Privacy Policy

of incaseof.law GmbH

1. Personal Data

Personal data includes all information relating to an identified or identifiable living natural person (the "data subject"). This information includes, for example, your name, address, email address, telephone number, date of birth, age, gender and social security number. There are also special categories of personal data, often referred to as "sensitive data". According to the GDPR, these include health data or data in the context of criminal proceedings.

2. Collection and Processing of Personal Data

Within the scope of this privacy policy, we want to explain to you in a clear, transparent and well-structured manner which data is collected during the proper use of our platform within the framework of the services we offer, and for what purpose it is used and processed by us.

We also use your data to analyse how you use our platform so that we can continuously improve the user experience. In addition, we use personal data to send advertising and newsletters to the extent permitted by law.

We process both data that you provide to us and data that arises in the course of the business relationship or that we collect from third parties.

2a. Data Sources When Connecting via Connector Partners

▶ New section pursuant to Art. 14 GDPR – applies to clients who access incaseof.law via partner platforms.

In addition to data that you provide to us directly, we may receive data from the following sources in the context of the Connector model:

Connector partner platforms: If you register with incaseof.law via a third-party platform cooperating with incaseof.law (Connector Partner, e.g. ibana Software GmbH, WinChim Software Engineering GmbH, TPA-CONNECT) or submit claim data via such a platform, we receive from that platform your master data (name, company name, address, email address, tax identification number) as well as the transmitted claim data. The legal basis for this processing is Art. 6(1)(b) GDPR (performance of a contract) as well as your consent to data transfer to incaseof.law given to the Connector Partner.

Authentication data for SSO connections: When using the Single Sign-On (SSO) procedure via OAuth 2.0, we receive from the Connector Partner an authentication token as well as the master data stored in your profile there, to the extent required for creating your account at incaseof.law. Further processing of this data takes place exclusively for the performance of the contract (Art. 6(1)(b) GDPR). No use of the SSO token data beyond this takes place.

Time of notification: In accordance with Art. 14(3)(a) GDPR, you will be informed about the origin of the data we process no later than upon your first use of the incaseof.law platform. This is done via the consent screen displayed at first login.

3. Data Controller

The controller responsible for data processing within the meaning of the GDPR is:

incaseof.law GmbH, Rathausstraße 21/13, 1010 Vienna, Austria

Email: datenschutz@incaseof.law

Website: www.incaseof.law

4. Data Security

Our goal is to manage your data with the utmost care and to take technical and organisational security measures to protect your data from loss and misuse.

Access to our website is secured via HTTPS if your browser supports SSL. This means that communication between your device and our servers is encrypted.

If you contact us by email, we point out that the confidentiality of the transmitted information cannot be guaranteed. The content of conventional emails can be viewed by third parties due to their technical design. To ensure adequate information and system security and to detect malware, we store log data relating to email traffic.

5. Purposes and Legal Basis of Data Processing

ICO primarily offers services in the field of out-of-court and judicial receivables management for businesses. In addition, we support businesses in answering legal questions of all kinds through automation-supported processing and preparation of the information provided by you and the use of licensed lawyers registered with us as partners.

Our range of services is aimed on the one hand at businesses that require out-of-court and judicial receivables management services or wish to have legal questions clarified. At the same time, our service offering in the area of the receivables management tool is also aimed at our clients' business partners (debtors) who can contact us via our platform, make payments or enter into payment-related agreements.

6. Categories of Data

6.1 Lawyers

If you are active on our platform as a lawyer or are applying to do so, we process the following data from you:

- Name and law firm name
- Law firm address

- Telephone number
- Professional title
- Bar association and lawyer number/code
- R-code for the Electronic Legal Communication (ERV)
- Value added tax identification number
- Professional indemnity insurance data
- Bank details (IBAN and account holder)
- Personal and professional details of persons authorised to represent the law firm
- Consent to terms of use, privacy policy and release from confidentiality obligations

6.2 Clients

If you use ICO's services as a representative of an organisation (company) or sub-organisation, we process the following data in the course of the business relationship:

- First and last name of the acting person(s)
- Email address of the acting person(s)
- Telephone number of the acting person(s)
- Gender / salutation of the acting person(s)
- Position or function of the acting person(s) within the (sub-)organisation
- Company name of the organisation or sub-organisation
- Business address of the organisation or sub-organisation
- If different, billing address of the organisation or sub-organisation
- If applicable, VAT identification number of the organisation or sub-organisation
- Details of the commissioned or used scope of services including invoice information (and any personal debtor data contained therein) in the case of use of the ICO receivables management tool
- Prices and payment terms of the services used
- Selected payment method for services and bank details (IBAN/BIC)
- Performance of legally effective actions (e.g. case creation, initiation/filing of dunning actions/execution applications via ERV)
- Information on the status and processing of the service (e.g. case status)
- **When connecting via a Connector Partner:** Authentication data (OAuth 2.0 token, session cookies) as well as the master data transmitted by the Connector Partner within the scope of the respective OAuth scope; log data on the granting and timing of the Connector consent (timestamp, user ID, IP address, version of the consent text displayed).

