

VIKEN-NTW - Data Processing Agreement

Model version 1.0 - launch version

Last updated: 24 July 2026

This Data Processing Agreement is a model agreement that is completed for each customer with the assignment, quotation or appendices. It applies where and insofar as VIKEN-NTW processes personal data on behalf of a customer.

Parties

1. The customer as stated in the quotation, order confirmation or Appendix 1, hereinafter: Customer or Controller;

2. Viken-WHB, trading under the trade name VIKEN-NTW, established at Vogelwikke 11, 6026 AK Maarheeze, the Netherlands, registered with the Dutch Chamber of Commerce under number 81074662, hereinafter: VIKEN-NTW or Processor.

Contact: contact@viken-ntw.com

Privacy and incident contact: privacy@viken-ntw.com

Website: <https://viken-ntw.com>

Recitals

- The Customer determines the purposes and means of the processing described in Appendix 1 and is in principle the Controller.
- VIKEN-NTW processes personal data for the performance of IT, domain, email, cloud, hosting, security, support, CRM, communication or automation services.
- For its own customer administration, invoicing, security, business operations and legal obligations, VIKEN-NTW may act as an independent Controller. This Agreement does not apply to those independent processing activities.
- Where the Customer itself acts as a Processor for a third party, VIKEN-NTW may act as a Sub-processor under this Agreement. The Customer then warrants that it is legally entitled to engage VIKEN-NTW.

1. Subject matter and order of precedence

VIKEN-NTW processes personal data only insofar as necessary for the agreed services and in accordance with documented instructions from the Customer.

The quotation, order confirmation, package description, this Agreement and the appendices together form the data processing arrangements. In the event of conflict, an expressly agreed customer-specific appendix prevails over this model.

This Agreement automatically applies to every assignment in which VIKEN-NTW actually acts as a Processor or Sub-processor, unless the parties sign another data processing agreement.

2. Duration

This Agreement applies from the moment VIKEN-NTW processes personal data on behalf of the Customer and continues for as long as the relevant services are provided.

Provisions relating to confidentiality, security incidents, audits, liability, return and deletion continue to apply insofar as their nature requires.

3. Instructions from the Customer

VIKEN-NTW processes personal data only on the basis of:

- the quotation, assignment or package description;
- settings and configurations approved by the Customer;
- support requests or change requests;
- additional written or digital instructions.

Where an instruction, in VIKEN-NTW's opinion, conflicts with applicable data protection law or causes a serious security risk, VIKEN-NTW informs the Customer unless prohibited by law. VIKEN-NTW may pause performance until a safe and lawful instruction has been confirmed.

VIKEN-NTW does not use personal data for its own marketing, sale to third parties or any incompatible purpose of its own.

4. Nature and purposes of processing

Depending on the assignment, processing may include:

- collecting, recording, organising, structuring and storing;
- configuring and managing accounts, roles and permissions;
- migrating, importing, exporting, linking and synchronising;
- hosting or making data technically available;
- sending business communications and automated messages;
- processing forms, calendars, CRM data and customer portals;
- securing, monitoring, restoring and troubleshooting;
- supporting users and carrying out management activities;
- deleting, anonymising, returning or making data inaccessible.

Processing is limited to the purposes recorded in the assignment and Appendix 1.

5. Possible scope per package

The actual processing is always determined in Appendix 1. As a starting point, the following classification may be used:

Goodwill Anchor

Limited processing for associations and non-profit organisations, for example contact persons, board members, members, volunteers, website visitors, forms, email, calendars and simple CRM or community functions.

Viken Essentials

Processing for domains, business email, Microsoft 365 or Google Workspace, user accounts, roles, permissions, cloud storage, basic security, support and, where agreed, website or form data.

Viken Sovereign

Additional processing for websites, hosting, forms, calendars, CRM, customer communication, automation, payments, WhatsApp, SMS, telephony, video, communities, customer portals, social media planning and email marketing.

