

Data Processing Agreement (DPA)

Schedule 2 to the Terms of Service for the electronic provision of services - Salecare

Language. This is a translation of the Polish document "Umowa Powierzenia Przetwarzania Danych Osobowych (DPA)", provided for convenience. The Polish version is the binding one; in the event of any discrepancy between the two, the Polish text prevails.

Preamble

1. This Data Processing Agreement (the **DPA**) constitutes **Schedule 2 to the Terms of Service** for the electronic provision of services - Salecare (the **Terms of Service**) and an integral part thereof. It is concluded between:
 - the **Controller** - the **User** (seller) who has concluded with the Operator an Agreement for the provision of the Service on the terms of the Terms of Service, and
 - the **Processor** - the **Operator (Service Provider)**: Piotr Hyra, conducting sole-trader business activity under the name **Simple Studio Piotr Hyra**, with its registered address at ul. Wręczycka 90, 42-133 Bieżeń, Poland, entered in the CEIDG register, VAT ID (NIP) 5742060804, REGON 365542882.
2. The DPA is accepted by the User upon conclusion of the Agreement (acceptance of the Terms of Service) and binds the parties for the term of the Agreement.
3. Capitalised terms not defined in the DPA have the meaning given to them in the Terms of Service. **GDPR** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
4. The DPA governs solely the processing of **personal data of the User's customers** (buyers/order recipients) and **of people writing to mailboxes the User has connected to the Service**, in respect of which **the User is the controller and the Operator is the processor**. Processing of data for which the Operator is the controller (including Account and billing data) is described in the **Privacy Policy** and is not covered by this DPA.

§ 1. Subject matter and nature of the entrustment

1. The Controller entrusts the Processor with the processing of personal data within the scope and for the purpose described in **Schedule A**, and the Processor undertakes to process such data solely on the terms set out in the DPA, the GDPR and other applicable data protection law.
2. The **subject matter, nature, purpose and duration** of the processing, the **type of personal data** and the **categories of data subjects** are set out in detail in **Schedule A** to the DPA (in accordance with Article 28(3) GDPR).
3. The entrustment is made for the purpose of, and to the extent necessary for, the Processor's provision of the Service to the Controller in accordance with the Terms of Service.

§ 2. Duration

1. The DPA applies for the term of the Agreement for the provision of the Service.
 2. Termination or expiry of the Agreement ends the DPA, subject to the handling of data after the end of processing (§ 11) and to provisions which by their nature survive (including those on confidentiality).
-

§ 3. Processor's obligations - general rules

The Processor undertakes in particular to:

1. **Process solely on documented instructions from the Controller** (Article 28(3)(a) GDPR), including with regard to transfers of data to a third country - unless required to do so by Union or Member State law; in such a case the Processor informs the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The Controller's **configuration and manner of use of the Service** in the Service panel, as well as the provisions of the Terms of Service and the DPA, also constitute documented instructions.
 2. **Immediately inform the Controller** if, in the Processor's opinion, an instruction given to it infringes the GDPR or other data protection provisions (second sentence of Article 28(3) GDPR).
 3. **Process the data solely within the scope and for the purpose** provided for in the DPA and the Terms of Service; the Processor does not process the entrusted data for its own purposes.
-

§ 4. Confidentiality

1. The Processor ensures that persons authorised to process the entrusted data have **committed themselves to confidentiality** or are under an appropriate statutory obligation of confidentiality (Article 28(3)(b) GDPR).
 2. The Processor limits access to the entrusted data to persons for whom it is necessary in order to deliver the Service, and grants and records processing authorisations.
-

§ 5. Security of processing

1. The Processor implements appropriate **technical and organisational measures** to ensure a level of security appropriate to the risk, in accordance with **Article 32 GDPR** (Article 28(3)(c) GDPR).
 2. A list of the security measures applied is set out in **Schedule C** to the DPA. The Processor may update them provided that at least an equivalent level of security is maintained.
-

§ 6. Sub-processing (further processors)

1. The Controller grants the Processor **general prior authorisation** to engage further processors (sub-processors) in order to deliver the Service (Article 28(2) GDPR). The named list of sub-processors, stating

the name, registered office, role, scope of data, processing location and transfer basis of each, is set out in **Schedule B** to the DPA, made available to the Controller together with the DPA before the Agreement is concluded.

