

Privacy Policy - Salecare

Language. This is a translation of the Polish document "Polityka Prywatności - Salecare", provided for convenience. The Polish version is the binding one; in the event of any discrepancy between the two, the Polish text prevails.

Introduction

1. This Privacy Policy (the **Policy**) describes the rules for processing personal data in connection with the use of the **Salecare** service (the **Service**) - a SaaS web application for sellers operating on the Allegro platform.
2. The Policy concerns personal data for which the **Operator (Service Provider) is the controller** - in particular the data of Users (sellers) who create and run an Account, billing data and the data of persons acting on the User's behalf.
3. **Personal data of the User's customers** (buyers/recipients of Allegro orders and people writing to mailboxes the User has connected to the Service), processed by the Service on the User's behalf, is subject to separate rules - in that respect **the User (seller) is the controller** and the Operator acts as a **processor** under the **Data Processing Agreement (DPA)**. Those rules are described in section 10 of the Policy and in the DPA itself (Schedule 2 to the Terms of Service).
4. Capitalised terms not defined in the Policy have the meaning given to them in the Terms of Service.

1. Data controller and contact

1. The controller of the personal data referred to in section 2 is the **Operator (Service Provider)**:
 - **Business name:** Simple Studio Piotr Hyra
 - **Legal form:** sole-trader business activity entered in the CEIDG register
 - **Address:** ul. Wręczycka 90, 42-133 Bieżeń, Poland
 - **VAT ID (NIP):** 5742060804 · **REGON:** 365542882
 - **E-mail address for data protection matters:** kontakt@salecare.pl
2. **Data Protection Officer (DPO).** The Operator has not appointed a Data Protection Officer - the statutory conditions requiring such an appointment are not met (Article 37 GDPR). For all data protection matters you may contact the Operator directly.
3. For all matters concerning the processing of personal data and the exercise of the rights referred to in section 8, you may contact the Operator at kontakt@salecare.pl.

2. What data we process and where it comes from

The Operator processes the following categories of data for which it is the controller:

1. **Account and contact data** - provided by the User on registration and while using the Service: the first name and surname of the person creating/operating the Account, e-mail address, sign-in credentials (the password is stored as a *hash*), optionally a telephone number, company details (name, address, VAT ID). If the User creates the Account or signs in through Google, Microsoft or Apple, the Operator receives the name and e-mail address from that service; that service is a separate controller of the sign-in data.
2. **Billing and tax data** - data necessary to issue an invoice and settle the Subscription and AI Wallet top-ups: company, address, VAT ID, the selected Plan, payment history, the payment token and technical transaction data (e.g. the last digits of the card number, the expiry date) received from the Payment Operator. **The Operator does not store the full card number or the CVC/CVV code.**
3. **Data retrieved from Allegro (on the User's instruction)** - in so far as it concerns the User as an entrepreneur (e.g. Allegro seller account identifiers, offer, settlement and commission data). This data is retrieved via the Allegro interface (API) on the basis of the authorisation granted by the User, and Allegro Ads advertising data is retrieved via the "Salecare Ads" extension from the User's Allegro Ads panel (see below). **Personal data of the User's customers** retrieved from Allegro orders is processed by the Operator as a processor - see section 10.
4. **Service usage data** - information about activity in the Service: operations performed, settings, use of AI features (the AI Assistant) and the related settlement of usage from the AI Wallet.
5. **Technical data and logs** - IP address, session identifiers, browser/device type, request dates and times, security events (sign-ins, errors). This data is collected automatically and serves to ensure security, diagnostics and the continuity of the Service.

Providing data is voluntary but necessary to conclude and perform the Agreement; providing invoicing data is additionally a statutory requirement (tax and accounting law). Without this data, use of the Service is not possible.

