



VISTA WEB LTD.

Privacy Policy

Version 3.0

Vista Web Ltd.

vistaweb.ltd & vistawebdesigns.co.uk



Table of Contents

- 1. Who We Are** Page 2
- 2. Controller and Processor** Page 3
- 3. Personal Information We Collect as Controller** Page 3-4
- 4. How We Use Information and Our Lawful Bases** Pages 4-6
- 5. Direct Marketing** Page 5
- 6. Where We Get Personal Information From** Page 7
- 7. Cookies and Similar Technologies** Page 7
- 8. Who We Share Information With** Pages 7-8
- 9. International Transfers** Pages 8-9
- 10. How Long We Keep Information** Pages 9-10
- 11. Security** Page 10
- 12. Your Data Protection Rights** Pages 10-11
- 13. How to Complain** Page 12
- 14. Processing We Do as Processor** Pages 12-13
- 15. Contact Us** Page 13
- 16. Changes to this Privacy Policy** Pages 5-6
- 17. Governing Law** Pages 5-6

This Privacy Policy is a public notice. It is not a consumer contract. Paid services are governed by the Master Services Agreement, the relevant service schedule and, where we process personal data on a client's behalf, the Data Processing Agreement.



Introduction

This Privacy Policy explains how Vista Web Ltd ("Vista Web", "we", "us", "our") collects, uses and looks after personal information.

It applies to:

- our public websites at vistawebdesigns.co.uk and vistaweb.ltd (together, the "Website");
- enquiries, proposals and business development;
- our contracts with business customers; and
- our own administration of those relationships, including billing, support metadata and access to our client portal.

Our websites and services are offered to businesses. They are not intended for personal or household use.

Use of the Website is also governed by our Website Terms of Use. Paid services are governed by our Master Services Agreement ("MSA"), the relevant service schedule or statement of work, and, where we process personal data on a client's behalf, our Data Processing Agreement ("DPA").

1. Who We Are

Vista Web Ltd is a company registered in England and Wales.

- Registered office: 3 Castlegate, Grantham, Lincolnshire, United Kingdom, NG31 6SF
- Company number: 15191885
- ICO number: ZB697434
- Privacy contact email: GDPR@vistaweb.ltd
- General contact email: contact@vistaweb.ltd
- Phone number: +44 1522 440425

We have not appointed a Data Protection Officer. Article 37 of the UK GDPR does not currently require us to do so. We will reassess that if the nature of our processing changes.

We are established in the United Kingdom. We do not appoint an Article 27 representative outside the UK.



2. Controller and Processor – read this first

We act in two different roles. The difference matters for your rights and for whose privacy notice applies.

When we are the controller

We decide the purposes and means of processing. That is the position for our own Website, sales pipeline, contracts, invoices, our record of who asked us to do what, staff and supplier files, and marketing to business contacts. Client and prospect records for those purposes are held in Twenty CRM, which we host ourselves. This Privacy Policy is the notice for that processing.

When we are the processor

If a business customer ("Client") has engaged us under the MSA and a service schedule, we process personal data that sits in that Client's systems or content on the Client's documented instructions and under the DPA. Typical examples are:

- content, accounts, logs and form submissions on a site we host;
- registrant and DNS data we handle so that a domain can be registered or renewed (the Client remains the registrant);
- mailbox content and metadata on an email platform we manage (currently Proton Mail for that service);
- analytics and search data we access to perform search-engine optimisation;
- materials a Client supplies during a website design and build; and
- files or messages a Client places in the client portal.

For that processing, the Client is the controller. The Client's own privacy notice applies to the people whose data is in those systems. We do not use that data for our own marketing. If you are a visitor, customer or staff member of one of our Clients, please contact that Client. If such a request reaches us, we will pass it to the Client and will not respond substantively except on the Client's instructions or as UK law requires.

The client portal is an access channel for the relationship. It is not itself a hosting, email, domain, SEO or website-build service. Processing in the portal follows the same split: we are controller of account and access records we need to run the portal; we are processor of Client personal data that a Client chooses to put there.