2. The Processor ensures that **the same data protection obligations** as set out in this DPA are imposed on any further processor by contract, in particular the obligation to provide sufficient guarantees to implement appropriate technical and organisational measures (Article 28(4) GDPR). The Processor remains fully liable to the Controller for the performance of that sub-processor's obligations.
 3. **Notification of changes.** The Processor informs the Controller of intended changes concerning the addition or replacement of sub-processors (e.g. by a notice in the Service panel or by e-mail) at least **30 days** before the change is made, giving the Controller the opportunity to **object**.
 4. **Right to object.** If the Controller raises a reasoned objection to a change of sub-processor within **30 days** of being informed, the parties will seek a solution in good faith. If no agreement is possible and the Processor decides to engage that sub-processor, the Controller is entitled to **terminate the Agreement** (on the terms of the Terms of Service); continued use of the Service after the change is made means no objection is raised.
-

§ 7. Assistance with data subject rights

1. Taking into account the nature of the processing, the Processor **assists the Controller in so far as possible** - by appropriate technical and organisational measures - in fulfilling the obligation to respond to requests from data subjects exercising their rights laid down in Chapter III of the GDPR (Articles 15-22) - Article 28(3)(e) GDPR.
 2. Where a data subject addresses a request directly to the Processor, the Processor will - where possible - forward that request to the Controller without undue delay and will not act on it itself without the Controller's instruction.
-

§ 8. Assistance with the obligations under Articles 32-36 GDPR

Taking into account the nature of the processing and the information available to it, the Processor **assists the Controller** in complying with the obligations set out in Articles 32-36 GDPR (Article 28(3)(f) GDPR), namely as regards:

1. ensuring the security of processing (Article 32);
 2. notifying **personal data breaches** to the supervisory authority (Article 33) - the Processor notifies the Controller of any breach of the security of the entrusted data **without undue delay** after becoming aware of it, providing the information necessary for the Controller to fulfil its obligations;
 3. communicating a breach to the data subjects (Article 34);
 4. carrying out **data protection impact assessments** (DPIA - Article 35) and prior consultation with the supervisory authority (Article 36).
-

§ 9. Audit and demonstrating compliance

1. The Processor **makes available to the Controller all information** necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and **allows for and contributes to audits, including inspections, conducted by the Controller** (or an auditor mandated by the Controller) - Article 28(3)(h) GDPR.
 2. The parties agree that audits take place: after prior notice given a reasonable time in advance (at least **14 days**), during business hours, in a manner that does not unduly interfere with the Processor's operations, and with respect for the confidentiality and security of the data of the Processor's other clients. In the first instance, the Processor may demonstrate compliance by making available current documentation, a description of security measures, or certifications/audit reports it holds.
 3. The Processor immediately informs the Controller if, in its opinion, an audit instruction infringes the GDPR or other data protection provisions.
-

§ 10. Transfers to third countries

1. As a rule, the entrusted data is processed within the European Economic Area (EEA).
 2. To the extent that delivery of the Service involves a transfer of the entrusted data to a third country (to the sub-processors listed in Schedule B that process data outside the EEA, in particular in the **United States**, including in connection with AI features initiated by the Controller), the transfer takes place solely in accordance with Chapter V GDPR: to the extent that the provider is certified under the **EU-US Data Privacy Framework** - on the basis of the European Commission's adequacy decision (Article 45 GDPR), and independently of that, applying the **standard contractual clauses (SCC)** adopted by the European Commission (Article 46 GDPR) as a supplementary safeguard, together with additional measures where required.
 3. Details of sub-processor locations and the basis for transfers are set out in **Schedule B**.
-

§ 11. Handling of data after the end of processing

1. After the provision of the Service ends (termination or expiry of the Agreement), the Processor - at the Controller's choice - **deletes or returns** to the Controller all entrusted personal data and deletes any existing copies thereof, unless Union or Member State law requires further storage of the data (Article 28(3)(g) GDPR).
 2. The Controller may download/export the entrusted data during the term of the Agreement and for **30 days** after it ends (the self-service download window, in accordance with Article 25 of Regulation (EU) 2023/2854 and § 18 of the Terms of Service). The Processor deletes the entrusted data and copies thereof after a grace period of **90 days** from the end of the Agreement, absent a different decision by the Controller, save for backups, which are deleted in line with their rotation cycle.
-

§ 12. Liability and final provisions

1. Each party is liable for damage caused by its processing which infringes the GDPR, on the terms set out in Article 82 GDPR. The limitations of liability arising from the Terms of Service apply to the extent permitted by mandatory provisions of law.
 2. Matters not governed by the DPA are subject to the provisions of the Terms of Service, the GDPR and Polish law.
 3. In the event of a conflict between the DPA and the Terms of Service, **the provisions of the DPA prevail** as regards the processing of the entrusted personal data.
 4. The DPA is amended following the procedure applicable to amendments of the Terms of Service (§ 19 of the Terms of Service), respecting the requirements of Article 28 GDPR.
-

