the provision of certification services by "Incode"

Version	Modified by	Modifications made	Date modified
1.0	SPB	Content	02/2025

Tabla de contenido

TABLE OF CONTENTS.....	4
SUBJECT.....	5
USING THE APPLICATION. TECHNICAL STEPS FOR CONCLUDING A SERVICE PROVISION CONTRACT	7
NAME, CHARACTERISTICS OF SERVICES AND ACTIVATION CONDITIONS	9
SPECIAL OBLIGATIONS OF THE PROVIDER WHEN THE USER HAS CONSUMER STATUS AS DEFINED BY LAW	12
RIGHTS AND OBLIGATIONS OF CLIENTS.....	13
RIGHTS, OBLIGATIONS AND WARRANTIES OF THE PROVIDER	15
TERMINATION.....	19
LIABILITY	20
LOGS.....	20
PERSONAL DATA PROTECTION	21
INTELLECTUAL PROPERTY	21
RIGHT TO APPEAL	22
DEFINITIONS.....	23
AMENDMENT AND ACCESS TO THE GENERAL TERMS AND CONDITIONS.....	24
OTHER CONDITIONS	25

Table of Contents

TABLE OF CONTENTS.....	4
1 SUBJECT.....	5
2 USING THE APPLICATION. TECHNICAL STEPS FOR CONCLUDING A SERVICE PROVISION CONTRACT	7
3 NAME, CHARACTERISTICS OF SERVICES AND ACTIVATION CONDITIONS	9
4 SPECIAL OBLIGATIONS OF THE PROVIDER WHEN THE USER HAS CONSUMER STATUS AS DEFINED BY LAW	12
5 RIGHTS AND OBLIGATIONS OF CLIENTS.....	13
6 RIGHTS, OBLIGATIONS AND WARRANTIES OF THE PROVIDER.....	15
7 TERMINATION.....	19
8 LIABILITY	20
9 LOGS.....	20
10 PERSONAL DATA PROTECTION	21
11 INTELLECTUAL PROPERTY	21
12 RIGHT TO APPEAL	22
13 DEFINITIONS.....	23
14 AMENDMENT AND ACCESS TO THE GENERAL TERMS AND CONDITIONS.....	24
15 OTHER CONDITIONS.....	25
APPENDIX 1	ERROR! BOOKMARK NOT DEFINED.
APPENDIX 2	ERROR! BOOKMARK NOT DEFINED.

SUBJECT

Art. 1. (1) These General Terms and Conditions are intended to regulate the relations between "INCODE" hereinafter referred to as the "Provider", and the users, hereinafter referred to as "Clients," of the mobile application for electronic certification services "Incode Omni" hereinafter referred to as the "Application."

(2) Information according to the Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trusted services for electronic transactions in the internal market (the "**eIDAS Regulation**"):

1. Provider's Name: Incode Czech Republic s.r.o.
2. Registered office address: Pujmanové 1753/10a, Nusle, 140 00 Prague 4, Czech Republic
3. Address for conducting business and address for submitting complaints by users:
4. Correspondence Contact:
5. Entry in public registers: C 419276
6. Supervisory authorities: Digital and Information Agency

GENERAL PROVISIONS AND CHARACTERISTICS OF THE APPLICATION

Art. 2. (1) "INCODE", is a commercial company certified in accordance with the eIDAS Regulation, registered in the national trust list of qualified certification service providers, maintained by the Digital and Information Agency, providing qualified certification services for issuing, maintaining, and managing certificates for electronic signatures, electronic seals, electronic identification, and other information certification services.

(2) The Provider provides services to the Client upon a request submitted through the mobile application, in compliance with the requirements sets out in Art. 24(1) of the eIDAS Regulation.

(3) The Provider requires information and documents necessary for providing the services to identify the Holder and verify the data provided when processing the service request.

(4) The Provider provides services to the Client free of charge or for a fee.

(5) The relationship between the Provider and the Client is governed by a contract, and these General Terms and Conditions are an integral part of it.

Art. 3. Incode is a mobile application for the provision, use, and management of the electronic certification services requested by the Client. Through it, users can:

1. Familiarize themselves with the General Terms and Conditions for the provision of certification services, the Privacy Policy, the current rules, practices, and procedures for using the services.
2. Register and create a profile for using the Application.
3. Conclude contracts for the provision of services offered by the Provider.
4. Make electronic statements regarding the conclusion or performance of contracts through the Application interface.
5. Make any payments related to the contracts concluded with the Provider, according to the supported payment methods.
6. Manage the requested services.

7. Receive up-to-date information on the services provided and promotions offered by the Provider.
8. Review the services, their characteristics, prices, and terms of provision.
9. Be informed about the rights arising from the law, mainly through the Application interface and the provided User's email address.
10. Receive information about upcoming changes in tariffs, General Terms and Conditions, policies, and practices for using the services.
11. Receive information about planned system maintenance and upcoming software updates.
12. Receive information about temporary interruptions in service provision due to reasons beyond the Provider's control.
- 13.** Exercise their right to withdrawal, where applicable, under the Consumer Protection Act.

Art. 4. The Provider provides the services and guarantees the rights of the Clients as stipulated in European and national regulations, within the principles of good faith, practices adopted, consumer or commercial law, criteria, and conditions.

Art. 5. (1) Clients enter into a contract for the provision of services offered by the Provider through the interface of the Application for electronic certification services.

(2) The contract is concluded in Czech or English and is stored in the Provider's database in the Application.

(3) The Provider provides the services requested by the Clients within the deadlines and conditions determined by the Provider, published in the Application, and in accordance with these General Terms and Conditions and the agreements between the parties.

(4) Clients pay the Provider a fee for the delivered services according to the terms published on the website, in the Application, and in these General Terms and Conditions. The fees are specified in Czech koruna (CZK), including value-added tax (VAT), if applicable. In case of a technical error in indicating the price of the services in the Application, the Provider immediately informs the Client of the correct price of the service and has the right to refuse an order placed due to a wrongly stated actual price.

(5) Depending on the payment method chosen by the Client, additional fees for processing the payment may be charged, determined by the provider of the payment system and are at the expense of the Client.

