Blackdown Digital

PRIVACY NOTICE

How we handle personal data

Your data, your rights, explained in plain English

Version 3.2 · Effective 15 November 2026 · Reviewed at least every 12 months

Applies to: enquirers, renewal-reminder and email-update subscribers, prospective clients, clients and people who buy our standalone products

Blackdown Digital Services Limited, trading as Blackdown Digital ("we", "us", "our"), protects your personal data and is open about how we use it. This notice explains what we collect, why, how long we keep it, and your rights under the UK GDPR and the Data Protection Act 2018.

1 Who we are and what this notice covers

Blackdown Digital Services Limited is the **controller** for the personal data we hold about people who enquire, renewal-reminder and email-update subscribers, prospective clients and other people we send marketing to, and for our own business records about clients and buyers. We are registered in England and Wales, company number 17517551, and registered with the Information Commissioner's Office (ICO), registration number ZC289048. Registered office: 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ. Founder and Principal Consultant: Chris J Hosgood.

When we handle personal data inside a client's systems and files to deliver our Cyber Essentials readiness services, we act as a **processor** and the client is the **controller**. Our Data Processing Agreement (version 3.2) governs that work. This notice describes it only so that you know who to contact.

Our website privacy policy at blackdowndigital.co.uk/legal/privacy summarises this notice and adds detail about the website: its forms, hosting and cookies. If the two differ, this notice applies.

2 What personal data we collect

From people who enquire (by email or phone)

- Your name, email address, telephone number (if provided), company name and any information you give us in your message or call

From renewal-reminder subscribers

- If you sign up on our website for a Cyber Essentials renewal reminder: your name, email address, business name and certificate expiry date

From email-update subscribers

- If you sign up on our website for Cyber Essentials email updates: your email address and, if you give it, your name, with a record of when you signed up and the wording you agreed to

From people who opt out

- If you use the opt-out page on our website, or ask us to stop our marketing emails: your email address, which we keep on a do-not-contact list

About prospective clients (from public sources)

- Business contact details, such as name, job title, work email address and phone number, taken from company websites, Companies House and professional networks such as LinkedIn
- If you ask for, or we offer you, our free email security check (the "free check"): public DNS records about your domain's email set-up (such as SPF, DKIM, DMARC and MX records), and whether your business's own website or service appears in Have I Been Pwned's public list of known breaches.
- The free check does not look up any staff or individual email addresses, and we never see or store passwords or breached content. The only personal data involved is the name and work email address of the person we send the report to, and any DMARC reporting address in your DNS records, which the report shows only by its domain.

From clients and buyers of standalone products (we are the controller)

- Contact details of the people we deal with, which you or your colleagues give us
- The address of your premises and the name of your site contact, where an on-site visit is booked
- Our correspondence with you, and the proposal you accepted
- Remote session logs: names, email addresses, device and connection details, and session times
- Billing details and records of invoices and payments. If you pay by card, your card details go directly to our payment provider, and we never see or store your full card number.
- If you buy one of our publications: your name, business name, contact and billing details.

On our client's behalf (we are the processor)

- Usernames, email addresses, job titles and account identifiers needed for the agreed package
- Computer and system configuration information, reports and files that may contain personal data
- Working notes we make during the work
- The Policy and Evidence Pack we prepare as part of Full Support. We make it on our own encrypted laptop, and it refers to job roles, never named people.

Our client is the controller of this data. **If it is your data, contact your employer first**, or whichever organisation is our client. If you send a request or complaint about it to us, we will pass it to our client within 2 working days, and we act only on our client's instructions.

We do not intentionally collect special category data. Please do not include sensitive personal information in your messages to us unless it is essential.

3 How we use personal data and our lawful bases

This table covers the data we hold as controller. Most people we deal with act for a company, so we rely mainly on legitimate interests. We rely on a contract only where you are a sole trader or partner, because then the contract is with you personally.

Purpose	Lawful basis
To respond to enquiries and arrange scoping calls	Legitimate interests (replying to people who contact us); steps before entering a contract, where you are a sole trader or partner
To provide the services and products ordered	Legitimate interests (delivering what your organisation has ordered); performance of a contract, where you are a sole trader or partner
To keep records of the work we have done, manage the client relationship and deal with any questions or claims	Legitimate interests (running our business and protecting our legal position)
To invoice for our services and products and take payment, including by card	Legitimate interests (being paid for our work); performance of a contract, where you are a sole trader or partner
To send the Cyber Essentials renewal reminder you asked for	Consent, which you can withdraw at any time by replying to a reminder or emailing us
To send the Cyber Essentials email updates you signed up for	Consent, which you can withdraw at any time using the link in any email, our opt-out page, or by emailing us
To keep a do-not-contact list, so we don't email people who have opted out	Legitimate interests (respecting your choice not to hear from us)
To tell businesses about our services, including occasional emails and free checks	Legitimate interests (promoting our services to businesses that may need them); consent, for sole traders and partnerships who have opted in
To keep our systems and the data we hold secure, including remote session logs	Legitimate interests (protecting our clients, our business and the data we hold)
To comply with legal and regulatory obligations (for example accounting and tax records, and answering data protection requests)	Legal obligation

