PRIVACY STATEMENT

Last updated: 10 November 2026 • version 2.3

1. Who we are

H3 Company B.V. (“H3”, “we”) is a limited liability company based in Amsterdam, the Netherlands (KvK 97964468). We advise organisations on AI adoption, process redesign and new business models, and deliver programmes and hands-on enablement. H3 Company B.V. is the controller for the personal data described in this statement, except for assessments as described in the next paragraph.
When we run an assessment such as Coherence Compass for an organisation, that organisation is the controller and we process the answers on its behalf under a data processing agreement. Recordings and transcripts of conversations and working sessions are not covered by that agreement: we make them as controller, also within an assignment (see sections 3 and 4). The notice shown at the start of the assessment says who is responsible, what we keep and for how long.
For Coherence Compass, the answers are stored with Supabase in Stockholm, Sweden, and the names and email addresses of participants with Upstash in London, United Kingdom. Invitations are sent by email through Resend from Ireland. The Coherence Compass app runs on Vercel in Frankfurt, Germany. We analyse the answers with AI through our business account with Anthropic (Claude Team). We keep Coherence Compass data for 24 months, including the link between your name and your answers, so that a later remeasurement can be compared with your own earlier answers. Your organisation can ask us to keep it for a shorter period.
Questions about how we handle your data? Email hello@h3.company. We aim to respond within five business days.

2. What data we collect and where it comes from

We collect personal data from several sources:

- Directly from you: when you contact us, book a conversation, complete the AI Horizon Scan, subscribe to Field Notes, sign a proposal or take part in a session or programme.
- Your employer or client organisation: when we receive participant lists for a programme, workshop or engagement.

- Publicly available professional sources: LinkedIn profiles and company websites, used for business-to-business contact with decision-makers.
- Meeting tools: we record and transcribe calls and video calls with us by default, with notice in advance. Any participant may object before, during or after the conversation; H3 will not record, or will stop recording, and will delete the recording and the transcript from its active systems within ten working days; copies in backups and version history are no longer used and disappear in accordance with their retention period (see section 3).
- Our website: statistics and marketing cookies when you visit h3.company and accept them via our cookie banner (see section 9).

The categories of data we typically process are: name, job title, employer, business email address, phone number, your AI Horizon Scan answers and result, and meeting or project content. We do not process special category data (such as health, religion or biometric data) in the normal course of our work, and our services are aimed at organisations, not at children.

Providing your data is voluntary. Without contact details we cannot answer a request, book a conversation or send you your AI Horizon Scan result; nothing else depends on it. Where we obtain your data from a public source or from your employer rather than from you, we tell you at our first contact with you (with a link to this statement), and in any case within one month.

3. Why we process your data and on what legal basis

Purpose	Legal basis (GDPR)	What this covers
Responding to your request	Art. 6.1.b, steps at your request, and Art. 6.1.f, our interest in answering enquiries	Contact form (including how you found us and the campaign link you arrived from), booking a conversation, sending your AI Horizon Scan result
Contract execution and delivery	Art. 6.1.b, performance of a contract	Client communication, programme and workshop delivery, project files, invoicing
Tax and financial obligations	Art. 6.1.c, legal obligation	Retention of financial records and invoices for 7 years under Dutch tax law

Field Notes newsletter	Art. 6.1.a, consent	Sending Field Notes to the address you subscribed with; unsubscribe at any time
Business-to-business contact	Art. 6.1.f, legitimate interest: our commercial interest in reaching decision-makers at organisations we can help	Contacting people based on publicly available professional profiles; weighed against your interests, and you can object at any time
AI-assisted service delivery	Art. 6.1.f, legitimate interest: delivering efficiently and keeping accurate engagement records	Use of AI tools for preparation, note-taking and internal workflows; no automated decisions are made
Meeting recording and transcription (by default)	Art. 6.1.f, legitimate interest: capturing agreements and action points accurately	Recordings and transcripts (with AI support) of calls and video calls with clients and business contacts, see the paragraph below this table
Recruitment	Art. 6.1.b, steps at your request before entering into a contract, and/or Art. 6.1.f, legitimate interest: a careful selection	Applications, interviews and their assessment. AI support (via Cloudflare, see section 5) helps prepare an assessment of job interviews; a person always makes the decision
Notes on the people we work with	Art. 6.1.f, legitimate interest: preparing well and following up accurately	Notes on contacts at our clients and prospects, see the paragraph below this table
Basic site statistics (no cookies)	Art. 6.1.f, legitimate interest: understanding aggregate site usage	Vercel Web Analytics: aggregated page views and referrers; nothing is stored on your device and you are not identified
Website statistics	Art. 6.1.a, consent via cookie banner	Google Analytics 4 and PostHog (product analytics). Neither is loaded until you accept statistics cookies; before that, no data about your visit is sent to Google or PostHog
Website marketing and retargeting	Art. 6.1.a, consent via cookie banner	LinkedIn Insight Tag and Meta Pixel; not loaded until you accept marketing cookies. For this collection we and LinkedIn and Meta are joint controllers, see section 5
Legal compliance	Art. 6.1.c, legal obligation	Responding to requests from the Dutch Data Protection Authority (AP) or court orders

