

Privacy Policy of SCCOT

SCCOT Application (app.sccot.pl), the sccot.pl website and business contacts · version of 1 November 2026, effective from 1 November 2026 · English translation for information purposes only; the Polish version is binding.

1. Controller of personal data

The controller of the personal data referred to in this Privacy Policy is Appi Soft Sp. z o.o., with its registered office in Chodzież, ul. Zwycięstwa 23, 64-800 Chodzież, entered in the register of entrepreneurs of the National Court Register under KRS number 0000867371, NIP 6070090336, REGON 387392804 (hereinafter: the "Controller"). In matters concerning the protection of personal data, the Controller may be contacted at the e-mail address kontakt@sccot.pl, by telephone at 502 634 517, or in writing at the address of the registered office. Capitalised terms have the meanings given to them in the Terms of Service of SCCOT.

2. Role of the Controller

- 1. The Controller acts as the controller** of the personal data of: Users of the Application (with respect to maintaining the Account, logging in, billing, technical support, security, communication, analytics and marketing), persons contacting the Controller and its business partners, visitors to the sccot.pl website, persons reporting illegal content, as well as data obtained from Google within an integration activated by the User (section 5).
- 2. The Controller processes data on behalf of** Subscribers with respect to the data entered by them into the Application, in particular data of their customers, business partners, contact persons, recipients of offers and documents, and correspondence conducted in the CRM module. The Subscriber is the controller of such data, and the Controller acts as a processor on the basis of the Data Processing Agreement. A person who has received an offer or a document via the Application should direct requests concerning their data to the sender; the Controller assists the sender in fulfilling such requests.

3. Scope, purposes and legal bases of processing

3.1. Users of the Application

Purpose	Data	Legal basis	Retention period
Creating and maintaining the Account, logging in (including via Google), provision of services	E-mail, password (stored in secured form), first name, surname, telephone, position or role, language, Google identifier, company data, year of birth and gender (if provided)	Contract (Article 6(1)(b) GDPR); with respect to employees and associates of the Subscriber: the Controller's legitimate interest consisting in the provision of the Services to the Subscriber (Article 6(1)(f) GDPR)	For the duration of the contract, including under the Free Plan; after deletion of the Account: 30 days to download the data, followed by deletion within 7 days; from backups in their rotation cycle, within a further 7 days
Adapting the Application to the Subscriber's business profile (onboarding wizard)	Industries, number of persons preparing offers, number of offers	Contract / legitimate interest	As above
Billing and invoices	Invoicing data, NIP, address, payment history (without card number)	Legal obligation (Article 6(1)(c) GDPR): tax and accounting regulations	5 years from the end of the year in which the tax liability arose
Technical support (chat, e-mail)	Account data, content of correspondence	Contract / legitimate interest	3 years from the end of the correspondence
Security, abuse prevention, form protection (reCAPTCHA), technical logs, error monitoring	IP address, browser data, identifiers, event logs	Legitimate interest of the Controller (Article 6(1)(f) GDPR)	14 days
Information on presence in the Application visible to	Date of last activity, current session	Legitimate interest of the Subscriber and the	Overwritten on an ongoing basis

Purpose	Data	Legal basis	Retention period
other Users of the Subscriber		Controller (organisation of work at the Subscriber)	
Communication concerning the Services (changes, renewals, payment reminders, outages)	E-mail, first name	Contract	For the duration of the contract
Direct marketing (newsletter, commercial information)	E-mail, first name, telephone	Consent (Article 6(1)(a) GDPR, Article 398 of the Polish Electronic Communications Law)	Until consent is withdrawn
Application usage analytics: statistics, measurement of feature effectiveness, interface analysis	Cookie identifiers, addresses of views visited, events, the User's identifier in the Application and basic information about the Subscriber and the Account (e.g. Plan, industry, number of offers, role), session recordings with masked text content (only the screen layout and cursor movement are recorded)	Consent (Article 6(1)(a) GDPR; Article 399 of the Polish Electronic Communications Law)	In accordance with the Cookie Policy
Marketing and measurement of advertising effectiveness (Google Ads, Meta pixel)	Advertising identifiers in cookies, events (registration, start of trial period, purchase including amount, currency and plan name)	Consent	In accordance with the Cookie Policy
Development of the Application and Subscriber support: analysis of feature usage carried out without the involvement of external tools	Described in section 3.5	Legitimate interest (Article 6(1)(f) GDPR) and, for part of the data, consent	Section 3.5
Establishment of and defence against claims	Data from the contract and correspondence	Legitimate interest	Until the limitation period for claims expires