Viken Compliant Pro

Processing involving increased privacy or security requirements. This may, only after explicit assessment and agreement, include special categories of personal data or health data. For such processing, additional measures, supplier choices, access restrictions, transfer assessments and, where necessary, a DPIA or sector-specific appendix are recorded.

A package name alone does not constitute permission to process all listed data. Only the actually agreed functions and Appendix 1 are authoritative.

6. Categories of data subjects

Depending on the assignment, data subjects may include:

- customers, clients or patients of the Customer;
- leads and website visitors;
- employees, applicants and contact persons;
- suppliers and business relations;
- directors, association members and volunteers;
- users of customer portals, communities, calendars or forms;
- other persons whose data the Customer lawfully processes in the systems.

7. Categories of personal data

Depending on the assignment, processing may include:

- name, address and contact details;
- account, user and authentication data;
- roles, permissions and access data;

- business communications;
- form, quiz, intake and calendar information;
- CRM, lead and customer data;
- invoice, payment and transaction data insofar as these form part of the linked workflow;
- technical configurations, IP addresses, device and log data;
- support information, documents and migration data;
- special categories of personal data, including health data, only where expressly agreed and lawfully and appropriately configured.

The Customer does not provide categories of personal data that are not necessary for the assignment.

8. Responsibilities of the Customer

The Customer:

- has a valid legal basis for the processing;
- informs data subjects appropriately;
- provides only lawful and necessary instructions;
- determines retention periods and access rights unless the parties expressly determine these together;
- ensures that users handle accounts, passwords and MFA carefully;
- reports changes in employees, authorisations, risks and processing purposes in good time;
- assesses whether a DPIA, consent, professional confidentiality or sector-specific obligation applies;
- does not use public forms or ordinary email for passwords, login codes or special category data where no secure route has been agreed.

9. Confidentiality

VIKEN-NTW ensures that persons acting under its authority who have access to personal data:

- process the data only for the assignment;
- are bound by an appropriate duty of confidentiality;
- have access only insofar as necessary for their role.

This obligation continues after termination.

10. Technical and organisational measures

VIKEN-NTW takes measures appropriate to the nature, scope, context and risk of the processing. Depending on the service, these may include:

- unique administrator and user accounts;
- roles, permissions and the principle of least privilege;
- MFA for administrators and, where appropriate, users;
- encrypted connections;

- encryption at rest where supported by the supplier;
- separation of customer environments;
- backups and recovery procedures where part of the service;
- security updates and configuration management;
- periodic review of administrator and support access;
- incident registration and continuity procedures;
- restricted and controlled support access;
- confidentiality arrangements and supplier assessment;
- logging where supported by the selected environment and appropriate to the risk;
- use of a password manager where configured or required by the assignment.

Appendix 2 describes the measures relevant to the Customer in more detail. VIKEN-NTW does not guarantee absolute security, but maintains an appropriate level of protection and improves measures when risks, services or technical possibilities change.

11. Access and support

VIKEN-NTW limits access to employees, contractors or support partners who need access for performance.

Support access may be activated temporarily and, where possible, limited in time, role and purpose. The Customer acknowledges that certain suppliers may themselves have technical access in accordance with their terms and security documentation.

12. Sub-processors

The Customer grants general authorisation for VIKEN-NTW to engage Sub-processors necessary for the assignment.

Depending on the selected services, these may include:

- HighLevel / LeadConnector for websites, hosting, forms, CRM, calendars, communication and automation;
- Microsoft for Microsoft 365, email, identity, documents and cloud storage;
- Google for Google Workspace, documents, email and cloud functionality;
- Cloudflare for DNS, security and network services;
- Openprovider and registries for domain registration and management;
- hosting, WordPress, email, telecom, SMS and video providers;
- Mollie, Stripe, banks and other payment providers for payment functionality;
- Meta / WhatsApp for communication where activated;
- AI, analytics, advertising or support providers only where actually activated for the assignment and appropriately assessed.

A supplier that is not used for the Customer is not an active Sub-processor for that Customer. The current customer-specific list is recorded in Appendix 3 or in an online Sub-processor overview.

