Privacy Notice

This Privacy Notice explains how Bishop Consultancy UK Ltd ("Bishop Consultancy", "we", "us", "our") collects, uses, and protects personal data relating to the individuals who subscribe to or make enquiries about our phishing simulation service and cyber security awareness training (the "Service") through our portal at portal.bishop-cyber.co.uk (the "Site").

This Notice applies to personal data that we process as a controller in our own right, including data relating to the individuals who set up and administer customer accounts, make payments, receive transactional communications from us, or contact us with enquiries.

It does not apply to personal data that we process as a processor on behalf of our subscribing customers in connection with the delivery of the Service (for example, the names and email addresses of our customers' employees who are enrolled in training or included in simulated phishing campaigns). That processing is governed by separate processor terms agreed with the relevant subscribing customer.

1. Who we are and how to contact us

1.1 Bishop Consultancy UK Ltd is the controller of the personal data described in this Notice. We are a company registered in England under company number 04456435 with a registered office at 5 Wainwright Way, Kesgrave, Ipswich, Suffolk, England, IP5 2XG.

1.2 We have not appointed a Data Protection Officer as we are not required to do so under the UK GDPR. Questions about this Notice or about how we handle personal data should be directed to Kevin Bishop, Director, using the contact details below:

Email: enquiries@bishop-consultancy.co.uk

Post: 5 Wainwright Way, Kesgrave, Ipswich, Suffolk, England, IP5 2XG

2. The personal data we collect

2.1 We collect the following categories of personal data about the individuals who subscribe to, administer, or enquire about the Service:

- Identity and contact data — name, job title, work email address, work telephone number, and the name and address of the organisation the individual represents;
- Account data — login credentials (stored in hashed form), subscription details, and account preferences;
- Transaction data — subscription orders placed, payment confirmation references returned by our payment processor, invoice and VAT records, and related billing history;
- Communications data — the content of enquiries and support requests sent to us, and transactional correspondence sent between us and the account holder;
- Authorised Use Declaration data — where the Service includes phishing simulation, the name, job title, email address, and signed acceptance of the individual completing the Declaration on the organisation's behalf;
- Domain verification data — the domain names submitted for use with the phishing simulation service, and the name and email address of the individual verifying each domain;

- Technical data — IP address, browser type, and basic session information captured automatically when the Site is accessed, for security and service-operation purposes.

2.2 We do not collect payment card details. All card payments are processed directly by our payment provider, Stripe (see section 6).

2.3 We do not knowingly collect personal data from children. The Service is offered only to business customers.

3. Where we obtain personal data

3.1 We obtain personal data from the following sources:

- Directly from you — when you sign up for the Service, complete an Authorised Use Declaration, verify a domain, contact us with an enquiry, or otherwise communicate with us;
- Automatically through the Site — when you visit the Site, we automatically collect limited technical data as described in section 2.1 and in our Cookie Policy;
- From our payment provider — payment confirmation references and transaction status updates returned by Stripe after a payment attempt.

4. How we use personal data and our legal bases

4.1 We process personal data for the purposes set out in the table below. The lawful bases on which we rely under Article 6 of the UK GDPR are identified against each purpose.

Purpose	Data used	Lawful basis	
Setting up and administering your account on the Site	Identity and contact data; account data; technical data		Performance of a contract (UK GDPR Art. 6(1)(b))
Processing your subscription order and renewals, issuing invoices, and handling refunds	Identity and contact data; transaction data		Performance of a contract (UK GDPR Art. 6(1)(b))
Taking payment for subscriptions and renewals	Transaction data (payment confirmation references only)		Performance of a contract (UK GDPR Art. 6(1)(b))
Sending transactional communications (welcome emails, invoices, renewal reminders, Authorised Use Declaration confirmations, domain verification emails, certificates, and service notices)	Identity and contact data; account data		Performance of a contract (UK GDPR Art. 6(1)(b))

