Binadit Data Processing Agreement

Version 2.0, effective 9 November 2026. For Agreements concluded before that date, this version applies from 9 December 2026. Earlier versions are available at binadit.com/dpa/archive.

Parties

1. The customer identified in the Agreement ("Customer"); and
2. Binadit B.V., a private limited company under Dutch law, registered with the Dutch Chamber of Commerce under number 80923216, with its registered office at Seinhuiswachter 2, 3034 KH Rotterdam, the Netherlands ("Binadit").

Background

1. Binadit provides hosting, infrastructure, managed, workspace and related services to Customer under the Agreement.
2. In providing those services, Binadit processes personal data on behalf of Customer as a processor within the meaning of Article 4(8) GDPR.
3. Article 28(3) GDPR requires that processing to be governed by a written contract. This Data Processing Agreement ("DPA") is that contract.

How this DPA applies. This DPA forms an integral part of the Agreement, as set out in Article 9 of the General Terms and Conditions. It applies automatically when Customer accepts the General Terms and Conditions or places an order, without a separate signature. On request, Binadit provides a countersigned copy.

Article 1. Definitions

1.1 Terms such as "personal data", "processing", "controller", "processor", "data subject", "personal data breach" and "supervisory authority" have the meaning given to them in the GDPR.

1.2 In this DPA:

- Agreement: the agreement between Customer and Binadit for the Services, including the General Terms and Conditions, the AUP and any order or quote.
- AUP: Binadit's Acceptable Use Policy, available at binadit.com/aup.
- Authorised Personnel: Binadit's employees and individual contractors who work under Binadit's direct instruction and supervision, on Binadit-managed accounts, and who are bound by written confidentiality obligations.
- Business Day: a weekday that is not a public holiday in the Netherlands.
- Consumer: a natural person who is not acting in the exercise of a profession or business.
- GDPR: Regulation (EU) 2016/679 (General Data Protection Regulation).
- General Terms and Conditions: Binadit's General Terms and Conditions, available at binadit.com/terms.
- Personal Data: personal data that Binadit processes on behalf of Customer in providing the Services, as described in Annex 1.
- Personal Data Breach: a personal data breach as defined in Article 4(12) GDPR affecting Personal Data.
- Portal: Binadit's customer portal at my.binadit.com.
- Privacy Statement: Binadit's Privacy Statement, available at binadit.com/privacy.
- Services: the services Binadit provides to Customer under the Agreement.
- Sub-processor: a third party engaged by Binadit that processes Personal Data on behalf of Customer. Authorised Personnel are not Sub-processors.

Article 2. Scope, roles and order of precedence

2.1 Customer is the controller and Binadit is the processor of the Personal Data.

2.2 Where Customer itself acts as a processor for a third party (for example an agency or reseller), Binadit acts as a sub-processor. Customer warrants that its controller has authorised the engagement of Binadit on the terms of this DPA. Customer remains Binadit's sole point of contact and passes on that controller's instructions.

2.3 This DPA does not cover data that Binadit processes as a controller, such as account, contract and billing data of Customer and its contact persons, support correspondence, and data needed to secure Binadit's network and prevent abuse. The Privacy Statement governs that processing.

2.4 For colocation services where Customer manages its own hardware and Binadit has no logical access, Binadit does not act as a processor. This DPA then applies only to the extent Binadit gains access to Personal Data, for example during remote hands work.

2.5 If Customer is a Consumer who uses the Services solely for personal or household activities, the GDPR may not apply to Customer's own processing (Article 2(2)(c) GDPR). Binadit nevertheless applies Articles 3 to 11 of this DPA to the data Customer stores using the Services, as if Customer were a controller.

2.6 Customer determines which Personal Data it processes using the Services and is responsible for having a lawful basis and for informing data subjects. Customer will only process special categories of personal data (Article 9 GDPR) or data relating to criminal convictions and offences (Article 10 GDPR) using the Services after it has assessed that the measures in Annex 2 are appropriate, and where needed has agreed additional measures with Binadit.

2.7 If this DPA conflicts with any other part of the Agreement regarding the processing of Personal Data, this DPA prevails, as set out in Article 3 of the General Terms and Conditions. The Annexes form part of this DPA. Nothing in the Agreement limits Binadit's obligations under the GDPR.

Article 3. Instructions

3.1 Binadit processes Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless Union or Member State law to which Binadit is subject requires otherwise. In that case Binadit informs Customer of that legal requirement before processing, unless that law prohibits this on important grounds of public interest.

