Version: v1.0 / 22-09-2026

Data Processing Agreement Lakeglide

Bos & Brouwer B.V.

Comprised of:

Part 1. Data Pro Statement

Part 2. Standard clauses for data processing

NLdigital version march 2025

This Data Processing Agreement and the standard clauses were originally drafted in Dutch. The English version is for convenience only. In case of conflict between the Dutch and the English version, the Dutch version prevails.

Part 1: Data Pro Statement

Part 1 of the data processing agreement of Bos & Brouwer B.V. for Lakeglide. This Data Pro Statement, together with the Standard Clauses for Data Processing (NLdigital, March 2025), constitutes the data processing agreement.

General information

1. **This Data Pro Statement was drawn up by the following data processor (verwerker):**
   Bos & Brouwer B.V. (KVK 99201089), Spiegeltuin 1, 5223 MZ 's-Hertogenbosch, the Netherlands.
   Lakeglide is a trade name of Bos & Brouwer B.V.

   If you have any queries about this Data Pro Statement or about data protection in general, please contact Roel Knitel, privacy@lakeglide.com.

2. **This Data Pro Statement shall enter into force on** 22-09-2026 (v1.0)
   We regularly revise this Data Pro Statement and the security measures it describes to ensure that we remain prepared and up to date with regard to data protection. We announce new versions by e-mail to the environment administrator designated by Client.

3. **This Data Pro Statement applies to the following products and services provided by data processor**
   Lakeglide, including all components delivered under that name and including use during a trial period.

4. **Description of product(s)/service(s)**
   Lakeglide is a managed data platform with which Client connects, models and analyses source data for management information purposes. The platform is hosted in the Azure tenant of data processor. Each Client has a dedicated Databricks workspace and a dedicated storage account.

5. **Intended use**
   The product is designed and built to process the following types of data:
   The product is designed and built to process personal data in the context of data storage, data processing and data analysis.

- identification data (such as name, user name or customer number);
- contact details (such as e-mail address, telephone number and address details);
- organisational or functional relationships (such as job title or department);
- customer and relationship data;
- transaction data;
- location data;
- usage data and log data generated by use of the platform.

These data may relate to the following categories of data subjects:

- users of the platform;
- contact persons at Client's customers, business relations and suppliers;

- employees of Client, insofar as they appear in the source data.

The processing of special categories of personal data, data regarding criminal convictions and offences, or personal numbers issued by the government was not taken into account for this product, unless expressly agreed otherwise in a specific assignment or module. Client needs to determine whether or not to use the product to process such data, and does so under its own responsibility.

The standard connectors and field mappings are configured so that fields intended for government-issued personal numbers or special categories of personal data are not ingested. Client remains responsible for the content of the source data they connect, including data contained in free-text fields or in fields used for a purpose other than the one they were designed for.

6. **Privacy by design/privacy by default**

- Personal data are processed within the Azure tenant of data processor. Each Client has a dedicated Databricks workspace and a dedicated storage account, so that the data of different Clients remain separated.
- All data are encrypted by default, both at rest and in transit.
- Designated columns are masked in the standard connector mapping.
- Access to Client's environment is limited to authorised persons and systems on a need-to-know basis, and takes place solely for administration, maintenance and the handling of support requests. All access to and use of personal data is monitored and logged for the purposes of security, control and incident detection.

7. **Data processor uses the Standard Clauses for Data Processing (NLdigital, version March 2025), which are attached to the Agreement as an addendum.**
8. **Data processor shall process the personal data provided by their clients within the EU/EEA, in the Azure region West Europe, unless another region has been agreed with Client in writing. An exception is the account metadata of platform users, see item 9.**

For the Databricks Designated Services, including AI functionality, processing outside the workspace geography is disabled and processing within that geography is enforced at workspace level.

1. Data processor uses the following sub-processors:

Data processor may use sub-processors in the performance of the services. Client hereby grants general authorisation for the engagement of the sub-processors listed below. Changes are announced by way of a revised Data Pro Statement, and Client is entitled to object to such changes.