Art. 6. (1) The Client and the Provider agree that all statements between them related to the conclusion and performance of the contract can be made electronically and through electronic statements within the meaning of the Act No. 297/2016 Coll., on Trust Services for Electronic Transactions ("**Act on Trust Services**") and the eIDAS Regulation.

(2) It is presumed that the electronic statements made by the Clients are made by the persons indicated in the data provided by the Client during registration, if the statement originates from the Client's profile in the Application.

USING THE APPLICATION. TECHNICAL STEPS FOR CONCLUDING A SERVICE PROVISION CONTRACT

Art. 7. (1) To use the services provided through the Application, available on Google Play and App Store, the Client must have a mobile device allowing its installation and ensuring connectivity of the mobile device to the internet.

(2) Browsing the Application (services, features, prices and conditions for provision, payment methods, policies, rules, and others) is entirely free and accessible.

(3) To request and use services, it is necessary to register in the Application. Registration is done simultaneously with placing an order and is associated with the mandatory provision of a service. Registration is carried out by filling in the "Request for Issuance of a Qualified Certificate" and concluding a contract for the provision of certification services in accordance with Article 2 of the Act on Trust Services.

Art. 8. (1) Registration is free and can be done by an individual who has reached the age of 18.

(2) In case the Client is a legal entity, they must provide data of the natural person authorized to represent the company - the holder of the requested qualified service.

Art. 9. (1) To register, the Client must provide identifying personal data according to Article 24 of the eIDAS Regulation and other applicable laws. In accordance with the requirements of the Act on Trust Services and other applicable laws, the Certificate Policy of INCODE and the relevant Certification Practice Statements of INCODE define, in particular, procedures related to:

- identification and authentication of the User (authorized representative of the User) when applying for registration;
- identification and authentication of the User (authorized representative of the User) when applying for a change of certificate status;
- identification and authentication of the User (authorized representative of the User) during confirmation of his possession of the private key corresponding to which the public key is provided for the generation of a qualified certificate;
- generation of a key pair of the User (authorized representative of the User);
- submission and processing of the User (authorized representative of the User) request for the generation of a qualified certificate, in the event that the key pair was generated by the User (authorized representative of the User) outside the premises of INCODE and/or in the absence of relevant personnel;
- generation of a qualified User certificate;
- the provision by INCODE of the generated qualified certificate to the User (authorized representative of the User) and the recognition of such qualified certificate by the User (authorized representative of the User);
- publication of the qualified certificate generated by INCODE;
- using a qualified certificate, as well as the corresponding private key by the User (authorized representative of the User);

- using a qualified certificate, as well as the corresponding public key by the Relying Parties;
- revocation of the qualified certificate of the User;
- suspension of the qualified certificate of the User;
- renewal of the qualified certificate of the User.

These General Terms and Conditions, as well as the list of documents necessary for the identification and authentication of the User (authorized representative of the User), as well as explanations regarding their registration, are published on the website of INCODE at the link <https://psc.incode.com/qtsp-legal-repository/>

Art. 10. (1) When registering, the Client undertakes to provide true and up-to-date data. The Client agrees to update the data provided in their registration in a timely manner in case of any changes.

(2) The username and password are determined by the Client through electronic registration in the Provider's Application.

(3) The Client declares that he/she is familiar with these General Terms and Conditions, policies, practices, and tariffs, agrees with their content, and unconditionally undertakes to comply with them.

(4) The Provider confirms the Client's registration by sending an SMS and an email to the phone number and email address specified by the client/certificate Holder, to which information for activating the registration is sent. The Client/certificate Holder confirms the registration and their email address by following the instructions provided in the messages sent by the Provider, notifying them of the completed registration. After confirmation, an account is created for the Client, and contractual relations arise between them and the Provider.

(5) The Provider is not responsible to the Client for incorrectly entered phone number and email address for receiving confirmation messages or the inability to log in to the profile and complete the registration due to a problem with the email address entered by the Client.

(6) The Client is obligated not to share their username and password with third parties.

Art. 11. After a successful registration, the Client gains full access to the functionalities of the Application and the requested services.

Art. 12. (1) To use the requested certification services through the Application, the Client must enter the chosen username and password for access when registering in the Application.

(2) Depending on the functionalities of their mobile device, the data for logging into the Application may include biometric data, PIN code, password, or other.

Art. 13. (1) Deleting the Application from the Client's/certificate Holder's device does not deactivate the profile and delete their registration.

(2) In case the Application is used by the Client/certificate Holder on multiple devices, deleting it from one of them does not terminate the contract unless the Client/certificate Holder has deactivated and deleted their profile.

(3) Deactivating and deleting the profile is considered a unilateral termination of the Contract for the provision of certification services by the Client or certificate Holder.

Art. 14. (1) The Contract for the provision of certification services is concluded through the mobile application for a period of 3 (three) years with the key generated by the Provider.

- (2) With the key issued according to the previous paragraph, the certificate Holder signs the electronic contract and the appendixes to it, thus completing the procedure for its conclusion.
- (3) The Contract enters into force after the actions in the previous paragraph are performed.
- (4) The party to the Contract with the Provider is the Client, in accordance with the data provided during registration.

NAME, CHARACTERISTICS OF SERVICES AND ACTIVATION CONDITIONS

Art. 15. (1) "Service" means the provision, administration, and support of the certification services provided by the Provider to meet the needs of the Clients.
(2) A detailed description of the services offered by the Provider is contained in Art. 21 of these General Terms and Conditions.

Art. 16. (1) All services provided by the Provider are associated with a specific plan and a minimum period, the information for which is available and explicitly stated on the website <https://psc.incode.com/qtsp-legal-repository/> and in the Application.
(2) Each service has limitations on the number of free authentications. After their use, payment for the "signing package" is required, although some services remain free (e.g., authentication through "Identita občana" (Citizen Identity) or other Czech e-government services such as "Portál občana" (Citizen Portal).
(3) Each Client can pay for an unlimited number of authentications for a period of 3 (three) years or request an additional service according to the pricing offers and technical capabilities of the Provider.
Limitations of the service if any specify

Art. 17. (1) After using the free number of authentications, the Provider allows the use of the service upon payment of the due remuneration by the Client, according to the selected configuration.
(2) The Client pays the due remuneration to the Provider at the beginning of each period, according to the maintained and announced payment methods.
(3) The 3 (three)-year period starts from the date of activating the service.
(4) The Provider activates the service immediately after validating the Client's identification and signing a service provision contract.