The "Salecare Ads" extension. The Allegro Ads features rely on an optional Chrome browser extension that the User installs voluntarily (§ 6 paragraph 10 of the Terms of Service). The extension runs solely in an open Allegro Ads panel tab, in the session the User is signed in to, and passes to the Service **advertising data only** (campaigns, ad groups, placements, statistics, bids and budgets). It passes no buyers' personal data and no order contents. The extension **does not read and does not transmit** Allegro sign-in credentials or Allegro cookies. Its storage (the browser's extension storage) holds the connection token for the Service, the advertising account identifier read from the panel, and state markers: the last sync date per account, the data range the panel accepted, a marker for a sync in progress (so several open panel tabs send the data once), and whether the tutorial has been seen. The extension also shows the User the recommendations and approved changes it fetches from the Service for the account open in the panel; that is the User's own data, displayed in their browser. Uninstalling the extension or disconnecting it in the Service (Settings → Salecare Ads) ends the transfer of data through this channel and invalidates the token.

3. Purposes and legal bases of processing

The Operator processes personal data solely for specified, lawful purposes. The legal bases are set out in Article 6 GDPR:

Purpose of processing	Legal basis (Article 6 GDPR)
Creating and running an Account, providing the Service, operating the Allegro integration	Article 6(1)(b) - performance of a contract
Handling payments, the Subscription and the AI Wallet	Article 6(1)(b) - performance of a contract
Issuing and storing invoices, keeping accounting and tax records (including KSeF), and for a User from another member state of the European Union, verifying the VAT number in the VIES system	Article 6(1)(c) - legal obligation (including the VAT Act, the Tax Ordinance, the Accounting Act)
Handling complaints and giving effect to data subject rights	Article 6(1)(c) - legal obligation; and (b) - performance of a contract
Ensuring the security of the Service, preventing abuse, logs and diagnostics	Article 6(1)(f) - legitimate interest (security of systems and data)
Establishing, exercising or defending legal claims	Article 6(1)(f) - legitimate interest
Service-related contact and information about material changes to the Service / Terms of Service	Article 6(1)(b) - performance of a contract; and (f) - legitimate interest
Replying to a message from the contact form and handling an access request from the form on the sign-up page (name, e-mail address, company name where given, message content)	Article 6(1)(b) - steps taken at the person's request prior to entering into a contract (the access request); and (f) - legitimate interest (replying to the message)
Marketing of our own services to existing Users (where carried out)	Article 6(1)(f) - legitimate interest; to the extent required by law - consent ((a)) and the prior consent to sending commercial information required by Article 398 of the Act of 12 July 2024 - Electronic Communications Law

The Operator does not take decisions in relation to Users based solely on automated processing which produce legal effects concerning them or similarly significantly affect them, within the meaning of Article 22 GDPR.

4. Recipients of the data

1. The Operator may disclose personal data only to entities authorised under the law and to **trusted providers (processors)** acting on its behalf, to the extent necessary to provide the Service. Processors are engaged under processing agreements meeting the requirements of Article 28 GDPR.
2. As regards data for which the **Operator is the controller**, the recipients are the following categories of entities:

Recipient category	Location	Purpose / scope
--------------------	----------	-----------------

