incode psc

Privacy Policy for Customers Personal Data

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

Information about the Personal Data Controller

Incode Czech Republic s.r.o., ID number: 22635891, address: Pujmanové 1753/10a, Nusle, 140 00 Praha 4, Czech Republic ("**Incode"**)

Information about the Data Protection Officer

- Name: Data Protection Office
- Address: Pujmanové 1753/10a, Nusle, 140 00 Praha 4, Czech Republic
- Email: dataprotection@incode.com

Information about the Competent Supervisory Authority

- Name: Office for Personal Data Protection
- Address: Pplk. Sochor 27, 170 00 Prague 7, Czech Republic
- Phone: +420 234 665 800
- Email: posta@uoou.gov.cz
- Website: http://www.uoou.cz/

Objectives and Scope of the Data Protection Policy

This policy aligns with the territorial and material scope of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data ("**GDPR**"), embracing its fundamental goals and other applicable laws such as Act no. 110/2019 Coll., on the Processing of Personal Data ("**Czech Personal Data Processing Act**").
Incode requires the collection and processing of personal data in order to conduct its activities lawfully, appropriately, and comprehensively. This pertains to personal data of employees, clients, and website/platform visitors.

Categories of Personal Data, Purposes, and Processing Grounds

Incode processes various categories of personal data of different subjects based on specific grounds, in accordance with pursued objectives. In compliance with Articles 13 and Article 14 of the GDPR and the principles of lawfulness, fairness, transparency, and data subjects' rights, this section outlines the necessary information to facilitate individuals' understanding and awareness regarding their personal data.

Categories of Personal Data provided by the Data Subject - Natural Person are as follows:

Data related to physical identity

- Name, middle name, and surname;
- Personal identification number/Date of birth/National identification number;
- Contacts: email, address, and phone number;
- Address: permanent or current;
- Data from identity documents (ID card): number, date of issue and expiration, issuing authority, citizenship, features, and images;
- Biometric data – photo/video image;
- IP address, mobile device model and software data.

Data related to economic identity

- Banking information: bank card number/account for payments;
- Profiles from payment systems such as PayPal/Epay/Revolut, etc.

Categories of personal data of the data subject provided by another source:

Data related to physical identity

- Data extracted during official verification for the validity of your identity document from official databases of competent authorities in the issuing state of the identity document (if access to these databases is available in the jurisdiction of the issuing state of the identity document);
- Data extracted from the machine-readable part or the NFC chip of the identity document (this may include a picture from official identity document databases);
- Signature, initials.

The data processing serves the following purposes, reflecting the grounds for their processing

The personal data received from the subject - a natural person will be used for the purposes of providing our services, in fulfillment of contractual relations, legal obligations applicable to the administrator, as well as for the protection of legitimate interests, namely:

- Creating a profile in the administrator's mobile application.
- Issuing electronic signatures for natural persons.
- Issuing electronic or digital signatures for the management and employees of legal entities.
- Issuing electronic seals for legal entities.
- Issuing electronic signatures for e-identification purposes.
- Creating and maintaining registries for reporting.

- Financial and accounting reporting.
- Taking actions upon request from the data subject to exercise their rights under the GDPR.
- Marketing purposes.
- Performing other functions delegated by law or contractual relationships.

The processing of the specified categories of personal data provided by you is based on:

- Article 6(1)(c) GDPR – Compliance with legal obligations applicable to the controller, including those set out in Regulation (EU) 910/2014 ("**eIDAS Regulation**") and other governing laws.
- Article 6(1)(b) GDPR – Processing necessary for the execution of a contract to which you are a party, or to take steps at your request prior to entering into a contract. For example, downloading our mobile application may require certain preliminary data processing.
- Article 6(1)(f) GDPR – Processing necessary for the purposes of legitimate interests pursued by the controller, provided such interests are not overridden by your rights and freedoms. This includes processing for direct marketing purposes, ensuring that you have the right to object to such processing at any time.
- Article 6(1)(a) GDPR – Processing of your personal data for direct marketing purposes (e.g., names and emails) may also be based on your freely given, specific, informed, and unambiguous consent where required by applicable law.
- Article 9(2)(a) GDPR – Processing of your biometric data (e.g., facial recognition and identity verification between your identity document and a real-time picture via a mobile device) will only be conducted based on your freely given, specific, informed, and unambiguous consent.