Recording meetings. To capture agreements and action points accurately, we record and transcribe (with AI support) calls, video calls and working sessions with clients and business contacts by default (see also Article 5.7 of the general terms). We do this as

controller, also within an assignment for a client. The legal basis is our legitimate interest (Art. 6.1.f GDPR). We announce this in the invitation H3 sends and always at the start of the conversation. Any participant may object before, during or after the conversation; H3 will not record, or will stop recording, and will delete the recording and the transcript from its active systems within ten working days; copies in backups and version history are no longer used and disappear in accordance with their retention period. How long we keep recordings, transcripts and minutes is set out in section 4.

Notes on the people we work with. To work well with the people at our clients and prospects, we keep notes on your role, what you told us, the positions you took in our meetings and what matters to you in the work. AI tools help us summarise these notes. We limit them to what was said or done, citing the source. We do not score people or record anything about health, private life or beliefs. You can ask to see these notes and object to them at hello@h3.company.

4. How long we keep your data

Category	Retention period	Basis
Contact and booking information	12 months after the last meaningful contact	Legitimate interest; follow-up
AI Horizon Scan answers and result	12 months after you receive your result	Delivering and following up on your result
Field Notes subscription	Until you unsubscribe	Consent; we keep the minimum needed to honour an unsubscribe
Financial records and invoices	7 years	Dutch tax law (Belastingdienst)
Client communications and project files	2 years after the end of an engagement	Legitimate interest; business continuity

Meeting recordings, transcripts and minutes	2 years after the end of the engagement (same as project files); without an engagement, 2 years after the last contact (same as prospect records); earlier on request; then deleted or anonymised in the active systems; copies in backups expire	Legitimate interest; engagement record
Prospect records that did not become clients	2 years after last contact	Legitimate interest; deleted on expiry or on request
Applications, interview notes and assessments in recruitment	4 weeks after the procedure ends, or 1 year with your written consent	Guidance of the Dutch Data Protection Authority; the longer period only with consent
Website statistics (GA4)	14 months	Consent; GA4 data-retention setting
Website product analytics (PostHog)	12 months	Consent; PostHog data-retention setting
Session recordings (PostHog)	30 days	Consent; PostHog recording-retention setting
Coherence Compass answers, and participant names and email addresses	24 months, including the link between name and answers for a later remeasurement, unless your organisation asks for a shorter period	Data processing agreement with your organisation
Marketing cookies (LinkedIn, Meta)	See the cookie table in section 9	Consent; per-provider cookie lifetime

After the applicable period, data is deleted or anonymised. You may request earlier deletion (see section 8).

5. Who we share your data with

Service providers acting on our behalf (processors). These services process personal data only on our instructions. The table lists each one, its location and the safeguard that protects transfers outside the European Economic Area.

Service	Purpose	Company based in	Where the data is stored	Legal safeguard
Vercel	Website hosting, server-side form handling, cookieless site statistics; hosting the Coherence Compass app and the client portal	US (Vercel Inc.)	Website and forms: US. Coherence Compass app and client portal: Frankfurt, Germany	Vercel DPA, SCC and EU-US Data Privacy Framework (DPF)
Resend	Delivering site messages, AI Horizon Scan results and Coherence Compass invitations by email	US (Plus Five Five, Inc.)	US; sending via Ireland	Resend DPA, SCC and DPF
Supabase	Storing Coherence Compass answers	Singapore (Supabase Pte. Ltd.)	Stockholm, Sweden (EU); support and administration from Singapore and the US	Supabase DPA with SCCs
Upstash	Storing the names and email addresses of Coherence Compass participants	US (Upstash, Inc.)	London, United Kingdom; support and administration from the US	EU adequacy decision for the United Kingdom (valid until 27 December 2031); Upstash DPA with DPF and SCCs
Google Workspace	Email, calendar, video calls and files	Ireland (Google Cloud EMEA Limited)	Worldwide in Google's data centres, including the EEA and the US	Cloud Data Processing Addendum, SCC and DPF

