



Data Protection Policy

Internal policy for the personal information handled by Brooks Beckman Ltd in its UK SME finance brokerage and associated business activities. This is not a replacement for a customer-facing privacy notice.

Document control	Details
Company	Brooks Beckman Ltd Company number 12918986 ICO ZA831470
Version and status	1.0 - draft for approval; not evidence of Board adoption
Prepared	16 October 2026
Policy owner	Data Protection Lead, designated by the directors
Approval and review	Director / Board approval required. Review at least annually after approval and following a material change.

1. Purpose, scope and regulatory context

Brooks Beckman Ltd ("the Firm") introduces and arranges funding across business loans, asset, property, invoice and tax finance. It acts as a credit broker, not the lender. It handles personal information relating to applicants, directors, beneficial owners, guarantors, representatives, partners, staff and other contacts.

This policy applies to directors, employees, contractors and service providers processing information on the Firm's behalf, in any format or system. It supports UK GDPR, the Data Protection Act 2018, applicable PECR requirements and relevant amendments under the Data (Use and Access) Act 2025. AML-specific legal bases and retention requirements apply where the Firm's activities are in scope; they must not be assumed from the business model of another firm.

The Firm is the controller for processing whose purposes and means it determines. Lenders, credit reference agencies and some other recipients may be independent controllers; a commercial relationship does not automatically make them processors. ICO registration: ZA831470. Data protection contact: Joel Brooks at joel@brooksbeckman.co.uk, 07778 097179.

Approval dependencies

Before adoption, directors must confirm the Data Protection Lead, approved suppliers, processing inventory, data locations, lawful bases, retention schedule and any regulated activity or MLR scope. The role is a Data Protection Lead; a statutory Data Protection Officer is appointed only if required or deliberately designated in accordance with the law.



2. Key terms and responsibilities

Term	Meaning
Personal data / data subject	Information relating to an identified or identifiable living person / that person.
Controller / processor	A controller decides why and how data is processed; a processor acts on a controller's documented instructions.
Special category data	Sensitive categories protected by Article 9, including health and certain biometric data.
Criminal offence data	Information within Article 10, including relevant allegations and criminal proceedings. Assess screening data case by case.
ROPA / LIA	Record of Processing Activities / Legitimate Interests Assessment.
DPIA / personal data breach	Data Protection Impact Assessment / a security incident affecting confidentiality, integrity or availability of personal data.
Rights request / DSAR	A request to exercise a data protection right / a subject access request.

Allocation of responsibilities

The directors are accountable for governance, resources, approval and material risk decisions. The Data Protection Lead maintains this policy, the ROPA, rights and breach registers, supplier assessments and privacy notices; coordinates requests and complaints; and escalates significant issues. The person responsible for information security implements access, logging, deletion and incident controls with approved IT providers.

All staff must use data only for authorised purposes, complete training, verify recipients and report suspected breaches or rights requests immediately. Named owners and absence cover must be recorded. Outsourcing does not transfer the Firm's accountability.

3. Principles

Staff apply lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. Collect only what a funding stage needs. Correct errors promptly. Do not reuse application information for incompatible purposes or circulate full identity and bank records to every potential lender.



4. Privacy information and collection

Give accessible privacy information at the point of collection, including through the website and application form, and when required for information obtained indirectly. Maintain separate notices for applicants and connected individuals, staff and recruitment, and website/marketing activity. Explain the Firm's identity and contacts, purposes and bases, legitimate interests, recipients, international transfers, retention, rights and ICO complaints.

A public privacy notice must describe actual brokerage processing and lender sharing, rather than importing a lender's account-management or credit-reporting practices. The internal policy and any Article 28 data-processing agreement are separate documents. An application checkbox is not a substitute for lawful-basis analysis or a complete notice.

Introducers must have an appropriate basis for providing personal information and communicate relevant privacy information. The Firm checks representative authority where needed. Direct collection through Jotform must use the approved company account, appropriate access controls and clear privacy links.

5. Lawful bases and processing inventory

Activity	Approach to lawful basis
Applications and lender introductions	Contract / steps requested by an individual where genuinely applicable; otherwise documented legitimate interests for company representatives, owners and guarantors. A company's contract is not automatically a contract with its directors.
Identity, fraud and screening checks	A specific legal obligation only where it applies to the Firm; otherwise a documented legitimate-interest or other valid basis. Record the assessment.
Lender sharing and communications	A basis appropriate to the requested brokerage service, necessity and recipient role; explain the sharing in privacy information.
Staff and suppliers	Contract, employment or other legal obligation, or legitimate interests as appropriate to the activity.
Commission, accounts and disputes	Applicable legal obligations and/or necessary, documented legitimate interests.
Marketing	Apply UK GDPR and PECR channel and recipient rules; do not assume all business email marketing is exempt or that an application constitutes marketing consent.

Record purpose, data categories, affected individuals, lawful basis, recipients, security, retention and transfers in the ROPA. Maintain LIAs where appropriate and review annually and on change. Identify Article 9 conditions and any required DPA 2018 Schedule 1 safeguards before processing special category data; identify a valid Article 10 gateway for criminal offence data.



6. Individual rights and complaints

Log and escalate requests for access, correction, erasure, restriction, portability, objection and applicable automated-decision safeguards. Verify identity proportionately. Apply the legal response period, normally one calendar month, and any lawful clarification, pause or extension mechanism only where the current law permits. Explain any applicable extension within the required period; an ordinary complaint does not replace a rights response.

Erasure is not absolute. Consider statutory retention, legal claims and exemptions individually and explain the decision where permitted. Direct-marketing objections must be actioned and a minimal suppression record retained where needed. Correct shared errors and notify recipients where required.

