

Cyber Security Privacy and Data Protection

A KPMG Service for G-Cloud 15



KPMG – About us

Scale/location/technologies

Our UK Cyber team

We've worked with countless organisations across multiple sectors, including financial services, life sciences, healthcare, government, telecommunications, energy and natural resources, and legal services. Our clients range in size from start ups looking to secure their solutions and organise their security controls, through the large multinational corporations hoping to optimise their environment, innovate according to best practice and meet the growing regulatory burden.



330+ professionals

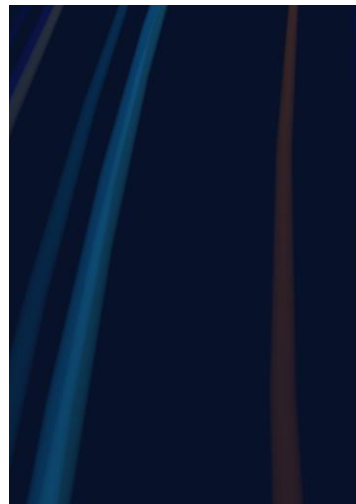
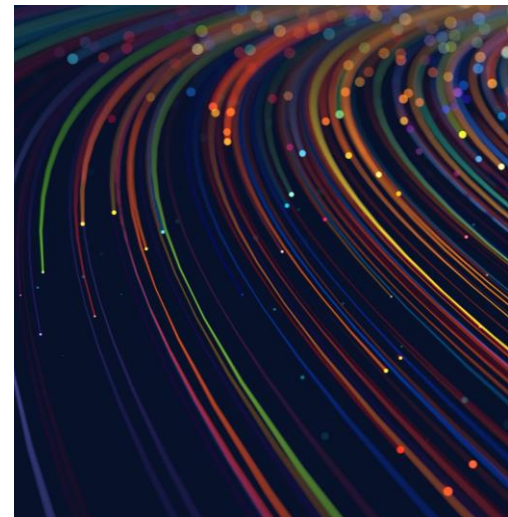
15 office locations

Part of a global team of
6200+ individuals

Our services

UK Cyber operates across 8 different service lines, catering to a wide range of governance and technical needs.

Cyber strategy 	Cyber risk 
Cyber resilience 	Privacy and data protection 
Cyber tech transformation 	Identity and access management 
Cyber defence services 	Cyber incident response 



KPMG Connected Technology

We have access to a 2000-strong team of client-facing technologists, with a diverse range of skills and experience.

Our technologists work with all the capabilities as part of the Consulting team – bringing together the diverse talents and expertise of our people, our technology, our alliance partners and our insights.

Together, we help clients to identify improvement opportunities by creating data driven insights, and develop technology strategies and drive change through our digital transformation services.

We can leverage this huge pool of talent to support the delivery of this engagement.

Cyber Security Privacy and Data Protection Service



Service Description:

KPMG's Cyber Security Privacy and Data Protection service assists organisations in managing exposure to privacy risks. We can assist with establishing a risk-based privacy framework that enables you to leverage the data you collect and process in a way that complies with the relevant legal and regulatory requirements, as well as implementing process and cultural changes.



What are the benefits of KPMG Cyber Security Privacy and Data Protection service?

- Streamlined privacy processes that align to your business.
- Create value through compliant use of personal information.
- Handle compliance requirements related to over retained data.
- Understand your organisation's privacy obligations, risks and compliance strategy.
- Be confident in decisions involving technology and personal information.
- Obtain clear view of what personal information is being processed.
- Be confident in your organisation's ability to manage data breaches.
- Gain increased trust from customers, employees and business partners.
- Gain greater speed and confidence in business decision making.
- Monitor internal and external compliance relating to privacy and security.
- Being prepared for GenAI as it is adopted and the associated risks.



