DATA PROCESSING AGREEMENT

How we process personal data on your behalf

Version	1.1
Effective date	April 18, 2026
Last updated	April 18, 2026

Introduction

This data processing agreement governs how xYnta Hosting B.V. handles personal data that you as a client store or process on our infrastructure. The agreement is based on the General Data Protection Regulation (GDPR) — the European privacy law.

This data processing agreement forms part of our general terms and conditions. By accepting the general terms and conditions, you also accept this data processing agreement. Both take effect at the same moment.

In this agreement we use the legal terms "Controller" (that is you as the client: you determine which data is processed and for what purpose) and "Processor" (that is us: we process the data on your behalf). Where legally possible, we simply write "you" and "we". For privacy questions and data breaches, you can reach us at info@xynta.nl.

Article 1 — Definitions

1. **GDPR:** the General Data Protection Regulation (EU 2016/679) — the European privacy law.
2. **Personal data:** any information relating to an identifiable natural person, as defined in the GDPR.
3. **Processing:** any operation performed on personal data, such as storing, reading, modifying or deleting.
4. **Controller:** you as the client — you determine which data is processed and for what purpose.
5. **Processor:** us — xYnta Hosting B.V. — we process data on your instruction and on your behalf.
6. **Sub-processor:** an external party we engage that may thereby gain access to personal data you store with us.
7. **Data breach:** a security incident in which personal data is accidentally or unlawfully destroyed, lost, altered or made accessible to unauthorised parties.
8. **Data subject:** the natural person to whom the personal data relates.

Article 2 — What do we process on your behalf?

1. We process personal data solely on your behalf and in accordance with your instructions, unless a legal obligation requires otherwise.
2. Processing takes place in the context of our hosting services: making hosting, server and network environments available and managing them. Because we manage the infrastructure, we have technical access to the environments in which you store data. We use that access only for management and maintenance purposes — not for our own ends.
3. You determine which data you store on our infrastructure. We have no visibility into the specific content of that data and are not responsible for it. The categories of data and data subjects that may fall under this agreement are described in Annex 1.
4. You warrant that the processing of personal data via our infrastructure is lawful and that you have all required legal bases and consents in place. If you process special categories of personal data via our infrastructure — such as health data, criminal data or biometric data — you inform us of this in advance so that we can implement additional measures if necessary. The personal data remains your property and that of the data subjects.

Article 3 — How long do we retain your data?

1. We retain personal data you store on our infrastructure for as long as your service is active. You can delete data yourself at any time via the client portal or control panel.
2. Technical data we generate ourselves in the context of management and security — such as log files and server statistics — is not retained longer than necessary. In practice we apply the following guidelines:
    a. Access and system logs: a maximum of ninety days, unless a security incident or legal obligation requires longer retention.
    b. Server statistics and performance data: a maximum of twelve months in aggregated form.
3. Upon termination of the agreement, we delete all data in accordance with the article on deletion of data after termination in our general terms and conditions: active data within seven days of the end date, back-ups and snapshots within thirty days of the end date.

Article 4 — What do we do to protect your data?

1. We comply with the obligations imposed on us as a processor by the GDPR and other applicable privacy legislation.
2. We ensure that employees and others who access personal data on our behalf are bound by a confidentiality obligation and act only on our instruction.
3. If we believe that an instruction from you conflicts with the GDPR or other applicable privacy legislation, we will notify you immediately. We are not obliged to carry out that instruction in such a case.
4. If you are required to carry out a data protection impact assessment (DPIA) and our processing is relevant to it, we will provide reasonable assistance upon your request.
5. We do not process personal data outside the European Economic Area (EEA), unless this is necessary for the performance of the services and a valid legal basis for the transfer exists under the GDPR. For transfers to Canada — where we may incidentally call on DirectAdmin for technical support — the adequacy decision of the European Commission for Canada serves as the legal basis. For transfers to countries without an adequacy decision, such as the United States and India, we rely on standard contractual clauses in accordance with Article 46 GDPR. Upon your request we will inform you of the countries in which processing takes place and the applicable safeguards.

Article 5 — How do we secure your data?

