

Data Processing Agreement

Annex 3 to the Terms of Service of SCCOT · version of 1 November 2026, effective from 1 November 2026 · English translation for information purposes only; the Polish version is binding.

§ 1. Parties and conclusion of the agreement

1. This agreement is concluded between the Subscriber as the data controller (hereinafter: the "Controller") and Appi Soft Sp. z o.o. with its registered office in Chodzież (hereinafter: the "Processor"), together with the agreement for the provision of the SCCOT Services, by acceptance of the Terms of Service. This agreement remains in force for the duration of the provision of the Services and for the period referred to in § 9.
2. This agreement is concluded on the basis of Article 28(3) GDPR. Terms not defined herein have the meaning given to them in the GDPR and in the Terms of Service.
3. This agreement does not apply to data of which the Processor is the controller, in particular Account, billing, marketing, security and support data, as well as **data on the use of the Application by the Controller and Users** (sessions, device type, activity in individual Modules), which the Processor processes for its own purposes of developing the Service and customer care. The rules for processing such data are set out in the Privacy Policy, section 3.5.

§ 2. Subject matter, nature and purpose of processing

1. The Controller entrusts the Processor with the processing of personal data entered into the Application by the Subscriber and Users solely for the purpose of providing the Services in accordance with the Terms of Service.
2. Nature of processing: storage, organisation, retrieval, display, generation of documents, sending of e-mail messages, making data available to End Customers and to integrations indicated by the Controller, creation of backup copies, erasure.
3. **Categories of data subjects:** the Controller's customers and business partners and their contact persons; recipients of offers and documents shared via a link; the Controller's employees and associates (to the extent of data entered into documents, projects and tickets); the Controller's subcontractors; senders and addressees of correspondence in the CRM Module; other persons whose data the Controller enters in free-text fields and files.
4. **Categories of data:** identification and contact data (first name, surname, company name, NIP, REGON, addresses, e-mail, telephone), data from offers, projects, invoices and tickets, labour cost data (e.g. names and rates), content of notes and correspondence, files and photographs (including metadata, e.g. location recorded in a photograph), information on the opening of a shared offer, the IP address of the recipient of a shared offer.
5. The Application is not intended for the processing of special categories of data (Article 9 GDPR), data relating to criminal convictions (Article 10 GDPR), PESEL numbers or scans of identity documents. If the Controller enters such data, it does so at its own responsibility and ensures a legal basis for their processing; the Processor applies to such data the security measures set out in Schedule 2.

§ 3. Obligations of the Processor

1. The Processor processes data solely on documented instructions from the Controller. An instruction within the meaning of Article 28(3)(a) GDPR includes in particular: acceptance of the Terms of Service, use by the Controller and Users of the functions of the Application in accordance with the Terms of Service, activation of a Module or an external integration (in particular Google Calendar, the Controller's own mail server in the CRM Module, the National e-Invoicing System (KSeF)) and a change of Plan. The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes data protection law.
2. The Processor ensures that persons authorised to process the data have committed themselves to confidentiality.
3. The Processor applies the technical and organisational measures set out in Schedule 2, appropriate to the risk (Article 32 GDPR).
4. The Processor assists the Controller, insofar as possible and taking into account the nature of the processing, in responding to requests from data subjects, in particular by means of the functions of the

Application enabling data to be searched, rectified, exported and erased. Requests addressed directly to the Processor are forwarded to the Controller within 7 days.

5. The Processor assists the Controller in ensuring compliance with the obligations under Articles 32–36 GDPR.
6. Authorised employees and associates of the Processor obtain access to data in the Controller's Account solely to the extent necessary for the provision of the Services, in particular to provide support, remedy a failure or error and ensure security.

§ 4. Sub-processors

1. The Controller grants the Processor general authorisation to engage sub-processors. The current List of Sub-processors constitutes Schedule 1 and is published together with this agreement on the website sccot.pl/regulaminy, in a dated version. Not all sub-processors listed in Schedule 1 participate in the processing of the data of every Controller; participation depends on the selected Plan and on the Modules and integrations activated by the Controller.
2. The Processor informs the Controller by e-mail of any intended addition or replacement of a sub-processor at least 14 days before the change. Within that period the Controller may raise a justified objection. If the parties do not agree on a solution, the Controller may terminate the agreement for the provision of the Services with effect from the date of the change.
3. The Processor imposes on sub-processors data protection obligations no less stringent than those arising from this agreement and is liable for their actions as for its own.
4. Providers of external services with which the Controller or a User activates an integration using their own account with such a service, in particular Google with respect to Google Calendar and the provider of the Controller's own mail server in the CRM Module, are not sub-processors. Data are transferred to such a service on the instructions of the Controller (§ 3(1)), and the scope of the data transferred is set out in the Module-Specific Terms and the Privacy Policy.

§ 5. Transfers of data outside the EEA

1. The Processor processes data on servers located in the European Economic Area: the Application servers, databases and files are located in Germany, and outgoing mail is sent from France. A transfer of data to a third country may take place only in the cases indicated in Schedule 1, on the basis of a European Commission decision finding an adequate level of protection (including the EU-US Data Privacy Framework) or standard contractual clauses.

