Kanso Sites - Data Processing Agreement (DPA)

Version: 18 September 2026

Kanso Sites: operated by Víctor Ribera in the Netherlands

Contact: hello@kansosites.nl

1. Purpose and application

This Data Processing Agreement (the **DPA**) applies where Kanso Sites processes Personal Data on behalf of a Client as a processor within the meaning of Regulation (EU) 2016/679 (the **GDPR**) in connection with services supplied under an agreement between Kanso Sites and that Client (the **Main Agreement**).

The Client is the **Controller** and Kanso Sites is the **Processor** for the processing covered by this DPA, unless a Project Document expressly identifies a different lawful allocation of roles for a particular processing activity.

This DPA forms part of the Main Agreement when the Main Agreement, proposal or other Project Document incorporates it by reference. If this DPA conflicts with the Main Agreement on a matter specifically concerning processing of Personal Data as processor, this DPA takes priority for that matter. The Main Agreement continues to govern commercial matters, including fees, intellectual property and liability, subject to mandatory data-protection law.

2. Definitions

Terms such as **Controller**, **Processor**, **Personal Data**, **Processing**, **Data Subject**, **Personal Data Breach** and **Supervisory Authority** have the meanings given in the GDPR.

Client Data means Personal Data processed by Kanso Sites on behalf of the Client under this DPA.

Subprocessor means another processor engaged by Kanso Sites to process Client Data on behalf of the Client.

3. Processing details

The subject matter, duration, nature and purpose of the Processing, together with the relevant data categories and Data Subjects, are described in **Schedule 1** and may be supplemented by the applicable proposal or Project Document.

Kanso Sites will process Client Data only as necessary to provide the agreed services and in accordance with documented instructions from the Client, unless Union or Member-State law requires otherwise. If legally permitted, Kanso Sites will inform the Client before carrying out processing required by such law.

The Main Agreement, this DPA, written project instructions and configuration choices made or approved by the Client constitute documented instructions for the purposes of this DPA.

If Kanso Sites reasonably believes that an instruction infringes applicable data-protection law, Kanso Sites may suspend the affected Processing and will inform the Client of the concern without undue delay.

4. Controller responsibilities

The Client is responsible for determining the lawful purposes and means of its Processing and for ensuring that its instructions to Kanso Sites comply with applicable law.

The Client will, where required:

- establish and document an appropriate legal basis for the Processing;
- provide legally required privacy information to Data Subjects;

- obtain any required consents or permissions;
- ensure that the Client has the right to provide the Client Data to Kanso Sites;
- minimise the Client Data provided to what is reasonably necessary; and
- ensure that its instructions do not require unlawful Processing.

Special-category Personal Data, criminal-offence data, government identification data, health data or other unusually sensitive data must not be supplied to Kanso Sites unless the Processing has been expressly agreed in writing and appropriate additional safeguards have been arranged.

5. Confidentiality and authorised personnel

Kanso Sites will ensure that people authorised to process Client Data are bound by an appropriate duty of confidentiality and receive access only where reasonably necessary for their role.

Access to Client Data will be limited according to the principle of least privilege so far as reasonably practicable for the services being supplied.

The confidentiality obligations in the Main Agreement also apply to Client Data.

6. Security measures

Taking into account the state of the art, implementation costs, the nature, scope, context and purposes of Processing and the risks to Data Subjects, Kanso Sites will implement appropriate technical and organisational measures designed to provide a level of security appropriate to the risk.

The baseline measures currently expected for relevant Kanso Sites processing are described in **Schedule 2**. The exact measures applicable to a project depend on the agreed services and systems involved.

Kanso Sites does not warrant that any system can be absolutely secure. Security obligations under this DPA are obligations to implement appropriate measures, not a guarantee that no incident can occur.

7. Subprocessors

The Client gives Kanso Sites general written authorisation to engage Subprocessors where reasonably necessary to provide the services.

Kanso Sites will ensure that each Subprocessor used to process Client Data is bound by data-protection obligations that provide a level of protection consistent with the requirements of Article 28 GDPR for the relevant Processing.

The initial categories and known service providers that may be used for covered Processing are described in **Schedule 3**. Only providers actually used for the relevant project apply.

Kanso Sites will inform the Client of an intended material addition or replacement of a Subprocessor that will process Client Data before that Subprocessor begins the relevant Processing, giving the Client a reasonable opportunity to object on data-protection grounds. Where advance notice is not reasonably possible because of an urgent security, legal or service-continuity need, Kanso Sites will inform the Client as soon as reasonably practicable. The parties will work in good faith to identify a commercially reasonable alternative to a reasonably objected-to Subprocessor. If no reasonable alternative is available, either party may terminate the affected Processing service, without affecting payment for services already supplied.

Kanso Sites remains responsible for its Subprocessors to the extent required by Article 28 GDPR.