Our service features

- Powered Privacy automation to orchestrate sustainable privacy operational processes.
- Identify risk areas where you may be failing to meet regulatory requirements.
- Support you to enhance and operate your key privacy processes and manage over retention of data
- Identify where personal information can be leveraged to create value.
- Find the appropriate privacy governance framework / operating model for your organization.
- Design pragmatic privacy structures and controls to manage privacy risk.
- Data discovery and harnessing privacy inventories and data mapping.
- Design record retention policies and implementation
- Develop training and awareness programmes tailored to your needs.
- Privacy impact assessments for business and technology projects/ transformation programmes.
- Assessing AI risk from Privacy and AI Governance risk assessments

KPMG Approach

Underlying approach

The **KPMG Privacy Management Framework** (diagram below) provides a practical and pragmatic structure for organising the day-to-day management and oversight of privacy activities. We use this framework to deliver privacy services to our clients and it is the basis of each of the privacy services we offer.

Privacy Principles

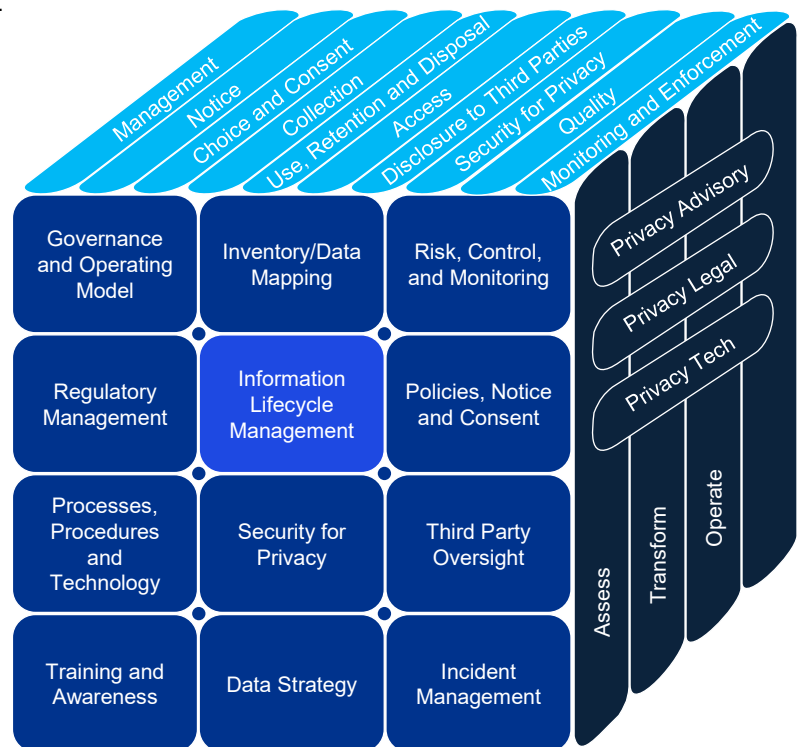
Privacy components are viewed against the internationally –recognized ‘Generally Accepted Privacy Principles’, which provide the foundation for our privacy management framework.

Privacy Management Framework

Our framework elements are the distinct components that organisations employ to help ensure compliance with applicable privacy laws and regulations. They provide a practical and pragmatic structure for organising the day-to-day management and oversight required to mitigate privacy risk exposures.

KPMG Support

Our privacy service line has been designed on the basis that organisations need tailored risk based solutions to address their individual privacy needs, risk appetite and future business strategy. Its modular and layered structure enables targeted and tailored solutions to be designed, developed, implemented and monitored consistently, cutting through the complexity of privacy and complex global organisations.



Our primary privacy services

Privacy Assessment

- Assessing your exposure to privacy risk and identify steps to remediate key areas of weakness inline with your risk appetite.
- Services include; Privacy Gap Analysis and Maturity Assessments; Privacy Audits; and, PrivacyStrategy and Roadmaps.

Privacy Transformation

- Working with you to transform your privacy compliance by implementing the necessary policies, processes and controls, which ultimately deliver your privacy strategy.
- Services include; Privacy Governance and Operating Model development; Privacy inventory and data mapping exercise; Privacy policy design; Privacy process implementation and Privacy training and awareness.