Art. 18. Services and the payment method can be managed through the functionalities of the Application, available in the Client's profile.

Art. 19. (1) The Client will receive a notification of the end of the service period no later than 30 days before its expiration.
(2) If the Client does not make a new payment for the requested service before its expiration, the paid service is terminated and transformed into a free one, and the registration made in the Application is preserved.

(3) Deleting one or more services from the Client's profile does not lead to the deletion of the entire profile.

Art. 20. (1) When the Client is a legal entity, it may request the use of several certification services with different titular persons in its profile.

(2) In the above scenario, the Holder can only be a natural person who has reached the age of 18 (in accordance with the requirements of Article 8(1) of these General Terms and Conditions.

(3) Each Holder is required to provide the required data according to Article 9 of these General Terms and Conditions and comply with the requirements of Article 10 thereof.

Art. 21. Description of Services:

- **Signatures for Natural Persons (Qualified Electronic Signature for Individuals - QES)**

The service "Qualified Electronic Signature for Individuals," provided by "INCODE", includes a certified assurance confirming the identity of the signer, their consent to the content of the electronic document, and ensures the integrity of the document. It is legally equivalent to a handwritten signature. This service facilitates electronic services, document exchange with administrations, online banking, and secure information exchange, such as signing contracts, encrypting emails, and initiating a digital process. The keys are securely stored in a Hardware Security Module (HSM) managed by "INCODE". They are accessible to the end user through a mobile application controlled by a PIN code known only to the user.

- **Signatures for Legal Persons (Qualified Electronic Signature for Legal Entities - QES)**

This service from "INCODE" allows legal entities to create legally binding electronic documents and represent themselves online to various institutions, including government and municipal administrations, banks, and payment institutions. It includes a qualified electronic signature presented by a natural person authorized by the legal entity. This signature certifies the identity of the signer, their consent to the content of the electronic document, and ensures the integrity of the document. It is legally equivalent to a handwritten signature. The keys are securely stored in a Hardware Security Module (HSM) managed by "INCODE". They are accessible to the end user through a mobile application controlled by a PIN code known only to the user.

- **e-Seals (Qualified Electronic Seal - QES)**

In addition, "INCODE" offers a qualified electronic seal specifically designed for legal entities. This seal confirms the origin and authenticity of the electronic document, serving as evidence that the document has been issued by the respective legal entity. The keys are securely stored in a Hardware Security Module (HSM) managed by "INCODE". They are accessible to the end user through a mobile application controlled by a PIN code known only to the user.

- **Online Signing**

The online portal for electronic signatures integrates the proposal for a qualified signature, providing users with a seamless, web-based interface for signing various types of documents, including PDF, XML, and other file formats. This portal uses secure solutions for remote signing, allowing users to easily identify themselves and sign documents with their unique identification data. The combination of convenience and high security ensures that each signature is legally binding and complies with relevant

regulations. Whether for individual or corporate use, this portal simplifies the signing and document management process in electronic format, improving efficiency and accessibility for users everywhere.

- **eID (Electronic Identification) API**

The Electronic Identification (eID) API offers a comprehensive solution for remote "Know Your Customer" (KYC) processes designed for integration with third-party systems. This advanced API facilitates secure and efficient identification of individuals remotely, using state-of-the-art identity authentication technology. It is designed to optimize the KYC process, ensure compliance with regulatory requirements, and provide a user-friendly interface. Ideal for businesses requiring identity verification when onboarding clients or authorizing transactions, this API streamlines the integration of secure electronic identification capabilities into existing digital platforms, enhancing security and trust in online interactions.

- **Server Signatures (Server-Side Signing - for seals)**

The Server-Side Signing API is designed for third-party systems that enable the automation of digital signing processes. This API allows seamless integration into existing workflows, facilitating the automatic signing of documents and data with legally binding digital signatures. It is particularly useful for businesses and organizations seeking to improve efficiency and security in document management. By automating the signing process, this API not only saves time but also ensures consistent compliance with digital signing standards, making it an ideal solution for enterprises looking to optimize and protect their digital transactions.

- **Timestamping**

The Qualified Timestamping API provides an easy solution for adding a timestamp to digital records. It uses a protocol compatible with standards, making it compatible with a wide range of systems. This API is ideal for easily and accurately timestamping the date and time of digital actions, such as document signing.

- **Validation (Qualified Validation)**

The qualified validation service offered by "INCODE" is a specialized service for verifying the validity and certified status of electronic signatures/seals and their certificates in electronically signed documents. This service, exclusively provided by a qualified and trusted service provider, delivers results through a secure, automated process, including electronic signature/seal validation from the validation service provider. This is essential for validating the authenticity of electronic documents, ensuring their reliability and authorship, and is an integral part of processes for handling electronic transactions and archiving. The service complies with the eIDAS Regulation and offers easy integration through an API, making it user-friendly and effective for validating signatures, certificates, and documents issued within the EU territory.

Art. 22. (1) Payment of amounts due from the Client to the Provider is carried out through:

1. Debit or credit card payment;
2. Using the "Wallet" service on the App Store or Google Play;
3. Through another established and indicated method specified by the Provider in the Application and on the website.

(2) The "Wallet" service on the App Store and Google Play provides the Client with the opportunity to pay for the value of subscription-based paid services:

1. The Client can subscribe through their Wallet to a specific plan, including a certain number of signings per month, with the amounts being paid monthly;
2. According to the functionality provided in the mobile application, when the number of signings or other certifying services covered by the subscription is exhausted, the Client may switch to another plan; otherwise, they should wait for the next subscription period.