8. International transfers

Kanso Sites will not transfer Client Data to a country outside the European Economic Area, or permit a Subprocessor to do so, unless the transfer is permitted under applicable data-protection law and any required transfer safeguards are in place.

Where required, an appropriate transfer mechanism will be used, such as an adequacy decision, the European Commission's Standard Contractual Clauses, the EU-U.S. Data Privacy Framework where applicable, or another lawful safeguard.

Where Kanso Sites is a processor and an external provider acts as its Subprocessor, Kanso Sites will use the processor-to-processor transfer mechanism required for that relationship where applicable.

9. Assistance with Data Subject rights

Taking into account the nature of the Processing, Kanso Sites will provide reasonable assistance to the Client, through appropriate technical and organisational measures where possible, so that the Client can respond to requests by Data Subjects exercising rights under the GDPR.

If Kanso Sites receives a request directly from a Data Subject relating to Client Data, Kanso Sites will not independently determine the request unless legally required to do so. Kanso Sites will forward the request to the Client without undue delay where the Client can reasonably be identified.

Extensive assistance outside the ordinary agreed services may be chargeable at the applicable agreed rate, except to the extent the assistance is required because of Kanso Sites' breach of this DPA.

10. Personal Data Breaches

Kanso Sites will notify the Client without undue delay after becoming aware of a Personal Data Breach affecting Client Data.

As information becomes available, Kanso Sites will provide reasonable details needed by the Client to assess the incident and meet its obligations under Articles 33 and 34 GDPR, including where relevant:

- the nature of the breach;
- the categories of affected data and Data Subjects;
- the likely consequences; and
- measures taken or proposed to contain, investigate and remediate the incident.

Kanso Sites' notification of an incident is not an admission of fault or liability.

The Client remains responsible for deciding whether notification to a Supervisory Authority or Data Subjects is legally required, unless applicable law assigns that responsibility differently.

11. DPIAs, consultations and compliance assistance

Taking into account the nature of the Processing and the information available to Kanso Sites, Kanso Sites will provide reasonable assistance with the Client's obligations under Articles 32 to 36 GDPR where the relevant obligation relates to the Processing performed by Kanso Sites.

This may include providing information reasonably required for a data-protection impact assessment or prior consultation with a Supervisory Authority.

Assistance that materially exceeds the ordinary agreed services may be chargeable at the applicable agreed rate unless it is required because of Kanso Sites' breach of this DPA.

12. Information and audits

Kanso Sites will make available information reasonably necessary to demonstrate compliance with the processor obligations in Article 28 GDPR.

Where reasonable documentary evidence is insufficient, the Client may request an audit relating to Processing under this DPA. Unless a Personal Data Breach, substantiated compliance concern or Supervisory Authority requires otherwise:

- audits will normally be limited to once in any 12-month period;
- reasonable advance notice must be given;
- remote review and existing independent reports or documentation should be used first where they can reasonably answer the question;
- the audit must minimise disruption and protect other customers' and third parties' confidential information; and
- the Client bears its own audit costs and Kanso Sites' reasonable additional costs, unless the audit identifies a material breach of this DPA by Kanso Sites.

An auditor must be independent, appropriately qualified and bound by confidentiality obligations.

13. Return and deletion

During the term of the Main Agreement, Kanso Sites will return or export Client Data where this forms part of the agreed services or where the parties reasonably agree an appropriate method.

When the Processing services end, the Client may instruct Kanso Sites to return or delete Client Data that remains under Kanso Sites' control. Unless applicable law requires retention or a Project Document states otherwise, Kanso Sites will delete or anonymise remaining active copies within **90 days** after the relevant Processing service ends.

Data held only in disaster-recovery or backup systems may remain until it is deleted through the normal backup rotation, provided it remains protected and is not restored or otherwise processed except for recovery, security or legal purposes.

Kanso Sites may retain information that it processes in its own capacity as controller, such as contract, billing, tax, security or legal records, where there is an independent lawful basis to retain it. Such information is outside the processor deletion obligation in this section.

14. Records and cooperation with authorities

Kanso Sites will maintain records of Processing activities where Article 30 GDPR requires it to do so for its processor activities.

Kanso Sites will reasonably cooperate with competent Supervisory Authorities in relation to Processing covered by this DPA where required by applicable law.

15. Liability and mandatory law

The liability provisions of the Main Agreement apply to this DPA to the extent permitted by applicable law.

Nothing in the Main Agreement or this DPA limits any responsibility that cannot lawfully be limited under the GDPR or other mandatory data-protection law.

Each party remains responsible for the obligations assigned to it by applicable data-protection law.

16. Duration and termination

This DPA starts when it is incorporated into the Main Agreement and continues for as long as Kanso Sites processes Client Data on behalf of the Client.