6.3 Debtors

Below we list possible data that we collect or derive from the data collected in connection with debtors. Please note that this does not necessarily mean that we actually process all of this data for each debtor.

Personal master data:

- Name and surname / company name
- Date of birth and/or age
- Gender, nationality, marital status

Contact data:

- Address, email address, telephone number

Identification data:

- Social security number or other unique identifiers / company register number

Risk data:

- Creditworthiness, risk class, claim amount and reason
- Account and payment information, payment agreements, default information and dunning history

6.3a Information for Debtors pursuant to Art. 14 GDPR

▶ New section – fulfilment of the information obligation pursuant to Art. 14 GDPR vis-à-vis debtors.

If you are contacted by incaseof.law as a debtor, your data was not collected directly from you, but from the creditor (client of incaseof.law) and, where applicable, from external databases. Pursuant to Art. 14 GDPR, we hereby inform you of the following aspects of processing:

Data sources: Your master data (name, address) and the claim data were transmitted to us by the creditor in the context of a collection engagement. In addition, we may query your address and creditworthiness data from CRIF GmbH (Austria) or comparable credit bureaus.

Purpose and legal basis: Processing takes place for the purpose of enforcing legitimate claims of the creditor (Art. 6(1)(f) GDPR – legitimate interest). A balancing of interests has been carried out; the creditor's legitimate interest in enforcing claims generally outweighs the interests of the debtor, as it involves the assertion of legally established claims.

Storage period: Debtor data is stored for the duration of the processing of the claim case and within the framework of the statutory retention periods.

Right to object: You have the right pursuant to Art. 21 GDPR to object to the processing of your data on the basis of Art. 6(1)(f) GDPR. Such an objection does not affect the legal validity of the claim itself and may lead to the case being transferred to the creditor or its lawyer.

Contact: For enquiries regarding data processing as a debtor, please contact datenschutz@incaseof.law.

6.4 Technically Required Data

For technical reasons, your browser transmits certain information to our web servers each time you access our website. We collect this information exclusively for statistical and technical purposes. The following data is collected:

- IP address of the accessing device
- Date and time of access

For registration and authentication we use a modern authentication platform which protects and manages your login details to provide you with a high level of security.

7. Legal Basis of Data Processing

7.1 Contractual obligations – Art. 6(1)(b) GDPR

Contractual relationships exist both with our clients, i.e. organisations and their representatives, and with the lawyers who use our platform. These contracts give rise to certain obligations whose fulfilment makes the processing of personal data indispensable.

7.2 Legal obligations – Art. 6(1)(c) GDPR

Processing may be required by law, including fulfilment of tax documentation and reporting obligations, and responding to enquiries from law enforcement or other authorities within the scope of their legal powers.

7.3 Legitimate interest – Art. 6(1)(f) GDPR

Processing may be based on Art. 6(1)(f) GDPR where necessary for the purposes of our or a third party's legitimate interests, provided these do not override the interests or fundamental rights and freedoms of the data subject. We see a legitimate interest in the following cases:

- Ensuring the operation and management of our website
- Responding to enquiries via our contact form
- Carrying out direct marketing measures
- Use of web analytics tools to optimise our online services
- Ensuring network and data security
- Providing technical support for our users
- Enforcement of legitimate claims against debtors in the context of the collection mandate

8. Cookies

We use cookies on our website. A cookie is a small file that stores specific internet settings and is downloaded to your device by your web browser the first time you visit a website. On a repeat visit to the website with the same device, the cookie with the stored data is either sent back to our website (first-party cookie) or to another website it belongs to (third-party cookie).

You can change your choice at any time using "Cookie settings" in the footer. Your choice is stored locally in your browser for up to twelve months. Optional measurement services only load after your corresponding consent.

Statistics and advertising measurement

With your consent, we use Google Analytics 4 to measure page views, successfully submitted contact enquiries and registration entry clicks. With your separate consent, we use Google Ads to measure advertising results and attribute enquiries to advertising clicks. Google Tag Manager manages this integration. These services are used exclusively on the marketing website

www.incaseof.law. In the customer portal (app.incaseof.law) and the debtor portal (payment.incaseof.law) only technically necessary cookies are used; no third-party measurement or advertising services are loaded there. The provider is Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland. Processing may include technical device and browser information, IP addresses, cookie identifiers and advertising click information. Processing in the United States is possible.

