Matreon

Data Processing Agreement

Last modified: November 2, 2026
PDF created on: November 25, 2026

> *This is an English translation of our Dutch Data Processing Agreement (Verwerkersovereenkomst). It is provided for convenience only; in case of any difference in meaning, the Dutch version prevails.*

Contents

Article 1. Definitions 1
Article 2. Formation, Subject Matter, Term, and Order of Precedence 1
Article 3. Nature, Purpose, and Scope of the Processing 2
Article 4. Controller's Instructions 2
Article 5. Confidentiality 2
Article 6. Security 2
Article 7. Sub-processors 3
Article 8. Transfers Outside the EEA 3
Article 9. Assistance with Data Subject Requests 3
Article 10. Notification of Personal Data Breaches 3
Article 11. Assistance with GDPR Compliance 4
Article 12. Audit and Information 4
Article 13. End of Processing: Deletion and Return 5
Article 14. Liability 5
Article 15. Final Provisions 5
Article 16. Acceptance 5
Annex 1: Description of the Processing 6
Annex 2: Security Measures 6
Annex 3: Sub-processors 7

This data processing agreement forms part of every agreement for a service that the customer orders from us. It is concluded as soon as the customer places an order or accepts a quote or agreement, without the need for a separate signature (see Article 2).

Parties

1. **Matreon IT**, located at Brakkeveldweg 53, 1782AE Den Helder, registered with the Netherlands Chamber of Commerce (Kamer van Koophandel) under number 96383801, hereinafter: **Processor**;
2. the **customer** that orders a service from Processor, as recorded in the order, quote, or customer account, hereinafter: **Controller**.

Processor and Controller are also referred to together as the **Parties**.

Recitals

- Processor provides web hosting, email, backup, and management services (managed services) to Controller on the basis of an order, quote, or agreement, including the general terms and conditions (hereinafter: the **Main Agreement**).
- In providing these services, Processor processes personal data on behalf of Controller.
- In this agreement, the Parties wish to set out their arrangements regarding the processing of that personal data, as referred to in Article 28 of the General Data Protection Regulation (GDPR).

The Parties agree as follows.

Article 1. Definitions

In this agreement, the terms **personal data**, **processing**, **controller**, **processor**, **data subject**, **personal data breach**, and **sub-processor** have the meanings given to them in the GDPR.

- **GDPR:** Regulation (EU) 2016/679 (General Data Protection Regulation).
- **Implementation Act:** the Dutch GDPR Implementation Act (Uitvoeringswet Algemene verordening gegevensbescherming).
- **Supervisory Authority:** the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).
- **Services:** the services that Processor provides to Controller under the Main Agreement.
- **Annex:** an annex to this agreement. The annexes form part of the agreement.

Article 2. Formation, Subject Matter, Term, and Order of Precedence

1. This agreement is concluded and takes effect at the moment Controller orders a Service or accepts a quote or agreement for a Service. By ordering or accepting, Controller also accepts this agreement. A separate signature is not required.
2. The Parties acknowledge that the order or acceptance by electronic means satisfies the requirement of Article 28(9) GDPR that the agreement be in writing, including in electronic form.
3. Processor records the acceptance (date, time, and version of this agreement), keeps the current and previous versions available on its website, and provides a copy upon request.
4. This agreement applies to all processing of personal data that Processor carries out for Controller in connection with the Services.

5. This agreement remains in effect for as long as Processor processes personal data for Controller. It does not terminate before the Main Agreement does, nor before Processor has complied with Article 13.
6. In the event of a conflict between this agreement and the Main Agreement (including the general terms and conditions), this agreement prevails insofar as it concerns the processing of personal data.

Article 3. Nature, Purpose, and Scope of the Processing

1. Processor processes personal data solely to provide the Services, as described in **Annex 1**.
2. Annex 1 also sets out the categories of data subjects, the types of personal data, and the duration of the processing.
3. Processor does not process personal data for its own purposes and does not itself determine the purpose or means of the processing, unless required to do so by law. In that case, Processor shall inform Controller of this in advance, unless the law prohibits it.

Article 4. Controller's Instructions

1. Processor processes personal data solely on the basis of Controller's documented instructions. This agreement, the Main Agreement, and the configuration that Controller itself applies in the Services constitute such instructions.
2. Controller warrants that the instructions and the processing comply with the GDPR, that it has a valid legal basis for the processing, and that it has informed the data subjects.
3. If Processor believes that an instruction infringes the GDPR or other data protection regulations, Processor shall immediately inform Controller. Processor may then suspend the execution of that instruction until Controller confirms or amends the instruction.
4. Processor does not view the content of the personal data, unless this is necessary for the Services (for example, when resolving an outage or at Controller's request) or required by law.

Article 5. Confidentiality

1. Processor ensures that all persons who have access to the personal data, such as employees and contractors, are bound by confidentiality, either contractually or by law.
2. Processor restricts access to the personal data to persons who need it to perform the Services.
3. This confidentiality obligation does not apply if Processor is required to disclose the data under a legal obligation or court order. Processor shall inform Controller of this in advance, unless the law prohibits it.