Recording, verifying, and enforcing the Authorised Use Declaration and domain verification requirements for the phishing simulation service	Authorised Use Declaration data; domain verification data		Performance of a contract (UK GDPR Art. 6(1)(b)) and legitimate interests (Art. 6(1)(f)) — ensuring the phishing simulation service is operated only against authorised domains
Responding to enquiries, support requests, and complaints	Identity and contact data; communications data		Legitimate interests (Art. 6(1)(f)) — responding to and managing communications from our customers and prospective customers
Keeping business, accounting, and tax records as required by law	Identity and contact data; transaction data; Authorised Use Declaration data; communications data		Legal obligation (Art. 6(1)(c)) — in particular the Companies Act 2006, the Value Added Tax Act 1994, and HMRC record-keeping requirements
Protecting the security and proper operation of the Site, preventing fraud, and investigating misuse	Account data; technical data		Legitimate interests (Art. 6(1)(f)) — protecting our systems, our customers, and third parties from misuse of the Service
Establishing, exercising, or defending legal claims	Any of the above categories as relevant		Legitimate interests (Art. 6(1)(f)) and legal obligation (Art. 6(1)(c))

4.2 We do not use personal data for direct marketing. We will not add you to a marketing mailing list or send you promotional communications about our Services unless you have expressly asked us to do so.

4.3 We do not use personal data for any form of automated decision-making or profiling that produces legal effects concerning individuals or similarly significantly affects them.

5. Who we share personal data with

5.1 We share personal data with the following categories of recipient:

- Sub-processors and service providers who help us deliver the Service, as listed in section 6;
- Professional advisers — our accountants, auditors, insurers, and legal advisers, where there is a legitimate need to do so;
- HMRC, regulators, and other authorities — where we are required to do so by law, including for VAT and corporation tax reporting;
- Courts, law enforcement, or similar bodies — where disclosure is required by a court order, subpoena, or valid legal process, or where it is reasonably necessary to protect the rights, property, or safety of Bishop Consultancy, our customers, or third parties.

5.2 We do not sell personal data. We do not share personal data with third parties for their own marketing purposes.

6. Sub-processors and service providers

6.1 The following service providers assist us in operating the portal and providing our services. Each is bound by a written contract that imposes appropriate data protection obligations.

We may store some or all of your personal data in countries outside of the UK and EEA. These are known as "third countries". When we do, we ensure that appropriate safeguards are in place to protect your data. These safeguards include ensuring that the level of protection in the destination country is not materially lower than that required under the Data Protection Legislation.

Sub-processor	Purpose	Location
Stripe Payments Europe Ltd	Payment processing, card authorisation, fraud detection, and processing of refunds	Ireland (primary); data may be transferred to Stripe group companies in the USA under UK IDTA safeguards
Hetzner Online GmbH	Hosting of the Site, the application server, and the database	EU (Germany)
Sendinblue SAS (trading as Brevo)	Outbound transactional email delivery (welcome, invoice, renewal, verification, and certificate emails)	EU (France, Germany, Belgium)
Microsoft Ireland Operations Ltd	Inbound email delivery (Microsoft 365 mailbox for the	EU (Ireland/Netherlands)

	enquiries mailbox) and cloud file storage (OneDrive) used for client documents where applicable	

6.2 We review our sub-processors periodically and may add or change sub-processors from time to time. Where a change materially affects the processing of personal data relating to you, we will update this Notice before the change takes effect.

7. International transfers

7.1 Most of our sub-processors host or process personal data within the United Kingdom or the European Economic Area, where equivalent data protection standards apply.

7.2 Where personal data is transferred to a country outside the UK and the EEA that has not been recognised by the UK Government as providing an adequate level of protection, we put in place appropriate safeguards in accordance with UK data protection law. The primary safeguard we rely on is the UK International Data Transfer Agreement ("UK IDTA") or the UK Addendum to the EU Standard Contractual Clauses, as set out in the sub-processor table above.

7.3 You may request further information about the safeguards in place for any specific transfer by contacting us using the details in section 1.

8. How long we keep personal data

8.1 We keep personal data only for as long as we need it for the purposes set out in this Notice, or for as long as we are required or permitted to keep it by law.