3. Personal Information We Collect as Controller

We may collect the following.

Identity and business contact data

Name, job title, company name, business email address, business telephone number,



postal address and similar details that you give us or that we obtain from publicly available business sources.

Company information

Company number, company name, VAT number and similar corporate identifiers.

Enquiry, contract and CRM records

Messages sent through the Website contact form or by email, proposal and negotiation records, signatures, the operational record of instructions once a contract is in place, and the related Client and prospect records we keep in Twenty CRM. Twenty CRM is hosted by us. It is not a third-party CRM SaaS product.

Device and technical data

Where you use the Website, our web server may record an IP address, browser type, operating system and the page requested in short-lived security logs. That is separate from the analytics described in section 7.

Usage data

Counts of pages viewed and similar traffic statistics, generated by our self-hosted Umami instance. Those statistics are not tied to your name, email address or another direct identifier. See section 7.

Payment and billing data

Billing address, invoice history, payment references and transaction history when you buy from us. We do not store full card numbers on our own devices. Card payments, if used, are taken by a payment provider.

Marketing preferences

Opt-out and suppression records, bounce information and similar preference data.

Recruitment data

If you apply for a role, the information in your application and CV.

We do not seek special category data or criminal-offence data through the Website or as a normal part of providing our services. If a Client places such data on systems we host or manage, we process it only as processor under the DPA, and only to the extent the service requires.

4. How We Use Information and Our Lawful Bases

Under UK data protection law we need a lawful basis for each use. The basis we rely on can affect which rights apply. The ICO explains lawful bases at ico.org.uk.



Priority	Meaning
To operate and secure the Website, including server logs	Legitimate interests — running and protecting a business website.
To consider and respond to an enquiry, prepare a proposal and enter a contract	Steps prior to a contract and, once agreed, performance of a contract with the business. Legitimate interests in running a B2B sales pipeline for prospect contacts who are not yet in contract.
To provide contracted services, authenticate Client staff, keep a record of instructions and run support	Performance of the contract . Legitimate interests in operating and evidencing a support function. Content of a ticket that is the Client's customer or end-user data is processor processing under the DPA, not this table.
To raise invoices, collect fees, keep accounting records and recover unpaid fees	Performance of the contract . Legal obligation — Companies Act and tax record-keeping.
To tell existing and prospective business customers about relevant services	Legitimate interests in B2B marketing of similar services to corporate contacts, subject to PECR as set out in section 5. You can object at any time.
To measure use of the Website and improve what we offer	Legitimate interests — measuring a business website with cookieless, self-hosted analytics that are not used to identify a visitor. See section 7.
To process transactions	Performance of the contract .
To find and prevent fraud and to investigate security incidents	Legitimate interests — network and information security and protection of the business.
To take or defend legal claims, obtain insurance and deal with the ICO or a court	Legal obligation where one exists. Otherwise legitimate interests in establishing, exercising or defending legal claims and obtaining insurance.
To recruit, pay and manage staff or contractors	Contract with the individual. Legal obligation for tax, right to work and similar duties.



Priority	Meaning
To manage suppliers	Contract , or legitimate interests in running the supplier file.
To comply with other legal obligations	Legal obligation.
To keep Client and prospect records in Twenty CRM	The same contract and legitimate-interests bases as the enquiry, sales and account work those records support. Twenty CRM is our filing system for that work, not a separate purpose.

We have considered the impact of our legitimate-interests processing on individuals. The data we use for sales and marketing is business contact data, the volumes are those of a small B2B supplier, and anyone can object. Website analytics are configured so that they are not used to identify a visitor. We do not consider that those interests are overridden.

We do not use automated decision-making that produces legal or similarly significant effects.

5. Direct Marketing

We may use publicly available business contact information, and contact details you have given us, to tell prospective and existing business customers about our services where we have a lawful basis to do so. That work may be done by our own staff or by contractors instructed by us, as described in section 8.

