Version: 1.0 / 1 December 2026

Data Processing Agreement Helios IT

Comprised of:

Part 1. Data Pro Statement

Part 2. Standard clauses for data processing

NLdigital version march 2025

This Data Processing Agreement and the standard clauses were originally drafted in Dutch. The English version is for convenience only. In case of conflict between the Dutch and the English version, the Dutch version prevails.

Part 1: Data Pro Statement

Along with the Standard Clauses for Data Processing, this Data Pro Statement constitutes the data processing agreement for the product or service provided by the company that has drawn up this Data Pro Statement.

General information

1. **This Data Pro Statement was drawn up by the following data processor (verwerker):**
   Helios IT Solutions B.V., Schipluidenlaan 4, 1062 HE Amsterdam, the Netherlands, Dutch Chamber of Commerce number 68332289.
   If you have any queries about this Data Pro Statement or data protection in general, please contact: privacy@helios-it.nl or +31 20 802 8000.

2. **This Data Pro Statement shall enter into force on 1 December 2026, version 1.0.**
   We regularly revise the security measures described in this Data Pro Statement to remain prepared and up to date with regard to data protection. We notify clients of new versions through our regular communication channels, including by e-mail or through the client environment.

3. **This Data Pro Statement applies to the following products and services provided by data processor:**
   Managed IT services; supply, implementation and management of Microsoft 365 and Google Workspace; service desk, monitoring and management through RMM; endpoint security and EDR/MDR; backup and recovery solutions; cloud, hosting and domain services; migrations of e-mail, server, on-premises and cloud environments; development and management of applications, dashboards and other client-specific systems; AI-related services, implementations and support; and other IT services specified in the Agreement with Client.

4. **Description of product(s)/service(s)**
   Helios IT Solutions B.V. provides business clients with one-stop IT services. The services include the supply of licences and services, implementation, management, security, monitoring, support, hosting, backup, recovery, migration and development of IT environments and client-specific solutions. The Agreement, quotation or service level agreement with Client specifies which services Client purchases.

5. **Intended use**
   The products and services are designed and built to process name, address and contact details; business and organisational data; account, user, identification, authentication and authorisation data; communication data, including e-mail and calendar data; document, file and application data; technical data, such as IP addresses and device, network, log and telemetry data; backup and recovery data; and other personal data stored or processed by Client within the supplied or managed systems. Data Subjects may include Client's employees, contractors, applicants, customers, suppliers, business contacts and users of Client's systems, websites, applications and portals, as well as other persons whose personal data Client processes within the IT environment supplied or managed by Helios IT.

- The services are not specifically intended for the processing of special categories of personal data, personal data relating to criminal convictions and offences, or personal identification numbers issued by public authorities. Depending on the data that Client processes in the supplied or managed systems, such data may nevertheless form part of the processing.
  The processing of such data using the products or services described above is subject to Client's assessment and responsibility. Client determines which data are processed within the supplied or managed systems.

6. **Privacy by design/privacy by default**
   Helios IT Solutions B.V. takes privacy by design and privacy by default into account when implementing and performing the services, insofar as appropriate to the nature and scope of the assignment. Helios IT applies appropriate access security, authorisations, logging, encryption and default settings. The final configuration and setup may also depend on Client's choices and instructions.

7. **Data processor uses the Standard Clauses for Data Processing included as Part 2 of this document. Together with this Data Pro Statement, those clauses constitute the data processing agreement.**

8. **Data processor may process personal data partly outside the EU/EEA. Where this involves a transfer to a third country, an appropriate level of protection is ensured through a valid transfer mechanism under the GDPR, such as an adequacy decision of the European Commission or the Standard Contractual Clauses (SCCs), supplemented by appropriate additional measures where necessary.**

