Blackdown Digital

DATA PROCESSING AGREEMENT

Processor Terms

UK GDPR Article 28 terms forming part of our Terms of Business

Blackdown Digital Services Limited · Company number 17517551
Version 3.2 · Effective 15 November 2026

This Data Processing Agreement ("DPA") forms part of each contract made under the Terms of Business between Blackdown Digital Services Limited, trading as Blackdown Digital, ICO registration number ZC289048 ("Processor", "we", "us"), and the Client ("Controller", "you"). It applies whenever the Processor processes Personal Data on the Controller's behalf in providing the Services.

1 Definitions

1.1 "Controller", "Processor", "Data Subject", "Personal Data", "Personal Data Breach" and "processing" have the meanings given in the UK GDPR.

1.2 "Services" has the meaning given in clause 1.11 of the Terms of Business.

1.3 "Subprocessor" means a third party that the Processor engages to process Personal Data on the Controller's behalf.

1.4 "Terms of Business" means the Processor's Terms of Business, version 3.2. The clause numbers of the Terms of Business cited in this DPA are those of version 3.2.

1.5 "UK GDPR" has the meaning given in section 3(10) of the Data Protection Act 2018, read together with that Act, in each case as amended from time to time (including by the Data (Use and Access) Act 2025).

1.6 Other capitalised terms, including "Order", "Business Day", "On-site Visit" and "Policy and Evidence Pack", have the meanings given in the Terms of Business.

2 Scope and roles

2.1 The Controller appoints the Processor to process Personal Data on its behalf, only for the purpose of providing the Services.

2.2 Schedule 1 sets out the subject matter, duration, nature and purpose of the processing, the types of Personal Data and the categories of Data Subjects.

2.3 The Controller is the controller of the Personal Data and the Processor is its processor. The Processor does not decide the purposes or means of the processing.

2.4 The Processor will process Personal Data only on the Controller's documented instructions, which include this DPA and the Order. The only exception is where UK law requires other processing. The Processor will then tell the Controller about that requirement before processing, unless the law prohibits this on important grounds of public interest.

2.5 The Processor will tell the Controller immediately if it believes an instruction infringes the UK GDPR or other UK data protection law.

3 Processor obligations

3.1 The Processor will:

(a) process Personal Data only as set out in clause 2.4;

(b) make sure that anyone it authorises to process Personal Data is bound by a duty of confidentiality;

(c) use appropriate technical and organisational measures to keep Personal Data secure, as described in Schedule 2;

(d) use Subprocessors only as set out in clause 5;

(e) taking into account the nature of the processing, help the Controller, by appropriate technical and organisational measures and as far as possible, to respond to Data Subjects who exercise their rights (see clause 7);

(f) help the Controller to comply with Articles 32 to 36 of the UK GDPR (security, breach notification, data protection impact assessments and prior consultation), taking into account the nature of the processing and the information available to the Processor;

(g) delete or return Personal Data as set out in clause 10; and

(h) provide information and allow audits as set out in clause 8.

4 Controller obligations

4.1 The Controller warrants that it has a lawful basis for the processing and that its instructions to the Processor are lawful.

4.2 The Controller is responsible for the accuracy, quality and legality of the Personal Data and for how it was obtained.

4.3 The Controller must not instruct the Processor to process Personal Data in a way that would put the Processor in breach of the UK GDPR.

5 Subprocessors

5.1 The Controller gives the Processor general authorisation to use Subprocessors. Current Subprocessors are listed in Schedule 3.

5.2 The Processor will give the Controller at least 14 days' written notice (email is sufficient) before adding or replacing a Subprocessor. The Controller may object in writing within those 14 days on reasonable data protection grounds. If the Controller does not object, the change is authorised.

5.3 If the Controller objects and the parties cannot resolve the objection within a further 14 days, either party may end the affected Services by written notice. The Controller must pay for work performed up to that date.