Marketing emails. We send them only to:

- business addresses at companies, LLPs, Scottish partnerships and other corporate bodies; and
- sole traders and other partnerships, only if they have agreed, or if all of these apply: they gave us their details when buying or enquiring about our services; the email is about our own similar services; and they could opt out easily when we collected the details.

Every marketing email gives you a simple way to opt out. You can object to our marketing at any time, and we will stop within 2 working days.

If you are a client, we need some information to carry out the work. If you don't provide it, we may not be able to deliver the services. We do not sell personal data, and we do not use it for automated decision-making or profiling.

4 Who we share personal data with

We do all the work ourselves and use no subcontractors. We share personal data only with:

- **Microsoft 365** (Microsoft), our processor for email, cloud storage of documents and files, and secure upload and sharing links (OneDrive and SharePoint).
- **Zoho Assist** (Zoho Corporation), our processor for remote support. It holds session details such as names, email addresses, device and connection details, and session times.
- **FreeAgent**, our processor for invoicing and bookkeeping.
- **Netlify**, our processor for website hosting. It receives the sign-up and opt-out forms submitted through our website.
- **Stripe**, our card payment provider, when you choose to pay an invoice by card. Stripe is our processor for taking the payment. It is also an independent controller when it uses payment information for its own regulated payment, fraud-prevention and legal-compliance purposes, under its own privacy notice (stripe.com/privacy).
- The Certification Body (the IASME-licensed body assessing our client's Cyber Essentials application), only if our client has agreed in writing.
- Our accountant, insurer or solicitor, only when they need the information to prepare our accounts, handle a claim or advise us.
- Regulators, courts or law enforcement, if the law requires us to.

Our processors must protect the data and use it only for the purposes we set. Microsoft 365 and Zoho Assist are the only providers that handle data we process on a client's behalf. They are the Subprocessors named in our Data Processing Agreement. FreeAgent, Stripe and Netlify handle only our own business data (billing, payments and website forms) and are not Subprocessors.

5 International transfers

We keep personal data in the United Kingdom or the European Economic Area (EEA) where we can. The UK treats the EEA as providing adequate protection for personal data. This table shows where each provider holds data and what protects it outside the UK.

Provider	Where the data is	Safeguard
Microsoft 365	Stored in the UK and EU. Microsoft may process limited data outside the UK and EU to provide support and run its service.	UK adequacy regulations for the EEA. The transfer safeguards in Microsoft's data protection terms for anything else.
Zoho Assist	Stored in the EU (the Netherlands, with a second data centre in Ireland). Zoho's own technical support staff outside the UK and EEA may access data remotely, only when needed to support the service. Zoho says no data is moved out of the EU.	UK adequacy regulations for the EEA. Zoho's intra-group Standard Contractual Clauses for any support access from outside the UK and EEA.

Provider	Where the data is	Safeguard
FreeAgent	Stored in Ireland. Some of FreeAgent's own subprocessors are outside the UK and EEA, for example in the United States.	UK adequacy regulations, or the UK Addendum to the EU Standard Contractual Clauses.
Stripe	We contract with Stripe Payments Europe, Limited (Ireland) and Stripe Payments UK Ltd. Stripe transfers data to the United States.	The UK Extension to the EU-US Data Privacy Framework (the "UK-US data bridge"), with the UK Addendum to the EU Standard Contractual Clauses as a fallback.
Netlify	Stored in the United States.	The UK Extension to the EU-US Data Privacy Framework, with the UK Addendum to the EU Standard Contractual Clauses as a fallback.

Email hello@blackdowndigital.co.uk if you want a copy of any of these safeguards.

6 How long we keep personal data

An engagement ends when its Order ends under clause 4.7 of our Terms of Business (version 3.2).