Sub-processor	Role	Within EU/EEA	Safeguards
Microsoft Azure	Cloud infrastructure, storage (ADLS Gen2), compute, Key Vault	Yes	Microsoft DPA, EU Data Boundary, encryption at rest and in transit, ISO 27001, SOC 1/2, SCCs
Databricks	Data processing platform (notebooks, jobs, Unity Catalog, clusters, Genie)	Partly*	Databricks DPA with SCCs, ISO 27001, SOC 2 Type II, EU-US Data Privacy Framework. See footnote *
Microsoft Entra ID and Entra External ID	Identity and access management for internal and external users	Yes	Part of the Microsoft DPA, RBAC, Conditional Access, EU Data Boundary
Azure Monitor / Log Analytics	Logging, monitoring and audit trails	Yes	Part of the Microsoft DPA, encrypted, RBAC, data in the selected Azure region
Vercel	Hosting of the web application	Yes**	DPA with SCCs
Neon	Application database	Yes**	DPA with SCCs
Resend	Transactional e-mail (login links, notifications)	Yes**	DPA with SCCs

* Client data remains stored in the Azure region West Europe, unless another region has been agreed with Client in writing. The account metadata of platform users, such as name and e-mail address, is also stored by Azure Databricks in the United States for account and access management purposes. Databricks covers this transfer through the Databricks Data Processing Addendum, which incorporates the EU Standard Contractual Clauses (SCCs).

** These parties are established in the United States and deliver their service from an EU region. Any transfer outside the EEA, for instance in the context of support, is covered by the SCCs agreed with these parties.

2. **Data processor shall support their clients in the following way when they receive requests from data subjects:**

- Client assesses the request and identifies the data subject, and processes the request in the source systems first. Deletion or rectification in the platform without prior processing in the source has no lasting effect, because the data are re-ingested at the next load.
- Following Client's instruction, data processor deletes or anonymises the relevant data in the history within the platform. Data processor does so within twenty working days of receiving the instruction, taking into account the nature and complexity of the request.
- All communication with data subjects takes place exclusively through Client. Data processor has no direct contact with data subjects and does not independently verify their identity.
- Where a support agreement applies, the costs of this support fall under the arrangements made therein. In other cases, support may be provided at data processor's standard rates.

3. **Data processor shall support their clients with Data Protection Impact Assessments (DPIA) in the following manner:**

- Upon a reasonable request by Client, data processor shall cooperate with a mandatory DPIA relating to the use of the platform and the associated services.
- This cooperation consists of providing relevant information about the operation of the services, the technical configuration, the processing activities and the technical and organisational security measures in place, insofar as such information is reasonably available to data processor.
- The cooperation is limited to the provision of information and does not include active participation in drawing up, reviewing or completing the DPIA. Client remains fully responsible for carrying out the DPIA and for its outcome.
- Support is provided once per mandatory DPIA, on a reasonable-efforts basis and without any guarantee as to the outcome.

4. **Once the Agreement has been terminated, data processor shall delete all personal data they process on behalf of Client within thirty days, in such a manner that the data can no longer be used and are rendered inaccessible.**

If Client has initiated a switch, this period commences after the end of the period during which Client was still able to retrieve their data. Deletion covers Client's entire storage account and the associated Databricks workspace. Historical versions of data remain available within the platform for a maximum of seven days through Delta time travel and are automatically purged thereafter.

5. **Returning of personal data once the Agreement has been terminated**

At Client's request, data processor shall provide the data in a machine-readable format, either as a CSV or Excel file, or through Delta Sharing if Client has its own Databricks environment. Data processor supports Client in switching to another provider or to an on-premises environment. The switch takes place within a transitional period of a maximum of thirty days following the end of the notice period, unless this is technically impossible and data processor substantiates this. After that period, Client can retrieve their data for at least a further thirty days.

Security policy

6. **Data processor has implemented the following security measures to protect their product or service:**

Data processor has implemented appropriate technical and organisational measures to protect personal data against loss, unauthorised access and unlawful processing. These measures are aligned with the nature of the services and the type of personal data processed.

- Pseudonymisation. Data are not pseudonymised by default. Designated columns are masked in the standard connector mapping, so that they do not enter the platform in identifiable form.
- Encryption. Data are stored encrypted and transmitted encrypted.
- Confidentiality, integrity, availability and resilience. Each Client has a dedicated Databricks workspace and a dedicated storage account. The services are protected by a segregated network environment. Access is limited to authorised persons and systems on a need-to-know basis and is monitored and logged. Security incidents and vulnerabilities are followed up in accordance with data processor's internal security and incident management procedures.
- Restoration after an incident. The platform holds data derived from Client's source systems. Those source systems remain the system of record. Restoration takes place by rolling data back through Delta time travel within a seven-day window, or by a full reload from the source systems. In addition, the redundancy of Azure Storage is relied upon.