Automated decision-making for creating a profile in the 'INCODE' Application. - validate

When utilizing the authentication services provided by the controller, it is necessary for your identity to be verified and confirmed through automated identification. This requirement stems from the regulatory demands concerning the services we provide as a qualified provider of authentication services. To register your profile, we need your consent for automated identification, by providing biometric data (facial imaging), which should be freely given, specific, informed, and unambiguous. Information about the conditions and methods of conducting the identification will be found in the informed consent statement itself.
Personal data is not used for incompatible purposes. Their processing is limited to the purposes for which the data is collected.

Incode does not collect and process personal data solely for the identification that relates to the following:

- Reveal racial or ethnic origin
- Reveal political, religious, or philosophical beliefs or membership in trade unions
- Genetic data, data concerning sexual life or sexual orientation

The administrator does not collect and process personal data of minors.

Cookies and other similar technologies

Incode and our vendors may use cookies and other similar technologies, such as pixels, tags, web beacons and trackers (collectively, "Cookies") on the Website. We may use Cookies for several purposes, including to:

- Store information to help the Website function properly,
- Help you access and navigate the Website more efficiently,
- Enable our servers to recognize your login information and preferences so that you do not need to enter the same information each time you visit the Website,
- Tell us how and when you visit and use our Services, including collecting information about which pages on our Website you viewed or links you clicked and how you interacted with our content during your visit or over multiple visits,
- Customizing your browsing experience by showing you information more likely to be relevant to you, and
- Delivering and customizing advertisements and tracking advertising campaigns.

We may use third-party technologies (such as the Meta Pixel and Hotjar) in connection with your activity on the Website, including for advertising purposes and to analyze your interactions and experiences with the Website, and including the features you engage with, how you navigate, and your click/touch, movement, scroll and keystroke activity. These technology companies and advertisers may use, store, or access cookies and other tracking technologies to collect or receive information from the Website and elsewhere on the internet. To change your privacy and advertising settings with Meta, log in to your Meta account and navigate to your account settings.

We may also use certain web analytics services, such as Google Analytics, to help analyze how people use our Website. We use this information to implement Google advertising features such as dynamic remarketing, interest-based advertising and demographics and interests reporting. For more information on how Google Analytics uses the data it collects, visit: google.com/policies/privacy/partners. To opt-out of Google Analytics, visit: tools.google.com/dlpage/gaoptout. To adjust your Google advertising settings, visit: adssettings.google.com.

You may be able to opt-out of certain interest-based advertising using the settings on your browser or mobile device. In addition, to opt-out of interest-based advertising from companies that participate in the Digital Advertising Alliance or European Interactive Digital Advertising Alliance opt-out programs, please visit: youradchoices.com/control and youronlinechoices.eu.

Please note that we or other parties may collect personal data about your online activities over time and across different devices and online websites when you use the Website.

Some browsers have incorporated "Do Not Track" (DNT) features that can send a signal to the websites you visit indicating you do not wish to be tracked. Because there is not a common understanding of how to interpret the DNT signal, our Website does not currently respond to browser DNT signals. Instead, you can use the range of tools described above to control data collection and use.

Categories of recipients of personal data

Incode may provide your personal data to third parties, with the primary purpose being the protection of your interests and security, regarding the fulfillment of regulatory and contractual obligations or specific tasks. Your personal data is not provided to third parties before ensuring that all technical and organizational measures have been taken to protect this data, with strict control to fulfill this purpose. We adhere, where applicable, for your data to be processed only under the instructions given on behalf of the controller – Incode.

Recipients of data, outside the controller, who:

Require information on a legal basis

- Government and municipal authorities, agencies, institutions, and other competent regulatory bodies, according to their powers (ministries, directorates, agencies, commissions, etc.).
- Judicial authorities (courts, prosecution, etc.).
- Regulatory bodies (the Office for Personal Data Protection, the Office for the Protection of Competition, and other bodies overseeing compliance with sector-specific regulations).
- Auditors and accreditation bodies.
- Legal entities, judicial executors.