1. We implement appropriate technical and organisational measures to protect personal data against loss, unlawful access, modification or disclosure. This is a best-efforts obligation — we cannot guarantee absolute security.
2. We treat our security measures as confidential. We do not provide detailed information about our security architecture or internal systems, because disclosure of that information could compromise the security of systems and data — including yours.
3. You are responsible for the security of your own systems, access management for your own users and the way in which you store and manage data on our infrastructure.

Article 6 — Who do we engage in performing the services?

1. By accepting this data processing agreement, you grant us general permission to engage the sub-processors listed in Annex 2. We distinguish two types:
2. a. **Fixed sub-processors:** parties that are structurally engaged in our service delivery and may therefore have access to data on our infrastructure.
   b. **Incidental sub-processors:** parties — such as software vendors or technical specialists — who only gain temporary access to a specific environment in the event of a concrete problem. We always ask for your permission in advance, on a case-by-case basis.
3. If we wish to engage a new fixed sub-processor or replace an existing one, we will notify you at least thirty days in advance. If you object and we cannot resolve the objection, you have the right to terminate the agreement with effect from the date on which the change takes effect.
4. We enter into a data processing agreement or equivalent arrangements with all fixed sub-processors that provide at least the same level of protection as this agreement. We remain responsible for their compliance with those arrangements.

Article 7 — What do we do in the event of a data breach?

1. If we discover or suspect a data breach involving personal data that you process on our infrastructure, we will notify you as soon as possible — and in any case within 48 hours of discovery. This allows you to assess whether you are required to report the breach to the Dutch Data Protection Authority or to data subjects. That is your responsibility as the Controller.
2. Our notification to you will contain, to the extent known at that time:
    a. a description of what has occurred;
    b. the categories of data subjects and personal data that may be affected;
    c. an estimate of the number of data subjects and records involved;
    d. our contact details for follow-up questions;
    e. the likely consequences;
    f. the measures we have taken or propose to limit the damage.
3. If you need additional information for your own notification, we will provide reasonable assistance upon request.
4. Our notification does not constitute an admission of fault or liability.

Article 8 — What do we do with requests from data subjects?

1. If a data subject submits a request to us to exercise their privacy rights — such as the right to access, rectify or erase their data — we will forward that request to you. You are responsible for handling it.
2. If you need our assistance in handling such a request, we will provide it to the extent that it concerns our processing activities.

Article 9 — How do we handle confidentiality?

1. All personal data we process under this agreement is treated as strictly confidential. We do not share it with others unless this is necessary for the performance of the services, you have given your consent, or a legal obligation requires it.
2. This confidentiality obligation continues after the termination of this data processing agreement.

Article 10 — How can you verify that we are complying?

1. You may send us a written questionnaire about compliance with this data processing agreement a maximum of once per year. We will respond within thirty days. Any costs you incur in preparing and reviewing the questionnaire are for your account.
2. If you have a specific and well-substantiated suspicion of a serious breach of this agreement, you may engage an independent auditor who is bound by confidentiality to carry out a limited audit. The following conditions apply:
    a. the audit must be announced in writing at least thirty days in advance;
    b. the audit may take place a maximum of once per twelve months;
    c. the scope of the audit is limited to compliance with this data processing agreement — not our internal security architecture or systems;
    d. we reserve the right to refuse disclosure of information where publication would compromise the security of systems or data;
    e. the costs of the audit are for your account;
    f. all parties involved treat the findings as confidential.
3. We assess the findings of an audit and determine ourselves in what manner and within a reasonable period — proportionate to the identified risk — we implement any improvements.

Article 11 — Liability

1. Our liability for loss arising from a failure to comply with this data processing agreement is limited in the same way as set out in our general terms and conditions. The liability limitation in our general terms and conditions applies to all claims under this data processing agreement.
2. We are not liable for loss arising from processing activities you carry out yourself, from incorrect or incomplete instructions on your part, or from your failure to comply with your own obligations under the GDPR or this agreement.
3. If a data subject or supervisory authority submits a claim to xYnta arising from a breach of the GDPR by you, you are responsible for handling that claim and any associated costs.
4. A claim for compensation lapses twelve months after the moment at which you were aware or could reasonably have been aware of the loss and the liable party.

Article 12 — How long does this agreement apply?

