
CYBER360 / SPECIALIST SERVICES

Data Privacy and Protection

Practical privacy. Clear accountability.

Connect privacy governance with the way your organisation collects, uses, shares and protects personal data. Cyber360 helps you assess maturity, prioritise risks and build practical privacy controls across the data lifecycle.

01 Clear scope

02 Practical evidence

03 Priorities for improvement

TRUSTED SECURITY ADVISORY

Advice that leads to action.

cyber360.co | info@cyber360.co | Privacy & data protection

01 / SCOPE & FOCUS

The right question. A useful assessment.

Connect privacy governance with the way your organisation collects, uses, shares and protects personal data. Cyber360 helps you assess maturity, prioritise risks and build practical privacy controls across the data lifecycle.

Maturity, obligations & governance

Agreed entities, markets, processing activities, policies, responsibilities and oversight arrangements.

A maturity assessment, applicability matrix and prioritised programme roadmap.

Data lifecycle & information protection

Collection, processing, storage, sharing, retention, deletion and associated systems.

An enterprise data inventory, processing maps and control improvement actions.

Privacy by design & impact assessment

Selected products, projects, analytics or AI use cases, design gates and change processes.

Impact-assessment tools, privacy engineering guidance and design checkpoints.

Rights, consent & preferences

Notices, rights intake, request fulfilment, consent where appropriate and preference changes.

Rights-management workflows, notice actions and consent or preference requirements.

Suppliers & international data flows

Vendors, processing arrangements, contractual safeguards, data locations and international sharing.

Supplier privacy toolkit, transfer review actions and accountability records.

People, incident readiness & improvement

Role-based awareness, incident escalation, investigation, notification decisions and programme reporting.

Training materials, incident playbook and ongoing review calendar.

02 / APPROACH & DELIVERABLES

From agreed scope to practical action.

Agree the context

Define business priorities, jurisdictions, processing scope and stakeholders.

Map and assess

Discover personal data flows and review maturity, safeguards and operational evidence.

Prioritise the response

Set actions around risks to individuals, obligations, business impact and dependencies.

Build the programme

Develop agreed governance, documentation, workflows and design guidance.

Enable the teams

Assign ownership, deliver awareness and walk through key operating processes.

Review and adapt

Measure progress, maintain evidence and reassess following material change.

WHAT YOU RECEIVE

For leadership & programme owners

- Privacy maturity and gap assessment with a phased roadmap.
- Jurisdiction and requirement applicability matrix.
- Governance model, responsibilities and reporting priorities.
- Review calendar and role-based awareness programme.

Operational & delivery teams

- Data inventory and lifecycle processing maps.
- Tailored policy, notice and rights-management materials.
- Impact-assessment and privacy-by-design toolkit.
- Supplier, transfer and incident-readiness procedures.

03 / PREPARATION & NEXT STEPS

Start with the right context.

Business & jurisdiction

- Identify operating entities, markets and relevant regulatory concerns.
- Confirm controller or processor roles and existing privacy ownership.

Data & evidence

- Share processing records, notices, retention schedules and system diagrams.
- Provide supplier lists, contracts and known cross-border data flows.

People & priorities

- Nominate privacy, legal, IT, HR, marketing and procurement contacts.
- Share open risks, previous incidents and upcoming projects.

Delivery & decisions

- Agree work packages, access, responsibilities and approval routes.
- Confirm when specialist legal review or system implementation is required.

PRACTICAL QUESTIONS

Is this focused on one privacy law?

No. The programme begins with your processing activities and relevant jurisdictions. Specific legal regimes and deliverables are agreed at scoping; common controls do not remove local obligations.

How is privacy different from cybersecurity?

Cybersecurity protects information and systems. Privacy also considers why personal data is used, how it affects individuals and whether practices are appropriate. The two disciplines work together.

Advisory support applies to the agreed scope. It does not guarantee compliance or regulatory approval. Specialist legal advice and formal audits are separately agreed.

Reference: NIST Privacy Framework (October 2026).

LET'S DISCUSS YOUR PRIORITIES

info@cyber360.co | cyber360.co

Contact Cyber360 to discuss your requirements.