Require information on a contractual basis

- Service providers (consultants, experts, accountants, evaluators, auditors, lawyers). Disclosure of data occurs only when there is a legitimate reason and based on a written agreement to ensure an adequate level of protection by the recipients.
- Banking and other payment institutions for the purpose of paying due amounts when necessary to verify your identity.
- Individuals entrusted with the maintenance of equipment, software, and hardware used for processing personal data necessary for the company's operations.
- Trusted partners.

Recipients of data within the controller

- Internal sharing among employees while fully complying with the adopted technical and organizational measures.

Technical and organizational measures for data protection

To ensure adequate protection of the data of its employees, clients, and partners, Incode implements all necessary organizational and technical measures outlined in the GDPR and eIDAS regulation, considering data protection in both the design phase and by default.
Protection of personal data in the design phase is expressed through appropriate technical and organizational measures introduced by Incode before the commencement of personal data processing (during the stage of defining the purposes and means of processing), ensuring their application throughout the data lifecycle. Suitable measures involve data encryption, implementing automated deadlines reporting functionalities, and automatic deletion upon expiration, among others.
Data protection is achieved by applying mechanisms that by default guarantee compliance with the following requirements:

- Only the minimum amount of personal data absolutely necessary to achieve the specific purpose is processed and operational procedures are carried out.
- Licensed software and certificates for electronic protection of systems and the internet platform/website/application are used.
- Encrypted emails with paid, private domains are used. Sending documents containing personal data and classified information to public domain email addresses is not carried out.
- Only employees requiring the relevant information for the execution of their job responsibilities have access to personal data.

- Personal data is not shared with other employees unless required to perform their duties.
- Employees are required to handle data with increased attention and responsibility throughout their work and granted access to the platform/application. They are also expected not to leave their devices unattended.
- Documents related to personal data processing of subjects are not stored in the company's office. Information is entirely digital and stored in cloud systems, following the policies of cloud service providers. There is a legal obligation to store certain documents containing personal data in paper format, which is done in a specially designated cabinet with a locking mechanism.
- The connection to cloud services is conducted via an HTTPS access channel, and every employee in the company is familiar with computer and information security policies. When these policies are updated, every relevant employee is notified of the changes.
- For our internal operations and processing of clients data, we use cloud platforms that provide remote access with user-level permissions and strict data security policies.
- Data access is granted to specific employees through individual work accounts for the execution of particular tasks.
- Upon release from their responsibilities, an individual loses immediate access to all associated data.
- A password creation policy and user rights have been established.
- Employees undergo training for proper compliance with the GDPR and the application of implemented technical and organizational measures and procedures.
- Data is stored for the minimum necessary duration to achieve the processing purposes, and after that period, it is deleted following appropriate rules and procedures.
- Data whose purpose for collection has expired is irreversibly destroyed with a deletion protocol.
- Any access, transmission, or sharing of data is permissible only when a valid legal basis is present (e.g., contract, data subject's consent, or our legal obligations).
- Sharing and downloading any data or confidential information accessed by employees for their work responsibilities is strictly prohibited. Storing such data on personal devices (including, but not limited to, laptops, tablets, mobile devices, cameras, or smartphones) or recording such data in any form (e.g., by taking a picture, video, screenshot, or other images) is also prohibited.
- The highest level of information and hardware security is implemented, in accordance with Article 8(2)(v) of the GDPR, to meet the requirements of Article 19 GDPR.

- Continuous system maintenance is performed 24/7 to minimize the possibility of security breaches, information leaks, and identity theft.
- A complete internal audit and system check are conducted every 12 months.
- In the event of a security breach, the service to the targeted individual(s) is temporarily or permanently suspended to prevent unauthorized actions by third parties.
- The controller takes necessary measures to ensure that the data processor and any individual, acting under the controller's authority, process this data only based on the controller's instruction for the respective purpose.
- In case of a breach of personal data security, the controller, upon awareness, will notify the competent supervisory authority, and if necessary, the data subject affected by the malicious actions.

Incode has the ability, when necessary for security purposes, to introduce an additional key for protection. To ensure maximum security during data processing, transmission, and storage, we may use additional protection mechanisms.

Data Transfer to Third Countries

Transfer of personal data to third countries is not conducted, and processing of personal data outside the European Union's framework does not take place.