3.2 Customer's documented instructions are the Agreement, this DPA, and Customer's use and configuration of the Services, including through the Portal, the API and support tickets. Further instructions must be given in writing (e-mail suffices) and must be consistent with the Services. If an instruction requires work beyond the Services, Binadit may decline it or perform it at its agreed rates after providing an estimate.

3.3 Binadit immediately informs Customer if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. Binadit may suspend performance of that instruction until Customer confirms or amends it. This does not oblige Binadit to carry out a full legal review of Customer's instructions.

3.4 Binadit does not process Personal Data for its own purposes. Binadit does not sell Personal Data, does not use it to train artificial intelligence models, does not share it with providers of artificial intelligence services, and does not analyse its content, except where necessary to provide the Services, to maintain their security, or on Customer's instruction.

Article 4. Confidentiality

4.1 Binadit ensures that persons authorised to process Personal Data have committed themselves in writing to confidentiality or are under an appropriate statutory obligation of confidentiality.

4.2 Binadit grants access to Personal Data only to Authorised Personnel who need it to perform the Services. Binadit does not access the content of Customer's data, such as mailboxes, files, databases or virtual machines, except: (a) at Customer's request or with Customer's consent, for example for support; (b) where strictly necessary to prevent or resolve

a security incident or abuse; or (c) where required by law. Such access is logged.

4.3 This Article survives termination of this DPA.

Article 5. Security of processing

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks for data subjects, Binadit implements appropriate technical and organisational measures as referred to in Article 32 GDPR. These include at least the measures in Annex 2.

5.2 Binadit may change these measures, provided the overall level of protection is not reduced. Binadit updates Annex 2 on binadit.com/dpa when it makes a material change.

5.3 Customer is responsible for the security of what it controls, as set out in the shared responsibility table in Annex 2. This includes its user accounts and passwords, enabling multi-factor authentication where offered, the operating system and applications on unmanaged servers, and its own backups unless Customer has ordered a backup service from Binadit or backups are included in the Service.

5.4 Customer has assessed the measures in Annex 2 and agrees that they provide an appropriate level of security for the processing described in Annex 1.

Article 6. Sub-processors

6.1 Customer grants Binadit general written authorisation to engage Sub-processors. The Sub-processors engaged at the effective date are listed in Annex 3 and at binadit.com/subprocessors.

6.2 Binadit informs Customer of any intended addition or replacement of a Sub-processor at least 30 days in advance, by e-mail to Customer's administrative contact in the Portal and by updating binadit.com/subprocessors. Where an urgent replacement is needed for the continuity or security of the Services, Binadit informs Customer as soon as possible, and the objection right in Article 6.3 applies from that notice.

6.3 Customer may object to a change in writing within 14 days of the notice, on reasonable grounds relating to data protection. The parties will then consult in good faith. If they do not find a solution within 30 days of the objection, Customer may terminate the affected Service, with effect no later than the date on which the new Sub-processor is engaged, without penalty and with a refund of fees prepaid for the period after termination. If Customer does not object within the term, the change is deemed accepted.

6.4 Binadit imposes on each Sub-processor, by written contract, the same data protection obligations as set out in this DPA, in particular providing sufficient guarantees to implement appropriate technical and organisational measures, as required by Article 28(4) GDPR.

6.5 Binadit remains fully liable to Customer for the performance of each Sub-processor's obligations, subject to Article 12.

Article 7. Location, international transfers and government access

7.1 Binadit stores and processes Personal Data, including backups, exclusively in data centres in the Netherlands, as listed in Annex 3.

7.2 Binadit does not transfer Personal Data to, or allow access to it from, a country outside the European Economic Area (EEA) without Customer's prior written consent. This does not apply to transfers that Customer itself initiates through its use of the Services, such as sending e-mail to recipients outside the EEA, its users logging in from abroad, or registering a domain name with a registry outside the EEA (for example for generic top-level domains such as .com). Domain name registries process registrant data as independent controllers under their own policies. Any other transfer to which Customer consents takes place only in compliance with Chapter V GDPR.

7.3 Binadit is a Dutch company, owned and managed in the Netherlands. At the effective date it has no parent company, subsidiary or establishment outside the EEA, and the Sub-processors in Annex 3 are established in the EEA. Binadit

informs Customer without undue delay if this changes.