3.2. Business partners and persons contacting the Controller

Purpose	Data	Legal basis	Retention period
Handling enquiries and correspondence	First name, surname, company, e-mail, telephone, content of the message	Legitimate interest of the Controller (Article 6(1)(f) GDPR)	3 years from the last contact
Conducting business relations and sales, arranging meetings	Contact details, position, history of contacts and meetings, sales notes	Legitimate interest	3 years from the last contact
Sending commercial information	E-mail, telephone	Consent	Until consent is withdrawn

3.3. Visitors to the sccot.pl website

In connection with the use of the sccot.pl website, the Controller processes data provided in forms and data collected by means of cookies, on the terms set out in the Cookie Policy (section 4).

Purpose	Data	Legal basis	Retention period
Responding to a message	First name, surname,	Legitimate interest (Article	3 years from the last

Purpose	Data	Legal basis	Retention period
sent via the contact form and conducting further business discussions	company, e-mail, telephone, content of the message	6(1)(f) GDPR)	contact
Business contact by electronic means or by telephone, where consent has been given in the form	E-mail, telephone	Consent (Article 6(1)(a) GDPR, Article 398 of the Polish Electronic Communications Law)	Until consent is withdrawn
Scheduling a presentation of the Application via the Brevo calendar	First name, surname, e-mail, telephone, company, selected date	Steps taken at the request of the data subject prior to entering into a contract (Article 6(1)(b) GDPR)	3 years from the last contact
Registration for and participation in online training	First name, surname, company, e-mail, telephone	Contract (Article 6(1)(b) GDPR)	3 years from the training
Sending the profitability calculator result to the indicated e-mail address	E-mail and data entered into the calculator	Action at the request of the data subject (Article 6(1)(b) GDPR)	Data are not stored; they are used solely for a one-time dispatch
Protection of forms against automated submissions (reCAPTCHA), server logs	IP address, browser data	Legitimate interest (Article 6(1)(f) GDPR)	14 days
Statistics and measurement of advertising effectiveness	Identifiers in cookies, subpages visited	Consent (Article 6(1)(a) GDPR, Article 399 of the Polish Electronic Communications Law)	In accordance with the Cookie Policy

3.4. Persons reporting illegal content (DSA)

Where content is reported which the reporting person considers illegal, the Controller processes the data provided in the report: first name and surname or name, e-mail address, the content of the report and the identification of the content to which the report relates.

Purpose	Legal basis	Retention period
Receiving and handling the report, notification of the decision and its statement of reasons	Legal obligation (Article 6(1)(c) GDPR) arising from Articles 16–17 of the Digital Services Act (DSA)	The time necessary to handle the report, followed by the period required by law
Data provided voluntarily beyond the scope necessary to handle the report	Consent (Article 6(1)(a) GDPR)	Until consent is withdrawn
Execution of orders of authorities and notification of suspected criminal offences (Article 18 DSA)	Legal obligation (Article 6(1)(c) GDPR)	The period required by law

3.5. Analysis of the use of the Application

The Controller analyses the manner in which the Application is used, including the extent of use of individual modules, the types of devices used and account activity. The analysis covers all Users, including employees and associates of the Subscriber. The data used for this purpose are processed exclusively by the Controller and are not transferred to providers of external analytics tools.

Purposes of processing: development and improvement of the Application, adaptation of the interface to the devices used by Users, identification of accounts with low activity in order to offer support to the Subscriber, and preparation of statistical summaries.