Data Retention Period

Incode typically ceases complete processing of personal data for the listed purposes upon termination of contractual relations or at the data subject's request. However, the data is not deleted before the expiration of the legally determined obligations for data retention, following the principle of limited storage. Your personal data will not be deleted or anonymized if it is necessary for ongoing legal, administrative proceedings, or proceedings relating to your complaint. The data is stored for a period not exceeding what is necessary. Below are the data retention periods for categories of data of particular significance.

Legally defined data retention periods:

- Information contained in the register under Articles 24 and 28 of the eIDAS Regulation - 10 years, including after the cessation of activity,
- Data processed based on the data subject's consent, excluding biometric data – until the consent is withdrawn;
- Data processed for compliance with our legal obligations under applicable laws will be retained for as long as required to fulfill these obligations (up to 10 years);
- Storage and processing of accounting data - 10 years from the year following the last payment,

Controller-defined retention periods:

- Biometric data processed during the data subject's identification in the registration and activation process of the Application – up to 5 minutes from the identification process;
- Data and records contained in log files gathered during unsuccessful identification and/or terminated data subject registration and Application activation processes – up to 2 years from the occurrence.

Security Incident Reporting

Incode has implemented a structured system for reporting security incidents. In the event of any data breach, Incode acts in full compliance with the GDPR to minimize potential harm. Where required, we promptly notify the Office for Personal Data Protection within the prescribed timeframe.
If a breach is likely to result in a high risk to the rights and freedoms of individuals, we will also inform the affected data subjects without undue delay. The incident response includes:

- Identifying and containing the breach;
- Assessing the impact and risk level;
- Implementing corrective actions to prevent recurrence;
- Documenting all incidents and remediation measures.

All security incidents are recorded internally, and our response procedures are regularly reviewed to ensure ongoing compliance and data protection.

Data Subject Rights – For Individuals

Right to Information and Access.

You have the right to request:

- *Information* about whether data concerning you is being processed, the purposes of such processing, the categories of data, and the recipients or categories of recipients to whom the data is disclosed;
- *A communication* in an intelligible form containing your personal data being processed, as well as any available information about their source;
- *Information* on the logic behind any automated processing of personal data related to you, at least in cases of automated decisions.

Right to Rectification.

In cases where we process incomplete or incorrect data, you have the right, at any time, to request:

- Deletion, correction, or blocking of your personal data whose processing does not comply with legal requirements;

- Notify third parties to whom your personal data has been disclosed of any deletions, corrections, or blocking, except where this is impossible or requires excessive effort.

Right to Erasure.

The right to erasure, or "the right to be forgotten," provides the ability, when you no longer wish your data to be processed and there are no legal bases for their storage, to request their deletion based on one of the following grounds:

- Personal data is no longer necessary for the purposes for which they were collected or otherwise processed;
- You withdraw your consent on which the data processing is based;
- You object to the processing and there is no overriding legal basis for the continuation of processing;
- Personal data have been processed unlawfully;
- Personal data must be erased to comply with a legal obligation;

"The right to be forgotten" is not an absolute right. There are situations in which the controller may refuse to erase the data, namely when the processing of specific data is necessary for any of the following purposes:

- Exercising the right to freedom of expression and information.
- Archiving for purposes in the public interest, scientific research, historical research, or statistical purposes.
- Establishing, exercising, or defending legal claims.

Right to object.

At any time, you have the right to object to the processing of your personal data where there is a legal basis for doing so. When the objection is justified, the personal data of the respective individual cannot be processed further.

Right to restrict processing.

You can request the restriction of the processing of personalized data if:

- You dispute the accuracy of the data for the period during which its accuracy is being verified; or
- Processing the data is without legal basis, but instead of deletion, you want their restricted processing; or
- We no longer need this data (for a specific purpose), but you need it to establish, exercise, or defend legal claims; or
- You have objected to the data processing while waiting for the administrator to verify the legality of the grounds.

Right to data portability.

You can request us to provide the personal data you have entrusted to us in an organized, structured, commonly used, and machine-readable format to another controller if:

- We process the data based on the contract and the consent declaration, which can be withdrawn, or based on contractual obligations, and
- The processing is carried out automatically.

Right to withdraw consent.

You have the right, at any time, to withdraw your consent for the processing of personal data if the processing is based on your consent. Such withdrawal does not affect the lawfulness of the processing based on the consent before its withdrawal.

