
CYBER360 / SPECIALIST SERVICES

GDPR Compliance

Practical privacy. Sustainable accountability.

Turn privacy obligations into clear responsibilities, practical controls and evidence of progress. Cyber360 helps you map personal data, address compliance gaps and build a privacy programme that supports your business.

01 Clear scope

02 Practical evidence

03 Priorities for improvement

TRUSTED SECURITY ADVISORY

Advice that leads to action.

cyber360.co | info@cyber360.co | UK & Middle East

01 / SCOPE & FOCUS

The right question. A useful assessment.

Turn privacy obligations into clear responsibilities, practical controls and evidence of progress. Cyber360 helps you map personal data, address compliance gaps and build a privacy programme that supports your business.

Data mapping & processing records

Agreed business units, systems, processing purposes, data categories, recipients, retention and transfers.

A processing inventory and records-of-processing framework with ownership and update responsibilities.

Gap assessment & governance

Privacy policies, notices, accountability arrangements, training and selected technical and organisational measures.

A gap report, prioritised roadmap and tailored privacy documentation suite.

Individual rights & transparency

Request intake, identity checks, search and review workflows, response templates and relevant privacy notices.

A rights-request workflow, tracking register and clear responsibilities for timely responses.

DPIAs & privacy by design

Proposed processing, project approval gates, data minimisation, retention and protection measures.

DPIA templates, assessment guidance and privacy checkpoints for design and delivery.

Suppliers & international transfers

Processors, subprocessors, contractual arrangements, data locations and cross-border processing flows.

A processor oversight toolkit, contract review actions and a transfer assessment record where agreed.

Breach readiness & ongoing assurance

Breach identification, escalation, investigation, risk assessment, notification decisions and review cycles.

A breach-response playbook, decision templates, training materials and compliance review calendar.

02 / APPROACH & DELIVERABLES

From agreed scope to practical action.

Define the context

Agree jurisdictions, business activities, stakeholders and the personal-data processing to be reviewed.

Discover the data

Map processing, systems, suppliers, purposes and data flows with accountable business owners.

Assess and prioritise

Review evidence against applicable obligations and prioritise gaps by risk to individuals and delivery impact.

Build practical controls

Develop agreed documentation, workflows, DPIA tools and supplier or rights-management procedures.

Prepare your people

Assign responsibilities, deliver role-based awareness and walk through key response scenarios.

Sustain the programme

Set review dates, evidence ownership and change triggers so privacy keeps pace with the business.

WHAT YOU RECEIVE

For leadership & privacy owners

- A gap assessment and risk-prioritised implementation roadmap.
- Processing inventory and records-of-processing framework.
- Governance responsibilities and tailored policy and notice actions.
- A review calendar and role-based awareness materials.

For operational & delivery teams

- Rights-request workflows, templates and a tracking register.
- DPIA screening and assessment tools with mitigation records.
- Processor oversight and international-transfer review actions.
- Breach escalation, risk assessment and notification decision templates.

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

Does EU GDPR apply to a business outside the EU?

It can. Relevant factors include an EEA establishment, offering goods or services to people in the EEA, or monitoring their behaviour there. Application depends on the processing and role; it is not determined simply by citizenship or having an EU customer.

Consulting supports the agreed scope and jurisdictions. It does not guarantee compliance or provide regulatory approval. Specialist legal advice is separately agreed.

References: EDPB GDPR guidance; ICO breach guidance (October 2026).

Does this also cover UK GDPR?

EU GDPR and UK data protection law are separate regimes. We confirm the jurisdictions and applicable requirements at scoping. UK-specific work is agreed expressly, taking account of current UK legislation and ICO guidance.

LET'S DISCUSS YOUR PRIORITIES

info@cyber360.co | cyber360.co

UK +44 20 3286 1927 | UAE +971 55 768 7199