Article 6. Security

1. Processor takes appropriate technical and organizational measures to protect the personal data against loss and against unlawful or unauthorized processing, alteration, disclosure, and access. In doing so, Processor takes into account the state of the art, the costs of implementation, the nature of the data, and the risks.
2. The minimum measures that Processor takes are set out in **Annex 2**.
3. Processor evaluates the measures regularly and adjusts them where necessary. Processor

shall not lower the level of security without Controller's prior written consent.
4. Controller is itself responsible for the security of its own accounts, passwords, applications, and content that it uses or manages in the Services.

Article 7. Sub-processors

1. Controller grants Processor general authorization to engage sub-processors. The sub-processors engaged as of the date of signing are listed in **Annex 3**.
2. Processor shall inform Controller in writing (for example, by email) of any intended changes, such as the addition or replacement of a sub-processor, at least 30 days in advance. Controller may submit a reasoned objection within 14 days after the notification.
3. If the Parties cannot reach agreement after consultation, Controller may terminate the affected Service effective as of the date on which the change takes effect, without penalty.
4. Processor shall impose on each sub-processor, by means of a written agreement, the same obligations as set out in this agreement, at least with respect to data protection and security.
5. Processor remains fully liable to Controller for the performance of the obligations of its sub-processors.

Article 8. Transfers Outside the EEA

1. Processor processes personal data within the European Economic Area (EEA), at the locations stated in Annex 1 and Annex 3.
2. Processor transfers personal data to, or has it processed in, a country outside the EEA only if Controller has given written consent for this (listing in Annex 3 constitutes consent) and an appropriate safeguard is in place. That safeguard is an adequacy decision of the European Commission, or the European Commission's standard contractual clauses with, where necessary, supplementary measures.
3. Upon request, Processor shall provide Controller with the chosen safeguard in writing.
4. Some of the sub-processors listed in Annex 3, such as Microsoft, are US companies or part of a US group. Under the US CLOUD Act, US authorities can require such parties to provide data, even when that data is stored within the EEA. As a result, personal data may be processed outside the EU.

Article 9. Assistance with Data Subject Requests

1. Processor assists Controller, insofar as possible, through appropriate technical and organizational measures in responding to requests from data subjects. This concerns the rights of access, rectification, erasure, restriction, portability, and objection.
2. If Processor receives a request directly from a data subject, Processor shall not respond to it itself, except to confirm that the request has been received and forwarded. Processor shall forward the request to Controller within 5 business days.
3. For assistance that goes beyond what can reasonably be considered part of the Services, Processor may charge the reasonable costs in accordance with its applicable rates, after prior notice.

Article 10. Notification of Personal Data Breaches

1. Processor shall notify Controller of a personal data breach affecting Controller's personal data

without undue delay, and in any event within 48 hours after becoming aware of it. The notification is sent to the email address of the customer account or to another contact address for security notifications that Controller has provided to Processor. Controller shall ensure that this address is kept up to date.

2. The notification contains, insofar as known:
    - the nature of the breach, the categories and approximate number of data subjects and data records concerned;
    - the likely cause and the consequences;
    - the contact details of the contact person at Processor;
    - the measures taken and proposed to end the breach and to mitigate its consequences.
3. If not all information is immediately available, Processor shall supplement the notification in phases, without undue delay.
4. Processor shall immediately take measures to end the breach and to prevent further breaches, and shall document all breaches.
5. Controller decides whether and how the breach is reported to the Supervisory Authority and to data subjects. Processor does not make such notifications itself, unless required to do so by law.

Article 11. Assistance with GDPR Compliance

Processor assists Controller, taking into account the nature of the processing and the information available to Processor, in complying with Controller's obligations regarding:

- the security of personal data (Article 32 GDPR);
- the notification of breaches (Articles 33 and 34 GDPR);
- data protection impact assessments and prior consultation of the Supervisory Authority (Articles 35 and 36 GDPR).

For assistance that goes beyond what can reasonably be considered part of the Services, Article 9(3) applies.

Article 12. Audit and Information

1. Upon request, Processor shall make available to Controller all information necessary to demonstrate that Processor complies with the obligations under Article 28 GDPR and this agreement. For this purpose, Processor may first refer to current certificates, audit reports, or comparable statements (for example, ISO 27001), insofar as these answer the questions.
2. If the information under paragraph 1 is insufficient, or if the Supervisory Authority requires it, Controller may have an audit carried out by an independent expert bound by confidentiality. Controller shall announce the audit in writing at least 30 days in advance, and no more than once per year, except in the event of a breach or a specific cause.
3. The audit takes place during business hours, disrupts Processor's business operations as little as possible, and does not cover data of other customers or confidential business information that is not relevant to this agreement.
4. Each Party bears its own costs. Processor may charge the reasonable internal costs of cooperating with an audit, unless the audit reveals serious shortcomings.
5. Processor shall implement reasonable recommendations from the audit within a period to be determined in consultation.