5.4 The Processor will impose on each Subprocessor data protection obligations that are no less protective than those in this DPA. The Processor remains fully liable to the Controller for each Subprocessor's performance of those obligations.

6 Personal data breach

6.1 The Processor will notify the Controller without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach affecting Personal Data processed under this DPA. The Processor will give notice by email to the Controller's contact named in the Order and, where the Order gives a phone number, by phone as well. The notice will name the person to contact at the Processor.

6.2 The notice will include, as far as the information is available: (a) the nature of the breach; (b) the categories and approximate number of Data Subjects and records concerned; (c) the likely consequences; and (d) the measures taken or proposed to deal with the breach. The Processor will send any information that is not available at first as soon as it has it.

6.3 The Processor will cooperate with the Controller and take reasonable steps to help investigate, contain and put right the breach.

7 Data subject rights and assistance

7.1 The Processor will forward to the Controller, within 2 Business Days of receiving it, any request from a Data Subject to exercise rights under the UK GDPR (including a data protection complaint) that relates to Personal Data processed under this DPA. The Processor will not respond to the request itself, except on the Controller's documented instructions or as the law requires. The Processor will give the Controller reasonable help in responding.

7.2 The Processor gives the help described in clauses 3.1(e), 3.1(f), 6.3 and 7.1 at no charge where the need arises from the Processor's own breach of this DPA. Otherwise the Processor may charge for help beyond 2 hours per request, at a rate the parties agree in writing before that further work starts.

8 Audits

8.1 On request, the Processor will give the Controller the information needed to show that the Processor complies with this DPA and with Article 28 of the UK GDPR. The Processor will allow and contribute to audits, including inspections, by the Controller or an auditor the Controller appoints.

8.2 The Processor may first answer an audit request by providing documents, such as its security policies and certifications, and answers to reasonable questions.

8.3 If an inspection is still needed, the Controller must give at least 30 days' written notice, or 5 Business Days' written notice after a Personal Data Breach. Inspections: (a) are carried out remotely, by video call and screen sharing, unless the parties agree otherwise in writing; (b) take place on Business Days between 9am and 5pm; (c) happen no more than once in any 12 months, unless the Information Commissioner requires one or one follows a Personal Data Breach; (d) are subject to a duty of confidentiality on the Controller and its auditor; and (e) must not unreasonably disrupt the Processor's business or expose another client's information.

8.4 The Controller pays the cost of any audit, unless the audit reveals a material breach of this DPA by the Processor.

9 Locations and international transfers

9.1 The Controller authorises the Processor to process Personal Data in the United Kingdom and the European Economic Area, using the Subprocessors and locations listed in Schedule 3. Schedule 3 also states where a Subprocessor may access or process limited Personal Data from elsewhere to support or run its service, and the safeguard that applies. The Controller gives this authorisation by accepting an Order (Terms of Business clause 11.4). Processing in any other location is allowed only under clause 9.2.

9.2 The Processor will not process Personal Data in, or transfer it to, any other location unless it has first: (a) given the Controller notice of the new location under clause 5.2, with the same right to object as for a new Subprocessor; and (b) put in place a safeguard that the UK GDPR allows, such as UK adequacy regulations, the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses.

10 Deletion or return of data

10.1 Within 30 days after an Order ends (Terms of Business clause 4.7), the Processor will delete all Personal Data processed under this DPA for that Order, including files, reports, working notes and copies. If the Controller asks before then, the Processor will first return a copy. The Processor keeps copies only where UK law requires it, or where the Controller asks in writing for them to be kept for a stated period of no more than 12 months. The Processor will confirm deletion in writing within 5 Business Days of the Controller's request.