Data processed without the User's consent

Scope of data	Source	Legal basis
Sessions: date and time of start and end,	Operation of the Application	Legitimate interest of the Controller

Scope of data	Source	Legal basis
separately for each device, and the marking of the first session on the Account		(Article 6(1)(f) GDPR): development of the Services and Subscriber support
Device type (computer, phone, tablet), operating system and its version, browser and its version	Information sent automatically by the browser	As above
Activity: number and creation dates of offers, projects, tickets, records and RMS items, and the method of creating an offer (from scratch, from a template, from a copy)	Data stored in the Application	As above

Data processed solely on the basis of the User's consent

Upon consent being given to the use of cookies in the "analytics" category, the Application additionally reads: the browser window width, the browser language, the time zone, the connection quality, information on the use of the Application installed on the device, and information on whether the device has a touch screen. This information serves to adapt the layout of the Application to the User's device.

The legal basis for processing is the User's consent (Article 6(1)(a) GDPR) in conjunction with Article 399 of the Polish Electronic Communications Law. Consent may be withdrawn at any time on the "Privacy settings" screen in the account menu in the Application. Withdrawal of consent does not affect the lawfulness of processing carried out before its withdrawal. **Refusal of consent does not limit the ability to use the Application.**

Scope excluded from the analysis

For the purposes of analysing the use of the Application, the Controller does not record the User's IP address or location data and does not track the User's activity outside the Application.

Retention period

Data	Period
Sessions	24 months from the end of the session, followed by automatic deletion
First session on the Account	For the lifetime of the Account; after 24 months only the date and device type are retained
All sessions after deletion of the Account	Deleted or anonymised
Data processed on the basis of consent	After consent is withdrawn, data are no longer collected. Data collected previously are retained until 24 months have elapsed, or deleted earlier at the User's request

4. Voluntary nature of providing data

Providing the data necessary to create an Account is voluntary but is a condition for using the Application. Providing invoicing data is mandatory in the case of paid Plans, as required by tax law. Giving consent to receive commercial information and to the use of cookies other than strictly necessary cookies is voluntary, and refusal does not limit the ability to use the Application.

5. Data obtained from Google and e-mail correspondence

5.1. Logging in with Google

Where the User logs in with a Google account, the Controller receives the Google account identifier, the e-mail address and the first name and surname of the User, solely for the purpose of creating the Account and logging in. The Controller does not store the profile picture or any other data from the Google account and does not retain access to the Google account after logging in.

5.2. Google Calendar integration

The integration is optional and is activated by the User independently in the Application settings. The Application requires full access to Google Calendar, because the function of taking over events as tickets requires the ability to write to the User's calendar. Access is used solely within the scope of the functions described below.

Data sent to Google: names of tickets, projects and offers assigned to the User, their dates and time zone, and an identifier enabling an event to be linked to a ticket, and in the case of tickets also their description, notes, type, priority and status, the names of the related business partner, offer and project together with a link to the Application, and the first names and surnames of the assigned persons. This content is entered by Users and may contain customer data. Amounts, attachments and participant data are not sent to Google. Once connected, the Application creates a "SCCOT Tickety" calendar in the User's Google account and saves the User's tickets in it. Saving projects and offers in the "SCCOT Projekty" and "SCCOT Oferty" calendars is enabled by the User independently in the profile settings in the Application. Events are saved exclusively in these calendars and in events taken over by the User as a ticket. Changes to a ticket taken over from an event, including its deletion, are carried over to that event in the User's calendar.

Data read from Google: the e-mail address of the Google account and the list of calendars; events from the primary calendar (this function can be disabled in the settings; only their title and times are displayed in the Application); with the consent of co-workers: their busy time slots (without titles); within the "take over as ticket" function: the event indicated by the User; changes made in Google to events created by the Application and to events taken over as a ticket, which are carried over to the Application. For this purpose, the Application receives notifications from Google about changes in the primary calendar and in the calendars created by the Application.