VIKEN-NTW imposes appropriate data protection obligations on Sub-processors insofar as VIKEN-NTW has the contractual position to do so.

13. New or changed Sub-processors

VIKEN-NTW informs the Customer of a relevant new or changed Sub-processor by email, customer portal or a durably accessible online overview.

The Customer may raise a reasoned objection within 30 days where the change demonstrably creates an unacceptable privacy or security risk. The parties then seek a reasonable solution. Where no solution is possible, the affected part may be terminated. An objection may not be based solely on preference where the Sub-processor is appropriately protected and necessary for the agreed service.

14. International transfers

Personal data may be processed outside the European Economic Area or accessed from outside the EEA where a valid transfer mechanism exists, such as:

- an adequacy decision;
- applicable Standard Contractual Clauses;
- another legally permitted safeguard or derogation.

Where the risk requires, additional technical or organisational measures are assessed. For Viken Compliant Pro and other high-risk processing, a more extensive transfer assessment may be included in Appendix 4.

The Customer acknowledges that global software suppliers may use multiple processing locations or support regions. VIKEN-NTW does not make any data localisation guarantee that has not been confirmed in writing and technically verified.

15. Data subject requests

Where VIKEN-NTW receives a request relating to data for which the Customer is responsible, VIKEN-NTW forwards the request to the Customer where possible and does not deal with it independently unless legally required.

VIKEN-NTW reasonably assists the Customer with requests for access, rectification, erasure, restriction, portability or objection, taking into account the nature of the processing and available functionality.

Routine assistance within the existing managed environment is included insofar as the package description provides. Extensive exports, recovery work, investigations or custom work may be charged as additional work.

16. DPIA, supervision and compliance

VIKEN-NTW provides reasonable information needed by the Customer for a DPIA, prior consultation or contact with a supervisory authority, insofar as the information relates to VIKEN-NTW's services.

Additional analyses, workshops, documentation or support outside the agreed scope are performed at the applicable rate. For Viken Compliant Pro, more extensive support may form part of the package or assignment.

VIKEN-NTW does not guarantee that the Customer's organisation automatically complies with all legislation, standards or sector requirements by purchasing a package.

17. Security incidents and personal data breaches

Where VIKEN-NTW discovers a security incident likely to affect the Customer's personal data, VIKEN-NTW informs the Customer without unreasonable delay after sufficient information is available to make a meaningful notification. VIKEN-NTW aims to do so no later than 24 hours after sufficient confirmation.

The notification includes, where available:

- the nature of the incident;
- affected systems, data and categories of data subjects;
- likely consequences;
- measures taken or proposed;
- a contact person;
- relevant available logs or timelines.

An initial notification may be incomplete and may be supplemented later. VIKEN-NTW does not notify the Dutch Data Protection Authority or data subjects on behalf of the Customer unless expressly instructed or legally required.

Incident contact: privacy@viken-ntw.com

18. Retention periods

The Customer determines the substantive retention periods for data in its systems unless the functionality or assignment provides otherwise.

As an operational starting policy, VIKEN-NTW may apply:

- active data: for the duration of the services;
- support and project information: for the duration of the relationship and up to 24 months afterwards;
- technical and security logs: generally up to 12 months;
- deleted data in backups: according to the normal cycle, generally within 30 to 90 days;
- data that VIKEN-NTW must independently retain for invoicing, administration, evidence or legal obligations: in accordance with the privacy policy and applicable law.

Customer-specific or stricter periods are recorded in Appendix 1.

19. Return, transfer and deletion

After termination, the Customer will in principle have 30 days to export data or complete a transfer, unless another period has been agreed or immediate restriction is necessary for security, misuse or a legal obligation.

On request and insofar as technically possible:

- data is returned in a commonly available format;
- accounts and management rights are transferred;
- data is deleted or made inaccessible.

After the export period, VIKEN-NTW may delete customer data from active systems or terminate access. Backup copies disappear according to the normal backup cycle. Statutory administration, security evidence and data retained by VIKEN-NTW as an independent Controller fall outside this deletion obligation.