10.2 Clause 10.1 does not apply to the Processor's own business records: the Order, invoices, payment records, the contact details of the people it deals with, premises and site contact details for On-site Visits, correspondence with the Controller and remote session logs. These are not Client Data (Terms of Business clause 1.3). The Processor holds them as a controller, not as a processor, and its Privacy Notice explains how it uses them (Terms of Business clause 11.5). It keeps them for 6 years from the end of the financial year in which the engagement ends, except remote session logs, which it keeps for 12 months from the session.

11 Liability

11.1 Liability under this DPA is subject to the limits and exclusions in clause 13 of the Terms of Business. Nothing in this DPA or the Terms of Business limits either party's liability for breach of the UK GDPR to the extent that the law prohibits that limit.

12 Term

12.1 This DPA applies for as long as the Processor processes Personal Data on the Controller's behalf. It continues after an Order ends for as long as is needed to return or delete the Personal Data, and for any copies kept under clause 10.1.

13 Acceptance, versions, precedence and notices

13.1 The Controller accepts this DPA by accepting an Order (Terms of Business clause 4.1). No signature is needed.

13.2 The version of this DPA in force at the date of an Order applies to that Order (Terms of Business clause 4.4). Any change to it for that Order must be agreed by both parties in writing.

13.3 If this DPA conflicts with the Terms of Business or an Order on a data protection matter, this DPA prevails (Terms of Business clause 4.3).

13.4 Notices under this DPA must be in writing and sent by email: to the Processor at hello@blackdowndigital.co.uk, and to the Controller at the address in the Order (Terms of Business clause 17.6). An email sent before 5pm on a Business Day is deemed received that day. Any other email is deemed received on the next Business Day. Clause 6.1 also applies to notice of a Personal Data Breach.

14 Governing law

14.1 This DPA is governed by the law of England and Wales. The courts of England and Wales have exclusive jurisdiction.

SCHEDULE 1
Details of processing

Subject matter	Providing the Services: the Cyber Essentials readiness services described in the Order.
Duration	For the duration of the relevant Order and up to 30 days afterwards, or for any longer period the Controller asks for under clause 10.1.
Nature and purpose	• Analysing the results of the Processor's device check software, run on the Controller's computers • Reviewing router and firewall configuration exports • Listing devices on the Controller's network from a computer's own records • Applying fixes the Controller approves • Providing remote support sessions • Accessing and reviewing, remotely or during On-site Visits, system configurations, user accounts and related information, to assess and fix controls against the Cyber Essentials requirements • For Full Support, configuring Microsoft 365 or Google Workspace with the Controller's permission • Preparing the Policy and Evidence Pack, which the Processor's toolkit produces on the Processor's own encrypted laptop and which refers to roles only, never to named individuals • Preparing reports and other documents, and giving guidance
Types of Personal Data	• Names, email addresses and job titles of users of the Controller's systems • Account identifiers, usernames, sign-in names, role information, admin rights, account status and last sign-in dates • Computer and device names, IP and MAC addresses, and other network identifiers • System configuration data that may contain Personal Data • Working notes made while providing the Services • Information shown on screen or transferred during a remote support session

Categories of Data Subjects	• Employees, contractors and other authorised users of the Controller's systems
Not covered	The Processor's own business records, including the contact details of the people it deals with, premises and site contact details for On-site Visits, correspondence with the Controller and remote session logs (clause 10.2).

SCHEDULE 2

Technical and organisational measures

The Processor uses the following measures, which are appropriate to the limited nature and volume of the processing:

- Access to the Controller's systems is limited to the Founder and Principal Consultant, and only for as long as is needed to perform the Services.
- During On-site Visits, the Controller's systems are accessed only with the Controller's permission. No paper records of the Controller's data are made or taken away, and none of the Controller's equipment is removed from the premises.
- The device check software reads system settings only. It does not read the contents of documents, emails or files.
- Device check downloads are licensed to the named Controller, stop working after the licence period (normally 30 days), install nothing and remove their working files when they close.
- For each computer, the device check produces a PDF report for the Controller and an encrypted data file holding the same findings. Only the Processor can open the encrypted data file, using its own in-house toolkit on its encrypted laptop. The Controller sends the Processor only the encrypted data file. The PDF report stays with the Controller for its own records.
- The Processor receives device check data files, configuration files and other files only through a private upload link that only the Processor can see, or by encrypted file transfer during an attended Zoho Assist session. Except as set out below, it never receives them by email, because configuration files can contain passwords and keys.
- The Processor shares reports only through access-restricted links. The recipient must verify their email address with a one-time code, and the links expire after 30 days and can be revoked. Except as set out below, reports are never sent as email attachments.
- The only exception: if the Controller cannot use these links, the Processor and the Controller may exchange files by email as AES-256 encrypted archives. The password is given by phone, never by email. Unencrypted files are never sent by email.
- The Controller's files, reports and other Personal Data are stored in Microsoft 365 (OneDrive and SharePoint), protected by multi-factor authentication, and, while being worked on, on the Processor's encrypted laptop. They are never stored in any other cloud service or on removable media. Passwords and keys found in configuration files are removed from reports.
- The Policy and Evidence Pack is produced by the Processor's toolkit on the Processor's own encrypted laptop, from the Controller's own reports. It refers to roles only, never to named individuals.
- The Processor's systems use multi-factor authentication, strong unique passwords and encrypted devices. Data is encrypted in transit.
- Remote sessions run through Zoho Assist. They are encrypted, start only when the person at the device gives permission on screen, can be ended by the Controller at any time, time out when idle and are logged.

- Unattended access is set up only if the Controller requests it in writing. The Processor removes it within 2 Business Days of the Order ending or of the Controller's written request, whichever is earlier.
- Temporary working files and notes are securely deleted within 30 days of the Order ending (clause 10.1). Within the same 30 days, the Processor removes any access it still has to the Controller's systems.
- Anyone with access to Personal Data is bound by a duty of confidentiality.
- The Processor reviews its access rights at least every 12 months and when an Order ends.

These measures are proportionate to a small specialist consultancy doing fixed-scope work, mostly remotely. The Controller is responsible for the security of its own systems, and for deciding whether its risks call for further measures.

SCHEDULE 3
Subprocessors

The Controller authorises the Processor to use the following Subprocessors. The Location column shows where each one stores Personal Data. Changes are made under clause 5.2.

Subprocessor	Purpose	Location
Microsoft 365 (Microsoft)	Email, secure cloud storage of files and reports, and secure file sharing and upload links (OneDrive and SharePoint)	UK and EU
Zoho Assist (Zoho Corporation)	Remote support sessions, including screen sharing and encrypted file transfer during an attended session	EU (the Netherlands, with Ireland as the secondary site)

Adequacy. The UK treats the European Economic Area as providing adequate protection for Personal Data, under UK adequacy regulations.

Support access from outside the UK and EEA. Zoho's own technical support staff outside the UK and EEA may access Zoho Assist data remotely, only when this is needed to support the service. Zoho states that no data is moved out of the EU. This access is covered by Standard Contractual Clauses between Zoho's group companies. Microsoft may process limited data outside the UK and EU to provide support and run its service, under the transfer safeguards in its own data protection terms. The Controller can ask the Processor by email for a copy of the relevant safeguards.

Providers that are not Subprocessors. The Processor uses FreeAgent for invoicing and accounts, Stripe for card payments, and Netlify to host its website and receive the sign-up and opt-out forms on its website. They receive only the Processor's own business and billing data, such as the contact and payment details on an invoice. They do not receive Personal Data processed under this DPA, so they are not Subprocessors. The Processor's Privacy Notice explains how it uses them, where they hold data and the safeguards that apply.

No subcontractors. The Processor carries out all analysis and report writing itself and uses no subcontractors (Terms of Business clause 17.3). The Subprocessors above only store and transmit data. Any other third party that would process Personal Data would be a new Subprocessor under clause 5.2.