1. This data processing agreement takes effect at the moment you accept our general terms and conditions and runs for the duration of the agreement between us.
2. If the agreement ends — for whatever reason — we will delete your personal data in accordance with the article on deletion of data after termination in our general terms and conditions: active data within seven days of the end date, back-ups and snapshots within thirty days of the end date. If you wish to receive your data in a specific format, this must be agreed in writing in advance and must be technically feasible.
3. We may amend this data processing agreement. Material changes will be communicated to you at least thirty days in advance. If you do not agree, you may terminate the agreement before the date on which the change takes effect. If you do not cancel, we will assume that you agree.

Article 13 — Applicable law

1. Dutch law applies to this data processing agreement.
2. Disputes arising from this data processing agreement will be submitted to the competent court in Rotterdam.

Annex 1 — What data do we process on your behalf?

How does this work in hosting?

The nature of our services — making hosting, server and network environments available and managing them — means that we have technical access to the infrastructure on which you store data. You determine which data that is. The categories below are therefore indicative and not exhaustive.

Categories of personal data

Depending on what you store on our infrastructure, the following categories of personal data may be processed:

- Identification data — such as names, usernames and customer numbers
- Contact details — such as email addresses, phone numbers and postal addresses
- Technical data — such as IP addresses, log files, session data and server statistics
- Communication data — such as email content transmitted via our mail servers
- Website data — such as content of websites and applications hosted on our infrastructure
- Account data — such as login credentials and access rights of your end users
- Other personal data you store on our infrastructure

We are not responsible for and have no visibility into the specific content of the data you store. If you process special categories of personal data — such as health data, criminal data or biometric data — you are solely responsible for the lawfulness of that processing and for all required legal bases and safeguards. You inform us of this in advance in accordance with Article 2.4.

Categories of data subjects

The data subjects involved depend on your activities. These may include, among others:

- Your clients or end users
- Your employees or contact persons
- Visitors to websites or applications hosted on our infrastructure
- Other individuals whose data you store on our infrastructure

---

Annex 2 — Who do we engage?

Fixed sub-processors

These parties are structurally involved in our service delivery and may therefore have access to data you store on our infrastructure:

Party	What do they do?	Based in
Previder B.V.	Data centre hosting and network infrastructure	Netherlands
i4Networks B.V.	Internet connectivity and transit services	Netherlands
TransIP B.V.	External servers for monitoring, DNS and managed environments	Netherlands
Tilaa B.V.	External servers for monitoring and managed environments	Netherlands
Openprovider	Domain name registration — processes registrant data of you or your clients	Netherlands
HostFact	Invoicing and client administration	Netherlands

Incidental sub-processors

These parties are only engaged in the event of a specific technical problem where temporary access to a particular environment is necessary. We always ask for your permission in advance — on a case-by-case basis. They are only engaged once you have given your consent:

Party	What do they do?	Based in
DirectAdmin (JBMC Software)	Technical support for issues with the control panel	Canada (EU adequacy decision)
Plesk International GmbH	Technical support for issues with the control panel	Germany
Proxmox Server Solutions GmbH	Technical support for issues with the virtualisation platform	Austria
JetBackup	Technical support for issues with the back-up software — back-ups are stored on xYnta's own servers	Israel (standard contractual clauses)
CloudLinux Inc.	Technical support for issues with the operating system	United States (standard contractual clauses)
Installatron	Installation and management of web applications — temporary access to hosting environment	United States (standard contractual clauses)
Releem	Database optimisation — analyses server statistics and configuration data	United States (standard contractual clauses)
cPGuard (OpShield LLP)	Security software that scans hosting environments for malware and threats	India (standard contractual clauses)
Other parties	Incidental technical support — only after your prior written consent on a case-by-case basis	Variable — we will inform you of the country and applicable safeguards on a case-by-case basis

For incidental sub-processors outside the EEA, we ensure appropriate safeguards under the GDPR are in place before access is granted. We will always inform you of this.

Changes

If we wish to engage a new fixed sub-processor, we will notify you at least thirty days in advance. The most current version of this annex is always available at xynta.com/data-processing-agreement.

The current version of this document is always available at:
https://www.xynta.com/en/legal/dpa
This PDF is a snapshot of version 1.1. Always verify you are reading the latest version.