Electronic mail and texts to individuals are also regulated by the Privacy and Electronic Communications Regulations 2003 (PECR):

- we use the PECR soft opt-in only where the contact is an existing customer, the message is about similar services, and an opt-out was offered when the details were collected and in every message;
- otherwise we obtain PECR consent before email or text marketing;
- we honour an opt-out and keep a suppression record so that we can continue to honour it.

You can object to direct marketing at any time by using the unsubscribe link in a message or by emailing GDPR@vistaweb.ltd. That right is not limited by the contract basis we may use for other processing.



6. Where We Get Personal Information From

- Directly from you, including the Website contact form, email, calls, meetings, contracts and the client portal.
- From the company you represent.
- From publicly available sources such as company websites, Companies House, business directories and professional networking platforms, where we collect business contact information to identify and contact prospective customers.
- From our own Website server logs and payment provider, where those services are used.
- From referees or previous employers if you apply for a role.

Contact, company and deal records created from those sources are stored in Twenty CRM on infrastructure we host. Umami analytics events are generated on our own infrastructure when a page is requested. They are described in section 7 and are not used as a source of contact details.

7. Cookies and Website Analytics

We do not use cookies on the Website. We do not use Google Analytics or any other third-party advertising or analytics pixel.

We measure traffic with Umami, which we host ourselves. It is configured not to set a cookie and not to store a name, email address, customer account or other direct identifier. A recorded visit may include the page path, the referring site, browser and device type, and a rough location (typically country or region) derived from the IP address at the time of the request. We do not keep that IP address as an analytics identifier, we do not build a profile of an identifiable person from those events, and we do not share Umami data with advertising networks.

Because the Website does not store or access information on your device through cookies, the PECR cookie rule does not apply to this measurement. If that configuration changes, we will update this notice before we start using cookies.

8. Who We Share Information With

We do not sell personal information.

We may share personal information with the following categories of recipient, and only as needed for the purpose in question:



- website hosting, DNS and, where used, content-delivery networks, so that the Website can be served and kept available;
- payment processors and our bank, to take and reconcile payment;
- the email or ticketing tools we use to receive enquiries and support our Clients;
- independent contractors who carry out marketing or sales work for us. They may be given access to relevant Client and prospect contact data, including records held in Twenty CRM, only so far as that work requires. They process that data on our documented instructions, under a data processing agreement and under confidentiality terms. They are not permitted to use it for their own marketing or to keep it after the engagement ends, except as UK law requires;
- other contractors and service providers who provide customer support, administrative or similar business services on our instructions, under confidentiality duties and, where they process personal data for us, under a data processing agreement;
- for Client services only, the sub-processors authorised under the Client DPA — including the United Kingdom host used for hosted sites, the domain registrar and relevant registries (including Nominet for .uk), the email platform (Proton Mail for the email management service), and SEO or analytics tools the Client has asked us to use;
- our accountant, HMRC and, if a fee is unpaid after notice, debt-recovery or solicitors to the extent that is proportionate;
- professional or legal advisers, insurers and brokers;
- a court of England and Wales, the ICO, or another authority if the law requires it; and
- publicly, on our Website, social media or other marketing materials, only to the extent we have agreed with the relevant Client (for example a case study or portfolio piece). We do not publish the personal data of a Client's customers or site visitors for that purpose.

Twenty CRM and Umami run on infrastructure we control. CRM records and analytics events are not sent to a third-party CRM or analytics vendor. A marketing or sales contractor accesses Twenty CRM only under the terms above.

If our business is transferred, personal information may pass to a successor so that the business can continue. We would take reasonable steps to keep it protected.

9. International Transfers

We process personal information in the United Kingdom as a default. Twenty CRM and Umami are self-hosted. They are not United States SaaS products.

Some infrastructure we use, including anycast DNS or a content-delivery network if one is in place, may process technical data outside the United Kingdom. A contractor may work from outside the United Kingdom only if a Chapter V safeguard is in place first. Where a transfer is restricted under UK GDPR Chapter V, we rely on:



- UK adequacy regulations; or
- the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses; or
- another lawful mechanism in Chapter V, including a relevant Article 49 derogation for an occasional transfer.

Client personal data processed under the Client DPA is not transferred outside the United Kingdom unless that DPA's transfer terms are met.

