

VIKEN-NTW - Privacy Policy

Version 1.0 - launch version

Last updated: 24 July 2026

1. Who is responsible?

Viken-WHB, trading under the trade name VIKEN-NTW, is responsible for the processing of personal data as described in this privacy policy.

Legal name: Viken-WHB

Trade name: VIKEN-NTW

Legal form: sole proprietorship

Chamber of Commerce registration number: 81074662

VAT identification number: NL031379138B01

Address: Vogelwikke 11, 6026 AK Maarheeze, the Netherlands

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

Email: contact@viken-ntw.com

Privacy contact: privacy@viken-ntw.com

VIKEN-NTW has not appointed a Data Protection Officer.

This privacy policy is primarily intended for business customers, entrepreneurs, practices, associations and non-profit organisations in the Netherlands and, where appropriate, within the European Economic Area. VIKEN-NTW uses viken-ntw.com as its primary domain. Local domains and spelling variants, including .nl and domains without a hyphen, may be used as aliases or redirects.

2. When do we process personal data?

We process personal data when someone:

- visits our website;
- submits an early access application, contact form, quiz, scan or intake form;
- contacts us by telephone, email, WhatsApp or another channel;
- requests a quotation or enters into an agreement with us;
- uses our services, support, hosting, management or automation environment;
- optionally gives consent for newsletters, analytics or marketing.

3. What personal data do we process?

Depending on the situation, we may process, among other things:

- name, company name, job title, address, email address and telephone number;
- preferred method of contact;
- information about the requested service, route, planning and support request;
- correspondence, quotations, agreements, invoices and payment details;

- domain, DNS, hosting, email and cloud configurations;
- account names, user roles, permissions, security settings and technical configurations;
- data from forms, calendars, CRM systems, customer portals and automations;
- technical data, such as IP address, browser information, date and time of submission, and system and security logs insofar as the systems used record these;
- data required for migration, support, recovery, troubleshooting or security investigations.

The early access form may record name, business email address, organisation, relevant route, support request, preferred start period, optional telephone number, contact preference, source information, date and time, technical log data and acceptance of the privacy policy.

We do not ask for passwords, login codes, medical information or confidential customer or client data through public forms. Only share such information through an explicitly agreed secure route.

Special categories of personal data, including health data, are not processed as standard. This only takes place within a separately agreed project where the processing is necessary, legally permitted and technically appropriately configured.

4. What do we use personal data for?

We use personal data for:

- assessing and following up early access and contact requests;
- carrying out an intake, scan or advisory engagement;
- preparing quotations, agreements and assignments;
- providing, managing, securing and supporting services;
- configuring domains, DNS, email, cloud, website foundations, forms, calendars, CRM, customer communications and automations;
- invoicing, payment processing and administration;
- preventing and investigating misuse, fraud and security incidents;
- complying with legal obligations and establishing, exercising or defending rights or claims;
- analytics of our own website, conversion measurement and marketing, but only where permitted and, where required, after consent has been given;
- newsletters or commercial updates, only after separate consent.

An early access application does not automatically result in subscription to a newsletter.

5. On what legal bases do we process data?

Depending on the processing, we rely on:

- taking steps prior to entering into a contract or performance of a contract;
- a legal obligation;
- legitimate interests, for example for business communications, security, fraud prevention, administration or improvement of our services;

- consent, for example for non-essential cookies or marketing emails.

Consent can be withdrawn at any time. Withdrawal does not have retroactive effect.

6. From whom do we receive data?

We receive data directly from the data subject, from the business customer or organisation for which we work, from systems managed by the customer, from suppliers required for the services, or from public business sources where this is reasonably necessary for contact or performance.

7. With whom do we share personal data?

We do not sell personal data and do not share personal data or tracking data with third parties for their own commercial marketing purposes.

