

Privacy Notice

Westbase B.V. — Last updated 22 April 2026

1. About this notice

Westbase B.V. (“Westbase”, “we”, “us”, “our”) respects your privacy. This privacy notice explains how we collect, use, and protect personal data when you interact with us as a customer, supplier, prospect, website visitor, applicant, or other contact.

Westbase B.V. is the data controller responsible for your personal data, registered at Zuiderloswal 15, 1216 CJ Hilversum, the Netherlands (KvK 75238969). We are part of the Westbase Group, which also includes Westbase Group Limited, Westbase Technology Limited, Control Ltd, MS (Distribution) UK Ltd, Wireless Coverage Ltd.

We process personal data in accordance with the EU General Data Protection Regulation (Regulation (EU) 2016/679, the “GDPR”) and the Dutch GDPR Implementation Act (Uitvoeringswet AVG).

2. Categories of personal data we collect

Depending on your relationship with us, we may collect the following categories of personal data:

- Identification and contact data (name, job title, employer, business email, business phone, postal address).
- Transaction and account data (orders, quotes, deliveries, invoices, payments, support tickets).
- Marketing and communications data (subscription preferences, event attendance, content downloads).
- Technical data (IP address, device and browser information, cookie identifiers, website usage).
- Recruitment data (CV, references, work eligibility, interview notes).
- Premises data (visitor sign-in, CCTV imagery).

We do not routinely collect special category personal data. Where we do (for example, accessibility requirements for an event), we do so on the basis of explicit consent or another lawful basis under Article 9 GDPR.

3. How we use your personal data

The table below sets out the categories of data subjects we deal with, the purposes for which we use their personal data, the lawful basis under Article 6 GDPR, and the retention period.

Who	Purpose & lawful basis	Retention
Customers and prospective customers	<p>Account management, order processing, delivery, invoicing, customer support, and direct marketing of related products/services.</p> <p>Lawful basis: performance of contract; legitimate interests (running our business and direct B2B marketing); consent (where required for electronic marketing).</p>	<p>Duration of the relationship plus 7 years (Dutch tax retention period under article 52 AWR).</p>
Suppliers and business partners	<p>Procurement, contract administration, payments, due diligence, and ongoing relationship management.</p> <p>Lawful basis: performance of contract; legitimate interests (running our business, vendor risk management).</p>	<p>Duration of the relationship plus 7 years.</p>
Website visitors	<p>Operating the website, security, analytics, and (with consent) marketing communications.</p> <p>Lawful basis: legitimate interests (security and analytics in aggregated form); consent (non-essential cookies and marketing).</p>	<p>Cookie data: per cookie notice (max 12 months for analytics; session for essential). Enquiry data: 24 months from last contact.</p>
Marketing recipients	<p>Sending newsletters, product updates, event invitations, and promotional content.</p> <p>Lawful basis: legitimate interests (B2B soft opt-in for existing customers); consent (all other recipients).</p>	<p>Until you unsubscribe, plus a suppression record retained indefinitely to honour your opt-out.</p>
Job applicants	<p>Recruitment, assessment, interview scheduling, and (if successful) onboarding.</p> <p>Lawful basis: steps prior to entering a contract; legitimate interests; consent (where applicable for talent pool retention).</p>	<p>Unsuccessful applicants: 6 months after the recruitment decision (or up to 24 months with consent for our talent pool).</p>
Employees and workers	<p>HR administration, payroll, benefits, performance management, statutory reporting.</p> <p>Lawful basis: performance of contract; legal obligation; legitimate interests.</p>	<p>Per our Employee Privacy Notice and statutory retention periods (typically 7 years post-employment for tax/payroll records).</p>
Visitors to our premises	<p>Site access, health and safety, and security (including CCTV).</p> <p>Lawful basis: legitimate interests (security of premises and personnel); legal obligation.</p>	<p>Sign-in records: 30 days. CCTV footage: 28 days unless required for an incident investigation.</p>
Professional advisers and authorities	<p>Engaging legal, audit, tax, and regulatory advisers; responding to lawful requests from authorities.</p> <p>Lawful basis: legitimate interests; legal obligation.</p>	<p>Duration of the engagement plus statutory retention periods.</p>

4. Sources of personal data

We collect personal data directly from you (for example when you complete a form, place an order, or apply for a role), from your employer or organisation (for example when you are named as a contact on a contract or purchase order), from publicly available sources (for example company websites, professional networks, and trade registers), and from third-party providers (for example credit reference agencies, recruitment platforms, and marketing data partners).