9. **Data processor uses the following sub-processors:**
   • Microsoft (Microsoft 365, Azure, Entra ID and Copilot): processing within the EU/EEA and, depending on the service and support, potentially in third countries; appropriate safeguards under the applicable Microsoft data processing terms.
   • Google (Google Workspace): processing within the EU/EEA and potentially in third countries; appropriate safeguards under the applicable Google data processing terms.
   • Hetzner Online GmbH (VPS hosting and cloud storage): processing within the EU/EEA.
   • Realtime Register B.V. (domain registration and management): processing within the EU/EEA.
   • NinjaOne (RMM, monitoring and SaaS backup): processing within the EU/EEA and potentially in third countries; appropriate safeguards under the applicable data processing terms.
   • SentinelOne (endpoint security, EDR and MDR): processing within the EU/EEA and potentially in third countries; appropriate safeguards under the applicable data processing terms.
   • Anthropic (Claude and AI-related services): processing potentially in third countries; appropriate safeguards under the applicable data processing terms.
   The sub-processors actually used depend on the services purchased by Client. Data processor shall notify Client of relevant changes in accordance with the Standard Clauses for Data Processing.

10. **Data processor shall support their clients in the following way when they receive requests from data subjects:**
Helios IT Solutions B.V. shall support Client following a reasonable written request in dealing with requests from Data Subjects, insofar as Client cannot perform the required actions independently. If a Data Subject contacts Helios IT directly, Helios IT shall in principle refer the Data Subject to Client. Work performed may be charged as additional work at the agreed or customary rates.

11. **Data processor shall support their clients with Data Protection Impact Assessments (DPIA) in the following manner:**
If Client is required to carry out a Data Protection Impact Assessment (DPIA), Helios IT Solutions B.V. shall provide appropriate assistance following a reasonable written request, insofar as the requested information and support relate to processing carried out by Helios IT. Work performed may be charged as additional work at the agreed or customary rates.

12. **Once the Agreement with a client has been terminated, data processor shall in principle delete the personal data processed on behalf of Client within three months, in such a manner that the data can no longer be used and are rendered inaccessible, unless otherwise agreed or a statutory retention obligation applies.**
For personal data contained in backups, log files and archives, deletion shall take place in accordance with the regular retention periods and deletion cycles of the relevant solution. During this period, the data shall not be processed for other purposes.

13. Returning personal data once the Agreement has been terminated
At Client's written request, Helios IT Solutions B.V. shall, insofar as technically and reasonably possible, make the personal data available in a commonly used format appropriate to the relevant service. Work relating to export, transfer or migration may be charged as additional work at the agreed or customary rates.

Security policy

14. **Data processor has implemented the following security measures to protect their product or service:**
Helios IT Solutions B.V. implements appropriate technical and organisational security measures, taking into account the nature of the services, the risks of the processing, the state of the art and the platforms used. These measures include:
• limiting access to employees who require access for their work;
• central and secure management of administrative accounts and credentials, including by means of a password vault;
• use of multi-factor authentication where available and appropriate;
• use of encryption for data at rest and in transit where appropriate, including the security features of the platforms and sub-processors used;
• logging of sign-ins and administrative activities within the principal management platforms so that relevant actions and access can be investigated retrospectively;
• automated execution and monitoring of backup tasks, with alerts when tasks fail or are not completed successfully;
• use of versioning, snapshots, redundancy and file system controls where supported by the selected solution;

• application of security updates and patches to systems managed by Helios IT where appropriate, including through automated management and monitoring tools;
• contractual confidentiality obligations for employees who may have access to personal data; and
• internal investigation and follow-up of identified security incidents and potential personal data breaches.
Helios IT reviews and improves these measures in response to developments, incidents, identified risks and changes in the services. The specific measures may differ by service and client environment.

15. **As at the effective date of this Data Pro Statement, data processor does not operate a formally certified Information Security Management System (ISMS).**

16. **As at the effective date of this Data Pro Statement, data processor does not hold external information security or privacy certifications.**

Data breach protocol

17. **In the event something does go wrong, data processor shall follow the following data breach protocol to ensure that clients are notified of incidents:**
Helios IT Solutions B.V. shall notify Client without undue delay after becoming aware of a personal data breach relating to personal data processed for Client in connection with the services. Helios IT shall provide, insofar as available, the information reasonably required by Client to assess the incident and comply with any statutory notification obligations. Security incidents and potential personal data breaches shall be investigated, contained and followed up internally as soon as possible after discovery. Notifications shall be made using Client's contact details known to Helios IT. For urgent coordination, Helios IT may be contacted at privacy@helios-it.nl or +31 20 802 8000.

