Last Updated: 2025-07-03

1. Introduction

Sales Automation B.V. (“Processor,” “Provider,” “we,” “us,” or “our,” a company registered in the Netherlands under Chamber of Commerce number 94072590) has entered into an agreement (the “Agreement”) with you (the “Controller,” “Customer,” “Client,” “you,” “your,” or “yours”) to provide certain services (the “Services”), as governed by our Terms and Conditions (which can be found at www.salesautomation.io/terms-and-conditions). Each of the Processor and Controller is referred to as a “Party,” and collectively, the “Parties.”

This Data Processing Agreement (“DPA”) is incorporated into and forms part of the Agreement. In the event of any conflict between this DPA and the Agreement, the provisions of this DPA shall prevail, solely with respect to the subject matter hereof.

The Parties have agreed to enter into this DPA to define how Personal Data will be processed, safeguarded, and managed in accordance with applicable data protection laws, including the GDPR, and to formalize their respective roles and responsibilities as Processor and Controller.

---

2. Definitions

The definitions used in this document are inherited from the “Definitions” section of our Terms and Conditions, which can be found at www.salesautomation.io/terms-and-conditions.

In addition, the definitions “Personal Data,” “Processing,” “Controller,” “Processor,” and “Data Subject” have the meanings given by the GDPR.

---

3. Data Processing

3.1. Roles of the Parties

For the purposes of the GDPR (and any other applicable data protection laws), We primarily act as a “Processor” on behalf of the Customer (the “Controller”) with respect to any Personal Data processed under the Agreement and this DPA.

However, We may also act as an independent Controller in situations where We determine the purposes and means of processing—for example, using Personal Data for Our own product communications, support, operational analytics, or other legitimate business needs as outlined in Our Privacy Policy. In these situations, the roles, responsibilities, and obligations applicable to Controllers under the GDPR apply to Us, and such processing is governed by Our Privacy Policy rather than this DPA.

3.2. Instruction to Process Personal Data

The Controller instructs the Processor to process Personal Data as described in Appendix A (“Data Processing Details”). This DPA governs the Processor’s Processing of Personal Data on the Controller’s behalf in connection with providing the Services.

For the avoidance of doubt, the Controller’s instructions under this DPA apply only to Personal Data processed by Us in our capacity as a Processor, and not to any processing activities for which We independently act as a Controller pursuant to Our Privacy Policy.

3.3. Purpose of Processing

The Processor processes Personal Data on the Controller’s behalf as necessary to provide, support, and improve the Services under the Agreement, in accordance with the Controller’s instructions and for purposes consistent with our Terms and Conditions, Privacy Policy, and this DPA. Any additional or differing instructions require mutual written agreement by the Parties.

3.4. Provider Obligations and Responsibilities

3.4.1. Assistance with Compliance

We will assist you in fulfilling your obligations under data protection laws, including:

- Responding to Data Subject requests
- Ensuring compliance with Articles 32 to 36 of the GDPR concerning security, breach notifications, impact assessments, and consultations.

3.4.2. Data Breach Notification

We will notify you without undue delay upon becoming aware of a Personal Data Breach, providing sufficient information to help you meet any legal obligations. The notification will as per GDPR guidelines:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe 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.

3.4.3. Data Protection Impact Assessments and Audit Rights

- Impact Assessments: We will provide reasonable assistance in conducting data protection impact assessments (DPIAs) and any required prior consultations with supervisory authorities, if applicable.
- Audit Rights: We will make available all information necessary to demonstrate our compliance with this DPA. You (or a designated auditor) have the right to audit our compliance, including inspections of relevant facilities and documentation, upon reasonable written notice and during an agreed time period.
- Cost and Confidentiality: The Controller is responsible for any costs associated with any impact assessment or audit. Both Parties must ensure the work is conducted under appropriate confidentiality obligations and does not unreasonably interfere with our operations or compromise the data of other customers.

3.4.4. No Reselling or Unauthorized Use of Data

The Processor will not sell, resell, or otherwise commercially exploit data provided by Controller, nor use it for any purpose other than those specified in this DPA.

3.4.5. Disclosure as Required by Law

The Processor may disclose Personal Data if and to the extent it is legally required to do so (e.g., in response to lawful requests by public authorities, subpoenas, or court orders). The Processor will use reasonable efforts to provide prompt notice to the Controller before any such disclosure, unless legally prohibited from doing so.

3.5. Customer Obligations and Responsibilities

3.5.1. Compliance with Laws

The Controller is responsible for ensuring that Processing of Personal Data under this DPA complies with all applicable laws, including (where relevant) obtaining necessary consents and providing required notices to Data Subjects.

