

Data Processing Agreement (DPA) — Loket

English translation — the French version is the governing version.

Between:

The professional holding the Loket account, as identified in their account settings — the "**Controller**";
and

Always Late Technologies BV ("Loket"), a company incorporated under Belgian law, Fonteyneweg 2, 1800 Vilvoorde, Belgium, BCE **1039.721.620**, VAT **BE 1039.721.620** — the "**Processor**";

pursuant to **Article 28 GDPR**, in addition to the terms of use (the "Main Agreement"). In the event of any conflict regarding data protection, this DPA prevails.

This agreement is **accepted electronically** when the Loket account is created, together with the Main Agreement. It therefore requires no handwritten signature and no paper counterpart.

1. Definitions

The terms of the GDPR (controller, processor, sub-processor, data subject, personal data breach, etc.) have the meaning given to them by the Regulation.

2. Purpose, roles and duration

2.1. The Processor hosts an application through which **the Controller's clients** submit documents through a link, without creating an account, for collection and provision to the Controller, for the benefit of the Controller.

2.2. **Roles.** The Controller determines the purposes and the means: it is the **controller**. Loket processes the data **solely to provide the Service and on the instructions** of the Controller: it is the **processor**.

2.3. **Duration.** For the entire duration of the Main Agreement and for as long as data is processed on behalf of the Controller.

3. Description of the processing

Detailed in **Annex 1**.

4. Obligations of the Processor

(a) **Instructions.** Process only on the documented instructions of the Controller (this DPA and normal use constituting instructions), save for a legal obligation (with prior information unless prohibited).

(b) **Confidentiality.** Bind authorised persons to confidentiality.

(c) **Security.** Measures under **Article 32 — Annex 3**.

(d) **Sub-processors.** Use them only in accordance with **Annex 2**, under a **general authorisation**, with **30 days'** prior information of any change and a right to object on legitimate grounds; equivalent obligations imposed by contract on each sub-processor.

(e) **Assistance.** Assist the Controller in responding to requests to exercise rights (via the **export** and **deletion** functions) and in complying with articles 32 to 36.

(f) **Personal data breach.** Notify the Controller **without undue delay** (at the latest within **48 hours**) with the information under art. 33 §3 available. Notification to the authority and to data subjects is the responsibility of the Controller.

(g) **End of the relationship.** **Delete or return** the data at the Controller's choice and destroy the copies, save for a legal obligation (art. 6).

(h) **Records & documentation.** Maintain the record (art. 30 §2) and demonstrate compliance with art. 28.

(i) **Audit.** Allow **annual** and post-incident audits, subject to reasonable notice and confidentiality; may be satisfied by the reports of the sub-processors.

5. Obligations of the Controller

Ensure a **legal basis**, inform its own clients, transmit only the necessary data, and configure the retention periods offered by the Service.

6. Fate of the data at the end of the contract

6.1. **The choice under Article 28.3(g) — return or deletion — belongs to the Controller**, and the Service makes it exercisable without going through the Processor: **return** is performed through the **export** function (a complete archive, database and files), available for as long as the account exists, **including throughout the window described in 6.2.**

6.2. **Absent a return, deletion is the default, at 90 days.** At the end of the subscription or of the trial, the account is **suspended**: collection stops, the data remains **intact and exportable**. The Processor notifies the Controller **30 days and then 7 days** before the deadline. At the end of the **90 days**, the account is **closed** — deletion of the database and the files, copies included — save for any legal retention obligation.

6.3. **The Controller may close the account at any time** from its settings, without waiting for the deadline. Early closure and automatic closure follow the **same, single deletion path**. Deleting a file effectively removes the files from storage.