Sensitive data: the content of events in the User's calendar is unrestricted and may contain particularly sensitive information (e.g. concerning a medical appointment). The Controller does not save the content of the User's private events in the database, does not analyse it and does not disclose it to anyone other than the User, including the owner of the Subscriber's account. Event data received from Google are stored temporarily in server memory, for no longer than 2 minutes, in order to speed up the display of the calendar. Only an event taken over by the User as a ticket is saved in the database.

Data stored: encrypted Google Calendar access credentials, the e-mail address of the Google account, calendar identifiers and links between events and tickets.

Disconnecting the integration: upon disconnection of the integration, the Controller deletes the access credentials and links and disables notifications about changes in the calendar. Calendars created by the Application remain in the User's Google account, and the User may delete them independently. The User may also revoke access at any time in the Google account settings. Upon deletion of the Account in the Application, the integration data are deleted.

Access to data: data from the integration are available exclusively to the User. The Controller's staff may view the integration settings only in connection with handling a User's request and with the User's consent, for security purposes (e.g. investigating an error or abuse), or where required by law.

Restrictions: data obtained from Google are used solely for the operation of the functions described. The Controller does not sell such data and does not use them for advertising purposes, creditworthiness assessment, or the development, training or improvement of artificial intelligence or machine learning models. Such data are not transferred to other entities unless this is necessary for the operation of the functions, required by law or necessary for security reasons.

The use and transfer to other applications of information received from Google APIs is carried out in accordance with the Google API Services User Data Policy, including the Limited Use requirements.

5.3. Calendar link (ICS)

The User may generate an address containing a random key at which the titles and dates of the User's tickets, projects, warranties and offers are available, in order to subscribe to them in another calendar program. Any person who knows this address has access to such data without logging in; therefore, the address should not be shared with third parties. The User may generate a new address at any time, which immediately invalidates the previous one.

5.4. E-mail correspondence

Messages sent by the Controller (registration confirmation, password change, notifications, payment reminders, newsletter) are sent via Sendinblue SAS (Brevo), with its registered office in France. The data are processed within the territory of the European Union.

E-mail in the CRM module is sent and received via the mail server indicated by the Subscriber in the mailbox settings; the e-mail provider is chosen by the Subscriber. The content and attachments of such correspondence are stored in the Application by the Controller as a processor, on the terms set out in the Data Processing Agreement.

6. Recipients of data

Personal data may be transferred to entities providing services to the Controller that are necessary for conducting its business and acting on its instructions, as well as to entities authorised under the law. Current list of recipients:

Recipient	Purpose	Location / transfer
Hetzner Online GmbH	Application and database servers, backups	Falkenstein, Germany (EEA)
Amazon Web Services EMEA SARL	File storage: attachments, photos, CRM correspondence	Frankfurt, Germany (EEA)
Sendinblue SAS (Brevo)	Transactional e-mail, newsletter, meeting booking	France (EEA)
Marcin Ćwiertnia JC HOST.PL, Modlniczka	Hosting of the sccot.pl website and handling of website forms	Poland
Stripe Payments Europe, Ltd.	Payment processing (card, BLIK, Przelewy24, bank transfer)	Ireland; part of the processing in the USA (DPF/SCC)
Fakturownia sp. z o.o.	Issuing the Controller's invoices	Poland
Intercom R&D Unlimited Company	Support chat	United States (EU–US Data Privacy Framework)
Functional Software, Inc. (Sentry)	Error monitoring (technical identifiers, no data from documents)	EU region (Germany); possible access from the USA (DPF)
Google Ireland Ltd	Logging in, Google Calendar (at the User's request), form protection (reCAPTCHA), website scripts, fonts	EEA + USA (DPF)
Google Ireland Ltd (Analytics and Ads)	Application usage statistics, measurement of advertising effectiveness	EEA + USA (DPF)
Meta Platforms Ireland Ltd	Measurement of advertising effectiveness (pixel)	EEA + USA (DPF)
Microsoft Corporation (Clarity)	Interface analysis: session recordings and heatmaps	USA (DPF)
Accounting firm and law firm serving the Controller	Accounting, legal services	Poland