3.5.2. Instructions

The Controller shall provide lawful, documented instructions to the Processor. The Processor shall not be liable for any Processing performed in accordance with those instructions if they cause or contribute to a violation of applicable laws. The Controller indemnifies and holds the Processor harmless against any fines, damages, or liabilities arising from such instructions.

3.5.3. Confidential or Sensitive Data

To the extent the Controller provides Personal Data that is confidential or sensitive, the Controller must ensure it has fulfilled all legal requirements (e.g., obtaining explicit consent or implementing additional safeguards) before transferring such data to the Processor.

---

4. Security

4.1. Security Measures

The Processor implements appropriate technical and organizational measures to ensure a level of security proportionate to the risk. Appendix B (Technical and Organizational Measures) provides a comprehensive overview of these measures. The Controller acknowledges that these measures are adequate and proportionate in view of the nature and context of the Processing.

4.2. CASA Tier 2 Certification

As part of commitment to robust application security, the Processor underwent a Cloud Application Security Assessment (CASA) by an authorized third party, validating compliance with CASA Tier 2 requirements. The assessment is based on OWASP ASVS standards under the App Defense Alliance framework. A copy of the certificate is available to the Controller upon request, subject to appropriate confidentiality obligations.

---

5. Sub-Processors

We keep your information confidential, but may disclose it to suppliers or subcontractors insofar as it is reasonably necessary for the purposes set out in this Data Processing Agreement.

This includes external third-party service providers, such as accountants, auditors, experts, lawyers and other outside professional advisors; IT systems, support and hosting service providers; technical engineers; data storage and cloud providers and similar third-party vendors and outsourced service providers that assist us in carrying out business activities.

5.1. General Authorization

The Controller grants the Processor a general authorization to engage sub-processors to carry out specific Processing activities necessary for the performance of the Services, subject to the terms of this DPA. The Processor remains responsible for any sub-processor’s performance of obligations under this DPA.

5.2. Introduction of New Sub-Processors

- Notification: The Processor will notify the Controller of any intended changes concerning the addition or replacement of sub-processors.
- Objection Period: The Controller may, within 14 days of receipt of such notification, object in writing to the appointment of the new sub-processor if it can reasonably demonstrate that the sub-processor's engagement would cause the Controller to be non-compliant with applicable data protection laws.
- Confirmation: If the Controller does not object in writing within 14 days, the Processor may deem the change accepted.
- Good-Faith Resolution: In the event of an objection, the Parties will discuss potential solutions in good faith. If the Processor cannot provide a reasonable accommodation to address the Controller's concerns, the Controller may, as its sole remedy, terminate the portion of the Services requiring the use of the new sub-processor without penalty.

---

6. Data Subject Rights

If we receive a request from a Data Subject to exercise their rights under data protection laws, we will:

- Inform you in a timely manner of the request.
- Not respond unless authorized by you or required by law.
- Provide reasonable assistance, insofar as possible, in fulfilling your obligation to respond.

---

7. International Data Transfers

The Controller instructs the Processor to process Personal Data outside the EU/EEA whenever necessary to provide the agreed Services. The Controller warrants that such instructions are lawful. The Processor will use its best efforts to ensure that any transfers of Personal Data comply with Chapter V of the GDPR, including any required safeguards or transfer mechanisms.

---

8. Data Retention and Deletion

We will hold your Personal Data only as long as necessary for the purposes set out in Appendix A (Data Processing Details), taking into account factors such as the nature and sensitivity of the data, potential risks, and applicable legal requirements. We invest in robust security measures to protect your data from unauthorized access or breaches, as further described in Appendix B (Technical and Organizational Measures).

Upon termination of the Agreement, and unless otherwise required by law, we will, at the Controller's request:

- Delete all Personal Data processed on your behalf.
- Delete all Personal Data provided by you.

---

9. Dispute Resolution and Governing Law

The dispute resolution and governing law provisions of this agreement shall be governed by and subject to the "Dispute Resolution and Governing Law" section of our Terms and Conditions, which can be found at www.salesautomation.io/terms-and-conditions.

10. Changes, Amendments and Termination

The provisions regarding changes, amendments, and termination of this agreement shall be governed by and subject to the "Changes, Amendments and Termination" section of our Terms and Conditions, which can be found at www.salesautomation.io/terms-and-conditions.

11. Contact Information

For inquiries or questions, please contact us at contact@salesautomation.io.