Payment services provider (payment operator) - Stripe Payments Europe, Limited	Ireland (EEA), and also the United States (Stripe, Inc.)	Handling payments for the Subscription and AI Wallet top-ups
Invoicing system provider - Infakt sp. z o.o.	Poland (EEA)	Issuing, sending and storing VAT invoices - invoicing data (company, address, VAT ID, e-mail address)
Providers of artificial intelligence tools - Google (Gemini API), Jina AI GmbH , AlphaAI Technologies Inc. (Tavily), Replicate, LLC	United States, Germany	Delivery of AI features (including the AI Assistant, offer drafts, semantic search, product photo editing) - processing the content of prompts sent to the model
E-mail delivery provider - Plus Five Five, Inc. (Resend)	European Union (Ireland) and United States	Sending e-mail messages from the Service (including address confirmation, notifications, payment reminders) - the e-mail address and the message content
Mailbox provider - Hostinger International Ltd.	European Union (Cyprus), with possible processing on the provider's infrastructure outside the EEA	Running the kontakt@salecare.pl mailbox (including contact form messages, complaints and personal data requests) and backup sending of e-mail messages from the Service - the e-mail address, the message content and the data given in it
Providers of error and application monitoring - Better Stack, Inc. and Laravel Holdings Inc. (Laravel Nightwatch)	Better Stack: United States (AWS region us-west-2); Laravel Nightwatch: United States, European Union or Australia, depending on the data region chosen for the application, provider established in the United States	Detecting and diagnosing errors - technical request data (including the IP address and the page address with its parameters) and the data of the signed-in person (identifier, name, e-mail address)
Content delivery network provider - Cloudflare, Inc.	Global network of data centres, including the United States	Encrypted connection to the Service and attack protection - all traffic to the Service passes through this network, including the IP address
Web font provider - BunnyWay d.o.o. (Bunny Fonts)	European Union (Slovenia), the provider's server network	Delivering the typeface shown on the Service's pages - the IP address and browser data when the font is downloaded

Server management provider - Laravel Holdings Inc. (Laravel Forge)	United States	Server and deployment management - technical administrative access to the servers
Web analytics provider - Google Ireland Limited / Google LLC (Google Analytics)	Ireland (EEA) / United States	Measuring traffic and use of the Service's public pages - only after the User consents to analytics files (see section 9 and the Cookie Policy)
Form protection provider - Google Ireland Limited / Google LLC (reCAPTCHA)	Ireland (EEA) / United States	Telling a human from a bot in the sign-up form, the contact form and the access request form - IP address, browser data and information about the interaction with the form, on the basis of the Operator's legitimate interest (Article 6(1)(f) GDPR) in protection against spam, mass account creation and abuse
Server infrastructure provider (hosting) - Hetzner Online GmbH	European Union (Germany or Finland)	Infrastructure, application and database hosting, backups
European Commission (VIES system) and, through it, the tax administration of the User's member state	European Union	Verifying the VAT number of a User from another member state of the European Union, from the moment the Service Provider settles VAT for such Users - the VAT number, the company name and address, and the Service Provider's VAT number as the requester
Technical (IT) support providers, accounting office, law firm	European Union (EEA)	Support in running and operating the business - to the extent necessary

3. Beyond the above categories, recipients of the data may also be public authorities - to the extent and on the basis provided for by law.
4. At the request of a data subject, the Operator will identify the **specific recipients** of their data (Article 15(1)(c) GDPR).
5. The named list of these entities, with the registered office, role, scope of data, processing location and transfer basis of each, is set out in **Schedule B to the DPA** (Schedule 2 to the Terms of Service). The same list covers the sub-processors that process **the data of the User's customers** (where the Operator is a processor).

5. Transfers of data to third countries

1. As a rule, data is processed within the European Economic Area (EEA).
2. Some of the recipients listed in section 4 are established or process data **outside the EEA, in particular in the United States** (including the providers of artificial intelligence tools, e-mail delivery, error monitoring, the content delivery network and server management). This involves a **transfer of data to a third country** within the meaning of Chapter V GDPR (Articles 44–49). Schedule B to the DPA states the location and the transfer basis for each of these entities.
3. The transfer takes place in accordance with Chapter V GDPR. To the extent that the recipient is certified under the **EU-US Data Privacy Framework**, the basis for the transfer is the **European Commission's adequacy decision** (Article 45 GDPR); independently of that, the **standard contractual clauses (SCC)** adopted by the European Commission (Article 46 GDPR) are applied, together with additional measures where required. Google, as the provider of the Gemini models, is contractually obliged not to use the transferred content to train models.
4. If the User consents to **analytics files**, data about the use of the Service's public pages processed within **Google Analytics** may be transferred to **Google LLC established in the United States**. Google LLC is certified under the **EU-US Data Privacy Framework**, so the basis for the transfer is the **European Commission's adequacy decision** (Article 45 GDPR); the **standard contractual clauses** apply in addition (Article 46 GDPR). Without the User's consent the tool is not loaded and no data is transferred.
5. When the User starts filling in the sign-up form, the contact form or the access request form, the Service loads **Google reCAPTCHA**, which involves sending the IP address, browser data and information about the interaction with the form to **Google Ireland Limited**, and - to the extent Google uses infrastructure in the United States - to **Google LLC**. Google LLC is certified under the **EU-US Data Privacy Framework**, so the basis for the transfer is the **European Commission's adequacy decision** (Article 45 GDPR); the **standard contractual clauses** apply in addition (Article 46 GDPR). Merely opening a page with such a form does not load reCAPTCHA, and Google verifies the answer itself when the form is submitted. The Service does not use reCAPTCHA on pages without such a form.
6. To limit the scope of data transferred outside the EEA, the Operator seeks to **minimise the data** sent to AI features. The User decides whether and to what extent to use the AI Assistant.
7. A copy of, or information about, the safeguards applied to transfers can be obtained by contacting the Operator at kontakt@salecare.pl.