Part 2: Standard Clauses for Data Processing

Version: March 2025

Along with the Data Pro Statement, these standard clauses constitute the data processing agreement. They also constitute an annex to the Agreement and to the appendices to this Agreement, e.g. any general terms and conditions which may apply.

Article 1. Definitions

The following terms have the following meanings ascribed to them in the present Standard Clauses for Data Processing, in the Data Pro Statement and in the Agreement:

1.1.1 **Dutch Data Protection Authority (AP):** the supervisory authority defined in Section 4.21 of the GDPR.
1.1.2 **GDPR:** the General Data Protection Regulation.
1.1.3 **Data Processor**: the party which, in their capacity as an ICT supplier, processes Personal Data on behalf of their Client as part of the performance of the Agreement.
1.1.4 **Data Pro Statement**: statement issued by Data Processor in which they provide information such as the intended use of their products and/or services, any security measures which have been implemented, sub-processors, data breach, certification and dealing with the rights of Data Subjects.
1.1.5 **Data Subject**: a natural person who can be identified, directly or indirectly.
1.1.6 **Client:** the party on whose behalf Data Processor processes Personal Data. Client can either be the controller (the party who determines the purpose and means of the processing) or another data processor.
1.1.7 **Agreement**: the agreement concluded between Client and Data Processor, based on which the ICT supplier provides services and/or products to Client, the data processing agreement forming part of this agreement.
1.1.8 **Personal Data** any and all information regarding a natural person who has been or can be identified, as defined in Article 4.1 of the GDPR, processed by Data Processor as required under the Agreement.
1.1.9 **Data Processing Agreement**: the present Standard Clauses for Data Processing , which, together with Data Processor's Data Pro Statement (or similar such information), constitute the data processing agreement within the meaning of Article 28.3 of the GDPR.

Article 2. General provisions

2.1.1 The present Standard Clauses for Data Processing apply to all Personal Data processing operations carried out by Data Processor in providing their products and services, as well as to all Agreements and offers. The applicability of Client's data processing agreements is explicitly rejected.
2.1.2 The Data Pro Statement, and particularly the security measures described in it, may be adapted from time to time to changing circumstances by Data Processor. Data Processor shall notify Client in the event of significant revisions. If Client in all reasonableness cannot agree to the revisions, Client shall be entitled to terminate the data processing agreement in writing, stating their reasons for doing so, within thirty days of having been served notice of the revisions.
2.1.3 Data Processor shall process the Personal Data on behalf of Client, in accordance with the written agreed upon instructions provided by Client by Data Processor.

2.1.4 Client or their customer shall serve as the controller within the meaning of the GDPR, shall have control over the processing of the Personal Data and shall determine the purpose and means of processing the Personal Data.

2.1.5 Data Processor shall serve as the processor within the meaning of the GDPR and shall therefore not determine the purpose and means of processing the Personal Data, and shall not make any decisions on the use of the Personal Data and other such matters.

2.1.6 Data Processor shall implement the GDPR as laid down in the present Standard Clauses for Data Processing, the Data Pro Statement and the Agreement. It is up to Client to assess, on the basis of this information, whether Data Processor is providing sufficient guarantees with regard to the implementation of appropriate technical and organisational measures in order to ensure that the processing operations meet the requirements of the GDPR and that Data Subjects' rights are sufficiently protected.

2.1.7 Client shall guarantee Data Processor that they act in accordance with the GDPR, that they provide a high level of protection for their systems and infrastructure at all time, that the nature, use and/or processing of the Personal Data are not unlawful and that they do not violate any third party's rights.

2.1.8 Administrative fines imposed on Client by the Dutch Data Protection Authority cannot be recovered from Data Processor.