Appendix A - Data Processing Details

1. List of Parties

Data Exporter (Controller):

Name: The Customer identified in the Agreement or Order Form

Address: As set forth in the Agreement or Order Form

Contact person's name, position, and contact details: As set forth in the Agreement or Order Form, or as otherwise provided by the Customer

Activities relevant to the data transferred under these Clauses: Processing Personal Data in connection with accessing and receiving the Services provided by the Data Importer, in accordance with the Agreement and this DPA

Signature and date: The parties agree that execution or electronic acceptance of the Agreement constitutes execution of this Appendix A by both parties

Role (controller/processor): Controller

Data Importer (Processor):

Name: Sales Automation B.V.

Address: Palestinastraat 60D, 3061HN Rotterdam, Netherlands

Contact person's name, position, and contact details: With any enquiries, please reach out to our legal team by email at contact@salesautomation.io

Activities relevant to the data transferred under these Clauses: Processing Personal Data for the purpose of providing, supporting, and improving the Services in accordance with the Agreement and this DPA

Signature and date: The parties agree that execution or electronic acceptance of the Agreement constitutes execution of this Appendix A by both parties

Role (controller/processor): Processor

---

2. Description of Transfer

Categories of Data Subjects

- The Customer's employees, contractors, or authorized end-users who access and receive the Services
- Potential or existing customers, leads, or other business contacts whose information is input into or collected by the Services, if applicable

Categories of Personal Data

- Business contact information (e.g., name, business email address, job title)
- Company information (e.g., employer, department)
- Technical information (e.g., IP address, device identifiers)
- Any other Personal Data that the Controller chooses to submit or collect via the Services

Special Category or Sensitive Data (if applicable)

- By default, none. The Controller agrees not to submit or otherwise make available any special categories of data (e.g., health data, biometric data, political opinions) without prior written notification to and approval by the Processor.
- If such data is processed, the Controller is responsible for ensuring that all required consents and safeguards are in place.

Frequency of the Transfer

- Continuous, for the duration of the Agreement, or as otherwise initiated by the Controller in using the Services.

Nature of the Processing

- Collection, storage, use, retrieval, modification, or deletion of Personal Data in order to deliver, maintain, and enhance the Services, and any other Processing as described in the Agreement or the DPA.

Purpose(s) of the Transfer and Further Processing

- To provide, support, and improve the Services under the Agreement, including, but not limited to, user authentication, feature enablement, technical support, routine business communications, or as otherwise instructed by the Controller.

Retention Period

- Unless otherwise requested by the Controller during the term of the Agreement, Personal Data will be retained for as long as necessary to fulfill the legitimate business purposes stated above or as required by law. Upon expiration or termination of the Agreement (and at the Controller’s request), Personal Data will be deleted or returned in accordance with the DPA.

Sub-Processors

- The Data Importer may engage sub-processors to carry out specific Processing activities in connection with providing and supporting the Services (e.g., hosting providers, analytics platforms, and more).

Appendix B - Technical and Organizational Measures

Note on Disclosure: The measures listed below are a partial overview of security practices in place. Additional security mechanisms are implemented but remain proprietary to the Processor and are not publicly disclosed to protect our intellectual property.

1. Technical Measures

The development of our platform follows modern software development best practices, with major influences including the classic 12-factor application approach, applied through a microservices architecture guided by Domain-Driven Design. To ensure appropriate level of security, our platform closely follows industry-recognized standards from OWASP (see OWASP's Top 10, 2021 edition: www.owasp.org/www-project-top-ten) as well as Google's expansion upon/interpretation thereof, called Cloud Application Security Assessment (CASA, see: www.appdefensealliance.dev/casa).

The platform in its entirety is deployed on the Google Cloud Platform (GCP, see: www.cloud.google.com/gcp).

In this section we will outline the most relevant security topics to emphasize our commitment to secure handling of any data entering our systems.

1.1. Software

Access Controls

As we do not own or access any shared workplaces or data centers, we rely on our cloud provider, Google, for physical access controls.

For logical access controls, we follow the principle of least privilege, applied using role-based access control (RBAC) methodology as supported by GCP. Access to any systems relevant to the development or operation of our services requires multi-factor authentication and, where relevant, IP allow-listing.

Imposed based on OWASP directives:

- A01:2021 - Broken Access Control

Authentication and Authorization

For user authentication we are relying on Google's Firebase (see: www.firebase.google.com/products/auth). Our servers internally verify the received token with Firebase to prevent token tampering attempts. After a successful verification, the request is then attributed to the internal identification of the user, which in turn evaluates which resources the user is authorized to interact with. Within our system, each resource is attributed to the user who created it and can only be accessed by that user through their internal (non-exposed) user ID.