Contact measurement events do not include names, email addresses, phone numbers or message text. You can use the website and contact form without granting optional consent. Further information: Google Privacy Policy.

9. Transmission of Data to Third Parties

ICO uses the services of third parties to handle certain complex data processing tasks. These service providers, acting as processors, are contractually obliged to treat your personal data confidentially and to process it exclusively within the scope of their task fulfilment.

The transfer of your personal data always takes place on the basis of legal provisions or in accordance with contractual agreements. We transmit your data in particular to companies that provide services on our behalf relating to order processing (case handling), customer service, marketing activities, sending email newsletters, optimisation of our website, and payment services.

In addition, personal data may be passed on to law enforcement authorities if required by law.

Connector Partners as data source and data recipient: In the context of Connector partnerships, the respective Connector Partners act both as a data source (transmission of client master data and claim data to ICO) and – to the extent that the Connector Partner receives case status information from ICO – as a data recipient. The Connector Partners' access to case data at ICO is limited to the data of the clients referred by them. A list of active Connector Partners and the respective data categories transmitted is available upon request at datenschutz@incaseof.law.

Enquiries through the website

When you use our contact form, we process the contact details, company information, enquiry topic and message you provide to handle your enquiry. We use Mailchimp to store the enquiry, Pipedrive to manage it and Slack for internal notifications. Contact enquiries concern prospective clients only; no case, claim or debtor data is processed through these services. Submitting an enquiry does not create a newsletter subscription or trigger a newsletter confirmation email. Existing subscriptions are not changed by a contact enquiry.

Mailchimp: Intuit Privacy Statement. Pipedrive: Pipedrive Privacy Notice. Slack: Slack Privacy Policy.

9a. Newsletter

If you subscribe to our newsletter, we process your e-mail address and, where provided, your name for the purpose of sending it (Art. 6(1)(a) GDPR; you may withdraw your consent at any time via the unsubscribe link). For dispatch we use Mailchimp (Intuit Inc., USA); processing takes place in the USA

on the basis of the EU-U.S. Data Privacy Framework and standard contractual clauses. Newsletters contain no client, case or debtor data, and no such data is transmitted to Mailchimp. Mailchimp: Intuit Privacy Statement.

9b. AI-assisted processing of documents

To capture invoice data from documents that clients upload in the customer portal, we use AI-assisted text recognition (Google Cloud Vertex AI, region europe-west3, Frankfurt am Main). The provider does not use the submitted content to train AI models. Documents transmitted by clients or Connector Partners via the application programming interface (API), as well as evidence provided in disputed cases, are not evaluated automatically but are read exclusively by members of our case team. The legal basis is Art. 6(1)(b) and (f) GDPR.

10. Transfer of Data to Third Countries

All processors we engage for case, contract or debtor data operate the data centres used for us within the European Union; no such data of our clients is processed outside the EU. Some providers are established in the USA and may access data in the course of support or maintenance; our newsletter (section 9a) is sent via a US provider under the safeguards described there. Where the said recipients are not located in the European Economic Area (EEA) and no adequacy decision by the EU Commission exists for the third country in question, ICO ensures that any data transfer takes place on the basis of standard contractual clauses pursuant to Commission Implementing Decision (EU) 2021/914 or that other appropriate safeguards within the meaning of Art. 46, 47 or 49 GDPR are provided. Where providers established in the USA are certified under the EU-U.S. Data Privacy Framework, we additionally rely on the Commission adequacy decision of 10 July 2023.

11. Sub-processors

Due to our business model and the complexity of today's data processing, it is essential that we engage third parties as sub-processors. These third-party providers support us in areas including hosting our website and application, communication, code management, database management, email delivery, authentication, task management, ticketing, cloud services, file upload and payment processing. The following list is identical to Annex 3 of our Data Processing Agreement and states, for each sub-processor, its seat, service and processing location.