6. Data retention period

1. Data is processed for the period necessary to achieve the purposes for which it was collected and, thereafter, for the period arising from the law or until claims become time-barred:
 - **Account data and User Data** - for the term of the Agreement; after it ends, the data is available for self-service download for **30 days** (the download window, in accordance with Article 25 of Regulation (EU) 2023/2854 and § 18 of the Terms of Service), and is then deleted or anonymised after a grace

period of **90 days** from the end, subject to the exceptions below;

- **invoices and settlement documents** - for the period required by tax and accounting law (as a rule **5 years** counted from the end of the calendar year in which the tax payment deadline fell); VAT invoices are issued and stored in the invoicing system of **Infakt sp. z o.o.**, and payment documents with the Payment Operator, where they are kept for the required period regardless of the deletion of the Account in the Service, and therefore operational billing data in the Service is deleted together with the Account; the exception is the record of the VAT number check in the VIES system (the VAT number, the register's answer with the company name and address, and the consultation number) and of the confirmation of the registered office of a company outside the European Union, which is the evidence for applying the reverse charge on the invoices and is kept for the same period as they are;
- **data from the contact form and from an access request** - for as long as needed to reply and deal with the matter, and for an access request until the Account is created, no longer than **12 months** after the last message on the matter; the server log entry recording that the form was sent (the e-mail address, and for an access request also the company name) is deleted after **14 days**;
- **data for the purposes of claims** - until the limitation period for claims arising from the Agreement expires;
- **logs and security data** - for **12 months**, unless longer retention is necessary to investigate a security incident.

2. After the relevant period expires, the data is deleted or irreversibly anonymised.

3. The rules for storing and deleting **the data of the User's customers** (where the Operator is a processor) are set out in the DPA.

7. Data security

The Operator applies technical and organisational measures appropriate to the risk (Article 32 GDPR), in particular: encryption of connections, access control and restriction on a need-to-know basis, separation of individual Users' data (so that one User cannot access another's data), regular backups, event logging and security monitoring.

8. Data subject rights

1. A data subject has the following rights:

- the **right of access** to the data and to obtain a copy of it (Article 15 GDPR);
- the **right to rectification** of inaccurate data or completion of incomplete data (Article 16 GDPR);
- the **right to erasure** ("the right to be forgotten") - in the situations set out in Article 17 GDPR;
- the **right to restriction of processing** (Article 18 GDPR);
- the **right to data portability** - as regards data processed on the basis of a contract or consent, by automated means (Article 20 GDPR);