§ 6. Personal data breaches

1. The Processor notifies the Controller of a personal data breach it has become aware of without undue delay, and no later than within 48 hours of becoming aware of it, providing the information referred to in Article 33(3) GDPR to the extent available (the remaining information without delay once established).
2. The Processor takes action to mitigate the effects of a breach and documents breaches.

§ 7. Audit

1. The Processor makes available to the Controller the information necessary to demonstrate compliance with the obligations under Article 28 GDPR, primarily in the form of written answers and documentation.
2. The Controller may carry out an audit, including an inspection, no more than once per calendar year, upon at least 30 days' prior notice. The audit is, as a rule, carried out remotely, on business days between 9:00 and 17:00, and lasts no longer than one business day. An inspection at the Processor's premises is possible where the remote form is insufficient to demonstrate compliance with the obligations under Article 28 GDPR or where a supervisory authority so requests, on a date agreed by the parties. The audit may not be carried out by an entity conducting business competing with the Processor, nor may it disrupt the Processor's business or breach the confidentiality of other customers' data. The costs of the audit are borne by the Controller.

§ 8. Liability

1. The liability of the parties under this agreement is subject to the limitations set out in § 12 of the Terms of Service, except for liability towards data subjects and cases in which a limitation is not permitted by law.
2. The Processor is not liable for the consequences of executing the Controller's instructions, including post-audit instructions and recommendations, if they are inconsistent with the GDPR or other generally applicable laws, of which the Processor has informed the Controller in accordance with § 3(1).

§ 9. Termination of processing

1. Following termination of the agreement for the provision of the Services, the Controller has 30 days to download the data using the export function (§ 17 of the Terms of Service). After that period, the Processor erases the data as follows: (a) from production systems within 7 days, (b) from cache, search indexes and logs containing data within 30 days, (c) from database backup copies in the course of their rotation cycle, no later than 7 days after erasure from production systems. Until erasure from backup copies, the data are not processed for any purpose other than restoring the Application after a failure. This provision does not apply to data whose further retention is required by law.
2. At the Controller's request, the Processor confirms the erasure of the data.

Schedule 1. List of Sub-processors

Version of 1 November 2026 · published on the website sccot.pl/regulaminy

Sub-processor	Scope / purpose	Processing location
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany	Application and database servers, backup copies	Falkenstein, Germany (EEA)
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg	File storage: attachments and photographs from the Application and correspondence and attachments of the CRM Module	Frankfurt, Germany (EEA)
Sendinblue SAS (Brevo), 106 boulevard Haussmann, 75008 Paris, France	Sending of e-mail messages: notifications, documents, confirmations, meeting bookings	France (EEA)
Functional Software, Inc. (Sentry), 45 Fremont St., San Francisco, USA	Error monitoring: technical identifiers, no data from documents	EU region (Germany); possible access from the USA (EU-US Data Privacy Framework)
Intercom R&D Unlimited Company, 2nd Floor, Stephen Court, Dublin, Ireland	Support chat: content of correspondence with the User	United States (EU-US Data Privacy Framework)

Schedule 2. Technical and organisational measures

The Processor applies the following technical and organisational measures, appropriate to the risk to the rights and freedoms of data subjects:

A. Infrastructure security

Measure	Description
Processing location	Application and database servers in a data centre within the European Economic Area (Falkenstein, Germany); files in a data centre in Frankfurt (Germany)
Encryption in transit	Connections to the Application and to providers' services encrypted using the HTTPS (TLS) protocol
Backup copies	Database and server backup once a day, retention of the last seven copies, encryption on the infrastructure provider's side. The ability to restore data from backup has been tested
Monitoring	Monitoring of the availability and performance of the Application and error monitoring, to which only technical identifiers are transmitted, without document content

B. Access control

Measure	Description
Data isolation between Controllers	Separation of the data of individual companies at Application level, verified by automated tests
User permissions	Roles and permissions granted by the Controller, in accordance with the principle of least privilege
Password storage	User passwords stored solely in the form of a cryptographic hash, which cannot be reversed
Protection of integration keys	Access tokens for external services activated by the User and API keys stored in encrypted form
Sign-in with a Google account	Option to use the security features of a Google account when signing in to the Application

C. Application security

Measure	Description
Protection against automated attacks	Protection of sign-in and registration forms against automated access attempts
Protection against actions performed without the User's knowledge	Security token for operations that modify data
Session expiry	Automatic termination of the session after a period of inactivity
Access control for materials shared via a link	Random, hard-to-guess addresses of offers, documents and the calendar; option to limit the access period and to generate a new address, which invalidates the previous one

D. Organisational measures

Measure	Description
Confidentiality	Persons authorised to process data are bound by confidentiality obligations (§ 3(2) of the Agreement)
Restriction of access to Accounts	Access by authorised employees and associates of the Processor to the Controller's Account solely to the extent necessary for the provision of the Services, on the terms set out in § 10 of the Terms of Service
Agreements with sub-processors	Processing entrusted to sub-processors solely on the basis of agreements ensuring a level of protection no lower than that arising from this Agreement

The Processor develops the measures applied as the Application develops. The Processor provides the Controller, at its request, with information on the measures currently applied, in accordance with § 7(1).