7. Data processor conforms to the principles of the following Information Security Management System (ISMS):

Data processor applies a structured approach to information security, laid down in internal procedures and partly embedded in the platforms and technologies used. Data processor conforms to the ISMS of NLdigital. In addition, data processor is working towards obtaining ISO/IEC 27001 certification. Until certification is obtained, data processor bases its security measures on the principles and best practices of that standard. At Client's request, data processor can provide further information on the progress of this process. This framework is evaluated periodically and adjusted where necessary.

8. Data processor has obtained the following labels and certificates

Data processor does not currently hold any labels or certificates. See item 15 for the ongoing ISO/IEC 27001 certification process.

Data breach protocol

9. In the event something does go wrong, data processor shall follow the following data breach protocol to ensure that clients are notified of incidents:

Data processor maintains a data breach protocol for identifying, assessing and handling security incidents and data breaches relating to the processing of personal data in the context of the services.

If data processor becomes aware of a suspected data breach, they shall assess without delay whether a personal data breach has occurred. If so, data processor shall inform Client within forty-eight hours of discovery. The notification is sent to the privacy contact person designated by Client and contains at least:

- the nature of the incident;
- the categories of personal data and of data subjects concerned;
- the estimated scale of the incident;
- the measures taken and proposed;
- a point of contact at data processor for further information.

The protocol provides for measures aimed at limiting the consequences of the incident, taking corrective action and preventing recurrence. Incidents are recorded and evaluated.

Data processor shall, insofar as reasonable, support Client in handling data breaches, including by providing additional information as it becomes available.

Data processor shall not notify the Dutch Data Protection Authority or data subjects themselves. Whether or not to notify them remains Client's responsibility.

Acceptance

This Data Pro Statement, together with the Standard Clauses for Data Processing (NLdigital, version March 2025), constitutes the data processing agreement. The data processing agreement forms part of the Agreement and enters into force at the moment the Agreement is concluded.

Acceptance takes place electronically upon entering into the Agreement. For each acceptance, data processor records the version number of this Data Pro Statement and of the Standard Clauses, the date and time of acceptance, and the identification of Client's environment or account.

Part 2: Standard Clauses for Data Processing

Version: March 2025

Along with the Data Pro Statement, these standard clauses constitute the data processing agreement. They also constitute an annex to the Agreement and to the appendices to this Agreement, e.g. any general terms and conditions which may apply.

Article 1. Definitions

The following terms have the following meanings ascribed to them in the present Standard Clauses for Data Processing, in the Data Pro Statement and in the Agreement:

1.1 **Dutch Data Protection Authority (AP):** the supervisory authority defined in Section 4.21 of the GDPR.

1.2 **GDPR:** the General Data Protection Regulation.

1.3 **Data Processor**: the party which, in their capacity as an ICT supplier, processes Personal Data on behalf of their Client as part of the performance of the Agreement.

1.4 **Data Pro Statement**: statement issued by Data Processor in which they provide information such as the intended use of their products and/or services, any security measures which have been implemented, sub-processors, data breach, certification and dealing with the rights of Data Subjects.

1.5 **Data Subject**: a natural person who can be identified, directly or indirectly.

1.6 **Client:** the party on whose behalf Data Processor processes Personal Data. Client can either be the controller (the party who determines the purpose and means of the processing) or another data processor.

1.7 **Agreement**: the agreement concluded between Client and Data Processor, based on which the ICT supplier provides services and/or products to Client, the data processing agreement forming part of this agreement.

1.8 **Personal Data** any and all information regarding a natural person who has been or can be identified, as defined in Article 4.1 of the GDPR, processed by Data Processor as required under the Agreement.

1.9 **Data Processing Agreement**: the present Standard Clauses for Data Processing , which, together with Data Processor's Data Pro Statement (or similar such information), constitute the data processing agreement within the meaning of Article 28.3 of the GDPR.

Article 2. General provisions

2.1 The present Standard Clauses for Data Processing apply to all Personal Data processing operations carried out by Data Processor in providing their products and services, as well as to all Agreements and offers. The applicability of Client's data processing agreements is explicitly rejected.

2.2 The Data Pro Statement, and particularly the security measures described in it, may be adapted from time to time to changing circumstances by Data Processor. Data Processor shall notify Client in the event of

significant revisions. If Client in all reasonableness cannot agree to the revisions, Client shall be entitled to terminate the data processing agreement in writing, stating their reasons for doing so, within thirty days of having been served notice of the revisions.

2.3 Data Processor shall process the Personal Data on behalf of Client, in accordance with the written agreed upon instructions provided by Client by Data Processor.