Schedule A - Description of the processing (Article 28(3) GDPR)

Element	Description
Subject matter of the processing	Processing of personal data of the Controller's customers (buyers) contained in orders and related correspondence, retrieved from Allegro, and of the data of people writing to mailboxes the Controller has connected to the Service, for the purpose of providing the Salecare Service.
Nature of the processing	Operations on data performed in an IT system (SaaS): retrieval via the Allegro interface (API), storage, organisation, display, analysis (including margin, returns and complaints analysis), export and - on the Controller's instruction - handling of correspondence/discussions and commission refund requests. Once a mailbox is connected, the Service retrieves all messages from the folder the Controller indicates (INBOX by default), without selecting senders, stores them together with their attachments, prepares their content for semantic search, creates reply drafts on the Controller's instruction and sends replies through that mailbox.
Purpose of the processing	Providing the Controller with the Service's features (analytics, order and correspondence handling, including from connected mailboxes, alerts, exports, AI Assistant) within the scope of the selected Plan, in accordance with the Terms of Service.

Element	Description
Duration	For the term of the Agreement for the provision of the Service, taking into account the grace period for the return/deletion of data (§ 11).
Type of personal data	Contact details of customers (buyers) from Allegro orders: first name, surname, address (delivery/billing), e-mail address, telephone number , order identifiers and correspondence/discussion data. From connected mailboxes: the sender's e-mail address, the name given in the message, the subject, the message content and attachments , and any other data the sender put in them. The Service does not retrieve the PESEL national identification number from Allegro and does not require special categories of data (Article 9 GDPR). Messages from a connected mailbox may contain such data where the sender put it in them.
Categories of data subjects	Customers (buyers/order recipients) of the Controller making purchases on the Controller's Allegro account. People writing to mailboxes the Controller has connected to the Service , including buyers from other sales channels, suppliers, carriers and other correspondents, as well as people whose data the sender put in a message.

Schedule B - List of sub-processors

The Processor uses the entities listed below. **Table 1** covers the sub-processors that the Controller's entrusted buyer data may reach. **Table 2** covers providers that receive no entrusted data and process only the Controller's own data as a User (including Account data and invoicing data), described in the Privacy Policy; they are listed here so that the whole list sits in one place.

The basis for transferring data outside the EEA is the European Commission's adequacy decision (the EU-US Data Privacy Framework, **DPF**, Article 45 GDPR), to the extent that the entity concerned is certified under it, and in addition the standard contractual clauses adopted by the European Commission (**SCC**, Article 46 GDPR), together with additional measures where required.

Table 1. Sub-processors that entrusted data may reach

Entity	Registered office	Role	Data	Processing location	Transfer outside the EEA
Hetzner Online GmbH	Gunzenhausen, Germany	Application and database servers, storage of files and backups	All Service data, including entrusted data	European Union (Germany or Finland)	Not applicable (EEA)
Cloudflare, Inc.	San Francisco, United States	Content delivery network, encrypted connection to the Service, attack protection	All traffic to the Service, including the IP address and the data sent	Global network of data centres, including the United States	DPF and SCC
Laravel Holdings Inc. (Laravel Forge)	United States	Server and deployment management, technical administrative access to the servers	Access to the servers holding the data; no permanent storage of Service data	United States	SCC
Laravel Holdings Inc. (Laravel Nightwatch)	United States	Monitoring of application performance and errors	Technical data on requests and jobs, including the visitor's IP address and the page address with its parameters (e.g. a search phrase typed in), data of the signed-in person (identifier, name, e-mail address), error content that may contain fragments of entrusted data	United States, European Union or Australia, depending on the data region chosen for the application; the provider is established in the United States	SCC

Entity	Registered office	Role	Data	Processing location	Transfer outside the EEA
Better Stack, Inc.	United States	Application error monitoring	Technical error data, including the page address with its parameters, that may contain fragments of entrusted data	United States (AWS region us-west-2)	DPF and SCC
Plus Five Five, Inc. (Resend)	San Francisco, United States	Sending e-mail messages from the Service	The recipient's e-mail address and the message content, which may contain order data and the buyer's login	European Union (Ireland, sending region) and United States	DPF and SCC
Google Cloud EMEA Limited and Google LLC (Gemini API)	Dublin, Ireland and Mountain View, United States	Artificial intelligence models for the AI Assistant, offer and reply drafts, the safety check of reply drafts and image generation	The content of prompts and the context passed to the model, including, on the Controller's instruction, messages from buyers and from correspondents of connected mailboxes, their logins or e-mail addresses and order data; product photos. The provider does not use this data to train models	United States and other countries where Google processes data	DPF and SCC