SPECIAL OBLIGATIONS OF THE PROVIDER WHEN THE USER HAS CONSUMER STATUS AS DEFINED BY LAW

Art. 23. The rules of Section V of these General Terms and Conditions apply to Clients for who ho, based on the information provided during registration in the Application or at the time of concluding the Contract for the provision of services, qualify as consumers under the applicable laws, specifically:

- Act No. 634/1992 Coll., on Consumer Protection (as amended), which defines consumer rights and obligations in the Czech Republic;
- Act No. 89/2012 Coll., the Civil Code, which governs general contractual obligations, including consumer contracts ("Civil Code");
- Act No. 480/2004 Coll., on Certain Information Society Services, which regulates electronic commerce and online service provision;
- Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on Consumer Rights, which provides harmonized rules on distance contracts and consumer protection within the EU;
- eIDAS Regulation, which establishes the legal effects of electronic transactions, including consumer rights regarding electronic trust services.

Art. 24. (1) The essential characteristics of the services offered by the Provider are defined in these General Terms and Conditions and in the profile of each service in the Application and on the website.

(2) The price of the services is determined by the Provider in the profile of each service in the Application and includes all taxes.

(3) The methods of payment, the conditions for providing the services, and the performance of the contract are determined in these General Terms and Conditions, as well as in the information provided to the Client on the Provider's website and Application.

(4) The information provided to Clients under this article shall be considered accurate and binding at the time of contract conclusion, as displayed on the Provider's website. Any modifications made after the contract has been concluded shall not affect the agreed terms unless explicitly accepted by the Client or required by law.

Art 25. Consumers agree that all information required by the above-mentioned applicable laws may be provided through the interface of the Application and the website.

Art. 26. (1) The consumer has the right, without owing compensation or penalty and without stating a reason, to withdraw from the contract within a period of 14 (fourteen) days from the date of conclusion of the contract. The consumer has the right to exercise the right of withdrawal under this article directly with the Provider through the standard form for withdrawal from the contract. The form for exercising the right to withdraw from the contract and Information regarding the exercise of the right to withdraw from the contract are available as Appendix 1 and Appendix 2 to these General Terms and Conditions.

(2) The right of withdrawal under paragraph 1 does not apply to the provision of services for which the service has been fully provided when the contract requires the consumer to pay, and performance has begun with the consumer's explicit prior consent and confirmation that the consumer is aware that they will lose their right of withdrawal once the contract is fully performed by the trader.

(3) When the Provider in the Application has not fulfilled its obligations to provide information as defined in the Civil Code, the consumer has the right to withdraw from the concluded contract within one year and 14 days, counted from the date of conclusion of the contract. When the information is provided to the consumer within the withdrawal period, it starts to run from the date of its provision.

(4) When the Consumer has exercised the right to withdraw from the distance or off-premises contract, the Provider reimburses all amounts received from the Consumer without undue delay and no later than 14 days from the date on which he was informed of the Consumer's decision to withdraw from the contract, and in case the service has already been terminated, the subject of the contract. The Provider reimburses the amounts received by bank transfer, unless the consumer has expressly agreed to the use of another payment instrument, and this sentence applies in case the right of withdrawal has been exercised within the 14-day period from the conclusion of the contract, and access to the service has been terminated within that 14-day period.

(5) For a purchase made by a legal entity or a natural person acting within the scope of their commercial or professional activity, such Clients shall not be considered consumers, and therefore do not benefit from the consumer rights set out in this Article, including but not limited to the right of withdrawal and certain warranty protections.

RIGHTS AND OBLIGATIONS OF CLIENTS

Art. 27. In connection with the execution of the service provision agreement, the Client has the right to:

1. Submit an electronic "Request for Issuance of a Qualified Certificate";
2. Electronically confirm the accuracy of the provided data;
3. Receive remote assistance and support;
4. Manage the services solely through the Provider's Application, authenticating with a username and password;
5. Request the immediate suspension or termination of the requested certification service from the Provider. In this case, the Provider is not obliged to refund the fee paid;
6. Receive a new certificate free of charge in the event of an objection under Article 28, paragraph 1, item 4, regarding discrepancies between the data provided by the Client and those published by the Provider in the certificate;

7. Receive notifications from the Provider in case of the suspension of the certificate's validity;
8. Submit inquiries and receive information through the Application or via email;
9. File a complaint if the services provided by the Provider do not comply with these General Terms and Conditions, adopted policies and rules, and the announced characteristics, parameters, and deadlines. The complaint can be submitted within 3 (three) days from the occurrence of the event in electronic form to the Provider's email address or through the functionalities provided in the Application and must contain Client's data, including the email address, as well as a description of the violated conditions;
10. Reject the Agreement, if there is one for a specific service provided through the Application, within a 14-day period from its conclusion with a unilateral written statement or an electronic statement. The use of the Application is voluntary. The Provider is not responsible for damages suffered by the Customer due to the use of the application.

By accepting these General Terms and Conditions, the Client expressly agrees that, once the Provider has commenced the provision of a cloud-based qualified electronic signature and/or another service through the Application, they will lose their right of withdrawal, provided that:

- The Client has given explicit consent to begin service provision before the expiry of the 14-day withdrawal period.
- The Client has been informed, prior to contract conclusion, that they will lose their right of withdrawal upon full provision of the service, in accordance with the applicable laws..

Art 28. (1) In connection with the execution of the Contract for the provision of certification services, the Client is obligated to:

1. Use the services in good faith, complying with the Contract, the provisions of these General Terms and Conditions, applicable national and European legislation, as well as the rules, policies, procedures, and instructions adopted by the Provider;
2. Provide accurate, true, complete, and up-to-date data that uniquely identify the identity of the certificate Holder and the Client;
3. Not impersonate another person or mislead the Provider or third parties about their identity;
4. Verify the accuracy of the content of the certificate and notify the Provider within a 3 (three) day period from its issuance in case of discrepancies between the presented information and the published information;
5. Immediately update the provided information through the respective functionalities in the application in case of a change in the information provided by them. In case of a change in the information provided by the Client in the application, the requested and issued certificates through the mobile application, which include updated data, are automatically terminated;
6. Not use the Application and the certificates available through it in case of compromise or suspicion of compromise of the "key" for using the Application or loss of control over the mobile device, by immediately taking action to suspend, block, or terminate the certificate by "INCODE";