Sections that by their nature are intended to continue after Processing ends, including confidentiality, audit rights relating to the Processing period, return/deletion, liability and legal obligations, remain effective for as long as necessary.

17. Governing law

The governing-law and dispute provisions of the Main Agreement apply to this DPA, subject to mandatory rights and jurisdiction under applicable data-protection law.

Schedule 1 - Processing Description

This Schedule applies unless the applicable Project Document states more specific processing details.

Subject matter

Development, configuration, migration, support, maintenance, troubleshooting, hosting-related assistance or other digital services described in the Main Agreement where those services require Kanso Sites to process Personal Data on behalf of the Client.

Duration

For the period during which Kanso Sites performs the relevant Processing services, followed by the return/deletion period described in this DPA.

Nature of Processing

Depending on the project, Processing may include access, collection through configured systems, consultation, storage, organisation, transmission, migration, retrieval, troubleshooting, modification, backup where in scope, export and deletion.

Purpose

To provide the services described in the Main Agreement, maintain agreed functionality, investigate technical issues, migrate or configure systems, provide support and perform other documented Client instructions consistent with the Main Agreement.

Categories of Data Subjects

As applicable to the project:

- Client employees, contractors and representatives;
- the Client's customers and prospective customers;
- website visitors and end users;
- users of systems, applications or ecommerce services operated by the Client; and
- other individuals whose Personal Data the Client lawfully makes available through the agreed systems.

Types of Personal Data

As applicable to the project:

- names and business contact details;
- email addresses and telephone numbers;
- account identifiers and usernames;

- IP addresses, device or request data and technical logs;
- website form submissions and messages;
- customer, lead or order information contained in the systems Kanso Sites is asked to work on;
- configuration, support or diagnostic data that may contain Personal Data; and
- other ordinary Personal Data expressly described in the Project Documents.

Special categories

No special-category Personal Data or criminal-offence data is intended to be processed under the standard DPA unless expressly identified and agreed in writing before Processing begins.

Schedule 2 - Baseline Technical and Organisational Measures

The measures below apply where relevant to the systems and services within Kanso Sites' control. They are proportionate baseline measures rather than a guarantee that every listed control is technically available in every third-party platform.

1. **Access control** - access to project systems and Client Data is limited to people who reasonably need it for the agreed work.
2. **Authentication** - strong passwords are used and multi-factor authentication is enabled where reasonably available and appropriate for systems containing or providing access to Client Data.
3. **Least privilege** - permissions are limited to the level reasonably necessary for the task.
4. **Secure transmission** - supported production web services use encrypted network transport such as HTTPS/TLS where reasonably available.
5. **Credential handling** - production credentials are not intentionally placed in public repositories or public project files; secrets are handled through appropriate environment or secret-management mechanisms where available.
6. **Development hygiene** - dependencies, frameworks and deployment environments are maintained with reasonable attention to security updates and known vulnerabilities relevant to the agreed service.
7. **Separation of environments** - development and production data are separated where reasonably practicable; production datasets are not copied into development environments unless necessary and appropriately protected.
8. **Data minimisation** - Kanso Sites aims to access and retain only the Client Data reasonably needed for the task.
9. **Logging and incident response** - relevant technical information may be used to identify, investigate and respond to security or operational incidents.
10. **Backups** - backups are used only where they are part of the agreed service or relevant provider functionality; backup scope and recovery guarantees are not implied unless expressly included in the project scope.
11. **Subprocessor review** - Kanso Sites uses service providers appropriate to the relevant task and seeks appropriate contractual and transfer safeguards where required for processor activities.
12. **Deletion and access removal** - access and active project data are removed or reduced when no longer reasonably needed, subject to the retention and deletion provisions of this DPA and the Main Agreement.

Schedule 3 - Initial Subprocessors

Only a provider actually used to process Client Data for the relevant project acts as a Subprocessor under this DPA.

Provider	Typical purpose	Typical location / transfer note
Netlify, Inc.	Website hosting, deployment and infrastructure where a Client project uses Netlify	Processing may involve the United States or other locations. Netlify publishes a DPA and uses recognised international-transfer mechanisms including Standard Contractual Clauses where applicable.
Plus Five Five, Inc. (Resend)	Transactional email or contact-form delivery where a Client project uses Resend	Resend states that customer data is stored in the United States and its DPA includes Standard Contractual Clauses, including processor-to-processor terms where Resend acts as a subprocessor.

Other project-specific Subprocessors may be identified in the proposal, project documentation or a written Subprocessor notice before they are used for covered Processing.

Ordinary business correspondence handled by Kanso Sites in its own capacity as controller is not automatically Client Data processed under this DPA. Clients should not send production datasets, passwords or special-category Personal Data through ordinary email unless a secure method and the relevant processor arrangements have been expressly agreed.