Privacy Operation

- Supporting you to enhance the operation of your key privacy processes to manage risk and drive innovation.
- Services include; Privacy Technology Deployment; Privacy Impact Assessments; Privacy Resource Augmentation; and, Privacy Incident Response.

Our Approach

Implementation Plan:

Privacy projects are delivered over five phases as follows:

Assess: In this phase the high-level scope, the project plan, the approaches and strategies for how the project will be implemented during the remainder of the project are documented and accepted. In addition, during this phase preparation for activities in the Validate phase take place.

Transform: In this phase the designs for the items in scope will be finalised, documented and accepted by the Customer to facilitate entry into the Construct phase.

Operate: In this phase the privacy processes and new products are configured, and integrations built in accordance with the design. A series of test phases collectively determine if the system was built in accordance with the design. Data is also cleansed in preparation for migration and tests will be conducted to confirm the ability to migrate and reconcile data from the legacy platforms to the new platform.

Evolve: During this phase the new platform is in production and the Customer starts operating the target processes on it, with the agreed level of post-go live Hypercare support.

Implementation Timeline

The implementation timeline is driven by a number of variables including the scale and complexity of each Customer's scope together with quality of data and availability of resources. We would agree the implementation plan, resource requirements and project milestones as part of the process of procuring our services.



Onboarding and offboarding support

The range of on-boarding activity required for clients adopting a KPMG privacy service would be agreed as part of the procurement of the service. As part of the service we build and agree a plan covering all relevant activities, planned times, durations, responsibilities, accountabilities and outputs.

Typical elements comprise:

Onboarding

- Development of the project charter, if needed, and associated project guiding principles
- Assistance to develop / articulate the case for change
- Change management and communications strategy to aid who needs to be communicated with, how and when in relation to the changes the project is planning to implement

Our cyber security strategy and transformation service includes the following components:

- Provision of orientation sessions in the Privacy Methodology, assets and principles to prepare clients teams for the program, including workshop execution
- Engagement with client teams to understand the 'as is', to take into account in change impact assessment during workshops
- Definition of collective roles and responsibilities including that for outputs
- Execution of a Project kick-off event and associated materials to formally launch the project and to aid new joiners in orientation

The migration of client data is considered on a bespoke basis in each project

Offboarding

Each implementation has a post go-live ("Evolve phase") in which KPMG will provide post go-live support working with each Clients Business as Usual (BAU) team to fully transition on-going service delivery to the Clients' BAU support team according to the agreed plan.

Why KPMG

We have a proven track record of delivering complex privacy projects for clients in a wide range of industries across the financial services, corporates and public sectors.

We are passionate about providing pragmatic advice and we understand that privacy is not standalone – it needs to work with the organisation in order to successfully identify and manage complex interdependencies and to implement change in a coordinated and manageable way.

We deep Privacy expertise, with 400+ International Association of Privacy Professionals (IAPP) members, including individual who hold the following qualifications: CIPP/E, CIPP/G, CIPP/US, CIPP/CCIPM and CIPT certifications. Our Privacy Advisory team includes consultants who have been seconded to the Information Commissioner's Office (ICO), gaining a first-hand understanding of regulatory expectations.

Case Study #1: Law enforcement

A law enforcement agency required KPMG's support with its data strategy and efforts to comply with data protection regulation. Working closely with them, we supported the development of a data strategy. We defined roles and responsibilities for the Data Office and supported the set-up of the Data Board. We aligned the data inventory with regulatory

Case Study #2: National Infrastructure

KPMG supported the client, who owns, operates and maintains the UK's national rail Infrastructure, with the redesign of their Data Storage Minimisation process for a trackside compliance system. KPMG created a process map of the current state, captured gaps and recommendations and designed a sustainable future state process which could:

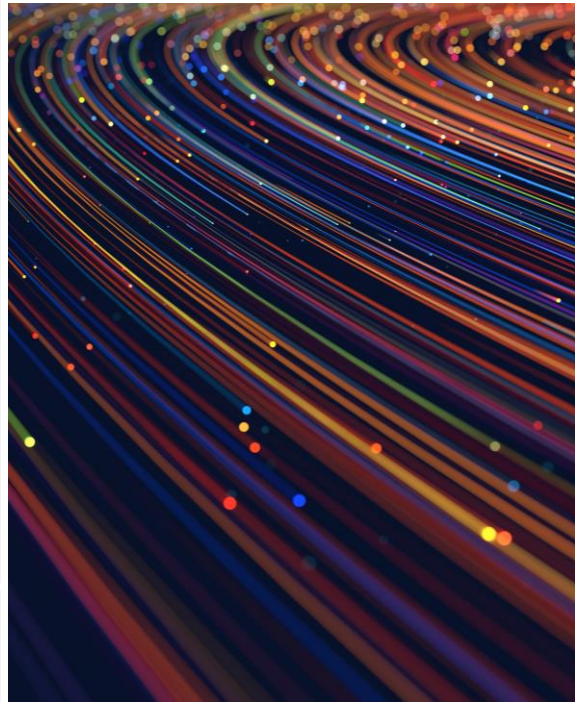
- achieve the client records retention policy and the salient GDPR requirements and;
- use technology and process automation as enablers.

A roadmap of sequenced activities was also provided to support the client embark on their journey to transition from the current to the future state.

Case Study #3: Global Pharmaceutical – Privacy Transformation Programme and Binding Corporate Rules (BCR)

With operations in over 100 countries, more than 50,000 staff were transferring personal information across global operations. Members of our team worked with this client to deliver a BCR project to legitimise international transfers. Our team:

- Ran an RFP process to secure appropriate legal support at cost effective rates.
- Provided a clear translation of the BCR requirements into tangible business requirements and delivered an effective and compelling "BCR story" which resulted in minimum comments from the BCR approving regulators.
- Produced a well managed, consolidated set of supporting documentation required by the BCR approving regulators.
- Transferred knowledge, increasing management and staff awareness of the key challenges and impacts of BCRs.



Case Study #4: Global Telecommunications and Media – Privacy Transformation Programme

KPMG One of the largest global telecommunications providers wanted to transform their approach to managing Privacy across the organisation. Members of our team leveraged our proprietary methodologies to:

- Transform the way the organisation thought about Privacy and level of risk. Develop and implement a tailored training strategy. Undertake a series of reviews across the business to identify areas of Privacy risk.
- Develop and implement a Privacy improvement programme to address the identified risk exposures in line with risk appetite. This comprised 33 improvement activities executed globally over a three year period..
- Left a flexible and sustainable approach for Privacy

Service Details

KPMG's Privacy Advisory Services help KPMG's clients to comply with regulatory requirements using KPMG's privacy and industry knowledge and technology expertise. We know Privacy and at KPMG we solve clients' problems using our expertise along with the different perspectives from KPMG's advisory, technology, risk and legal teams.

Privacy risk advisory

Privacy is not a standalone exercise. KPMG will help your privacy team to work across the enterprise in order to successfully manage complex interdependencies with other programmes and connect to strategic priorities for your business. With 400+ International Association of Privacy Professionals (IAPP) members, our global team also hold the IAPP's certifications including some of the first 50 Fellows of Information Privacy globally. We support clients across the full lifecycle of their Privacy journeys.

Privacy legal

Our KPMG Legal Services includes privacy lawyers who can work shoulder to shoulder with our advisory team in an integrated manner. We can offer support with reviewing and developing procedural documentation and legal policies, and providing a legal opinion on regulatory risk exposure and compliance obligations. We therefore have an integrated approach to provide our clients with the support and advice required to help meet regulatory requirements.

Privacy technology services

KPMG has over 5,000 Technology specialists globally, including deep integration experts, who help design, support, implement and embed privacy technology. We work closely with top technology companies and our global alliance partners, including organisations such as ServiceNow, Appian, OneTrust and BigID. Together, we collaborate to embed KPMG advice and privacy expertise into leading digital platforms. Our KPMG Privacy technology team have developed the 'Powered Privacy Gold Build' using privacy enhancing technologies to best help our clients manage and protect personal data with a range of partner vendors.