Sub-processors (as of 4 October 2026):

- Supabase Inc., San Francisco (USA) – Database, authentication, file storage of the platform – processing location: AWS eu-west-1, Ireland (test: eu-north-1, Stockholm) – EU region; Data Privacy Framework, SCC
- Railway Corp., San Francisco (USA) – Application servers (API, ERV gateway, PDF rendering, database) – processing location: Google Cloud europe-west4, Netherlands – EU region; SCC
- Vercel Inc., San Francisco (USA) – Web applications (customer portal, debtor portal, website, API docs) – processing location: fra1, Frankfurt (DE) – EU region; Data Privacy Framework, SCC
- Google Cloud EMEA Ltd., Dublin (IE) – AI-based document extraction (Vertex AI); sign-in via Google account (optional) – processing location: europe-west3, Frankfurt (DE); no use for training

– EU processing; Google Cloud DPA

- Twilio Ireland Ltd., Dublin (IE) – SMS, one-time codes, portal chat – processing location: Region IE1, Ireland – EU region; Twilio DPA
- Twilio SendGrid (Twilio Ireland Ltd.), Dublin (IE) – Transactional e-mail delivery – processing location: EU data residency – EU region; Twilio DPA
- Functional Software Inc. (Sentry), San Francisco (USA) – Error and performance monitoring – processing location: EU region, Frankfurt (DE) – EU region; Data Privacy Framework, SCC
- Cloudflare Inc., San Francisco (USA) – Network proxy, attack protection, bot check (transit) – processing location: Processing at EU locations; no storage of content data – Data Privacy Framework, SCC
- DIMOCO Payments GmbH, Vienna (AT) – Payment processing in the debtor portal – processing location: Austria – EU
- Österreichische Post AG (Einfach-Brief), Vienna (AT) – Printing and postal dispatch of letters – processing location: Austria – EU
- MANZ Solutions GmbH, Vienna (AT) – Electronic legal communication Austria (webERV) – processing location: Austria – EU
- procilon GmbH, Taucha (DE) – Electronic legal communication Germany (EGVP/EDA), from go-live – processing location: Germany – EU
- maesn GmbH, Berlin (DE) – Connection of accounting systems (sevDesk, Business Central, Odoo, Xero), only where used by the Client – processing location: EU – EU
- Pipedrive OÜ, Tallinn (EE) – Customer relationship management (Client master data, no debtor data) – processing location: EU – EU
- Slack Technologies Ltd., Dublin (IE) – Internal system notifications without personal case data – processing location: EU/USA – Data Privacy Framework, SCC
- Registered lawyers who are engaged in individual cases for legal out-of-court or judicial receivables management, following prior authorisation by the client (Austria, Germany).

Where a transfer of your personal data to countries outside the European Economic Area is necessary, we take appropriate protective measures, in particular the use of standard data protection clauses of the EU Commission pursuant to Art. 46 GDPR.

12. Data Retention

ICO retains your personal data for as long as necessary for the fulfilment of the purposes for which it was collected. In certain cases, however, we may be obliged to retain data for a specified period due to statutory or contractual requirements. We ensure that your personal data is protected and handled correctly throughout the retention period in accordance with this privacy policy and applicable data protection laws.

13. Your Data Protection Rights

You have the right to obtain information at any time about the personal data stored at ICO. This includes the right to find out where this data comes from, to whom it is transmitted and for what purpose it is processed. You also have the right to rectification, data portability and, under certain

circumstances, to object to or to restriction of the processing or deletion of your data.

Special features of Connector connections: If your data was transmitted to ICO by a Connector Partner, you have the right to obtain from ICO information on the scope of this transmission. The right to erasure (Art. 17 GDPR) relates to the data stored at ICO; deletion of data at the Connector Partner must be requested from that party separately. Please note that deletion of data stored at ICO may be restricted during ongoing collection proceedings due to statutory retention obligations.

If you believe that the processing of your personal data violates data protection regulations or that your data protection rights have been violated in any other way, you may lodge a complaint with the competent supervisory authority.

Austrian Data Protection Authority (Datenschutzbehörde), Barichgasse 40-42, 1030 Vienna, Phone: +43 1 52 152-0, Email: dsb@dsb.gv.at

In Germany: The Federal Commissioner for Data Protection and Freedom of Information (BfDI), Graurheindorfer Str. 153, 53117 Bonn, Email: poststelle@bfdi.bund.de

14. Contact

If you have questions about the processing of your personal data, wish to exercise your data protection rights or have other data protection concerns, please contact ICO at the following address:

incaseof.law GmbH, Rathausstraße 21/13, 1010 Vienna, Austria

Dr. Maximilian Kindler, LL.M., MBA

Email: datenschutz@incaseof.law

15. Changes to the Privacy Policy

ICO reserves the right to update or amend this privacy policy in order to adapt it to technical developments or legal changes, or in the course of the introduction of new services or products. Changes will always be published on our website. We therefore recommend that you regularly check the ICO website for updates to the privacy policy.

incaseof.law GmbH – Version 2.3 / 2026

Where we process personal data on behalf of our clients, we conclude a data processing agreement pursuant to Art. 28 GDPR. The contract text is available here: Data Processing Agreement (AVV, German) and English.

Previous versions

- Version 2.2 / 2026 (PDF)