We may share data with suppliers insofar as this is necessary for the services. Depending on the selected service, this may include:

- HighLevel / LeadConnector for websites, forms, CRM, calendars, automation, communication and hosting;
- Microsoft and Google for business email, documents and cloud environments;
- Cloudflare and Openprovider for DNS, security and domain management;
- hosting, email, WordPress, video and support providers where these are used for the assignment;
- Mollie, Stripe and banks for payments and financial administration;
- Meta / WhatsApp and other communication providers where these functions are activated;
- analytics, advertising or AI providers only where these are actually activated and used on an appropriate legal basis;
- professional advisers, supervisory authorities or public authorities where legally required.

For the first early access form, HighLevel / LeadConnector is used. The form may temporarily be processed within an existing HighLevel environment managed by Viken-WHB. The application is functionally separated within that environment and internally forwarded for personal follow-up from VIKEN-NTW. This temporary route does not send automatic marketing emails under another brand to the applicant.

Where a supplier processes personal data on our behalf, we enter into appropriate data processing arrangements where required. Some suppliers determine the purposes and means of processing themselves for certain activities and may therefore act as independent controllers.

8. International processing

Some suppliers may process personal data outside the European Economic Area or access it from another country. We use such suppliers only where a valid legal basis for the transfer

exists, for example an adequacy decision, applicable Standard Contractual Clauses or another permitted transfer mechanism. Where appropriate, we assess additional technical and organisational measures.

For Compliant Pro and other assignments involving increased privacy or security risks, a more extensive assessment of international transfers may form part of the assignment.

9. How long do we retain data?

We do not retain personal data for longer than necessary. As a starting policy, unless another period is necessary or agreed, we apply:

- early access or contact request without a customer relationship: up to 12 months after the last substantive contact;
- rejected or unsuitable application: up to 6 months after closure;
- quotation data without an agreement: up to 12 months after expiry or last contact;
- operational customer and project data: for the duration of the customer relationship and in principle up to 24 months afterwards, unless transfer, security, evidence or a longer statutory retention period requires otherwise;
- support communications: for the duration of the customer relationship and up to 24 months afterwards;
- technical and security logs: generally up to 12 months, unless an incident, supplier, legal obligation or security interest requires another period;
- deleted data in backups: according to the normal backup cycle of the relevant supplier, generally within 30 to 90 days;
- invoices and tax administration: at least 7 years, or longer where a specific statutory retention obligation applies;
- consent, withdrawal and objection records: up to 5 years after the record is no longer actively required, insofar as necessary to demonstrate compliance.

We may retain data for longer where this is necessary for ongoing litigation, a legal obligation, a security investigation or the establishment, exercise or defence of a legal right.

10. How do we protect personal data?

We take appropriate technical and organisational measures depending on the service and the risk. These may include:

- unique accounts, roles and restricted access rights;
- MFA for administrators and, where appropriate, users;
- encrypted connections and encryption at rest where supported by the supplier;
- separation of customer environments;
- backups and recovery procedures where these form part of the service;
- security updates, periodic access reviews and incident registration;
- restricted and controlled support access;
- confidentiality arrangements and supplier assessments.

No technical environment is completely risk-free. We therefore cannot guarantee absolute security, but we act with due care and take measures appropriate to the nature of the processing.

11. Automated decision-making

We do not make decisions based solely on automated processing that produce legal effects for an individual or similarly significantly affect an individual.

12. Rights of data subjects

Depending on the situation, an individual may request:

- access;
- rectification;
- erasure;
- restriction of processing;
- data portability;
- objection;
- withdrawal of consent.

Send a request to privacy@viken-ntw.com. We may request additional information to verify the identity of the requester. We respond within the statutory period.

A data subject may also lodge a complaint with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

13. Cookies and similar technologies

More information is available in our Cookie Policy. Non-essential cookies and similar technologies are only used after consent has been given where required.

14. Changes

We may amend this privacy policy when our services, suppliers or legal obligations change. The most recent version is available at <https://viken-ntw.com>.

15. Contact

VIKEN-NTW / Viken-WHB
Vogelwikke 11
6026 AK Maarheeze
the Netherlands
Email: contact@viken-ntw.com

Privacy: privacy@viken-ntw.com

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