By default, without a confirmed authentication the user is granted access to no resources.

Imposed based on OWASP directives:

- A01:2021 - Broken Access Control
- A02:2021 - Cryptographic Failures
- A07:2021 - Identification and Authentication Failures

Network security

The majority of the services that constitute the platform are not exposed to the public internet due to ingress controls, such as firewall rules and private networking. They are hosted on Google Cloud Platform using serverless services (such as Cloud Run) that communicate over our Virtual Private Cloud (VPC) network.

For added security, any communication between services requires authentication using ID tokens obtained via IAM credentials. The calling service uses its service account credentials to obtain a short-lived ID token for the target service's URL (the audience). This ID token is included in the request headers, allowing the target service to verify the caller's identity and ensure that only authorized requests are accepted.

For public, internet-facing services, the network security measures put in place consist of but are not limited to:

- Rate Limiting / Throttling
- Authentication
- Strict cross-origin resource sharing (CORS) policies
- Strict content security policies (CSP's)

Imposed based on OWASP directives:

- A01:2021 - Broken Access Control
- A03:2021 - Injection
- A04:2021 - Insecure Design
- A05:2021 - Security Misconfiguration

Application Layer(s)

In order to further protect the system from SQL injection attacks (or similar types of attacks like SSRF, RCE, etc.), all internet-facing systems sanitize and validate input data. Furthermore, any interaction with data takes place via ORM-based systems. To avoid breaches at the component level, we only work with reputable, regularly updated libraries.

Imposed based on OWASP directives:

- A03:2021 - Injection
- A05:2021 - Security Misconfiguration
- A06:2021 - Vulnerable and Outdated Components
- A08:2021 - Software and Data Integrity Failures
- A10:2021 - Server-Side Request Forgery (SSRF)

Monitoring and Logging

To ensure full observability of our systems, all transactions are logged to GCP. Logs contain only necessary information to ensure proper operation of our systems. These logs are also used for automatic monitoring of unusual activities and errors that, in turn, get reported to the DPL as soon as they occur. This automatic alerting system ensures a timely response from Sales Automation B.V.

Imposed based on OWASP directives:

- A09:2021 - Security Logging and Monitoring Failures

1.2. Data

Encryption

- **At Rest:** Where required, we rely on Fernet (symmetric encryption). In order to read the encrypted data, a secret key is required. In the case of a database breach, this renders the protected data unreadable. All sensitive keys are stored using Google's secret management services, making them inaccessible to unauthorized parties.

- **In Transit:** All transactions are made over TLS-secured HTTP. In certain cases, as an extra security measure, we rely on end-to-end encryption.
- **In Use:** We do not rely on encryption of in-use data as we are not working with any "Sensitive Personal Data" per GDPR definition.

Imposed based on OWASP directives:

- A02:2021 - Cryptographic Failures
- A08:2021 - Software and Data Integrity Failures

Storage

We do not retain data for longer periods than deemed necessary given its purpose. Critical data is backed up daily or on-demand.

For the most common retention topics, please note:

- Transaction and Application logs are retained for 30 days
- User provided data is retained as long the user account remains active
- Backups of crucial data are retained for 30 days

Transfers

Sales Automation B.V. primarily stores data on servers located in the Netherlands. However, when working with certain service providers or processing activities, personal data may be transferred to and processed in other countries.

- **EU Data Storage:** We prioritize storing and processing data within the European Economic Area (EEA).
- **Third-Party Providers:** When engaging third-party providers that process data outside the EEA, we ensure that appropriate safeguards are in place, such as:

  Adequacy Decisions: Transferring data to countries that the European Commission has deemed to have adequate data protection laws.

  Additional Measures: Assessing and implementing supplementary technical and organizational measures as needed.

- **User Notification:** Data subjects are informed about international data transfers in our Privacy Policy and DPA, including the safeguards in place.

---

2. Organizational Measures

2.1. Data Subject Rights Management

Procedures for Requests

We respect every user's right to access, rectify and erase data going through our systems as per GDPR guidelines. All users have the right to send a request to contact@salesautomation.io to invoke their rights, and should expect a timely reaction by Sales Automation B.V. to carry out their request within the boundaries laid out by GDPR.

We reserve the right to conduct identity verification of the individual making the request.

Communication Channels

As per information stated on our contact page (see: www.salesautomation.io/contact), the user can email or call us with their request.

2.2. Incident Response and Reporting

In the event of breach or any other incident impacting our users, we will act in accordance with GDPR Articles 33 and 34, which includes timely notification of the relevant supervisory authority and, where required, affected Data Subjects.