2.4 Client or their customer shall serve as the controller within the meaning of the GDPR, shall have control over the processing of the Personal Data and shall determine the purpose and means of processing the Personal Data.

2.5 Data Processor shall serve as the processor within the meaning of the GDPR and shall therefore not determine the purpose and means of processing the Personal Data, and shall not make any decisions on the use of the Personal Data and other such matters.

2.6 Data Processor shall implement the GDPR as laid down in the present Standard Clauses for Data Processing, the Data Pro Statement and the Agreement. It is up to Client to assess, on the basis of this information, whether Data Processor is providing sufficient guarantees with regard to the implementation of appropriate technical and organisational measures in order to ensure that the processing operations meet the requirements of the GDPR and that Data Subjects' rights are sufficiently protected.

2.7 Client shall guarantee Data Processor that they act in accordance with the GDPR, that they provide a high level of protection for their systems and infrastructure at all time, that the nature, use and/or processing of the Personal Data are not unlawful and that they do not violate any third party's rights.

2.8 Administrative fines imposed on Client by the Dutch Data Protection Authority cannot be recovered from Data Processor.

Article 3. Security

3.1 Data Processor shall implement the technical and organisational security measures set out in their Data Pro Statement. In implementing the technical and organisational security measures, Data Processor shall take into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing and the intended use of their products and services, and the risk in processing the data of varying likelihood and severity inherent to the rights and freedoms of Data Subjects that are to be expected considering the nature of the intended use of Data Processor's products and services.

3.2 Unless explicitly stated otherwise in the Data Pro Statement, the products and services provided by Data Processor shall not be equipped to process special categories of personal data or data relating to criminal convictions and offences.

3.3 Data Processor seeks to ensure that the security measures they shall implement are appropriate for the manner in which Data Processor intends to use the products and services.

3.4 In Client's opinion, said security measures provide a level of security that is tailored to the risk inherent in the processing of the Personal Data used or provided by Client, taking into account the factors referred to in Article 3.1.

3.5 Data Processor shall be entitled to adjust the security measures they have implemented if to their discretion such is necessary for a continued provision of an appropriate level of security. Data Processor shall record any significant adjustments they chooses to make, e.g. in a revised Data Pro Statement, and shall notify Client of said adjustments where relevant.

3.6 Client may request Data Processor to implement further security measures. Data Processor shall not be obliged to honour such requests to adjust their security measures. If Data Processor makes any adjustments to their security measures at Client's request, Data Processor is entitled to invoice Client for the costs associated with said adjustments. Data Processor shall not be required to actually implement the requested security measures until both Parties have agreed upon them in writing. .

Article 4. Data breaches

4.1 Data Processor does not guarantee that their security measures shall be effective under all circumstances. If Data Processor discovers a data breach within the meaning of Article 4 sub 12 of the GDPR, they shall notify Client without undue delay. The "Data Breach Protocol" section of the Data Pro Statement outlines the way in which Data Processor shall notify Client of data breaches.

4.2 It is up to the Controller (the Client or their customer) to assess whether the data breach of which Data Processor has notified the Controller must be reported to the Dutch Data Protection Authority or to the Data Subject concerned. The Controller (Client or their customer) shall at all times remain responsible for reporting data breaches which must be reported to the Dutch Data Protection Authority and/or Data Subjects pursuant to Articles 33 and 34 of the GDPR. Data Processor is not obliged to report data breaches to the Dutch Data Protection Authority and/or to the Data Subject.

4.3 Where necessary, Data Processor shall provide further information on the data breach and shall assist Client to meet their breach notification requirements within the meaning of Articles 33 and 34 of the GDPR by providing all the necessary information available to Data Processor.

4.4 If Data Processor incurs any reasonable costs in doing so, they are entitled invoice Client for these, at the rates applicable at the time.

Article 5. Confidentiality

5.1 Data Processor shall ensure that the persons processing Personal Data acting under its authority have committed themselves to confidentiality.

5.2 Data Processor shall be entitled to provide third parties with Personal Data if and insofar as such is necessary due to a court order, statutory provision or order issued by a competent government authority.

5.3 Any and all access and/or identification codes, certificates, information regarding access and/or password policies provided by Data Processor to Client, and any and all information provided by Data Processor to Client detailing the technical and organisational security measures included in the Data Pro Statement are

confidential and shall be treated as such by Client and shall only be disclosed to authorised employees of Client. Client shall ensure that their employees comply with the requirements described in this article.

Article 6. Term and termination

6.1 This data processing agreement constitutes part of the Agreement, and any new or subsequent agreement arising from it and shall enter into force at the time of the conclusion of the Agreement and shall remain effective for an indefinite period.