Type of data	How long we keep it
Enquiries from people who contacted us first, which do not become client work	12 months from our last contact with you.
Renewal reminder details	Until you ask us to stop. If you do not become a client, we delete them 12 months after your certificate expiry date. If you gave no expiry date, we delete them once the single reminder has been sent. We use them only for the reminder.
Email update sign-ups	Until you ask us to stop. We keep a record of when and how you signed up for as long as we email you.
Do-not-contact list	Your email address only, for as long as we send marketing emails.
Business contacts we approached first, and free check results	2 years from our last contact, or until you object or unsubscribe, whichever is sooner. After that we keep only a minimal record of your opt-out, so we don't contact you again.
Our business records about clients and buyers: proposals, invoices, payment records and correspondence	6 years from the end of the financial year in which the engagement ends or, for a standalone product, in which you buy it. This covers accounting, tax and potential claims.
Remote session logs	12 months from the session, then deleted from Zoho Assist.

Type of data	How long we keep it
Working notes we make during an engagement	Deleted within 30 days after the engagement ends. Correspondence is kept with our business records, as above.
Client data we handle as processor: reports, configuration files, other client files and copies	Deleted within 30 days after the engagement ends. If the client asks before then, we return a copy first. We keep copies longer only where UK law requires it, or where the client asks in writing for a stated period (no longer than 12 months), after which we delete them.

When a period ends we delete or securely destroy the data, unless the law requires us to keep it longer.

7 Your rights

Under the UK GDPR you have the right to:

- Access the personal data we hold about you.
- Ask us to correct inaccurate data.
- Ask us to erase data in certain circumstances.
- Ask us to restrict processing in certain circumstances.
- Object to processing based on legitimate interests, and object to direct marketing at any time.
- Request a copy of data you provided to us in a portable format.
- Withdraw your consent at any time, where we rely on it (renewal reminders, email updates and other opted-in marketing).

To use any of these rights, contact us using the details in section 10. Requests are free. We may ask you to confirm your identity. We will respond within one month. If a request is complex, the law allows us to extend this by up to two further months, and we will tell you if we need to. If we hold your data only on a client's behalf, send your request to that client (see section 2).

7.1 Making a complaint

If you are unhappy with how we have handled your personal data, you have the right to complain to us. Email hello@blackdowndigital.co.uk with "Data protection complaint" in the subject line, or contact us by any other means in section 10. We will acknowledge your complaint within 30 days, look into it without undue delay, keep you updated, and tell you the outcome.

You also have the right to complain to the Information Commissioner's Office at any time, at ico.org.uk or on 0303 123 1113.

8 Security

We take appropriate technical and organisational measures to protect personal data. As a small consultancy, the measures are proportionate to the limited volume and nature of the data we handle. They include:

- **Access.** Access controls, multi-factor authentication, encrypted devices and secure deletion of temporary files.

- **Storage.** Client files and reports are stored in Microsoft 365 (OneDrive and SharePoint), protected by multi-factor authentication, and, while being worked on, on our encrypted laptop. Never in any other cloud service or on removable media. Only our consultant accesses them. The data file our device check produces for us is encrypted when it is created, and only we can open it, in our own in-house toolkit.
- **File transfer.** We never send or accept files as ordinary email attachments. Files are exchanged through private OneDrive upload and sharing links, or by encrypted transfer during an attended Zoho Assist session. If you can't use either, files can be sent as an AES-256 encrypted archive, with the password given by phone. Unencrypted files are never sent by email.
- **Remote sessions.** Sessions are encrypted and start only when the person at the device gives permission. Unattended access is set up only at the client's written request. We remove it within 2 working days of the engagement ending, or of the client's written request, whichever is earlier.
- **Paper.** We mainly work remotely and do not keep paper records of client data, including during on-site visits.

9 Changes to this notice

We review this notice at least once a year and may update it. The current version and its date are always linked from blackdowndigital.co.uk/legal/privacy. If we make a material change, we will email current clients, and renewal-reminder and email-update subscribers, at least 14 days before it takes effect, and summarise the change at the top of the notice.

10 Contact us

If you have any questions about this notice or how we handle personal data, please contact:

Contact	Chris J Hosgood, Founder and Principal Consultant
Email	hello@blackdowndigital.co.uk
Telephone	01823 589771
Registered office	71-75 Shelton Street, Covent Garden, London, WC2H 9JQ
Company number	17517551
ICO registration	ZC289048

Blackdown Digital

Blackdown Digital Services Limited, trading as Blackdown Digital. Registered in England and Wales.
Registered office: 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ · ICO registration ZC289048
Company number 17517551 · hello@blackdowndigital.co.uk · 01823 589771 · blackdowndigital.co.uk

Privacy Notice · Version 3.2 · Effective 15 November 2026