



**DataOne**  
RELIABLE DATACENTER FACILITIES

CUSTOMER DOCUMENTATION

# Data Processing Agreement

## DataOne

A model GDPR Article 28 data processing agreement, for customers who require one in connection with DataOne's colocation and management & support services.

---

**Version**

1.0

**Published**

October 2026

**Applies to**

All DataOne services

## Contents

- |                                            |                                 |
|--------------------------------------------|---------------------------------|
| 1. Parties and scope                       | 9. Data breach notification     |
| 2. Definitions                             | 10. International transfers     |
| 3. Subject matter and duration             | 11. Audit rights                |
| 4. Nature, purpose and scope of processing | 12. Return and deletion of data |
| 5. Processor's obligations                 | 13. Liability and term          |
| 6. Security measures                       | 14. Annex 1: Processing details |
| 7. Sub-processors                          | 15. Signatures                  |
| 8. Assistance to the controller            |                                 |

**Who needs this.** DataOne provides colocation (housing): customers own, operate and control their own equipment, and DataOne does not host or run customer content itself. This agreement is relevant mainly where DataOne's management & support staff may incidentally access customer equipment (e.g. remote hands), and where DataOne processes facility access and badge data about customer's authorized personnel. If none of this applies to your use of DataOne's services, you likely do not need this agreement — contact us if you are unsure.

### 1 Parties and scope

1.1 This Data Processing Agreement ("DPA") is entered into between DataOne (KVK 74775855, VAT NL860022158B01), Bruynvisweg 11, 1531 AX Wormer, the Netherlands ("Processor"), and the customer named in the signature block below ("Controller"), together "the parties".

1.2 This DPA forms part of, and supplements, the Terms and Conditions and/or the service agreement between the parties (the "Principal Agreement"). In the event of a conflict between this DPA and the Principal Agreement regarding the processing of personal data, this DPA prevails.

### 2 Definitions

2.1 Terms such as "personal data", "processing", "controller", "processor", "data subject", "sub-processor" and "personal data breach" have the meaning given to them in Regulation (EU) 2016/679 (the "GDPR").

### 3 Subject matter and duration

3.1 The subject matter of this DPA is the processing of personal data by the Processor on behalf of the Controller, as further described in Annex 1. This DPA takes effect on the date the Principal Agreement takes effect and remains in force for as long as the Processor processes personal data on behalf of the Controller under the Principal Agreement.

### 4 Nature, purpose and scope of processing

4.1 The Processor processes personal data only to the extent necessary to provide colocation (housing) and, where agreed, management & support services, and only for the purposes set out in

Annex 1. The Processor does not process the content of data stored on Controller's equipment, except where Processor staff incidentally and necessarily access such equipment while performing agreed remote-hands or support work at Controller's request.

4.2 The Processor will not process personal data for any purpose other than as instructed by the Controller, as set out in this DPA and the Principal Agreement, unless required to do so by EU or Dutch law, in which case the Processor will inform the Controller of that legal requirement before processing, unless the law prohibits this.

## **5 Processor's obligations**

5.1 The Processor will: (a) process personal data only on documented instructions from the Controller; (b) ensure that persons authorized to process personal data are bound by confidentiality; (c) implement appropriate technical and organizational measures as described in article 6; (d) assist the Controller as described in article 8; (e) make available information reasonably necessary to demonstrate compliance with this article; and (f) immediately inform the Controller if, in the Processor's opinion, an instruction infringes the GDPR or other applicable data protection law.

## **6 Security measures**

6.1 The Processor implements appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, having regard to the state of the art, the costs of implementation, and the nature, scope, context and purpose of the processing. These measures include, as applicable: physical access control to the facility in accordance with the Facility Guide (badges, escort requirements, 24/7 monitoring); logical access control to DataOne's own systems used to manage facility access; and confidentiality obligations for DataOne personnel.

## **7 Sub-processors**

7.1 The Processor may engage sub-processors to perform specific processing activities on its behalf, provided that the Processor imposes data protection obligations on the sub-processor that are no less protective than those set out in this DPA, and remains fully liable to the Controller for the sub-processor's performance.

7.2 The Processor will inform the Controller of any intended changes concerning the addition or replacement of sub-processors, giving the Controller the opportunity to object on reasonable, documented grounds related to data protection.

## **8 Assistance to the controller**

8.1 Taking into account the nature of the processing, the Processor will assist the Controller, insofar as reasonably possible, in responding to requests from data subjects exercising their rights under the GDPR, and in the Controller's compliance with its obligations regarding the security of processing, breach notification, data protection impact assessments and prior consultation with supervisory authorities, to the extent these relate to the Processor's processing under this DPA.

## **9 Data breach notification**

9.1 The Processor will notify the Controller without undue delay, and in any case within 48 hours, after becoming aware of a personal data breach affecting personal data processed under this DPA, providing the information reasonably available to enable the Controller to meet its own notification obligations under the GDPR.

## **10 International transfers**

10.1 The Processor processes personal data within the European Economic Area. The Processor will not transfer personal data to a country outside the EEA without an adequate level of protection, unless appropriate safeguards under the GDPR are in place and the Controller has been informed in advance.

## **11 Audit rights**

11.1 The Processor will make available to the Controller the information reasonably necessary to demonstrate compliance with this DPA, and will allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller, subject to reasonable advance notice, confidentiality, and limited to once per year unless a personal data breach has occurred or a supervisory authority requires otherwise.

## **12 Return and deletion of data**

12.1 At the end of the provision of services relating to processing, the Processor will, at the Controller's choice, delete or return all personal data to the Controller, and delete existing copies, unless EU or Dutch law requires storage of the personal data.

## **13 Liability and term**

13.1 Liability under this DPA is subject to the limitations and exclusions of liability set out in the Principal Agreement. This DPA terminates automatically upon termination of the Principal Agreement, without prejudice to any provisions of this DPA which by their nature are intended to survive termination (including articles 9, 11 and 12).

## **14 Annex 1: Processing details**

|                                    |                                                                                                                                                                                                                                                                                                   |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CATEGORIES OF DATA SUBJECTS</b> | Controller's authorized personnel and visitors who access the DataOne facility (e.g. employees, contractors); where applicable, individuals whose data is incidentally present on Controller's equipment during agreed remote-hands or support work.                                              |
| <b>CATEGORIES OF PERSONAL DATA</b> | Name, employer/company, photo ID details and photograph (for badge issuance), badge/access credentials, facility access and visitor logs; incidentally, any personal data contained on Controller's equipment, only to the extent Processor staff access it while performing agreed support work. |

|                              |                                                                                                                                                                                       |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PURPOSE OF PROCESSING</b> | Granting and administering physical access to the facility; facility security and safety; performing agreed management & support (remote hands) services at Controller's request.     |
| <b>DURATION</b>              | For the term of the Principal Agreement, and afterwards only as required by applicable law (e.g. access log retention periods).                                                       |
| <b>SUB-PROCESSORS</b>        | None engaged by default for this processing. Any sub-processor used for facility security systems (e.g. badge/access control software) will be communicated to Controller on request. |

## 15 Signatures

**For DataOne**

**For the Controller (customer)**

\_\_\_\_\_  
Name, title

\_\_\_\_\_  
Company name

\_\_\_\_\_  
Date, signature

\_\_\_\_\_  
Name, title

\_\_\_\_\_  
Date, signature

DataOne • KVK 74775855 • VAT NL860022158B01 • Bruynvisweg 11, 1531 AX Wormer, Netherlands • dataone.nl