Entity	Registered office	Role	Data	Processing location	Transfer outside the EEA
Jina AI GmbH (Elastic group)	Berlin, Germany	Turning texts into vectors and ranking them for semantic search and the knowledge base	Texts of offers, products and seller replies; in discussion search, the subject, the buyer's login or the sender's e-mail address and fragments of the latest messages, including from connected mailboxes	The provider's cloud infrastructure, which may include countries outside the EEA	SCC, where data leaves the EEA
Hostinger International Ltd.	Larnaca, Cyprus	The kontakt@salecar.e.pl mailbox (the Controller's requests and correspondence) and backup sending of e-mail messages from the Service	The sender's or recipient's e-mail address and the message content, which may contain order data and the buyer's login	European Union, with possible processing on the provider's infrastructure outside the EEA	SCC, where data leaves the EEA

Table 2. Providers that receive no entrusted data

Entity	Registered office	Role	Data	Processing location	Transfer outside the EEA
Stripe Payments Europe, Limited	Dublin, Ireland	Handling payments for the Subscription and AI Wallet top-ups	The payer's (Controller's) data and transaction data	Ireland and United States (Stripe, Inc.)	DPF and SCC
Infakt sp. z o.o.	Kraków, Poland	Issuing, sending and storing VAT invoices	The Controller's invoicing data (company, address, VAT ID, e-mail address)	Poland	Not applicable (EEA)

Entity	Registered office	Role	Data	Processing location	Transfer outside the EEA
AlphaAI Technologies Inc. (Tavily)	New York, United States	Searching the web for product information when creating offer drafts	Product queries (name, EAN code, manufacturer)	United States	SCC
Replicate, LLC	San Francisco, United States	Removing backgrounds and cutting out products in photos	Product photos	United States	SCC
Google Ireland Limited and Google LLC (reCAPTCHA)	Dublin, Ireland and Mountain View, United States	Protecting the sign-up form, the contact form and the access request form against bots	IP address, browser data and information about the interaction with the form	Ireland and United States	DPF and SCC
Google Ireland Limited and Google LLC (Google Analytics)	Dublin, Ireland and Mountain View, United States	Measuring traffic on the Service's public pages, only after consent to analytics files	Cookie identifiers and visit data	Ireland and United States	DPF and SCC
BunnyWay d.o.o. (Bunny Fonts)	Slovenia	Delivering the typeface shown on the Service's pages	IP address and browser data when the font is downloaded	The provider's server network, provider established in the European Union	Not applicable (EEA)

Updating the list. The Processor informs the Controller of an intended addition or replacement of a sub-processor in accordance with § 6 (advance notice and the right to object). The current list is always available in this Schedule, and upon request sent to kontakt@salecare.pl the Processor also provides information about the processing agreements concluded with the sub-processors.

Note. Some features of the Service run on infrastructure controlled by the Processor and do not involve any additional external sub-processors.

Allegro. Allegro, from which data is retrieved on the Controller's instruction, is a **separate, independent controller** in respect of that data and is not a sub-processor of the Processor within the meaning of this DPA.

Schedule C - Technical and organisational measures (Article 32 GDPR)

The Processor applies in particular the following security measures:

1. **Encryption of connections** - communication with the Service and between its components takes place over an encrypted connection.
2. **Access control** - access to data on a need-to-know and least-privilege basis; authentication of Users (passwords stored as hashes); a record of authorisations.
3. **Separation of User data** - logical separation of individual Users' data, so that one User cannot access another's data.
4. **Backups** - regular backups allowing data to be restored in the event of a failure.
5. **Logging and monitoring** - logging of security and access events, monitoring for irregularities.
6. **Data minimisation** - limiting the scope of data retrieved from Allegro and of data sent to AI features to the necessary minimum.
7. **Sub-processor management** - verification of sub-processors' security guarantees and imposition of equivalent obligations on them (§ 6).
8. **Testing and assessing effectiveness** - regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of the processing (Article 32(1)(d) GDPR).

The Processor periodically reviews and - in line with the risk and the state of the art - updates the above measures, maintaining at least an equivalent level of security.