Screen potentially sensitive financial-crime records before disclosure. Assess a specific lawful exemption and whether disclosure would prejudice a relevant investigation; do not apply an automatic exclusion to every document mentioning AML. Record the decision and obtain specialist advice when necessary.

Data protection complaints are handled under the Complaints Policy. Provide a usable complaint route, acknowledge within the internal three-business-day target and no later than 30 calendar days, investigate and communicate progress and the outcome without undue delay. Individuals may approach the ICO. Maintain a separate view of rights-request and breach deadlines.

7. Sharing and third parties

Share with lenders, funders, introducers, professional advisers, checking providers, technology processors and authorities only where justified. Lenders determine their own lending decisions and processing where they act as independent controllers. Brokerage staff must verify recipients, use secure channels, minimise disclosures and record the purpose and basis.

Before engaging a processor, assess security, data locations, deletion, assistance, breach notification and sub-processing. Put an Article 28 agreement in place with documented instructions, confidentiality, security, assistance, audit and end-of-service provisions. Use prior specific or general written authorisation for sub-processors with the required notice and objection arrangements. Identify joint-controller situations and agree responsibilities where applicable.

Jotform and the website are part of the supplier assessment; any CRM, automation, screening or storage provider must be approved for Brooks Beckman before use. Existing accounts or contracts belonging to another company are not treated as approval. No unconfirmed supplier appointment is asserted by this policy.



8. Security, incidents and personal data breaches

Use role-based access, least privilege, multi-factor authentication where available, secure devices, encryption appropriate to the risk, tested backups and controlled document sharing. Review access on joining, role changes and departure. Do not place identity records or application files in public website folders or send bank-detail changes without independent checks.

A breach includes misdirected email, lost devices, unauthorised access, malicious encryption, inappropriate disclosure and destruction or loss of availability. Staff must report actual or suspected incidents immediately to the Data Protection Lead and preserve relevant evidence. Record when the Firm became aware; the clock does not start only when a manager reads the report.

The Lead assesses containment, scope, sensitivity and risk; records the facts and decisions; and coordinates recovery. Notify the ICO without undue delay and, where feasible, within 72 hours of awareness unless the breach is unlikely to result in a risk to individuals' rights and freedoms. Explain a delay and provide information in phases where needed. Notify affected individuals without undue delay where the high-risk threshold applies, subject to lawful exceptions.

Record every personal data breach and the assessment even where no notification is made. Require processors to alert the Firm without undue delay and provide assistance. Review lessons learned, remediation owners and closure evidence; escalate material incidents to directors.

9. DPIAs, transfers and automation

Screen new or significantly changed processing for a DPIA before implementation, including potentially high-risk biometric, screening, open-banking, monitoring or automated assessment. The Lead coordinates mitigations, consultation and approval. Seek ICO prior consultation where legally required because a high residual risk remains.

For restricted international transfers, identify a valid mechanism such as UK adequacy regulations, an IDTA or UK Addendum with the required transfer assessment, or a lawfully available exception. Record onward transfers, overseas access and supplier data locations; cloud use alone does not establish adequate safeguards.

As an internal standard, the Firm requires meaningful human review of significant brokerage routing or assessment decisions. Lenders' final credit decisions remain theirs. Before introducing solely automated significant decisions, assess the current UK GDPR framework, including Articles 22A-22D where applicable, transparency, lawful bases, special category restrictions and rights to information, representations, human intervention and challenge.



10. Retention, deletion and training

The schedule below is a proposed internal standard and must be checked against the actual processing inventory, limitation risks and applicable law before adoption. It is not a statement that every category has a statutory minimum. Retain only what is necessary, document legal holds and review extensions. Confirm processor deletion and backup expiry arrangements; restrict held data from routine use.

Category	Proposed standard and review
Brokerage application, advice/arranging and commission records	Normally six years after service or relationship closure, subject to necessity and legal-claims review. Do not import a lender's full loan-life retention without a reason.
AML/KYC and transaction records	Where MLR Regulation 40 applies, normally five years from the relevant end event, with deletion and extension rules assessed under that regulation. Where it does not, set a justified period in the ROPA.
Guarantee or deed copies	Retain only if needed for the broking service or claims. Assess any twelve-year deed-related extension individually; it is not a blanket retention rule.
Complaints	Normally six years from closure as a documented internal standard; apply any overriding regulatory retention rule.
Employees / unsuccessful recruitment	Normally six years after employment; unsuccessful candidate records normally six months, with a justified, limited extension where appropriate.
Marketing	Review at least annually; remove inactive leads after three years unless another documented basis applies. Keep proportionate suppression information.
Access and security logs	Normally 12 months, extend up to 24 months where justified by security, audit or incident needs.
Governance / legal holds	Retain official company records for the applicable legal period; review personal data and legal holds rather than treating all Board material as permanently necessary.

Staff complete induction and annual data protection training covering secure use, sharing, rights, complaints and breach escalation. Record completion and remediate gaps. The directors review compliance information and approve material changes. Policy breaches are investigated and may lead to appropriate disciplinary or contractual action.

Approval record and review

Record approver, effective date, named Lead, supplier register and adopted retention periods. Review within twelve months of approval or sooner after an incident, legal change or material processing change.

Reference points: UK GDPR and DPA 2018 as amended; Data (Use and Access) Act 2025; ICO guidance on data protection complaints, breaches, individual rights, processors, transfers and DPIAs. Official guidance: <https://ico.org.uk/for-organisations/> ; legislation: <https://www.legislation.gov.uk/ukpga/2025/18/contents>