- the **right to object** to processing based on a legitimate interest (Article 21 GDPR);
 - the **right not to be subject** to a decision based solely on automated processing, including profiling (Article 22 GDPR);
 - where processing is based on consent - the **right to withdraw it** at any time, without affecting the lawfulness of processing carried out before the withdrawal.
2. To exercise these rights, please contact the Operator at kontakt@salecare.pl. The Operator responds without undue delay and no later than within one month of receiving the request (with the possibility of an extension in accordance with Article 12 GDPR).
 3. **Complaint to a supervisory authority.** A data subject has the right to lodge a complaint with the supervisory authority - the **President of the Personal Data Protection Office (PUODO)**, ul. Stawki 2, 00-193 Warsaw, Poland, <https://uodo.gov.pl>.
 4. Where a request concerns **data of a User's customer** (where the User is the controller and the Operator a processor), the Operator will - where possible - forward the request to the relevant User (controller) and support them in handling it in accordance with the DPA.
-

9. Cookies

1. The Service uses cookies and similar technologies in order to provide the Service correctly, remember the User's preferences and - with consent - measure traffic. A detailed list of files, their purposes and storage times is set out in the separate **Cookie Policy** available in the Service.
2. **Necessary files** (including maintaining the session and authenticating a signed-in User, protection against CSRF attacks, protecting the sign-up, contact and access request forms against bots with **Google reCAPTCHA**, remembering the cookie choice itself) are required for the Service to work and are used on the basis of **Article 399(3) of the Act of 12 July 2024 - Electronic Communications Law (PKE)**. Their use **does not require prior consent**.
3. **Preference files** (remembering the chosen language, theme or interface layout) are saved solely as a result of an **explicit action by the User** and serve to deliver the function they requested - they are used on the basis of **Article 399(3) PKE** and likewise **do not require prior consent**.
4. **Analytics files** are used solely **after obtaining the User's prior consent**, given through the **consent banner**. The basis is **Article 399(1) PKE** and **Article 6(1)(a) GDPR** (consent). In this category the Service uses **Google Analytics** (loaded only after consent is given). **The Service does not use marketing or advertising files.**
5. Consent is voluntary and may be **withdrawn or changed at any time** through the "Cookie settings" link in the footer of the home page and of the pages describing the Service's features. After consent is withdrawn, the Service stops loading the analytics tool and deletes the cookies it saved. Withdrawing consent does not affect the lawfulness of processing carried out before the withdrawal.
6. The User may also manage cookies in their browser settings, including deleting or blocking them; restricting necessary cookies may, however, prevent the Service from working correctly (e.g. signing in).

7. Using Google Analytics may involve a **transfer of data to a third country (the USA)** - on the terms and with the safeguards described in section 5.
-

10. Personal data of the User's customers (the processor role)

1. As part of the Service, the Service processes **personal data of the User's customers** (buyers/order recipients), retrieved from Allegro on the User's behalf - in particular: first name, surname, address, e-mail address, telephone number. **The Service does not retrieve the PESEL national identification number from Allegro.** If the User connects a mailbox to the Service, the Service retrieves on the User's behalf all messages from the folder the User indicates (INBOX by default), together with the senders' addresses and details, the message content and attachments; in this respect, too, the Operator acts as a processor.
 2. In respect of this data, **the User (seller) is the controller**, deciding on the purposes and means of its processing, and **the Operator acts solely as a processor** - processing the data only on the User's documented instructions, for the purpose of providing the Service.
 3. The rules for this processing - including the subject matter, duration, nature and purpose of the processing, the type of data, the categories of data subjects, the parties' obligations, sub-processing and security measures - are set out in the **Data Processing Agreement (DPA)**, which constitutes **Schedule 2 to the Terms of Service** and is accepted by the User upon conclusion of the Agreement.
 4. **The Operator bears no controller's liability towards the User's customers** for this data; the controller's obligations (including the information obligation under Articles 13/14 GDPR towards its own customers and the legal basis for processing) rest with the User.
-

11. Changes to the Privacy Policy

1. The Operator may update the Policy, in particular where the law, the scope of the Service, the list of sub-processors or the safeguards applied change.
 2. The Operator informs Users of material changes in the manner customary in the Service (e.g. by a notice in the panel or by e-mail), with appropriate advance notice, at least 14 days before the change takes effect.
 3. The current version of the Policy is available in the Service at all times, together with the date of its last update.
-