Right to fill a complaint.

If you believe that we are violating applicable regulations, please contact us to clarify the issue. Of course, you have the right to file a complaint with the respective authority. The supervisory authority in the Czech Republic is the Office for Personal Data Protection, with its registered office at Pplk. Sochor 27, 170 00 Prague 7 (http://www.uoou.cz/).

Right to obtain compensation.

According to Section 39 of the Czech Personal Data Processing Act and Article 82(1) GDPR, anyone who has suffered damages as a result of a breach of the provisions of the GDPR or other applicable data protection laws has the right to obtain compensation through a lawsuit before the competent judicial authority.

Exercising Your Rights

Requests to exercise your rights should be submitted to one of the following email addresses: dataprotection@incode.com

They should be signed with a Qualified Electronic Signature (QES) or by another method verifying indisputably the will of the person submitting the request. We respond to your request within one month of its submission. When an objectively necessary longer period is required, for instance, to collect all requested data or when it significantly hampers our operation, this period can be extended with up to 30 days. In our decision, we grant or refuse access and/or the requested information, always providing a reasoned response.

The minimum information contained in the request should be as follows: name, contact details, description of the request and signature. If the request is submitted on behalf of another person, a Power of Attorney or other proof of authorization may be required.

Concerning the aforementioned rights: to information, to correction, the "right to be forgotten," to object, to restriction of processing, to not be subject to a decision based solely on automated processing, to withdraw consent, to file a complaint, and in view of the actions of the administrator in connection with these rights, a specific register is created to record all actions carried out.

The initial provision of a response to a submitted request is free of charge. In cases of excessiveness (repetition - more than 2/ two/ requests of the same substance within a period of 12/ twelve/ months) or apparent lack of merit in the requests from the same subject, the Controller may request a reasonable fee for executing the request or refuse to act on the request.

Principles of Personal Data Processing, in accordance with the GDPR

- "Lawfulness, fairness, and transparency" - Your data is processed in compliance with applicable legislation, fairly, and in a transparent manner towards the data subject.
- "Limitation of purpose" - Your data is collected for specific, explicitly stated, and legitimate purposes and is not processed further in a manner incompatible with these purposes.
- "Data minimization" - The types of data we collect are suitable, related, and limited to the necessary minimum in connection with the purposes for which the personal data is processed.
- "Accuracy" - Accurate and, if necessary, to be kept up to date, taking all reasonable measures to ensure the timely deletion or correction of inaccurate personal data, considering the purposes for which they are processed.
- "Limitation of storage" - Your data is stored in a form that allows the identification of the data subject for a period no longer than necessary for the purposes for which the personal data is processed.
- "Integrity and confidentiality" - Processed in a way that ensures an appropriate level of security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using suitable technical or organizational measures.

Definitions

Term	Definition
Personal data	any information related to an identified or identifiable natural person.
Data subject	an individual who can be identified directly or indirectly, especially through an identifier such as a name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Processing	any operation or set of operations performed on personal data or sets of personal data, whether by automated means or not, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.
Restriction of processing	marking stored personal data with the aim of limiting their processing in the future.
Pseudonymization	processing personal data in a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Controller	a natural or legal individual, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such

	processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Processor	a natural or legal individual, public authority, agency, or other body which processes personal data on behalf of the controller**.**
Consent of the data subject	any freely given, specific, informed, and unambiguous indication of the data subject's wishes, which, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.
Profiling	any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning the performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements of that natural person.
Automated decision-making	the ability to make decisions using technological means without human intervention.
Electronic identification	the process of using data in electronic form for the identification of individuals, which data uniquely represents a natural or legal individual or a natural person representing a legal entity.
Trusted parties	recipients of Qualified Electronic Signatures (QES), for example, as part of electronic statements, which rely on the authentication and/or electronic signatures verified by the public key of that certificate.
Personal data breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data that is

	transmitted, stored, or otherwise processed.
Recipient	a natural or legal individual, public authority, agency, or another body to whom personal data are disclosed, whether a third party or not. Public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law are not considered recipients. The processing of such data by those public authorities complies with applicable data protection rules in line with the purposes of the processing.
Third country	any state that is not a member of the European Union or a party to the Agreement on the European Economic Area.

Incode PSC