7.4 If Binadit receives a request from a public authority to disclose Personal Data, Binadit will:

1. where possible, redirect the authority to Customer;
2. inform Customer promptly, unless the law prohibits this;
3. assess the lawfulness of the request and challenge it where it has reasonable grounds to consider it unlawful;
4. honour a request from an authority outside the EEA only if it is based on an international agreement, such as a mutual legal assistance treaty, in accordance with Article 48 GDPR; and
5. disclose no more Personal Data than is strictly required.

Article 8. Assistance to the Controller

8.1 Taking into account the nature of the processing, Binadit assists Customer by appropriate technical and organisational measures, insofar as possible, in responding to requests from data subjects exercising their rights under Chapter III GDPR. Binadit does this primarily through self-service functions in the Services, such as export, correction and deletion. If Binadit receives such a request directly, it forwards it to Customer within 5 Business Days and does not respond to it, other than to refer the data subject to Customer.

8.2 Taking into account the nature of the processing and the information available to Binadit, Binadit assists Customer in complying with its obligations under Articles 32 to 36 GDPR: security of processing, notification of personal data breaches, data protection impact assessments and prior consultation of the supervisory authority.

8.3 Assistance is included in the fees where it requires limited effort (up to two hours per request) or results from a breach of this DPA by Binadit. Other assistance is charged at Binadit's rates in the Agreement, after Binadit has given Customer an estimate.

8.4 Binadit cooperates, on request, with the supervisory authority in the performance of its tasks.

Article 9. Personal data breaches

9.1 Binadit notifies Customer without undue delay after becoming aware of a Personal Data Breach, and in any event within 48 hours.

9.2 The notification describes, to the extent known:

1. the nature of the breach, including the categories and approximate number of data subjects and of records concerned;
2. the name and contact details of Binadit's contact point;
3. the likely consequences of the breach; and
4. the measures taken or proposed to address the breach and mitigate its possible adverse effects.

Where not all information is available at once, Binadit provides it in phases without undue further delay.

9.3 Binadit takes reasonable measures to contain and investigate the breach and to mitigate its effects, keeps Customer informed, and documents every Personal Data Breach, including its facts, effects and remedial action.

9.4 Customer decides whether to notify the supervisory authority and data subjects. Binadit does not do so on Customer's behalf unless Customer instructs it or the law requires it.

9.5 Binadit sends notifications to the security contact Customer has registered in the Portal or, if none is registered, to the administrative contact. Customer keeps these contacts up to date.

9.6 Unsuccessful attempts that do not compromise the security of Personal Data, such as port scans, failed login attempts and denial-of-service attacks without data compromise, are not Personal Data Breaches. A notification under this Article is not an admission of fault or liability.

Article 10. Information and audits

10.1 Binadit makes available to Customer all information necessary to demonstrate compliance with Article 28 GDPR. This includes this DPA and its Annexes, the ISO 27001 certificates of the data centres in Annex 3, a description of how Binadit applies the ISO 27001 standard in its own operations, and answers to one reasonable security questionnaire per year.

10.2 Binadit allows for and contributes to audits, including inspections, conducted by Customer or an independent auditor mandated by Customer. An auditor must be bound by confidentiality and may not be a competitor of Binadit. Audits take place at most once per 12 months, unless: (a) a Personal Data Breach has occurred at Binadit; (b) a supervisory authority requires an audit; or (c) Customer has concrete indications that Binadit does not comply with this DPA.

10.3 Customer announces an audit in writing at least 30 days in advance, with its proposed scope, or at least 5 Business Days in advance in the cases under 10.2 (a) to (c). Audits take place during business hours, without unreasonably disrupting Binadit's operations, and without access to data of other customers. Physical access to data centres follows the data centre operator's access procedures.

10.4 Customer bears its own audit costs and those of its auditor, as well as Binadit's reasonable time beyond one Business Day per audit at the rates in the Agreement. If the audit shows that Binadit materially fails to comply with this DPA, Binadit bears its own costs and remedies the failure at its own expense within a reasonable period.

10.5 Customer shares the audit report with Binadit. The report is confidential.

10.6 Nothing in this Article limits the powers of a supervisory authority.

Article 11. Return and deletion

11.1 During the term of the Agreement, Customer can export its Personal Data through the self-service functions of the Services in a commonly used, machine-readable format, as described at binadit.com/data-portability.

11.2 When the Agreement or a Service ends, Article 14 of the General Terms and Conditions (switching and data portability) applies. Customer may retrieve its Personal Data during a data retrieval period of at least 30 days. At Customer's request, Binadit returns the Personal Data in a commonly used, machine-readable format, free of charge.