7. Keep the "key" for using the Application and not provide it to third parties. The responsibility for the consequences resulting from actions performed using the "key" lies solely with the certificate Holder;
 8. Use the services provided by the Provider only with licensed software;
 9. Install the software independently and provide the equipment for access to the services independently;
 10. Pay the agreed remuneration to the Provider for using the services, including during temporary suspension or termination of access to the requested services due to a committed violation;
 11. Not modify or tamper with the software included in the services or use the services in a way intended to avoid fees or increase usage limits;
 12. Notify the Provider of any committed or discovered violation in the use of the provided services, known to the Client/Certificate Holder, as well as not engage in Malicious Actions contrary to these General Terms and Conditions, the terms of use of the site, and the implemented policies and rules for using the services.
- (2) In connection with the execution of the contract for the provision of certification services, the Certificate Holder is obligated to:
1. In execution of the measures under Article 24(2)(e) and (f) of the eIDAS Regulation and for the prevention of unauthorized use of the services by a person impersonating the Certificate Holder, provide the Provider with a copy of their identity document in electronic format.
 2. In case a personal identification code (PIN) is provided for accessing the services, change the code before using the services;
 3. Keep the means of access to the services in a way that protects them against compromise, loss, disclosure, modification, and unauthorized use.
- (3) The Certificate Holder is personally and solely responsible for the confidentiality and integrity of the means of access to the services. Any use of the means of access to the services is considered an action of the Certificate Holder.

RIGHTS, OBLIGATIONS AND WARRANTIES OF THE PROVIDER

Art. 29. In connection with the execution of the service provision agreement, the Provider has the right to:

1. Receive remuneration for the provided services.
2. Change the prices and parameters of the offered services or terminate their provision, provided that:
 - The change is based on justified reasons, including but not limited to changes in applicable law, inflation, or modifications in agreements with third-party technology providers.
 - The Client receives at least 30 days' prior written notice before any price or service modifications take effect.
 - The Client has the right to terminate the contract if they do not accept changes as foreseen in the Article 44(2) of these General Terms and Conditions.

3. Request and process all data necessary for the successful identification and registration of the Client and for the verification of the data provided by the Client, as well as any additional information necessary for the provision of services.
4. Refuse to provide a specific service when the Client does not meet the requirements and conditions for entering into an agreement.
5. At its discretion and without prior warning, suspend or temporarily limit the Client's access to the services if there is information or suspicion that the Client is using them in violation of applicable laws or the General Terms and Conditions.
6. Temporarily suspend the provision of services or limit their parameters during planned maintenance, technical malfunction resolution, or addressing security-related issues.
7. Make changes by adding, removing, or modifying parts of the service level agreement in accordance with the terms of use (SLA).
8. Independently assess the severity of violations and the need to stop or terminate access to the services.
9. Adopt policies and rules for using the services.

Art. 30. (1) In connection with the execution of the service provision agreement, the Provider is obliged to:

1. Provide the Client with access to manage the services through the functionalities of the Application.
2. Provide the services according to the requested plan and parameters.
3. Provide technical support for the service, including sending notifications by email or in the Client's profile about changes in the service, suggestions for improving the service, adding new features, or transitioning to a plan with different parameters.
4. Ensure suitable conditions for the technical functioning of the services.
5. Maintain the parameters of the services and their connectivity 24/7 by continuously monitoring the technical integrity of the services.
6. Maintain the services in technical working order.
7. Suspend the effect of a certificate issued by the Provider for the necessary period under the circumstances but for no more than 48 hours:
 - at the request of the Holder, without having to verify identity or representative authority;
 - at the request of a person who, under the circumstances, can be seen to know about security breaches of the private key, as a representative, partner, employee, family member, etc.;
 - at the request of the Digital Information Agency or in other circumstances foreseen by law.
8. Provide, according to its technical capabilities and the circumstances, a high level of security for the technical equipment used to provide the services, in compliance with Article 8 of the eIDAS Regulation.
9. Keep an electronic register (database) in which it publishes the certificates used in its activities as a provider, the issued certificates, and the list of certificates.
10. Take immediate action regarding the suspension, resumption, and termination of the effect of certificates issued by him when the relevant grounds for this are established.
11. Immediately inform the Client of circumstances regarding the validity or reliability of a certificate issued by him, as well as its temporary suspension.
12. Conduct external audits at least once every 2 years by independent auditors to verify compliance with the requirements of the eIDAS Regulation and the applied policy.

13. Not use the collected and stored information for purposes other than those related to its activities.

(2) SERVICE LEVEL AGREEMENT (SLA)

The Provider undertakes to:

1. Provide a guaranteed time for the restoration of interrupted service within a period of 48 (forty-eight) hours on business days. The period starts from the moment of reporting a problem, accepted and confirmed by "INCODE".
2. Ensure a guaranteed level of service availability for an annual period equal to 98%. Availability represents the total time within the calendar year during which the Client has the opportunity to use the services with the agreed-upon parameters. This availability parameter does not include planned technical maintenance, as well as interruptions beyond the control of "INCODE".
3. Provide technical support for the services 24 (twenty-four) hours a day, 365 days a year, by registering and resolving technical issues within the technological service time.
4. Monitor the proper functioning of the services to ensure their continuity.
5. In the event of a security breach or integrity violation that has a significant impact on the provided authentication service or on stored personal data, "INCODE" notifies the supervisory authority without undue delay, but in any case within 24 hours from the moment it became aware of the incident, and, where applicable, other competent authorities, such as the competent national authority in the field of information security or the data protection authority, in accordance with the deadlines provided by the legislation. When there is a likelihood that the security breach or integrity violation may have a negative impact on the Client, "INCODE" notifies the breach or integrity violation and the relevant person without undue delay.
6. The Provider has developed a procedure for submitting, reviewing, and resolving complaints and claims through which "INCODE" serves its Clients.
7. The described Service Level Agreement (SLA) applies only to Clients for whom specific service level parameters have not been individually agreed upon, different from those described.
8. The described Service Level Agreement (SLA) applies only to services that the Client uses and for which the Client pays.

Art. 31. (1) The Provider carries out its activities by applying the following guarantees:

1. Adheres strictly to the conditions in these General Terms and Conditions, the requirements of the eIDAS Regulation, Regulation (EU) 2016/679 ("**GDPR**"), and applicable legislation when conducting its activities as a Provider of qualified certification services.
2. The provided services do not violate the copyrights and licensing rights of third parties.
3. Utilizes technical equipment and technologies that ensure the reliability of systems, technical and cryptographic security during the execution of processes, including a secure and protected mechanism/device for key generation and electronic signature/seal creation in its infrastructure.
4. Issues qualified certificates for electronic signatures/seals after verifying the presented information with legally acceptable means.
5. Safely stores and maintains information related to the issued certificates and the operational work of the systems.

