Bayliss and Grove Ltd

GDRP and Data Protection Policy

Version: 1.1

Date: November 2025

Owner: Director

Policy Statement

Bayliss and Grove Ltd ("the Company") is committed to protecting the privacy and security of all personal data entrusted to us. We handle client and supplier information with the highest standards of care and in full compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

We are registered with the Information Commissioner's Office (ICO) under registration number **ZC041764**.

This policy explains how we collect, use, store, and protect personal data, and outlines the rights of individuals whose data we process.

1. Data We Collect

In the course of providing our services, Bayliss and Grove Ltd may collect and process the following personal data:

- Names
- Email addresses
- Telephone numbers
- Credit or debit card information
- Bank Account information
- Billing address

This information is collected directly from clients, suppliers, and partners through business correspondence, the Bayliss C Grove website, contracts, and communications.

2. How We Use Personal Data

Personal data is used only for legitimate business purposes, including:

- Delivering procurement consultancy and training services
- Managing supplier and client relationships
- Communicating via email, telephone, and other channels

- Administrative and compliance purposes
- To process payments made
- To pay invoices received

Specific Payment Information

When you book training through our website, we collect payment details necessary to process your transaction. This includes your credit or debit card information, billing address, and contact details.

Legal Basis for Processing

We process payment data under contract necessity (to complete your booking) and comply with legal obligations related to financial record-keeping.

How We Handle Your Payment Data

- We do not store full card details on our servers.
- All payment transactions are processed securely through a PCI DSS-compliant payment gateway.
- Sensitive authentication data (such as CVV/CVC codes) is never stored after the transaction is completed.

Security Measures

We use encryption and secure protocols to protect payment information during transmission. Our payment processor applies industry-standard security measures, including tokenization and fraud prevention systems.

Data Retention

Payment-related data is retained only as long as necessary for transaction processing and legal obligations (e.g., tax and accounting requirements). We do not keep card details beyond what is legally permitted.

We do not sell or misuse personal data.

3. Legal Basis for Processing

Bayliss and Grove Ltd processes personal data under the following lawful bases:

- **Contractual necessity**: To fulfil our consultancy services.
- **Legitimate interests**: To manage business relationships and communications.
- **Consent**: For specific uses such as marketing communications only when consented.

4. Data Storage and Security

We take the security of personal data seriously and employ robust measures to protect it:

- **Email:** All email communications are conducted through Microsoft Outlook, which provides enterprise-grade encryption, secure authentication, and advanced threat protection.
- **Cloud Storage**: Data is stored securely within Microsoft 365 services, protected by multi-factor authentication and access controls.
- **Access Control**: Only authorised personnel with a legitimate business need can access personal data.
- **Device Security**: Company devices are protected with up-to-date antivirus software, firewalls, and regular patching.
- **Backups**: Data is backed up regularly to secure servers to prevent loss.

5. Data Retention

Personal data is retained only for as long as necessary to fulfil contractual obligations and legal requirements. Once data is no longer required, it will be securely deleted or anonymised.

6. Marketing Communications

Bayliss and Grove Ltd will only send marketing communications where individuals have explicitly opted in or to generic public email addresses under legitimate interest.

- Clients and contacts may opt in via consent forms or email correspondence.
- Individuals may opt out at any time by emailing **info@baylissandgrove.co.uk**.
- Marketing data is stored securely and used solely for the purposes consented to.

7. Individual Rights

Under GDPR, individuals have the following rights:

- Right to access their personal data
- Right to rectification of inaccurate data
- Right to erasure (“right to be forgotten”)
- Right to restrict processing
- Right to data portability
- Right to object to processing
- Right not to be subject to automated decision-making

All enquiries, including subject access requests, should be directed to:
info@baylissandgrove.co.uk

8. Data Breach Management

In the unlikely event of a data breach, Bayliss and Grove Ltd will:

- Investigate and contain the breach immediately.
- Notify the Information Commissioner's Office (ICO) within 72 hours if required.
- Inform affected individuals where there is a high risk to their rights and freedoms.
- Document all breaches and remedial actions taken.

G. Responsibilities

- **Directors**: Ensure overall compliance and governance.
- **Employees**: Handle personal data responsibly and report any concerns.

10. Use of Sub-Processors

Bayliss and Grove Ltd may engage carefully selected third-party service providers ("sub-processors") to support the delivery of our services. These sub-processors may provide services such as IT support, cloud hosting, communications, or other operational functions.