11.3 Within 30 days after the data retrieval period ends, Binadit deletes the Personal Data from its production systems, unless Union or Member State law requires Binadit to store it.

11.4 Personal Data in backups is deleted through the regular backup rotation, at the latest 90 days after deletion from production systems. Until then, backups remain encrypted and protected under this DPA and are restored only for disaster recovery.

11.5 On request, Binadit confirms the deletion in writing.

11.6 This Article does not limit Customer's rights under Chapter VI of Regulation (EU) 2023/2854 (Data Act).

Article 12. Liability

12.1 Binadit is liable for damage caused by processing only where it has not complied with obligations of the GDPR specifically directed to processors or with this DPA, or where it has acted outside or contrary to Customer's lawful instructions (Article 82(2) GDPR).

12.2 The limitations and exclusions of liability in Article 10 of the General Terms and Conditions apply to all liability of Binadit under this DPA, including liability for Sub-processors. The liability of Binadit under the Agreement and this DPA together never exceeds those limits.

12.3 These limitations do not apply to damage caused by intent or deliberate recklessness of Binadit's management, or to the extent mandatory law does not permit them. If Customer is a Consumer, Article 16 of the General Terms and Conditions applies.

12.4 Each party bears any administrative fine imposed on it by a supervisory authority. Neither party may recover such a fine from the other party.

12.5 Customer indemnifies Binadit against claims of third parties, including data subjects, to the extent those claims result from processing without a lawful basis, from Customer's instructions, or from content Customer processes using the Services.

12.6 A claim for damages under this DPA lapses if Customer has not notified Binadit of it in writing within 12 months after Customer became aware or could reasonably have become aware of the damage.

Article 13. Term, changes and governing law

13.1 This DPA remains in force for as long as Binadit processes Personal Data on behalf of Customer, including during the retrieval and deletion periods in Article 11. Provisions that by their nature are intended to survive, such as confidentiality, deletion and liability, survive termination.

13.2 Binadit may amend this DPA in accordance with Article 17 of the General Terms and Conditions, with at least 30 days' notice for existing Agreements. If an amendment materially reduces the protection of Personal Data, Customer may terminate the affected Services before the amendment takes effect, without penalty. Amendments required by law or by a supervisory authority take effect on the date stated in the notice. Binadit keeps earlier versions available at binadit.com/dpa/archive.

13.3 If a provision of this DPA is invalid, the remaining provisions remain in force and the parties replace the invalid provision with a valid one that comes as close as possible to its purpose. If this DPA falls short of Article 28 GDPR, Article 28 GDPR prevails.

13.4 This DPA is governed by Dutch law. Article 18 of the General Terms and Conditions (disputes) applies, including the rules for Consumers in Article 16.

13.5 The English version of this DPA prevails over any translation.

Annex 1. Description of the processing

Customer determines the purposes of the processing. Binadit processes Personal Data only to provide the Services ordered. Processing is continuous for the term of the Agreement, followed by the retrieval and deletion periods in Article 11.

Service	Nature of the processing	Categories of data subjects	Categories of Personal Data
Web hosting	Hosting of websites, databases and e-mail; backup and restore	Customer's website visitors, customers, employees and e-mail correspondents	Website and database content, e-mail, visitor log data such as IP addresses
VPS, dedicated and GPU servers (unmanaged)	Storage and computing on Binadit infrastructure; Binadit operates power, network, hypervisor and, if ordered, backups, without access to content in normal operation	Determined by Customer	Determined by Customer
Managed services (managed cloud, managed servers and databases, e-commerce hosting, DevOps, migrations)	Hosting, administration, maintenance, monitoring, migration, backup and restore, support access	Customer's employees, customers, end users and contacts	Data stored by Customer's applications, such as account, contact, order and usage data and logs

Service	Nature of the processing	Categories of data subjects	Categories of Personal Data
Binadit Workspace (mail, calendar, contacts, Drive, Meet, Receive, appointment pages, chat, online office)	Storage, transmission, synchronisation, search indexing, spam and malware filtering, backup	Customer's users and their correspondents, meeting participants and guests, people who book appointments, senders and recipients of files	Names, e-mail addresses, phone numbers, message content and attachments, calendar entries, contacts, files, chat messages, meeting metadata (names, IP addresses, times), appointment details, log data. Meet audio and video is transmitted in real time and not recorded
Domain registration and DNS	Registration and management of domain names with registries through TransIP; DNS hosting	Domain registrants and their contact persons	Name, address, e-mail address and phone number of the registrant and contacts; DNS records
Colocation with remote hands	Only physical handling of Customer's hardware on request; Article 2.4 applies	Determined by Customer	Determined by Customer
Code scans, US exposure scans, sovereignty assessments and consultancy	Analysis of code, repositories, configurations and documents supplied by Customer; reporting. Source material is deleted within 30 days after delivery of the report	Customer's developers and employees, and persons whose data appears in the material	Commit metadata (names, e-mail addresses), personal data in code, test data, configuration or documents

Special categories. Customer may store special categories of personal data using the Services, subject to Article 2.6. Binadit does not know whether it does so.