6. Adheres to established procedures and rules for technical and physical control, following the conditions in its Practices and Policies when providing qualified certification services.
7. Upon request, issue the corresponding types of certificates, following the conditions and procedures in this document, the relevant Policies and Practices, and generally accepted standards.
8. Provides the capability for immediate suspension and termination of the validity of a qualified certificate.
9. Terminates and suspends the validity of certificates under the conditions and procedures of the respective Policies and Practices.
10. Immediately notify interested parties (Relying Parties) after the suspension of a certificate.
11. Ensures conditions for the precise determination of the time of issuance, suspension, renewal, and termination of the validity of certificates.
12. Performs procedures for the identification and authentication of the Holder.
13. Implements measures against tampering with certificates and the confidentiality of data accessed during the signature/seal creation process.
14. Uses reliable systems for storing and managing certificates.
15. Provides only duly authorized employees with access to make changes to data, establish the authenticity and validity of certificates.
16. Takes immediate action in case of technical problems related to security.
17. Cancels the validity of a qualified certificate upon its expiration.
18. Informs Holders and Relying Parties about their obligations and duty of care when using and relying on the provided certification services, as well as the correct and secure use of issued certificates and related certification services.
19. Uses and stores collected personal and other information solely for the purposes of its activity in providing certification services in accordance with applicable legislation.
20. Does not store or copy data for the creation of user private keys unless providing the service of remote signing according to the eIDAS Regulation.
21. Maintains available financial resources to enable the conduct of its activities or takes out insurance for the duration of its activity.
22. Maintains trusted personnel possessing the necessary expertise, experience, and qualifications to perform the activity.
23. Publishes in its certificate register all certificates issued by it, in accordance with legal requirements.
24. Maintains an up-to-date register of revoked and terminated certificates (CRL).
25. Publishes on its website circumstances and electronic documents, in accordance with this document and applicable legislation.
26. Ensures protection against changes to the certificate register from unauthorized and unlawful access or due to accidental events.
27. Conducts periodic internal audits.
28. Conducts periodic external audits by independent auditors.
29. Uses certified software and hardware in its activities, as well as secure and reliable technological systems.

(2) SERVICE LIMITATIONS

1. Technological Limitations. The Qualified Electronic Signature (QES) service relies on industry-standard cryptographic technologies, secure storage mechanisms, and

network infrastructure to ensure compliance with eIDAS regulatory framework. However, the following limitations apply:

- **Device Compatibility:** The service may require the use of specific operating systems or mobile devices.
 - **Internet and Network Dependency:** The service requires an active internet connection for certain functionalities, including identity verification, certificate issuance, and signature validation. Service disruptions due to network failures, latency issues, or outages may affect availability.
 - **Software Updates and Compatibility:** Periodic software updates may be required for security and compliance reasons. Users must ensure they are using the latest version of the service to maintain compatibility and security.
2. **Accessibility and Limitations for Persons with Disabilities.** The QES service is committed to ensuring accessibility in compliance with applicable accessibility standards. However, the following limitations may apply:
- **Screen Reader and Assistive Technology Compatibility:** While the service is designed to support assistive technologies, certain functionalities (such as biometric verification) may not be fully compatible with all screen readers or accessibility tools.
 - **Manual Input Requirements:** The service may require users to manually enter information, interact with security mechanisms (e.g., OTP entry, multi-factor authentication), or perform identity verification steps that may not be fully accessible to individuals with certain disabilities.
 - **Biometric Authentication Limitations:** Some identity verification processes may rely on facial recognition, fingerprint scanning, or other biometric methods, which may not be suitable for users with certain physical disabilities or conditions.

TERMINATION

Art. 32. The service is terminated:

- Upon the expiration of the validity period of the certificate(s).
- With the termination of the certificates' validity, based on the relevant grounds, according to the applicable laws.
- If it is established that the certificate was issued based on incorrect data provided by the Client.
- In case of termination, liquidation, or insolvency declaration of the Provider, in accordance to the established Termination plan.
- Upon the request of the Holder after verifying their identity.
- In case of death or placement under interdiction of the Holder - a natural person.
- In case of termination of the legal entity of the Client or deletion of the Client - a sole trader from the commercial register.
- Upon order of a competent authority.
- In case of Force Majeure Event, for which circumstance the parties owe proper notification to each other.
- In case of a breach of the obligations of the Client, as described in these General Terms and Conditions. In this case, termination is done unilaterally by the Provider, including electronically, without a refund of fees paid.

Art. 33. In the event that the contract is terminated due to the fault of the Client (as defined in Article 28), the Client shall not be entitled to any compensation or refund for fees already paid, unless otherwise required by applicable law.

Art. 34. The Provider has the right, at its discretion, without prior notice and without owing compensation, to unilaterally terminate the contract if it determines that the provided services are used in violation of these General Terms and Conditions, the Policies implemented by the Provider, the applicable laws commonly accepted ethical norms and rules of conduct, or commonly accepted rules for the use of services.

LIABILITY

Art. 35. "INCODE" is liable under Article 13 of the eIDAS Regulation for damages caused intentionally or due to negligence by a natural or legal person as a result of the non-performance of its obligations.

Art. 36. "INCODE" is not obligated and does not have the objective possibility to control the manner and/or purposes for which the Client uses the provided services, nor is it obliged to seek facts and circumstances indicating the commission of unlawful activities.

Art. 37. Limitation of liability of "INCODE":

1. The Provider is not liable for damages and missed benefits resulting from the non-fulfillment of the Client's obligations specified in the General Terms and Conditions or in all other documents constituting an integral part of the Contract, as well as for damages caused by the non-fulfillment of the Client's obligations according to the applicable Policies and Practices of "INCODE" or the applicable legislation, unless stated otherwise by applicable laws.
2. The Provider is not responsible in cases where the incurred damages result from a lack of due care, non-performance of obligations,
3. The Provider is not responsible for illegal actions by the Client/Holder or the Trusting party;
4. The Provider is not responsible for the poor quality and functionality of the software products and hardware devices used by the Client/Holder and the Trusting party;

Art. 38. Clients bear full responsibility for using content that is an object protected by copyright and related rights.

