

INFORMATION SECURITY POLICY SUITE

Data Protection and Compliance Policy

Glaxtons Consulting Limited

REF GCL-DPC-01

VERSION 6.0

CLASSIFICATION Confidential, internal and authorised third parties

DOCUMENT REFERENCE	GCL-DPC-01
CLASSIFICATION	Confidential, internal and authorised third parties
POLICY OWNER	Data Protection Lead
APPROVED BY	The Board of Glaxtons Consulting Limited
EFFECTIVE DATE	May 2026
NEXT SCHEDULED REVIEW	May 2027
APPLIES TO	Glaxtons Consulting Limited, 3 More London Place, London SE1 2RE

1 Purpose

This policy ensures the Company handles personal data and other regulated information lawfully, retains records only for as long as necessary, and can demonstrate compliance to clients and regulators.

2 Scope

This policy applies to all personal data and other regulated records processed by the Company, wherever they are held.

3 Definitions

In this policy, "Company" means Glaxtons Consulting Limited, "Personnel" means employees, workers, contractors, consultants and temporary staff of the Company, and "client" means any current or prospective client, customer or partner of the Company.

4 Policy

4.1 Retention

The Company maintains a documented retention schedule setting defined retention periods for each principal category of record it holds, including financial and accounting records, employee records, client and bid records, and security logs, reflecting applicable statutory requirements and the Company's legitimate business needs.

Records are securely disposed of, in accordance with the Data Security Policy, once the applicable retention period expires.

4.2 International data transfers

Where the Company stores, processes or transmits data outside the United Kingdom, or discloses data to individuals or entities located overseas, including in the United States, it identifies an appropriate transfer mechanism recognised under the UK GDPR, such as the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or reliance on an applicable adequacy regulation, and carries out a transfer risk assessment before the transfer takes place.

4.3 Protection of personal data

The Company maintains documented procedures for handling personal data proportionate to its legal sensitivity, value and criticality, including data classification, access restriction on a need to know basis, encryption in accordance with the Data Security Policy, and completion of a data protection impact assessment for any processing activity likely to result in high risk to individuals.

4.4 Independent security audit

The Company arranges an independent review of its information security controls at least annually, comprising an internal audit against this policy suite together with the external assessments described in the Risk Assessment and Vulnerability Management Policy. Findings are reported to the Board and tracked to closure.

4.5 Sharing of audit outcomes

Summaries of independent audit or assessment outcomes, including relevant penetration test or certification reports, are made available to clients and prospective clients on request, subject to the client first entering into a non-disclosure agreement with the Company.

5 Alignment with client due diligence requests

This policy addresses the following reference points commonly raised in client and prospective client vendor due diligence and security assessments: V.RA-31, V.RA-32, V.RA-33, V.RA-34, V.RA-35. Where a client raises a due diligence question falling within this policy's scope, the relevant section of this policy may be used as the basis for the Company's response, subject to review by the Operations Director.

6 Roles and responsibilities

- The Data Protection Lead owns the retention schedule, transfer risk assessments and data protection impact assessments.
- The Operations Director owns the independent audit programme.
- The Board reviews audit findings and approves the annual audit plan.

7 Non-compliance and exceptions

Breach of this policy may result in disciplinary action up to and including dismissal, and, in the case of a contractor, consultant or supplier, termination of the relevant engagement or contract. Any exception to this policy must be

requested in writing, is subject to a documented risk assessment, and requires the approval of the Operations Director before it takes effect.

8 Related policies

- Information Security Policy
- Data Security Policy
- Risk Assessment and Vulnerability Management Policy
- Third Party and Supplier Security Policy

9 Version history

VERSION	DATE	SUMMARY OF CHANGE	AUTHOR
6.0	May 2026	Scheduled annual review, reissued and approved by the Board.	Legal Department

Glaxtons Consulting Limited · 3 More London Place, London SE1 2RE · 020 3668 5488 · info@glaxtons.co.uk · glaxtons.co.uk
This document is issued under the Company's information security policy suite and is reviewed at least annually. Printed copies are uncontrolled.