

Data Processing Agreement (model) - marXact B.V.

Version: 1.0, 30 September 2026 **Applies to:** UNI-Cloud, UNI-Collect (cloud sync), UNI-Machine (cloud sync) and related support services **Form of acceptance:** electronic acceptance in UNI-Cloud by the customer's account administrator, or as part of the order or subscription.

Parties

1. **The customer** that has concluded an agreement with marXact for the services listed above, as identified in its UNI-Cloud account or order (the "Controller", or "you"); and
2. **marXact B.V.**, Marathon 3J, 1213 PB Hilversum, the Netherlands, Chamber of Commerce number 68076622 (the "Processor", "marXact", or "we").

Where you yourself process the personal data on behalf of a third party (for example as a contractor for a network operator), you act as processor towards that third party and we act as your sub-processor. The obligations in this DPA then apply between you and us in the same way.

1. Subject and relation to the agreement

1.1 This DPA forms an integral part of the agreement between you and marXact, including our General Terms of Delivery (the "Agreement"). It governs the processing of personal data that we carry out on your behalf when providing the services (Article 28 GDPR).

1.2 If this DPA and the Agreement conflict on the processing of personal data, this DPA prevails.

1.3 This DPA does not cover personal data we process as controller for our own purposes, such as customer administration, invoicing and business communications. That processing is described in our Privacy Policy at <https://marxact.com/privacy-policy/>.

2. Description of the processing

2.1 The nature, purpose, categories of data and categories of data subjects are described in Annex 1.

2.2 We process the personal data only to provide, secure, support and maintain the services under the Agreement.

3. Instructions

3.1 We process the personal data only on your documented instructions. The Agreement, this DPA and your use and configuration of the services are your complete instructions at the time of acceptance. Further instructions must be given in writing and must be reasonable and in line with the services.

3.2 We will inform you promptly if, in our opinion, an instruction infringes the GDPR or other data protection law.

3.3 If EU or member state law requires us to process personal data other than on your instructions, we will inform you before processing, unless that law prohibits this.

4. Confidentiality

4.1 We ensure that everyone who processes the personal data on our behalf is bound by a duty of confidentiality, by contract or by law.

5. Security

5.1 We take appropriate technical and organisational measures to protect the personal data against loss and against any form of unlawful processing, taking into account the state of the art, the costs and the risks. These measures are described in Annex 3.

5.2 We may change these measures, provided the overall level of protection does not decrease.

6. Sub-processors

6.1 You give us general written authorisation to engage sub-processors. The sub-processors in use at the time of acceptance are listed in Annex 2.

6.2 We will inform you at least 30 days in advance of any addition or replacement of a sub-processor, by email to the account administrator or through a notice in UNI-Cloud. You may object on reasonable grounds related to data protection within that period. If we cannot reasonably accommodate the objection, you may terminate the affected service with effect from the date the new sub-processor is engaged, without penalty.

6.3 We impose the same data protection obligations on each sub-processor as set out in this DPA, by written contract. We remain responsible to you for the performance of our sub-processors.

7. Transfers outside the EEA

7.1 Personal data in UNI-Cloud is stored in the European Economic Area, at data centres in the Netherlands. A sub-processor may only process personal data outside the European Economic Area if an appropriate safeguard under Chapter V GDPR applies, such as an adequacy decision (including the EU-US Data Privacy Framework) or the EU Standard Contractual Clauses. Annex 2 states the location and safeguard per sub-processor.

8. Assistance

8.1 Taking into account the nature of the processing, we assist you by appropriate technical and organisational measures in responding to requests from data subjects. If a data subject sends such a request to us, we will forward it to you without undue delay and will not respond to it ourselves, unless you instruct us to.

8.2 We assist you, on request, in complying with your obligations regarding security, data breach notification, data protection impact assessments and prior consultation (Articles 32 to 36 GDPR), taking into account the information available to us.

8.3 We may charge reasonable costs for assistance that goes beyond what the services normally offer, after informing you in advance.

9. Personal data breaches

9.1 We notify you without undue delay, and in any case within 48 hours after becoming aware of it, of a personal data breach affecting the personal data we process on your behalf.