7. Transfers outside the EU

7.1. Data **at rest** hosted in the **EU (Frankfurt)** — Annex 2.

7.2. As some sub-processors are established **in the United States**, transfers are framed by the **SCCs** and/or the **Data Privacy Framework** provided for in their respective agreements. As at **28 July 2026**, the three US sub-processors hold an **active** Data Privacy Framework certification: **Vercel Inc.** (EU-US, Swiss-US and UK extension); **Neon**, covered by the certification of **Databricks, Inc.** of which it is part; **Resend** (EU-US and UK extension, recertification in progress at that date). This status is **re-verified every quarter** and the contractual documents are updated if it changes.

8. Liability and governing law

8.1. As between the parties, liability is allocated under the Main Agreement and the GDPR, including the limitations in the Main Agreement, but only to the extent permitted by applicable mandatory law.

8.2. Nothing in this DPA limits the rights of data subjects, the powers of a supervisory authority, or the allocation and rights of recourse provided for in Article 82 of the GDPR.

8.3. **Belgian law**; courts of **Brussels**.

Annex 1 — Description of the processing

Purpose	Collection, submission, storage and return of supporting documents between the Controller and its clients.
Nature	Hosting, storage, transmission, deletion.
Data subjects	Clients of the Controller and third parties whose documents are uploaded.
Categories of data	identification and contact data; the content of the documents submitted (identity documents, deeds, financial or property documents). May include sensitive / high-risk data depending on the documents requested — see DPIA note.
Duration	Duration of the relationship + 90 days (return window, art. 6); link expiration configurable.

DPIA note: the **Controller** must assess whether a **DPIA (art. 35)** is required on its side (identity documents, sensitive data, regulated clientele). **Loket** provides the technical elements.

Annex 2 — Authorised sub-processors

Sub-processor	Role	Data location	Transfer
Vercel Inc. (US)	App + file hosting (Blob)	Files fra1 / EU	DPF active (EU-US, Swiss-US, UK Extension)
Neon (a Databricks company) (US)	Database	eu-central-1 / EU	DPF active via Databricks, Inc.
Resend (US)	Transactional emails (links, notifications)	Email addresses + content	DPF active (re-certification under review as of 2026-07-28)

Annex 3 — Technical and organisational measures (art. 32)

- **Encryption in transit:** HTTPS/TLS end to end. Neon enforces TLS 1.2/1.3; Vercel uses HTTPS/TLS 1.3; Resend TLS 1.3.
- **Encryption at rest:**
 - database (**Neon**): **AES-256** (documented by Neon);
 - submitted files (**Vercel Blob**): **AES-256**, applied before writing to disk (documented by Vercel);
 - email (**Resend**): data encrypted at rest; **the algorithm is not publicly documented by Resend**, so it is not asserted here.
- **Partitioning by account:** access limited to the account holder; any access outside the perimeter fails.
- **Non-guessable upload links:** random tokens, non-listable, configurable expiration.
- **Authentication:** single-use login links (24 h).
- **Restricted access:** private storage (non-public URLs, random suffix). Administrative access goes through the hosting providers' consoles, protected by strong authentication, and is limited to one person. **Loket does not currently implement an application-level audit log of administrative access:** the available logging is the platforms' own (Neon, Vercel).
- **File controls:** allowed types, a maximum size of 100 MB, no more than 20 files per requested item, and usage quotas checked before upload or download. **Loket does not scan files for malware;** these controls do not guarantee that a file is free from malware.
- **Effective deletion:** file deleted = files deleted; account deleted = database + files purge.
- **Backups:**
 - database (**Neon**): point-in-time restore over a **7-day** window, measured on 1 August 2026. The recovery procedure requires an isolated restore and verification before any action on production;
 - submitted files (**Vercel Blob**): replicated storage, stated durability of 99.999999999% and availability of 99.99%. **Vercel offers no client-side file restore:** a deleted file is not recoverable.
- **Sub-processor certifications:** Vercel — SOC 2 Type II and ISO 27001:2022; Neon — annual SOC 2 Type II and ISO 27001 audits; Resend — SOC 2 Type II.

Version 2026-08-01.1 — accepted electronically when the Loket account is created. No handwritten signature is required; the evidence of acceptance is the timestamp kept by Loket with the Controller's account.