Google Analytics 4	Website statistics; loaded only after you accept statistics cookies	US	US	Google Ads Data Processing Terms, DPF
PostHog	Website product analytics and session recordings with form input masked (how visitors use the site); loaded only after you accept statistics cookies	US (PostHog, Inc.)	US	PostHog DPA, SCC and DPF
Anthropic (Claude)	AI assistance for preparation, notes and internal workflows, and analysing Coherence Compass answers	US; our contracting party is Anthropic Ireland, Limited	US	Business account (Claude Team): Data Processing Agreement with SCCs; no model training on our data
Fireflies.ai	Recording, transcribing and summarising meetings (by default, with notice in advance; see section 3)	US (Fireflies AI Corp)	US	Fireflies DPA, SCC and DPF
Granola	Recording, transcribing and summarising meetings (by default, with notice in advance; see section 3)	US	US	Granola DPA with standard contractual clauses
Unipile	Connecting our mailbox, LinkedIn and WhatsApp to our AI assistant	France (Unipile SAS)	France; optional proxies outside the EEA (US, Singapore, Israel)	Unipile DPA; SCC for proxies outside the EEA
Composio	Connecting our AI assistant to email, calendar, documents and CRM	US (Composio, Inc.)	US	Composio DPA and SCC
Attio	Relationship management (CRM)	UK (Attio Ltd)	Google Cloud, region not public; sub-processors in the US	Attio DPA with SCC and the UK addendum

n8n	Calendar connection that adds the recording service to meetings	Germany (n8n GmbH)	EU (Microsoft Azure); support also from the US and the UK	n8n DPA with SCC
Cal.com	Scheduling when you book a conversation	US (Cal.com, Inc.)	US	Cal.com DPA, DPF
Notion	Internal knowledge base and team workspace	US (Notion Labs, Inc.)	US	Notion DPA, DPF
Slack	Internal messages	US (Salesforce)	US	Slack DPA, DPF
GitHub	Storage of our documents and reports	US (GitHub, Inc.)	US	GitHub DPA, SCC and DPF
Cloudflare	Domain management; AI support in assessing job interviews	US (Cloudflare, Inc.)	Global network, including the EEA and the US	Cloudflare DPA, SCC and DPF

A complete list of our service providers and sub-processors, including those we use for client work, is at h3.company/legal.

Advertising platforms (joint controllers). If you accept marketing cookies, **LinkedIn** (Insight Tag) and **Meta** (Meta Pixel) collect data about your visit for retargeting and campaign measurement. For that collection on our site we are joint controllers with them; they then process the data under their own responsibility and privacy policies: LinkedIn, Meta. Both are US companies relying on SCCs and the EU-US Data Privacy Framework. You can withdraw at any time via the cookie banner, and you can also exercise your rights with them directly.

Other recipients. Where necessary we share limited data with our accountant and bookkeeping software, our bank and payment providers, legal advisers, and public authorities (such as the Belastingdienst or the Autoriteit Persoonsgegevens) when the law requires it.

We do not sell your personal data. We do not share your data with other organisations for their own marketing purposes. If we are required by law to disclose data to a public authority, we do so only to the extent legally required.

6. International data transfers

Several of the services above are based in, or route data through, the United States. Where this is the case we rely on the European Commission's Standard Contractual Clauses (SCCs), the EU adequacy decision for the United Kingdom (for Upstash) and, where the provider is certified, the EU-US Data Privacy Framework (DPF) as the legal mechanism for the transfer. The AI services we use for client work run on business terms with a data processing agreement and do not use your data to train their models. Providers may keep limited data for security and abuse monitoring under their own terms. Data may be processed in the US. You can request a copy of the safeguards we rely on (the SCCs) by emailing hello@h3.company.

7. Automated decision-making and AI tools

We use AI tools (including Claude by Anthropic) to assist with preparation, note summarisation and internal workflow tasks, and to analyse Coherence Compass answers for the organisation that commissioned the assessment. For client work we use business AI accounts only. No automated decisions are made that produce legal or similarly significant effects on individuals. A person at H3 reviews AI-generated output before it is used in client-facing work.

The AI Horizon Scan generates a result from the answers you give. That result is informational: it is not a decision about you and has no legal or similarly significant effect.

We make no automated decisions about individuals, including on creditworthiness or employment suitability. In recruitment, AI helps prepare an assessment of job interviews; a person at H3 always makes the decision (see section 3).