Article 3. Security

3.1.1 Data Processor shall implement the technical and organisational security measures set out in their Data Pro Statement. In implementing the technical and organisational security measures, Data Processor shall take into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing and the intended use of their products and services, and the risk in processing the data of varying likelihood and severity inherent to the rights and freedoms of Data Subjects that are to be expected considering the nature of the intended use of Data Processor's products and services.

3.1.2 Unless explicitly stated otherwise in the Data Pro Statement, the products and services provided by Data Processor shall not be equipped to process special categories of personal data or data relating to criminal convictions and offences.

3.1.3 Data Processor seeks to ensure that the security measures they shall implement are appropriate for the manner in which Data Processor intends to use the products and services.

3.1.4 In Client's opinion, said security measures provide a level of security that is tailored to the risk inherent in the processing of the Personal Data used or provided by Client, taking into account the factors referred to in Article 3.1.

3.1.5 Data Processor shall be entitled to adjust the security measures they have implemented if to their discretion such is necessary for a continued provision of an appropriate level of security. Data Processor shall record any significant adjustments they chooses to make, e.g. in a revised Data Pro Statement, and shall notify Client of said adjustments where relevant.

3.1.6 Client may request Data Processor to implement further security measures. Data Processor shall not be obliged to honour such requests to adjust their security measures. If Data Processor makes any adjustments to their security measures at Client's request, Data Processor is entitled to invoice Client for the costs associated with said adjustments. Data Processor shall not be required to actually implement the requested security measures until both Parties have agreed upon them in writing. .

Article 4. Data breaches

4.1.1 Data Processor does not guarantee that their security measures shall be effective under all circumstances. If Data Processor discovers a data breach within the meaning of Article 4 sub 12 of the GDPR, they shall notify Client without undue delay. The "Data Breach Protocol" section of the Data Pro Statement outlines the way in which Data Processor shall notify Client of data breaches.

4.1.2 It is up to the Controller (the Client or their customer) to assess whether the data breach of which Data Processor has notified the Controller must be reported to the Dutch Data Protection Authority or to the Data Subject concerned. The Controller (Client or their customer) shall at all times remain responsible for reporting data breaches which must be reported to the Dutch Data Protection Authority and/or Data Subjects pursuant to Articles 33 and 34 of the GDPR. Data Processor is not obliged to report data breaches to the Dutch Data Protection Authority and/or to the Data Subject.

4.1.3 Where necessary, Data Processor shall provide further information on the data breach and shall assist Client to meet their breach notification requirements within the meaning of Articles 33 and 34 of the GDPR by providing all the necessary information available to Data Processor.

4.1.4 If Data Processor incurs any reasonable costs in doing so, they are entitled invoice Client for these, at the rates applicable at the time.

Article 5. Confidentiality

5.1.1 Data Processor shall ensure that the persons processing Personal Data acting under its authority have committed themselves to confidentiality.

5.1.2 Data Processor shall be entitled to provide third parties with Personal Data if and insofar as such is necessary due to a court order, statutory provision or order issued by a competent government authority.

5.1.3 Any and all access and/or identification codes, certificates, information regarding access and/or password policies provided by Data Processor to Client, and any and all information provided by Data Processor to Client detailing the technical and organisational security measures included in the Data Pro Statement are confidential and shall be treated as such by Client and shall only be disclosed to authorised employees of Client. Client shall ensure that their employees comply with the requirements described in this article.

Article 6. Term and termination

6.1.1 This data processing agreement constitutes part of the Agreement, and any new or subsequent agreement arising from it and shall enter into force at the time of the conclusion of the Agreement and shall remain effective for an indefinite period.

6.1.2 This data processing agreement shall end by operation of law upon termination of the Agreement or upon termination of any new or subsequent agreement arising from it between parties.

6.1.3 If the data processing agreement is terminated, Data Processor shall delete all Personal Data they currently store and which they have obtained from Client within the timeframe laid down in the Data Pro Statement, in such a way that the Personal Data can no longer be used and shall have been *rendered inaccessible*. Alternatively, if such has been agreed, Data Processor shall return the Personal Data to Client in a machine-readable format.