LOGS

Art. 39. (1) The Provider keeps event data in log files containing the following information:

1. System logs - records regarding the operation of the system collected by the services and tools of the operating system. These logs are kept for a minimum of 3 (three) years;
2. Audit logs - a set of records in chronological order related to security that provide documentary evidence of the sequence of activities that have affected a particular operation, procedure, or event. These records are kept for a minimum of 3 (three) years;

3. Application logs - records with information about events that occurred within the functionality of the Application. This information includes errors, warnings, as well as informational events. These records are kept for a minimum of 1 (one) year.

(2) The Provider records the exact time of significant events for the management of activities, such as key management, clock synchronization, events related to the identification of individuals, issuance of certificates, and others.

(3) Events are registered in a way that cannot be easily accessed, deleted, or destroyed and are reliably transferred to long-term archives within the time frame in which they need to be stored.

PERSONAL DATA PROTECTION

Art. 40. (1) The Provider takes necessary technical and organizational measures to protect the personal data of the Client/Holder in accordance with the GDPR.

(2) The Provider adopts and declares a Privacy Policy on its website and in the Application.

(3) Providing personal data according to the Act on Trust Services is mandatory. The refusal of the Client/Holder to provide personal data required by the Act on Trust Services and by the GDPR Regulation (is grounds for refusing to provide services.

(4) The Provider will use the data solely for the purposes of its activity as a provider of qualified certification services.

Art. 41. (1) At any time, the Provider has the right to request the Client/Holder to authenticate and verify the authenticity of any of the circumstances and personal data declared during registration.

(2) In case, for any reason, the Client/Holder has forgotten or lost their username and password, the Provider has the right to apply a procedure for lost or forgotten usernames and passwords, only upon a request made by the Client/Holder.

INTELLECTUAL PROPERTY

Art. 42. The relationship between "INCODE" and the Client regarding intellectual property rights is regulated as follows:

1. Intellectual property rights over the trademark, logo, mobile application, and all other software applications and products, databases, and other materials and resources related to the provision of services, are subject to protection under Czech Act No. 121/2000 Coll., on Copyright, Rights Related to Copyright, and Amendments to Certain Laws, belong to "INCODE" or the respective entity that has transferred the right to use to "INCODE" and cannot be used in violation of applicable legislation.
2. The Client's right to access the services does not include the right to copy or reproduce information and use objects of intellectual property unless it concerns an insignificant amount of information intended for personal use, provided that it does not unjustifiably impair the legitimate interests of authors or other holders of intellectual property rights, and in case the copying or reproduction is done for non-commercial purposes. Regardless of the above, the client has no right to remove trademarks and other

intellectual property rights markings from the materials available to him, whether the holder of the respective rights is "INCODE" or a third party.

RIGHT TO APPEAL

Art. 43. (1) Every Client/Holder has the right to file a complaint with:

1. The Provider "INCODE".

1.1. All disputes arising from a contract for the provision of certification services concluded under these General Terms and Conditions, or related to, will be resolved by mutual agreement between "INCODE" and the Client/Holder. Complaints regarding the use of certificates and certification services provided by the Provider are considered upon submission of a written document to the address: Pujmanové 1753/10a, Nusle, 140 00 Prague 4, Czech Republic or by e-mail to: psc@incode.com.

1.2. When implementing this procedure, the complainant receives a response within 1 (one) month from the receipt of the complaint, except in cases where applicable legislation expressly provides for a different response deadline.

1.3. This period and procedure do not apply to disputes, complaints, and claims related to the processing of personal data. Such requests are considered in accordance with the applicable Data Protection Policy of the Provider and according to the deadlines and requirements of the GDPR Regulation and the applicable legislation.

2. Czech Trade Inspection Authority responsible for consumer protection for the Client/Holder who qualifies as a "consumer".

2.1 The complaint must include: the name of the authority to which the complaint is submitted; the name, postal and/or email address of the complainant; against whom the complaint is filed, specifying the name of the merchant or commercial entity, as well as its registered office or management address; the complaints and requests of the complainant; the signature of the person submitting it, when submitted on paper, or of his/her proxy; in the event that the complaint is submitted by proxy, a power of attorney is attached; in case the complaint is submitted electronically, it does not need to be signed with an electronic signature; evidence available to the complainant - a copy of cash receipts, invoices, contracts, and others on which he/she bases his/her claim.

2.2 The complaint may be submitted to the address: Gorazdova 1969/24, 120 00 Nové Město - or electronically at: E-podatelna - COI.

2.3 Consumers may also resolve disputes through the Czech out-of-court dispute resolution platform operated by the Czech Trade Inspection Authority or through the European Commission's Online Dispute Resolution (ODR) platform at <https://ec.europa.eu/consumers/odr>. On this platform, consumers can find a list of alternative dispute resolution bodies that can assist in out-of-court/alternative dispute resolution. "INCODE" does not wish and is not obliged to participate in dispute resolution procedures before alternative dispute resolution bodies unless such an obligation is expressly provided for in the applicable legislation, or the Provider has given its express consent to participate in such a procedure.