If you prefer that we do not use AI tools on your messages or meeting notes, tell us at hello@h3.company and we will handle them without AI, unless the law requires otherwise. For meetings, this means: H3 will not record, or will stop recording, and will delete the recording and the transcript from its active systems within ten working days; copies in backups and version history are no longer used and disappear in accordance with their retention period (see section 3).

8. Your rights

Under the GDPR you have the following rights regarding your personal data:

- Access: request a copy of the data we hold about you.

- Rectification: ask us to correct inaccurate data.
- Erasure: ask us to delete your data where we have no overriding legal obligation to keep it.
- Restriction: ask us to limit how we use your data while a dispute is resolved.
- Data portability: receive your data in a structured, machine-readable format.
- Objection: object to processing based on legitimate interest. We will stop unless we can demonstrate compelling legitimate grounds that override your interests. If you object to direct marketing, we always stop.
- Withdraw consent: where processing is based on consent (newsletter, cookies), withdraw it at any time. Withdrawal does not affect the lawfulness of processing before withdrawal.

How to exercise your rights: email hello@h3.company with a clear description of your request. We respond within one month. For complex requests we may extend this by a further two months and will tell you within the first month if so. We do not charge a fee. If you are not satisfied with our response, you can lodge a complaint with the Dutch Data Protection Authority: autoriteitpersoonsgegevens.nl.

9. Cookies

Our website uses cookies and similar technologies in three categories that you choose via our cookie banner, plus one cookieless measurement that does not depend on your choice (listed below). You can change your cookie preferences at any time: the “Cookies” button in the bottom-left corner of every page reopens the banner, and withdrawing is as easy as accepting.

- Necessary (no consent required): strictly needed for the site to work, including remembering your cookie choice.
- Statistics (consent required): Google Analytics 4 and PostHog (product analytics), to understand how visitors use and move through the site. Neither is loaded until you accept statistics: before that, nothing is sent to Google or PostHog and nothing of theirs is stored on your device. Once loaded, both set an identifier that recognises your browser on a later visit. PostHog runs in the United States. With statistics consent, PostHog also makes session recordings: how a page is scrolled and clicked, so we can see where the site is unclear. Everything you type into a form is masked and never recorded. Recordings are kept for 30 days. Withdrawing removes the Google Analytics and PostHog cookies we set and reloads the page, after which neither is loaded.

- Marketing (consent required): the LinkedIn Insight Tag and Meta Pixel, used to show relevant content to people who visited h3.company and to measure campaigns. Neither is loaded until you accept marketing. For this collection we and LinkedIn and Meta are joint controllers, see section 5. Withdrawing removes the Meta cookies we set and reloads the page, after which neither is loaded; cookies that LinkedIn sets on its own domain are managed through your LinkedIn account settings.
- Site statistics without cookies (no consent required, legitimate interest, see section 3): Vercel Web Analytics counts aggregated page views and referrers. It sets no cookie and stores nothing on your device, and it does not identify you.

Cookie	Provider	Category	Purpose	Lifetime
h3-consent.* (currently v1)	H3 (local storage)	Necessary	Remembers your cookie choice	12 months, or until you clear it or change your choice
None (no cookie)	Vercel Web Analytics	Site statistics	Aggregated page views and referrers; nothing stored on your device	n/a
_ga, _ga_*	Google Analytics	Statistics	Distinguishes visitors and sessions	Up to 2 years
ph_*_posthog (cookie and local storage)	PostHog	Statistics	Distinguishes visitors and sessions (product analytics)	Up to 12 months
li_sugr, lidc, bcookie, li_gc, UserMatchHistory, AnalyticsSyncHistory, ln_or	LinkedIn	Marketing	Retargeting and ad measurement	1 day to 1 year
_fbp, _fbc	Meta	Marketing	Retargeting and ad measurement	90 days

10. Security

We take appropriate technical and organisational measures to protect your personal data against loss, unauthorised access or disclosure, including access controls, two-factor

authentication on key systems, and encryption in transit and at rest where supported by our providers.
In the event of a personal data breach that poses a risk to your rights and freedoms, we notify the Dutch Data Protection Authority within 72 hours and inform affected individuals without undue delay.

11. Changes to this statement

We may update this statement as our services or legal obligations change. The date at the top reflects the most recent version. For material changes affecting existing clients, we notify you directly.
This statement is also available in Dutch. Both versions say the same; should they differ, the version most favourable to you applies.

12. Contact

Controller: H3 Company B.V. • KvK: 97964468
Address: Jacob Bontiusplaats 9, 1018 LL Amsterdam, the Netherlands
Email: hello@h3.company • Website: h3.company