Retention. Binadit retains Personal Data for the term of the Agreement and as described in Article 11. Technical log data is retained for up to 6 months, unless it is needed longer to investigate a specific incident.

Annex 2. Technical and organisational measures

Binadit runs its Services on its own hardware and on dedicated infrastructure in ISO 27001-certified data centres in the Netherlands. Binadit works according to the ISO 27001 standard.

Physical security

- Hardware housed in ISO 27001-certified data centres with access control, video surveillance, fire suppression, redundant power and cooling.
- Physical access only for authorised persons, under the data centre operator's registration procedures.

Access control

- Least-privilege, role-based access for Authorised Personnel; access rights reviewed every 6 months and revoked immediately on departure.
- Multi-factor authentication for all administrative access to systems, the Portal and infrastructure.
- Administrative access only through secured channels (VPN or SSH key-based access); administrative actions are logged.

Encryption

- Data in transit encrypted with TLS 1.2 or higher for all customer-facing services.
- Storage disks and backups encrypted at rest.

Isolation and network security

- Customer environments separated by KVM virtualisation and network segmentation.
- Firewalls and DDoS mitigation at the network edge.

Availability and backups

- Encrypted backups stored at a separate data centre location in the Netherlands; restores tested periodically.
- Redundant network connectivity; 24/7 on-call rotation for incidents.

Monitoring, logging and vulnerability management

- Central logging of security-relevant events, retained for up to 6 months and protected against alteration.
- Security patches applied based on risk; critical patches on managed systems as soon as possible, normally within 72 hours.
- Regular vulnerability scans of Binadit's infrastructure.

Organisation and personnel

- Written confidentiality obligations for all Authorised Personnel, including individual contractors.
- Security awareness training for Authorised Personnel at least once a year.
- Documented incident response procedure, including breach notification under Article 9.
- Sub-processors selected and reviewed on their security guarantees.
- No use of artificial intelligence services that receive Customer data.

Shared responsibility

Area	Binadit	Customer
Data centre, hardware, network, hypervisor	Yes	No
Operating system and applications on unmanaged servers	No	Yes
Operating system and platform on web hosting, managed services and Workspace	Yes	No
User accounts, passwords, enabling MFA, user permissions	Provides the tools	Yes
Backups	If ordered or included in the Service	Otherwise
Lawfulness of the data and its processing	No	Yes

Annex 3. Sub-processors and data centres

This list is also published at binadit.com/subprocessors. All parties are established in the Netherlands and all data centres are ISO 27001-certified.

Party	Role	Location	Access to Personal Data
TransIP B.V.	Domain registration, server infrastructure and off-site backups	TransIP data centre, Amsterdam, the Netherlands	Logical access to infrastructure possible; backups are encrypted by Binadit before storage
Smartdc B.V.	Colocation data centre housing Binadit's own hardware	Smartdc Rotterdam, Van Nelleweg 1, Rotterdam, the Netherlands	Physical access only, no logical access

Individual contractors who work as Authorised Personnel are not Sub-processors. They work within the EEA, on Binadit-managed accounts with multi-factor authentication, under written confidentiality obligations. Binadit does not use artificial intelligence services or other external software services that receive Customer data.

Annex 4. Contact points

Purpose	Binadit	Customer
Privacy questions, data subject requests, audits	contact@binadit.com, +31 10 477 5362	Administrative contact in the Portal
Personal Data Breaches and security incidents	support@binadit.com (monitored 24/7), +31 10 477 5362	Security contact in the Portal
Sub-processor changes and DPA amendments	Sent from contact@binadit.com	Administrative contact in the Portal
Abuse reports	abuse@binadit.com	Not applicable

Postal address: Binadit B.V., Seinhuiswachter 2, 3034 KH Rotterdam, the Netherlands. Chamber of Commerce number 80923216.