6.1.4 If Data Processor incurs any costs associated with the provisions of Article 6.3, they shall be entitled to invoice Client for said costs. Further arrangements relating to this subject can be laid down in the Data Pro Statement.

6.1.5 The provisions of Article 6.3 do not apply if Data Processor is prevented from removing or returning the Personal Data in full or in part by a statutory provision. In such instances, Data Processor shall only continue to process the Personal Data insofar as such is necessary by virtue of their statutory obligations. Furthermore, the provisions of Article 6.3 shall not apply if Data Processor is the Controller of the Personal Data within the meaning of the GDPR.

Article 7. The rights of Data Subjects, Data Protection Impact Assessments (DPIA) and auditing rights

7.1.1 Where possible, Data Processor shall cooperate with reasonable requests made by Client relating to Data Subjects who invoke their rights from Client. If Data Processor is directly approached by a Data Subject, they shall refer the Data Subject to Client where possible.

7.1.2 If Client is required to carry out a Data Protection Impact Assessment or a subsequent consultation within the meaning of Articles 35 and 36 of the GDPR, Data Processor shall cooperate with such, following a reasonable request to do so.

7.1.3 Data Processor will lend their cooperation to Client's requests for the deletion of personal data insofar as Client cannot carry this out themself.

7.1.4 Data Processor shall be able to demonstrate their compliance with their requirements under the data processing agreement by means of a valid Data Processing Certificate or an equivalent certificate or audit report (third-party memorandum) issued by an independent expert.

7.1.5 In addition, at Client's request, Data Processor shall provide all other information that is reasonably required to demonstrate compliance with the arrangements made in this data processing agreement. If, in spite of the foregoing, Client has grounds to believe that the Personal Data are not processed in accordance with the data processing agreement, Client shall be entitled to have an audit performed (at their own expense) not more than once every year by an independent, certified, external expert who has demonstrable experience with the type of data processing operations carried out under the Agreement. The scope of the audit shall be limited to verifying that Data Processor is complying with the arrangements made regarding the processing of the Personal Data as set forth in the present data processing agreement. The expert shall be subject to a duty of confidentiality with regard to his/her findings and shall only notify Client of matters which cause Data Processor to fail to comply with their obligations under the data processing agreement. The expert shall furnish Data Processor with a copy of his/her report. Data Processor shall be entitled to reject an audit or instruction issued by the expert if to their discretion the audit or instruction is inconsistent with the GDPR or any other law, or that it constitutes an unacceptable breach of the security measures they have implemented.

7.1.6 The parties shall consult each other on the findings of the report at their earliest convenience. The parties shall implement the measures for improvement suggested in the report insofar as they can be reasonably expected to do so. Data Processor shall implement the proposed measures for improvement insofar as to their discretion such are appropriate, taking into account the processing risks associated with their product or service, the state of the art, the costs of implementation, the market in which they operate, and the intended use of the product or service.

7.1.7 Data Processor shall be entitled to invoice Client for any costs they incur in implementing the measures referred to in this article.

Article 8. Sub-processors

8.1.1 Data Processor has specified in the Data Pro Statement whether Data Processor uses any third parties (sub-processors) to help them process the Personal Data, and if so, which third parties.

8.1.2 Client hereby authorises Data Processor to hire other sub-processors to meet their obligations under the Agreement.

8.1.3 Data Processor shall notify Client of any changes concerning the addition or replacement of the third parties (sub-processors) hired by Data Processor, e.g. through a revised Data Pro Statement. Client shall be entitled to object to such changes . Data Processor shall ensure that any third parties they hire shall commit to ensuring the same level of Personal Data protection as the security level Data Processor is bound to provide to the Client pursuant to the Data Pro Statement.

Article 9. Other provisions

These Standard Clauses for Data Processing, along with the Data Pro Statement, constitute an integral part of the Agreement. Therefore, any and all rights and obligations arising from the Agreement, including any applicable general terms and conditions and/or limitations of liability, shall also apply to the data processing agreement.