8.2 Our standard retention periods are:

8.2.1 Account and subscription records (including Authorised Use Declarations, domain verification records, and order history): for the duration of your subscription and for 6 years from the end of the subscription term, to meet our legal obligations under the Companies Act 2006, the Value Added Tax Act 1994, and HMRC record-keeping requirements, and to allow for the limitation periods under the Limitation Act 1980.

8.2.2 Invoice, VAT, and accounting records: 6 years from the end of the financial year to which they relate.

8.2.3 Enquiries, support, and general correspondence: up to 2 years from the last communication, unless retained for longer as part of an ongoing matter or under one of the other categories in this section.

8.2.4 Technical logs and security-related records: up to 12 months from the date of collection, except where retained for longer in connection with a specific security incident or investigation.

8.2.5 Backups: personal data held in backups is overwritten on rolling cycles and in any event is fully purged within 30 days of the expiry of the underlying retention period.

8.3 At the end of the applicable retention period, personal data is securely deleted or anonymised.

9. How we protect personal data

9.1 We use a range of technical and organisational measures to protect personal data against unauthorised access, loss, alteration, or disclosure, including:

- Transport encryption (TLS 1.2 or higher) on all connections to the Site and to our sub-processors;
- Encryption at rest for server disks and database backups;

- Role-based access controls, unique personal accounts, and multi-factor authentication for administrative access;
- Regular security patching and monitoring of servers and software;
- A documented incident response procedure covering identification, containment, notification, and remediation of security incidents;
- Staff confidentiality obligations and data protection training for personnel with access to personal data;
- Cyber Essentials certification, with IASME Cyber Assurance Level 1 and 2 in progress.

9.2 No system is completely secure. Where we become aware of a personal data breach that is likely to result in a risk to the rights and freedoms of affected individuals, we will notify the Information Commissioner's Office within 72 hours, and will notify affected individuals directly where the risk to their rights and freedoms is high, in accordance with UK GDPR.

10. Your rights

10.1 Under UK data protection law, you have the following rights in relation to the personal data we hold about you:

- The right to be informed — about how we use your personal data (this Notice is part of how we meet that right);
- The right of access — to receive a copy of the personal data we hold about you;
- The right to rectification — to have inaccurate personal data corrected, and incomplete data completed;
- The right to erasure — to have personal data deleted in certain circumstances (the "right to be forgotten");
- The right to restrict processing — to limit how we use your personal data in certain circumstances;
- The right to data portability — to receive certain of your personal data in a commonly used machine-readable format;
- The right to object — to processing based on legitimate interests;
- Rights relating to automated decision-making and profiling — as noted in section 4.3, we do not carry out such processing.

10.2 To exercise any of these rights, please contact us using the details in section 1. We will respond within one month of receiving a valid request. We may extend this by up to two further months for particularly complex requests, and will tell you if we need to do so.

10.3 We may ask you for information to verify your identity before acting on a request. We will not charge a fee unless the request is manifestly unfounded, excessive, or repetitive.

10.4 Some rights are qualified and may not apply in every circumstance. Where we cannot give effect to a right, we will explain why.

11. Complaints

11.1 If you are concerned about the way we have handled your personal data, we would like to hear from you first so that we can try to put things right. Please contact us using the details in section 1.

11.2 You also have the right to lodge a complaint with the Information Commissioner's Office, the UK's supervisory authority for data protection matters:

Information Commissioner's Office

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

Helpline: 0303 123 1113
Website: ico.org.uk

12. Cookies

12.1 The Site uses a small number of strictly necessary cookies to operate correctly. Full details of the cookies used, including their names, purposes, and durations, are set out in our Cookie Policy (BC-CKY-001).

13. Changes to this Notice

13.1 We may update this Notice from time to time to reflect changes in our processing activities, our sub-processors, or applicable law. The latest version is always available on the Site. Where the change is material, we will give you reasonable advance notice, for example by email to the account holder's registered email address.

13.2 This version was published on the date shown below.

Bishop Consultancy UK Ltd
Ipswich, England
enquiries@bishop-consultancy.co.uk
bishop-consultancy.co.uk