The Privacy Technology framework is divided into five pillars which aim to achieve the following:

Privacy Process Automation: Reducing the dependency on manual processes, allowing our clients to create financial and operational efficiencies and create opportunity for development..

Data Discovery Automation: Allowing our clients to discover and develop a holistic understanding of their personal data footprint for profiling, curating, creating, and updating data use cases.

Retention & Deletion: Enabling our clients to respond to regulatory expectations with how they retain and delete personal data. By governing exponential data growth whilst optimising storage costs and reducing noncompliance risks, our Retention & Deletion solutions aim to ease our clients' frustrations with data handling requirements.

Privacy Enhancing Technologies (PETs): Implementing advanced technological controls using our specialised teams in KPMG.

AI Governance: Our KPMG AI Governance framework uses our understanding of data holistically to manage our client's use of AI. Our inhouse experts can leverage industry leading technology, approaches, and tools to enable the use of AI without increasing risk of noncompliance.

Service Details

Privacy risk advisory in detail

Strategy, Design & Roadmap: comprehensive data protection strategies and plans to assess, implement, and enhance privacy operations in organisations, ensuring regulatory compliance.

Gap & Maturity Assessments: Analysis of existing material and gap identification in accordance to internal or external requirements.

DPO as a Service: Supporting internal data privacy processes in the place of a DPO.

Asset Inventory & Management

ROPA & Data Mapping: Supporting creation or completion of RoPa or Data mapping exercises to identify data locations.

Inventory / Data Catalogue: Supporting the creation or completion of data inventories for IT assets and data classification.

Data Discovery: Manual or technology based data discovery across multiple systems and categorization via tagging.

Retention & Deletion: Updating of retention and destruction policies and ensuring over retained documents are deleted.

Privacy Risk Management

Risk & Control Management: SME support analysing and assessing current risk and controls and offering solutions to increase maturity.

Audits: Providing SME analysis of current landscape in accordance to KPMG 12 domains within the Privacy Framework.

Regulatory Management

Regulatory Request Management: Providing support and assistance for regulatory requests from data protection supervisory authorities

Incident & Breach Management: Assisting in setting up robust protocols for handling data security incidents, minimizing privacy risks, ensuring compliance, and maintaining trust through prompt action in identifying, notifying, and resolving potential data compromises.



Notice & Consent Management

Choice & Consent Management: Analysis of current consent mechanisms including but not limited too cookie consent and offering solutions for BAU collection.

Security for Privacy

Privacy Assessments: Supporting or completing DPIAs/PIAs/LIAs/TIAs and introducing a process to continue into BAU.

Security for Privacy (PET): Providing SME analysis on data security tools implementations for IAM, Encryption, data lost prevention, and other privacy enhancing technologies.

Third Party Risk Management Support and analysis of current Third party data privacy risk management processes and providing new and improved procedures and policies.

Data Subject Requests SME support and resource help in designing and responding to DSR requests within a company including process automation.

Manage Privacy Processes

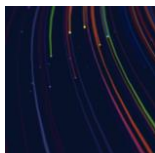
Governance & Policies, SOPs: SME review of current policy suite and offerings of improvements/re-writes.

Monitoring & Reporting KPIs: SME support defining reporting dashboards, metric collation and key performance indicators

Data Transfers & Data Sovereignty: Analysis of current international data transfers and collaborative review with the legal team.

Privacy Training & Awareness: SME led sessions covering data privacy topics to be delivered to various internal client teams.

AI Governance & Ethics: Our KPMG Trusted AI Framework uses our understanding of data holistically to manage our client's use of AI. Our inhouse experts can leverage industry leading technology, approaches, and tools to enable the use of AI without increasing risk of noncompliance.





kpmg.com/uk

© 2026 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. Document Classification: KPMG Confidential

Document Classification: KPMG Confidential

CREATE. | CRT164925A January 2026