6.2 This data processing agreement shall end by operation of law upon termination of the Agreement or upon termination of any new or subsequent agreement arising from it between parties.

6.3 If the data processing agreement is terminated, Data Processor shall delete all Personal Data they currently store and which they have obtained from Client within the timeframe laid down in the Data Pro Statement, in such a way that the Personal Data can no longer be used and shall have been *rendered inaccessible*. Alternatively, if such has been agreed, Data Processor shall return the Personal Data to Client in a machine-readable format.

6.4 If Data Processor incurs any costs associated with the provisions of Article 6.3, they shall be entitled to invoice Client for said costs. Further arrangements relating to this subject can be laid down in the Data Pro Statement.

6.5 The provisions of Article 6.3 do not apply if Data Processor is prevented from removing or returning the Personal Data in full or in part by a statutory provision. In such instances, Data Processor shall only continue to process the Personal Data insofar as such is necessary by virtue of their statutory obligations. Furthermore, the provisions of Article 6.3 shall not apply if Data Processor is the Controller of the Personal Data within the meaning of the GDPR.

Article 7. The rights of Data Subjects, Data Protection Impact Assessments (DPIA) and auditing rights

7.1 Where possible, Data Processor shall cooperate with reasonable requests made by Client relating to Data Subjects who invoke their rights from Client. If Data Processor is directly approached by a Data Subject, they shall refer the Data Subject to Client where possible.

7.2 If Client is required to carry out a Data Protection Impact Assessment or a subsequent consultation within the meaning of Articles 35 and 36 of the GDPR, Data Processor shall cooperate with such, following a reasonable request to do so.

7.3 Data Processor will lend their cooperation to Client's requests for the deletion of personal data insofar as Client cannot carry this out themself.

7.4 Data Processor shall be able to demonstrate their compliance with their requirements under the data processing agreement by means of a valid Data Processing Certificate or an equivalent certificate or audit report (third-party memorandum) issued by an independent expert.

7.5 In addition, at Client's request, Data Processor shall provide all other information that is reasonably required to demonstrate compliance with the arrangements made in this data processing agreement. If, in spite of the foregoing, Client has grounds to believe that the Personal Data are not processed in accordance with the data processing agreement, Client shall be entitled to have an audit performed (at their own expense) not more than once every year by an independent, certified, external expert who has demonstrable experience with the type of data processing operations carried out under the Agreement. The scope of the audit shall be limited to verifying that Data Processor is complying with the arrangements made regarding the processing of the Personal Data as set forth in the present data processing agreement. The expert shall be subject to a duty of confidentiality with regard to his/her findings and shall only notify Client of matters which cause Data Processor to fail to comply with their obligations under the data processing agreement. The expert shall furnish Data Processor with a copy of his/her report. Data Processor shall be entitled to reject an audit or instruction issued by the expert if to their discretion the audit or instruction is inconsistent with the GDPR or any other law, or that it constitutes an unacceptable breach of the security measures they have implemented.

7.6 The parties shall consult each other on the findings of the report at their earliest convenience. The parties shall implement the measures for improvement suggested in the report insofar as they can be reasonably expected to do so. Data Processor shall implement the proposed measures for improvement insofar as to their discretion such are appropriate, taking into account the processing risks associated with their product or service, the state of the art, the costs of implementation, the market in which they operate, and the intended use of the product or service.

7.7 Data Processor shall be entitled to invoice Client for any costs they incur in implementing the measures referred to in this article.

Article 8. Sub-processors

8.1 Data Processor has specified in the Data Pro Statement whether Data Processor uses any third parties (sub-processors) to help them process the Personal Data, and if so, which third parties.

8.2 Client hereby authorises Data Processor to hire other sub-processors to meet their obligations under the Agreement.

8.3 Data Processor shall notify Client of any changes concerning the addition or replacement of the third parties (sub-processors) hired by Data Processor, e.g. through a revised Data Pro Statement. Client shall be entitled to object to such changes . Data Processor shall ensure that any third parties they hire shall commit to ensuring the same level of Personal Data protection as the security level Data Processor is bound to provide to the Client pursuant to the Data Pro Statement.

Article 9. Other provisions

These Standard Clauses for Data Processing, along with the Data Pro Statement, constitute an integral part of the Agreement. Therefore, any and all rights and obligations arising from the Agreement, including any applicable general terms and conditions and/or limitations of liability, shall also apply to the data processing agreement.