- Compliance: All sub-processors are required to comply with UK GDPR and the Data Protection Act 2018.
- Security: Sub-processors must implement appropriate technical and organisational measures to protect personal data.
- Transparency: Bayliss and Grove Ltd maintains a list of current sub-processors, which will be updated as new providers are engaged.
- Client Assurance: We only appoint sub-processors where it is necessary for business operations and where equivalent data protection standards are guaranteed.

Current Sub-Processors

- **Microsoft 365 (Teams, email, cloud storage, collaboration tools)**

  We use Microsoft 365 services, including Teams for webinars and Outlook for email. Microsoft acts as a data processor under GDPR. Microsoft applies industry-standard security controls such as encryption, access management, and continuous monitoring. Microsoft engages approved sub-processors (including affiliates and selected third parties) to deliver these services, all bound by GDPR-compliant contracts. Because Microsoft operates globally, personal data may be transferred outside the UK/EEA. These transfers are protected by Standard Contractual Clauses, adequacy decisions, and Microsoft's EU Data Boundary commitments. For more details, see https://learn.microsoft.com/en-us/compliance/regulatory/gdpr

- **Xero (Accounting)**

  We use Xero as our cloud-based accounting and bookkeeping platform. In this role,

Xero acts as a data processor on our behalf under the General Data Protection Regulation (GDPR). Xero processes certain personal data (such as customer details, invoices, and financial records) solely to provide accounting, reporting, and related services.

Xero is contractually bound to implement appropriate technical and organisational measures to protect your data and to process it only according to our instructions. For more details, see Xero's Data Processing Agreement.

International Data Transfers

Xero operates globally, which means your personal data may be transferred outside the UK or European Economic Area (EEA), including to New Zealand, Australia, and the United States. These transfers are made:

- To countries with an adequacy decision (where the European Commission or UK authorities have confirmed equivalent data protection standards), or
- Using appropriate safeguards, such as Standard Contractual Clauses (SCCs), in compliance with GDPR Chapter V.

Security Measures

Xero applies industry-standard security practices, including:

- Encryption of data in transit and at rest
- Access controls and authentication
- Regular vulnerability assessments, monitoring, and independent audits

- **Wix Payments**

When you book training through our website, payments are processed via Wix Payments, a PCI DSS-compliant service integrated into our platform. Wix Payments handles your credit or debit card details securely using:

- Encryption during transmission and storage
- Tokenization to prevent exposure of card numbers
- Fraud prevention systems and regular security audits

We do not store full card details on our servers. Sensitive authentication data (such as CVV/CVC codes) is never retained after the transaction. Payment-related data is kept only as long as necessary for transaction processing and legal obligations (e.g., tax and accounting).

Data may be transferred to other Wix group entities worldwide to provide services.

Wix engages third-party sub-processors for tasks such as:

- Payment processing and settlement
- Fraud detection and prevention
- Cloud hosting and storage
- Customer support tools
- Each sub-processor only has access to the minimum data necessary to perform its role.

- Wix provides an up-to-date public list of sub-processors, including names and locations, and notifies users of changes.

You can view the official list of Wix's sub-processors on their Help Center: https://support.wix.com/en/article/list-of-wixs-sub-processors

- **Wix**
  We use Wix as our website hosting provider. In this role, Wix acts as a data processor on our behalf under the General Data Protection Regulation (GDPR). Wix processes certain personal data (such as IP addresses and server logs) solely to provide hosting and related services.

  Wix is contractually bound to implement appropriate technical and organisational measures to protect your data and to process it only according to our instructions. For more details, see https://support.wix.com/en/article/wixs-data-processing-agreement-for-wix-users

  International Data Transfers

  Wix operates globally, which means your personal data may be transferred outside the UK or European Economic Area (EEA), including to the United States. These transfers are made:

  - To countries with an adequacy decision (where the European Commission or UK authorities have confirmed equivalent data protection standards), or
  - Using appropriate safeguards, such as Standard Contractual Clauses (SCCs), in compliance with GDPR Chapter V.

Security Measures

Wix applies industry-standard security practices, including:

- Encryption of data in transit and at rest
- Access controls and authentication
- Regular vulnerability assessments and monitoring

11. Review and Updates

This policy will be reviewed annually or sooner if required by changes in legislation, business practices, or regulatory guidance.

Contact Information

For questions, subject access requests, or to opt out of marketing communications, please contact info@baylissandgrove.co.uk