6.1. Head of the National Revenue Administration (KSeF)

Where functions for issuing, sending or receiving structured invoices are used, the data contained in invoices are transferred via the National e-Invoicing System (KSeF). The transfer takes place on the instructions of the Subscriber, in connection with the performance of its obligations under tax law. With respect to the processing of data in KSeF, the Head of the National Revenue Administration (KAS) acts as a **separate controller** under the law; detailed information is provided in the information clauses of the National Revenue Administration.

7. Transfer of data to third countries

Personal data are, as a rule, processed within the European Economic Area. The Application servers and files are located in Germany, and e-mail is sent from France. Where data are processed by a provider outside the EEA (section 6), the transfer takes place on the basis of a European Commission decision finding an adequate level of protection (including the EU–US Data Privacy Framework with respect to certified entities) or standard contractual clauses approved by the European Commission. A copy of the safeguards applied may be obtained by contacting the Controller.

8. Rights of data subjects

The data subject has the right of access to the data and to obtain a copy thereof, the right to rectification, erasure, restriction of processing and data portability, the right to withdraw consent at any time (without affecting the lawfulness of processing carried out before its withdrawal), and the right to lodge a complaint with the President of the Personal Data Protection Office (UODO) (ul. Stawki 2, 00-193 Warszawa). Consent to receive commercial information may be withdrawn in the account settings or electronically, and consent to the use of cookies via the "Cookie settings" link in the website footer or on the "Privacy settings" screen in the account menu in the Application. The right to object is described in section 10.

The User may download a copy of the data from the Application independently in the account settings and, until this function is made available, upon request sent to kontakt@sccot.pl, free of charge, within 14 days.

9. Account activity score and automated decision-making

On the basis of the data described in section 3.5, the Controller calculates an **account activity score**, which determines the degree of use of the Application by the Subscriber, in particular the frequency of logging in and of creating offers, projects and tickets. The score is calculated **for the Subscriber as a whole, and not for individual Users**, and serves to identify accounts with low activity in order to offer support to the Subscriber.

The calculation of the score constitutes profiling within the meaning of Article 4(4) GDPR. **It does not constitute automated decision-making within the meaning of Article 22 GDPR:** the score does not produce legal effects or similarly significantly affect the User's situation, does not determine access to, the scope of or the price of the Services, and the decision to contact the Subscriber is taken by a member of the Controller's staff.

The Controller does not take decisions based solely on automated processing which would produce legal effects concerning the data subject or similarly significantly affect the data subject.

10. Right to object

The data subject has the right to object at any time to the processing of their data on the basis of the Controller's legitimate interest, including to the analysis of the use of the Application (section 3.5) and the calculation of the account activity score (section 9), on grounds relating to their particular situation. Upon receipt of an objection, the Controller shall cease processing such data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject.

An objection to the processing of data for direct marketing purposes may be lodged at any time and does not require justification. Upon its receipt, the Controller shall promptly cease processing the data for that purpose.

An objection may be submitted to kontakt@sccot.pl or in writing to the address of the Controller's registered office.

11. Cookies

The rules for the use of cookies and similar technologies are set out in the Cookie Policy available at sccot.pl/regulaminy. Consent to the use of cookies other than strictly necessary cookies may be changed at any time: on the sccot.pl website via the "Cookie settings" link in the footer, and in the Application on the "Privacy settings" screen in the account menu.

12. Changes to the Privacy Policy

The Controller informs of material changes to the Privacy Policy electronically or in the Application. Previous versions are available at sccot.pl/regulaminy.

Google user data (Limited Use disclosure)

SCCOT's use and transfer to any other app of information received from Google APIs will adhere to the Google API Services User Data Policy (<https://developers.google.com/terms/api-services-user-data-policy>), including the Limited Use requirements.