3. The Digital and Information Agency.

3.1 The complaint may be submitted by e-mail to: posta@dia.gov.cz

4. Dispute resolution through judicial proceedings.

4.1 If no agreement is reached between the parties, the dispute will be referred for resolution to the competent court.

DEFINITIONS

1. **"INCODE"** is a commercial company registered in the Commercial Register maintained by the Municipal Court in Prague, with Identification No. 22635891, having its registered office and address for correspondence at: address Pujmanové 1753/10a, Nusle, 140 00 Prague 4, Czech Republic, e-mail: psc@incode.com The company is certified for compliance with the eIDAS Regulation, providing qualified certification services, and is listed in the national trusted list of qualified trust service providers maintained by the Digital and Information Agency, part of the general trusted list of all European Union Member States.
2. **"Provider of Certification Services" (Provider)** is "INCODE", a legal entity providing one or more certification services.
3. **"Certification Service"** means an electronic service, usually provided for remuneration, involving:
 - a) Creating, verifying, and validating electronic signatures, electronic seals, or electronic time stamps, electronic registered delivery services, as well as certificates related to these services; or
 - b) Creating, verifying, and validating certificates of authenticity for websites; or
 - c) Storing electronic signatures, seals, or certificates related to these services.
4. **"Qualified Certification Service"** means a certification service that meets the applicable requirements defined in the eIDAS Regulation.
5. **"Electronic Identification"** means the process of using data in electronic form to identify individuals or legal entities, with these data uniquely representing a particular natural or legal person, or a natural person representing a legal entity.
6. **"Authentication"** means the electronic process that allows the electronic identification of a natural or legal person or the verification of the origin and integrity of data in electronic form.
7. **"Electronic Document"** is any content stored in electronic form, specifically textual or audio content, visual or audio-visual recordings.
8. **"Electronic Signature"** means data in electronic form that is added to other data in electronic form or logically linked to it and used by the signatory of the electronic signature.
9. **"Qualified Electronic Signature"** means an enhanced electronic signature created by a qualified electronic signature creation device and based on a qualified certificate for electronic signatures.
10. **"Electronic Seal"** means data in electronic form that is added to other data in electronic form or is logically linked to them to ensure the origin and integrity of the latter.
11. **"Qualified Electronic Seal"** means an enhanced electronic seal created by a qualified electronic seal creation device and based on a qualified certificate for an electronic seal.
12. **"Electronic Time Stamp"** means data in electronic form that links other data in electronic form to a specific moment in time and serves as evidence that the said data existed at that particular moment.
13. **"Qualified Electronic Time Stamp"** means an electronic time stamp that meets the requirements set out in Articles 41 and 42 of the eIDAS Regulation.

14. **"Validation"** means the process of verifying and confirming the validity of an electronic signature or seal.
15. **"Client"** is a legal entity, a party to these General Terms and Conditions with the Provider for the use of certification services provided by the Provider. In the case where the Client is a natural person, the same is the "Holder" as per item 16.
16. **"Holder"** is a natural person, the direct user of the services.
17. **"Relying Party"** means a natural or legal person relying on electronic identification or certification services.
18. **"Consumer"** means any natural person acquiring goods or using services not intended for the conduct of commercial or professional activity, and any natural person acting as a party to a contract under the Consumer Protection Act acting outside the scope of their commercial or professional activity.
19. **"Force Majeure Event"** is an unforeseen circumstance at the time of the conclusion of the General Terms and Conditions, an extraordinary event that objectively makes the provision of services impossible.
20. **"Log File"** - a file containing system information about the operation of the Application and information about the user's actions.
21. **"Malicious Actions"** are actions or inactions that violate Internet ethics or cause harm to individuals connected to the Internet or associated networks, sending unsolicited emails (spam, junk mail), channel flooding (flood), gaining unauthorized access to resources with others' rights and passwords, exploiting deficiencies in systems for personal gain or obtaining information (hack), performing actions that may qualify as industrial espionage or sabotage, damaging or destroying systems or information arrays (crack), sending "Trojan horses" or installing viruses or remote control systems, disrupting the normal operation of other Internet users and associated networks, or committing any other actions that may be classified as a crime or administrative offense under n law or other applicable law.

AMENDMENT AND ACCESS TO THE GENERAL TERMS AND CONDITIONS

Art. 44. (1) These General Terms and Conditions may be amended by the Provider, for which the latter will notify all Clients/Holders with registered accounts in advance of any such amendment via email and/or an in-app notification.

(2) The Provider and the Client/Holder agree that any supplement and amendment to these General Terms and Conditions will take effect concerning the Client/Holder after explicit notification by the Provider. If the Client/Holder does not reject the changes within the provided 14-day period, they shall be deemed accepted. The Client/Holder has the right to reject the amendments and to terminate the contract without penalty within 14-day period starting from the day where the amendments were notified.

(3) The Client/Holder agrees that all statements by the Provider regarding the amendment of these General Terms and Conditions will be published in the Application and on the website, as well as sent to the email address provided by the Client/Holder during registration. If legally required, amendments shall be signed electronically in accordance with Act on Trust Services.

Art. 45. The Provider publishes these General Terms and Conditions at <https://psc.incode.com/qtsp-legal-repository/> along with all additions and amendments to them.

OTHER CONDITIONS

Art. 46. (1) Upon request from the competent state authority in cases established by law, the Provider is obliged to provide necessary information regarding the recipient of the service and their activity. According to Section 18 of Act on Trust Services, the Provider is required to retain the information under Article 24(2)(b) of the eIDAS Regulation for a period of 10 years, including after the termination of the activity, unless a different retention period is required by applicable law

(2) When carrying out the actions under paragraph 1, the Provider is not obliged to notify the Client, except in cases expressly defined by law.

(3) The Client is not entitled to claim compensation for damages resulting from actions of the Provider under paragraph 1.

Art. 47. (1) The Client and the Provider undertake to mutually protect their rights and legitimate interests, as well as to keep their trade secrets, which become their property in the process of contract execution and these General Terms and Conditions.

(2) The parties undertake, during and after the expiration of the contract period, not to publicly disclose written or oral correspondence conducted between them, unless required by the applicable laws. Publication of correspondence in print and electronic media, internet forums, personal or public websites, etc., may be considered as public disclosure.


Art. 48. In case of contradiction between these General Terms and Conditions and agreements in an individual contract between the Provider and the Client, the clauses of the individual contract shall prevail.

Art. 49. The possible invalidity of any of the provisions of these General Terms and Conditions shall not lead to the invalidity of the entire contract.

Art. 50. For matters not regulated in these General Terms and Conditions related to the performance and interpretation of the Contract, the current regulatory framework on the territory of the Czech Republic shall apply.

Art. 51. These General Terms and Conditions shall be governed by the laws of the Czech Republic. Any disputes shall be resolved by the competent courts of the Czech Republic.

Art. 52. These General Terms and Conditions enter into force for all Clients of the Provider on March 1st, 2025.



psc@incode.com
psc.incode.com

Incode PSC

incode^{psc}

psc@incode.com

psc.incode.com