Article 13. End of Processing: Deletion and Return

1. Upon expiry of the Main Agreement, or earlier if Controller so requests, Processor shall delete or return all of Controller's personal data, at Controller's option. This takes place within 30 days after expiry. Controller shall communicate its choice within 14 days after expiry. If it fails to do so, Processor shall delete the data.
2. Processor shall also delete existing copies and backups, no later than within 0 days after expiry, unless the law requires the data to be retained.
3. Upon request, Processor shall confirm the deletion in writing.
4. Data is returned in a commonly used, machine-readable format. The reasonable costs of doing so may be charged in accordance with the applicable rates.

Article 14. Liability

1. The liability of the Parties under this agreement is governed by the liability provisions of the Main Agreement and the associated general terms and conditions, including any limitations.
2. This is without prejudice to the liability of the Parties toward data subjects under Article 82 GDPR and the rights of recourse between the Parties arising from it.
3. Limitations of liability do not apply in the event of intent or deliberate recklessness on the part of Processor, or to the extent excluded by law.

Article 15. Final Provisions

1. Processor may amend this agreement. Processor shall notify Controller of an amendment in writing (for example, by email) at least 30 days in advance. If the amendment is unfavorable to Controller, Controller may terminate the affected Service effective as of the date on which the amendment takes effect. Amendments required by changes to the GDPR or by obligations imposed by the Supervisory Authority take effect immediately. Other arrangements regarding the processing of personal data apply only if the Parties have agreed to them in writing.
2. If a provision is null and void or voidable, the remaining provisions remain in effect. The Parties shall then replace that provision with a valid provision that has, as far as possible, the same purport.
3. This agreement is governed by Dutch law. Disputes shall be submitted to the competent court in Alkmaar, unless the Main Agreement provides otherwise.
4. Contact persons for privacy matters:
    - Processor: privacy@matreon.nl
    - Controller: the email address of the customer account, unless Controller has provided a different address.

Article 16. Acceptance

A separate signature is not required. This agreement is accepted at the moment Controller orders a Service or accepts a quote or agreement for a Service (Article 2). During the ordering process, Processor refers to this agreement, for example with the text: "I agree to the general terms and conditions and the data processing agreement", with a link to this text.

Annex 1: Description of the Processing

Item	Description
Subject matter and purpose	Providing the Services that Controller orders from Processor, such as web hosting, email hosting, backups, domain management, and managed IT services (MSP)
Nature of the processing	Storing, hosting, backing up, restoring, transmitting, managing, and editing (insofar as necessary for maintenance, support, and security) data that Controller places in or manages through the Services
Categories of data subjects	Persons whose data Controller stores in the Services or has managed through the Services, such as customers, employees, website visitors, suppliers, and other business contacts of Controller
Types of personal data	Data that Controller itself places in the Services, such as name, contact and account data, IP addresses, log files, email content and metadata, and data in websites and databases. Controller determines what this data is
Special categories or criminal records data	Not intended for storage, unless Controller notifies Processor of this in writing in advance and the Parties make additional arrangements
Duration	Term of the Main Agreement, plus the wind-down period under Article 13
Location(s) of processing	Qupra B.V.: DC1, DC2; Hetzner: FSN1

Annex 2: Security Measures

Processor takes at least the following measures. They are periodically evaluated and updated.

Organizational

- Information security and privacy policy, with designated responsible person(s).
- Confidentiality agreements and regular awareness training for employees.
- Procedures for reporting and handling incidents and personal data breaches.
- Supplier management: data processing agreements and assessment of sub-processors.

Access Control

- Need-based access (least privilege) and role-based authorizations.
- Unique accounts, strong password requirements, and multi-factor authentication for administrators and management environments.
- Timely revocation of access upon termination of employment or change of role.
- Logging of administrative actions on systems that contain personal data.

Technical

- Encrypted connections (TLS) for data traffic and administration.
- Encryption of data at rest where reasonably possible, and encrypted backups.
- Network segmentation, firewalls, and detection of abuse and attacks.
- Timely installation of security updates and patches; periodic vulnerability scans.
- Malware protection and monitoring of systems.
- Separation of customer environments.

Continuity and Recovery

- Regular backups (at least once a day) with periodic restore tests.
- Availability measures, such as redundancy of power, network, and storage.
- Disaster recovery plan for critical systems.

Physical

- Data centers with access control, CCTV surveillance, fire protection, and backup power supply.
- Visitor registration and escort.

Data Deletion

- Secure deletion or destruction of data carriers and data after the end of the agreement.

Annex 3: Sub-processors

Sub-processor	Service or activity	Location of processing	Transfer outside the EEA and safeguard
Qupra B.V.	Data center and infrastructure	Netherlands	No: safeguard
Microsoft	Email delivery or security	United States	Yes: safeguard

Processor's transaction processors and external accounting provider do not process any personal data that Controller stores in the Services and are therefore not sub-processors under this agreement.