5. Recipients and disclosures

We share personal data with the following categories of recipients:

- Other Westbase Group entities, for centralised operations, customer support, and marketing.
- Service providers acting on our behalf as processors, including IT and hosting providers, CRM and ERP providers, payment and accounting providers, logistics and delivery partners, marketing agencies, and professional advisers.
- Manufacturers and distributors whose products we resell, where this is necessary to fulfil orders or honour warranties.
- Public authorities and regulators where required by law (including the Belastingdienst and law enforcement).
- Acquirers or successors in the event of a merger, acquisition, or business reorganisation.

We do not sell personal data.

6. International transfers

Where we transfer personal data outside the European Economic Area (for example to group entities in the United Kingdom or the United States, or to service providers based outside the EEA), we rely on one of the following safeguards:

- An adequacy decision adopted by the European Commission (for example the UK adequacy decision).
- Standard Contractual Clauses (Module 1, 2, or 3 as applicable) supplemented, where required, by additional technical and organisational measures following a transfer impact assessment.
- Certification under an approved transfer mechanism (for example the EU–US Data Privacy Framework where the importer is certified).

You may request a copy of the relevant transfer safeguard by contacting us at the address in section 12.

7. Retention

We retain personal data for the periods set out in the table in section 3, or for longer where required by law (for example the seven-year fiscal retention period under article 52 of the Algemene wet inzake rijksbelastingen) or to establish, exercise, or defend legal claims. When data is no longer required, we securely delete or anonymise it.

8. Security

We have implemented appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, or unauthorised disclosure or access. These include access controls, encryption in transit and (where appropriate) at rest, supplier due diligence, and security awareness training. We will notify you and the Autoriteit Persoonsgegevens of any personal data breach where required by Articles 33 and 34 GDPR.

9. Your rights

Subject to the conditions set out in the GDPR, you have the right to:

- Access the personal data we hold about you (Article 15).
- Have inaccurate or incomplete data corrected (Article 16).
- Have data erased in certain circumstances (Article 17).
- Request restriction of processing (Article 18).
- Receive your data in a portable format (Article 20).
- Object to processing based on legitimate interests or for direct marketing (Article 21).
- Withdraw consent at any time, where processing is based on consent (Article 7(3)). Withdrawal does not affect the lawfulness of processing carried out before withdrawal.
- Not be subject to a decision based solely on automated processing that produces legal effects (Article 22). We do not currently carry out such automated decision-making.

To exercise your rights, contact us at the address in section 12. We will respond within one month, extendable by two further months for complex requests in accordance with Article 12(3).

10. Cookies and similar technologies

Our website uses essential cookies to operate, and (with your consent) analytics and marketing cookies. You can manage your preferences via the cookie banner or your browser settings. For details, see our cookie notice.

11. Complaints and supervisory authority

If you have a concern about how we handle your personal data, please contact us first using the details in section 12 so we can try to resolve it. You also have the right to lodge a complaint with the Dutch Data Protection Authority:

Autoriteit Persoonsgegevens

PO Box 93374, 2509 AJ Den Haag, the Netherlands

Telephone: +31 (0)70 888 8500

<https://autoriteitpersoonsgegevens.nl>

12. Contact

Questions about this notice or requests to exercise your rights should be sent to:

Westbase B.V. — Privacy

Zuiderloswal 15, 1216 CJ Hilversum, the Netherlands

gdpr@westbase.io

13. Changes to this notice

We may update this notice from time to time. The current version is always available at eu.westbase.io/privacy-policy. We will notify you of material changes where required by law.