10. How Long We Keep Information

We keep information only for as long as we need it for the purpose we collected it, including any legal, accounting or reporting requirement. The periods below are the ones we actually use.

Priority	Meaning
Website server logs	90 days, unless needed for a live security investigation
Umami analytics events	Kept as anonymous or aggregated traffic statistics for measuring the Website. Not used to identify a person. Reviewed at least annually.
Enquiry and prospect files in Twenty CRM, including the Website contact form	24 months after the last meaningful contact or quote
Signed contracts, schedules and the related Twenty CRM Client record	Life of the contract plus 6 years (ordinary limitation period in England and Wales)
Invoices and accounting records	6 years after the end of the financial year
Support tickets and our record of instructions	24 months after the relevant service schedule ends, longer if a claim is reasonably in view
Marketing suppression / opt-out	For as long as needed to honour the opt-out
Security logs on our own systems	12 months, longer for a live investigation



Priority	Meaning
Job applications (not hired)	12 months from the decision
Client personal data on hosted sites, mailboxes and similar systems	The term of the relevant service schedule, then return or deletion under the DPA. Residual encrypted backups expire on their cycle. We do not set a separate retention purpose of our own for that data.

If you want more detail about a particular file, contact us using the details in section 15.

11. Security

The security of your personal information matters to us. We use technical and organisational measures appropriate to the risk. Client and prospect records in Twenty CRM and Website analytics in Umami are held on infrastructure we host. For processing we do as processor for a Client, the measures are described in Annex 2 of the DPA and include, as relevant to the service actually engaged, access control, encryption in transit, backup, staff confidentiality and a United Kingdom or adequacy-territory host for production hosting.

No method of transmission over the internet and no method of electronic storage is completely secure. We cannot guarantee absolute security. You remain responsible for the credentials issued to you, for your own devices, and for what you choose to send us.

12. Your Data Protection Rights

This section is written under the UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025. Those are the laws that govern us.

You have the following rights, subject to the exemptions that UK law allows:

- **Access** — to ask for copies of your personal information and for related information about how we use it.
- **Rectification** — to ask us to correct inaccurate or incomplete personal information.
- **Erasure** — to ask us to delete personal information in the circumstances the UK GDPR sets out.
- **Restriction** — to ask us to limit how we use personal information in the circumstances the UK GDPR sets out.



- **Objection** — to object to processing based on legitimate interests. You have an absolute right to object to processing for direct marketing.
- **Portability** — to ask us to transfer personal information you gave us to you or to another organisation, where the basis is consent or contract and the processing is automated.
- **Withdrawal of consent** — where we rely on consent, to withdraw it at any time. Withdrawal does not affect processing already carried out.
- Rights in relation to automated decision-making and profiling — we do not carry out automated decision-making of the kind these rights address.

Which rights apply can depend on the lawful basis. The ICO publishes guidance on the rights and the exemptions that may apply.

If you make a request, we will respond without undue delay and in any event within one month, or within any longer period UK law allows for a complex or numerous request.

To make a request, email GDPR@vistaweb.ltd. We may need to verify that we are dealing with the right person.

These rights are about processing we do as controller, including records in Twenty CRM. Requests about data on a Client's website, mailbox or other Client system should be sent to that Client. We will forward a request of that kind to the Client.

A request that only concerns an anonymous Umami traffic statistic will usually have nothing identifiable to give you. That does not affect a request about an enquiry, a contract, a CRM record or any other file that does identify you.

Visitors outside the United Kingdom

If you are in the European Economic Area, the EU GDPR may also give you rights against a controller who offers goods or services to you or who monitors your behaviour in the EEA. Our Website is an information and enquiry channel for UK and other business customers. We do not target consumers in the EEA. If EU GDPR rights apply to a particular interaction, you can use the same contact address and we will deal with the request in line with the law that actually applies.

If you are a California resident, the CCPA / CPRA may give you rights to know, delete and opt out of sale or sharing. We do not sell personal information. You can use the same contact address. Those statutes do not change the fact that our contracts and this notice are governed by the law of England and Wales.



