Data Processing Agreement

MERIDIAN AUTOMATION LTD · Signed 6 November 2026 · https://www.the-meridian.ai/dpa

Standard contractual clauses

Section I

Clause 1: Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2: Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3: Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4: Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Optional: Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

Section II: Obligations of the Parties

Clause 6: Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7: Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

(a) The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended

changes of that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8: Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its

obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9: Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(2) the likely consequences of the personal data breach;

(3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

Section III: Final provisions

Clause 10: Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I: List of parties

Controller(s):

1. Name: the organization that accepts the Meridian Terms of Service, as named in its Meridian account.

Address: the address in its Meridian billing details.

Contact person's name, position and contact details: the owner of the organization's Meridian account.

Signature and accession date: acceptance of the Meridian Terms of Service, on the date of acceptance.

Processor(s):

1. Name: MERIDIAN AUTOMATION LTD

Address: 128 Derech HaHagana, Tel Aviv-Yafo 6742289, Israel

Contact person's name, position and contact details: Sacha LEVY, Chief Executive Officer, privacy@the-meridian.ai

Signature and accession date:



Sacha LEVY, 6 November 2026

ANNEX II: Description of the processing

Categories of data subjects whose personal data is processed

Merchants that install the controller's Shopify apps, and their staff. Customers of those merchants, where the controller's apps process their data. The controller's affiliates.

Categories of personal data processed

Contact details (names, email addresses, phone numbers). Store details, subscriptions and billing history. App usage events and email engagement. App Store reviews. Personal data the controller's apps store in their databases or files, which may include Shopify customer data (names, email addresses, phone numbers, addresses, orders). Affiliate details and commissions. IP addresses and request data in logs.

Sensitive data processed (if applicable) and applied restrictions or safeguards

None.

Nature of the processing

Hosting, storage, backup, transmission and deletion of data, and sending email, as the controller configures the Meridian service.

Purpose(s) for which the personal data is processed on behalf of the controller

Providing the Meridian service to the controller: hosting its Shopify apps and their databases, billing its merchants, CRM and analytics, automations and email, affiliates and App Store tools.

Duration of the processing

For as long as the controller uses the Meridian service, and then until the personal data is deleted or returned under Clause 10(d).

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

As set out in Annex IV, for the duration of the processing above.

ANNEX III: Technical and organisational measures including technical and organisational measures to ensure the security of the data

Measures of pseudonymisation and encryption of personal data

Data is encrypted at rest with Google-managed keys: databases, database backups and stored files. Data is encrypted in transit with TLS on every connection to the service from outside Meridian's private network.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Each environment of an app runs separately, with its own database and secrets. Databases are on a private network, reachable only by the app. Secrets are stored in Google Secret Manager.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Production databases are backed up daily.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

A vulnerability scan runs after each production deployment.

Measures for user identification and authorisation

Individual user accounts, two-factor authentication, and roles that limit each user to the organization and apps they are given.

Measures for the protection of data during transmission

TLS on every connection to the service from outside Meridian's private network. Inside it, services are reachable only from Meridian's own systems.

Measures for ensuring physical security of locations at which personal data are processed

Processing takes place in Google Cloud data centres.

Measures for ensuring events logging

On the Enterprise plan, an activity log records changes made through the service, with the user and the time.

Measures for internal IT and IT security governance and management

Meridian staff access personal data only as needed to provide and support the service, under a duty of confidentiality. Security incidents are handled under a written incident response policy.

Measures for ensuring limited data retention

Production database backups are kept 7 days on the Lite plan, 30 days on the Pro plan, and as agreed on the Enterprise plan.

Measures for allowing data portability and ensuring erasure

The controller can export its data at any time. When the controller cancels an app, its data is exported to the controller and then deleted.

Description of the specific technical and organisational measures to be taken by the processor to be able to provide assistance to the controller

Requests from data subjects and questions about the processing: privacy@the-meridian.ai. Personal data breaches are notified by email to the owner of the controller's Meridian account.

ANNEX IV: List of sub-processors

The controller has authorised the use of the following sub-processors:

1. Name: Google Cloud EMEA Limited (Google Cloud Platform)

Address: 70 Sir John Rogerson's Quay, Dublin 2, Ireland

Contact person's name, position and contact details: Data Protection Team, https://support.google.com/cloud/contact/dpo

Description of the processing: hosting, databases, file storage, messaging and logs for the Meridian service. Hosting, databases and files are in the EU (Belgium).

2. Name: Twilio Inc. (SendGrid)

Address: 101 Spear Street, 5th Floor, San Francisco, CA 94105, USA

Contact person's name, position and contact details: Twilio Privacy, privacy@twilio.com

Description of the processing: sending email, in the EU.

3. Name: Functional Software, Inc. d/b/a Sentry

Address: 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA

Contact person's name, position and contact details: Virginia Badenhope, General Counsel, legal@sentry.io. EU representative: Sentry Software Netherlands B.V., Schiphol Boulevard 359, 1118 BJ Amsterdam Schiphol, compliance@sentry.io

Description of the processing: error monitoring of the Meridian dashboard and API, in the EU.

4. Name: Anthropic, PBC

Address: 548 Market St, PMB 90375, San Francisco, CA 94104, USA

Contact person's name, position and contact details: Privacy, privacy@anthropic.com

Description of the processing: the in-app assistant (organization and app names, email template names and subjects, and the user's messages) and the analysis of Shopify API changes (code from the controller's connected GitHub repository), in the United States.

5. Name: Voyage AI Innovations, Inc.

Address: Palo Alto, California, USA

Contact person's name, position and contact details: Legal, legal@voyageai.com

Description of the processing: text embeddings of the in-app assistant's messages, in the United States.

6. Name: Anysphere, Inc. (Cursor)

Address: 2261 Market Street STE 86466, San Francisco, CA 94114, USA

Contact person's name, position and contact details: Legal, legal@cursor.com

Description of the processing: Meridian's internal support agent, which can read the controller's store records, including merchant and contact email addresses, in the United States.

7. Name: PostHog, Inc.

Address: 2261 Market St., #4008, San Francisco, CA 94114, USA

Contact person's name, position and contact details: Privacy, privacy@posthog.com

Description of the processing: product analytics of the Meridian dashboard and API (user identifiers, usage events and session replays of the dashboard), in the EU (Frankfurt, Germany).