9.2 The notification contains, as far as available: the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed. We provide information in stages where it is not all available at once.

9.3 You decide whether the breach must be notified to the supervisory authority or to data subjects. We will not notify them on your behalf unless you instruct us to or the law requires it.

10. Audits

10.1 We make available to you all information reasonably necessary to demonstrate compliance with Article 28 GDPR.

10.2 You may have an audit carried out once per year, or more often after a personal data breach, by an independent auditor bound by confidentiality, with at least 30 days' notice, during office hours and without disrupting our operations. We may first offer a written response or an existing report. You bear the costs of the audit, unless it shows a material breach of this DPA by us.

11. Term, return and deletion

11.1 This DPA applies as long as we process personal data on your behalf under the Agreement.

11.2 During the Agreement you can export your data yourself through the export functions of UNI-Cloud. Switching to another provider is governed by Articles 5.5 to 5.7 of our General Terms of Delivery.

11.3 After the Agreement ends, we delete the personal data within 90 days, including copies, unless EU or member state law requires us to retain it. Backups are overwritten in the normal backup cycle of 30 days. On request we confirm the deletion in writing.

12. Liability

12.1 The limitations of liability in the Agreement apply to this DPA.

13. Changes, applicable law and disputes

13.1 We may amend this DPA, for example when the law or our sub-processors change. We will inform you at least 30 days in advance. Changes that reduce the protection of personal data require your acceptance.

13.2 This DPA is governed by Dutch law. Disputes are settled by the court designated in the Agreement.

Annex 1 - Description of the processing

Nature of the processing	Storage, hosting, synchronisation, display, export, backup, support and technical maintenance
Purpose	Providing the services under the Agreement: collecting, storing, sharing and exporting field and measurement data, managing projects and users, and providing support
Categories of data subjects	Your employees, field workers and other users of your account; persons whose data appears in your projects (for example in photos, notes or address details)
Categories of personal data	User account data (name, email address, phone number, role, login and usage data, device identifiers); measurement data linked to a user (coordinates, timestamps, device and user ID); photos, scans, attachments and notes; address and parcel details in projects
Special categories	None intended. You will not store special categories of personal data in the services.
Duration	For the duration of the Agreement, plus the deletion period in clause 11.3

Annex 2 - Sub-processors

Sub-processor	Service	Location of processing	Safeguard for transfers
TransIP B.V. (team.blue)	Hosting UNI-Cloud	Netherlands	Not applicable (EEA)
Cyso Group B.V. / Cyso Cloud	Hosting UNI-Cloud	Netherlands	Not applicable (EEA)
Help Scout PBC	Support tickets, only when you send us project data in a support request	USA	EU-US Data Privacy Framework and SCCs
Atlassian (Jira, Confluence, Rovo)	Bug and issue tracking, only when project data is needed to solve a problem	EU (Germany, data residency); provider based in Australia	SCCs and EU-US Data Privacy Framework

Sub-processor	Service	Location of processing	Safeguard for transfers
Salesforce (Slack)	Internal communication about support cases	EU (Frankfurt, Germany, data residency); provider based in USA	EU-US Data Privacy Framework, SCCs and BCRs
Microsoft Ireland (Microsoft 365)	Email about support cases	EU (EU Data Boundary)	SCCs and EU-US Data Privacy Framework
Anthropic PBC (Claude)	Analysis of support and development questions. Only object coordinates and technical data, after removing names, user IDs, photos of people and address or owner details	USA	SCCs (included in Anthropic's DPA)

Annex 3 - Technical and organisational measures

- Hosting in ISO 27001-certified data centres of TransIP and Cyso in the Netherlands
- Encryption in transit (TLS 1.2 or higher) and at rest (AES-256)
- Role-based access for customer users; administrator manages users in the account
- Multi-factor authentication available for users
- Access by marXact staff on a need-to-know basis, bound by confidentiality
- Daily backups, retained for 30 days
- Logging of access to production systems
- Incident response procedure with notification within 48 hours (clause 9)
- Secure development: code review for every change, including AI-assisted code
- Person responsible for information security: Raoul van Ginkel