13. How to Complain

If you have a concern about our use of your personal data, contact us first using the details in section 15.

If you remain unhappy, you can complain to the Information Commissioner's Office, which is the UK supervisory authority.

Information Commissioner's Office

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

- Helpline: 0303 123 1113
- Complaints: www.ico.org.uk/make-a-complaint

14. Processing We Do as Processor

This section is for transparency. It does not replace the DPA.

Where a Client has engaged the relevant service, we process the following categories on that Client's documented instructions.

Hosting and management

Storage, backup, monitoring and technical processing of whatever the Client places on the hosted environment, including visitor identifiers, form submissions, account credentials if stored, uploaded content and logs. Production hosting is in the United Kingdom (London) or another adequacy territory named in the service schedule.

Deletion and return at the end of the service follow the DPA, not a retention period of our own.

Domain management and initial acquisition

Registration, renewal, DNS and transfer administration. Types of data are registrant and administrative contact details required by the registrar and the registry. The Client remains the registrant.

Email management

Mailbox hosting, routing, filtering and related administration on the platform named in the email schedule (Proton Mail on the current specimen). Types of data are mailbox content and metadata of the Client's users and of people who send mail to them. We read mailbox content only as needed to deliver the service or on documented instructions. Archive and legal hold are not part of the standard service unless separately scheduled.

Search-engine optimisation

Technical audits, keyword and ranking work, crawl and analytics review, and reporting. Types of data are primarily aggregated or pseudonymised analytics, and contact details of the Client's staff. We do not use this data for our own marketing. We do not guarantee rankings



Website design and build

Personal data in materials the Client supplies, and in staging or project environments, for as long as needed to perform the statement of work. When the site is hosted by us afterwards, the hosting description above applies.

Client portal

Account identifiers and access logs we need to run the portal (controller); any Client personal data a Client uploads into the portal (processor). Portal access ends when no MSA service schedule remains, as the portal schedule provides.

Future services

If we add a service under the MSA, the DPA's modular annex is updated by the new schedule. Processing stays limited to what is reasonably necessary to perform that schedule.

We use sub-processors in the categories listed in the Client DPA (hosting, registrar and registry, email platform, DNS/CDN, SEO tooling, support tools, and professional advisers where access is incidental). We remain responsible to the Client for those sub-processors to the extent Article 28(4) UK GDPR requires, subject to the limitation of liability in the MSA.

Twenty CRM holds our own Client and prospect file. It is not a place in which we store a Client's end-user data as processor, unless a Client has expressly instructed us to put that data there.

If we become aware of a personal data breach affecting Client personal data, we notify the Client without undue delay and in any event within 48 hours of becoming aware, as the DPA requires. The Client remains responsible for deciding whether to notify the ICO or affected individuals, unless the law imposes that duty directly on us.

15. Contact Us

Questions about this Privacy Policy, or a request to exercise data protection rights, should be sent to:

- Email: **GDPR@vistaweb.ltd**
- Post: Vista Web Ltd, 3 Castlegate, Grantham, Lincolnshire, NG31 6SF
- Website: **vistawebdesigns.co.uk** or **vistaweb.ltd**

General business enquiries can go to **contact@vistaweb.ltd**.



16. Changes to this Privacy Policy

We may update this Privacy Policy where it is reasonable to do so, including to reflect a change in law, in our processing, or in the services we offer. The current version will be published on the Website with a revised "Last Updated" date.

Material changes that affect a contracted Client's processor relationship are dealt with through the DPA and the relevant service schedule, not only by this notice.

17. Governing Law

This Privacy Policy is issued by a company established in England and Wales. The processing it describes is designed to meet the UK GDPR and the Data Protection Act 2018.

Our Website Terms of Use, MSA, DPA and service schedules are governed by the law of England and Wales. The courts of England and Wales have exclusive jurisdiction over disputes under those contracts. Nothing in this notice is intended to confer a right on a consumer or on a person who is not a party to those contracts, except so far as data protection law gives a data subject a right that cannot be excluded