The Customer is responsible for timely download and verification unless VIKEN-NTW has agreed in writing to perform the export or migration.

20. Audits and information

On request, VIKEN-NTW provides reasonable information about compliance and measures, for example relevant certifications, supplier documentation, policy information or answers to a reasonable questionnaire.

The Customer may in principle conduct one audit or additional information request per calendar year. An additional audit is possible after a relevant incident, at the request of a supervisory authority or where there is a concrete indication of serious non-compliance.

An audit:

- is announced at least 30 days in advance, except in demonstrable urgency;
- takes place during normal working hours;
- disrupts services and security as little as possible;
- protects information of other customers and trade secrets;

- is preferably carried out remotely or through documentation first.

The costs of an audit or out-of-scope assistance are borne by the Customer unless the audit confirms a material failure attributable to VIKEN-NTW. In that case, VIKEN-NTW bears the reasonable direct costs insofar as appropriate.

21. Continuity

VIKEN-NTW maintains appropriate continuity and recovery measures within the limits of the package and the suppliers used. The Customer acknowledges that not every service offers the same backup, recovery or availability options.

If a supplier is replaced or becomes unavailable, VIKEN-NTW may deploy a functionally suitable alternative, taking into account privacy, security and the agreed scope.

22. Liability

Liability under this Data Processing Agreement follows the liability arrangement in the main agreement or general terms and conditions.

Nothing in this Agreement limits the rights of data subjects or liability that may not be excluded under mandatory data protection law. The parties cooperate to limit damage and allocate recourse fairly in proportion to each party's responsibility for the infringement or damage.

23. Termination

This Data Processing Agreement ends when VIKEN-NTW no longer processes personal data on behalf of the Customer and the return and deletion obligations have been completed.

Termination of a specific service terminates only the processing relating to that service. The Agreement remains in force for remaining services.

24. Governing law and disputes

This Agreement is governed by Dutch law.

The parties first seek to resolve a dispute by consultation. For business parties, the competent court of the District Court of East Brabant (Rechtbank Oost-Brabant) has jurisdiction, unless mandatory law provides otherwise.

25. Amendments

VIKEN-NTW may amend this model due to legislation, security, suppliers or services. A material amendment affecting an ongoing customer is announced in an appropriate manner. Customer-specific signed arrangements remain in force until amended by the parties.

Appendix 1 - Description of processing

To be completed for each customer:

- Customer name and details;
- relevant assignment, package and duration;
- purposes and nature of processing;
- systems and modules;
- categories of data subjects;
- categories of personal data;
- special categories of personal data, where permitted;
- retention periods;
- contact persons and instruction route;
- arrangements for export, deletion and assistance.

Appendix 2 - Technical and organisational measures

To be selected and completed for each customer:

- identity, accounts and MFA;
- roles and permissions;
- encryption and connections;
- logging and monitoring where configured;
- backup and recovery;
- update and configuration management;
- incident management;
- support access;
- separation of environments;
- continuity;
- additional Compliant Pro measures.

Appendix 3 - Sub-processors

To be included for each customer:

- supplier and legal entity;
- service and purpose;
- categories of data;
- processing locations or relevant region;
- transfer mechanism where applicable;
- date of addition or change.

Appendix 4 - International transfers and additional conditions

Where relevant, include:

- countries and recipient suppliers;
- adequacy decision, SCCs or other mechanism;
- transfer impact assessment or risk assessment;
- additional technical and organisational measures;
- sector-specific or contractual restrictions.

Signature or digital acceptance

This model agreement becomes part of the assignment by signature, digital acceptance or reference in the quotation or order confirmation.

Customer:

Organisation name: _____

Name of authorised representative: _____

Date: _____

Signature / digital acceptance: _____

VIKEN-NTW / Viken-WHB:

Name: Kevin Willem Joannes Antonius Winkel

Date: _____

Signature / digital acceptance: _____

—