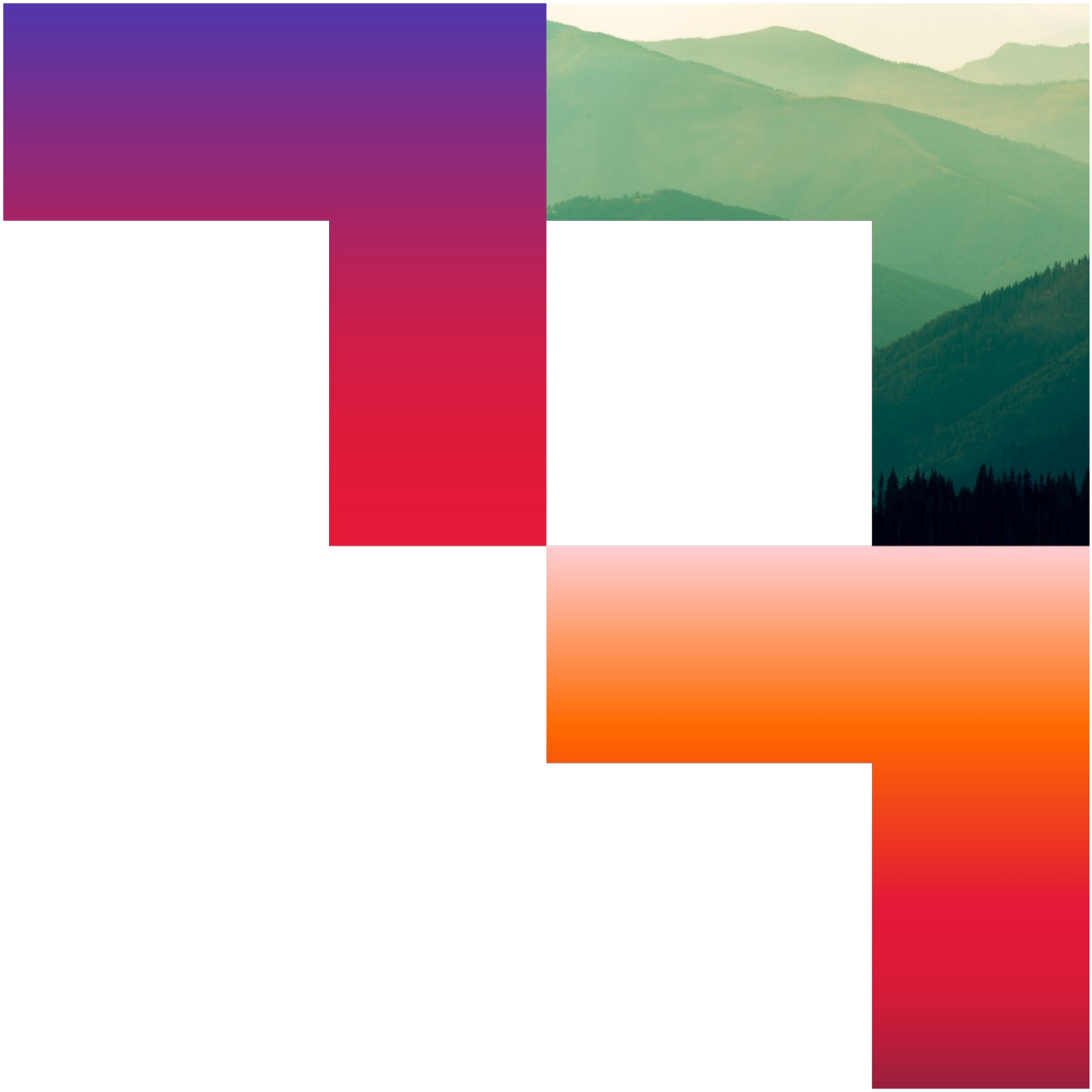


Data Privacy Impact Assessment (DPIA)

Contracting body

30 Jan 2026

Issue 1.0

Table of contents

Service Definition overview

A Data Privacy Impact Assessment (DPIA) is a key assessment in risk management and demonstrating compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) of 2018 within the UK. For organisations with operations or establishments within the European Union, DPIAs are also a mandatory requirement under the EU GDPR, which remains closely aligned with UK GDPR but is overseen by EU supervisory authorities.

Completion of a DPIA should be undertaken by an experienced practitioner for all personal data that any organisation is collating, or processing to ensure appropriate controls are implemented.

CGI can draw upon a team of experienced consultants who have extensive privacy experience as Data Protection Officer's (DPOs) and who are certified practitioners in GDPR and DPA. This includes experience supporting organisations that must comply with both UK GDPR and EU GDPR, ensuring consistency while accounting for jurisdictional differences in regulatory oversight and enforcement.

Our DPIA service builds on our cyber security background by utilising our member expertise who have undertaken this process for a wide range of organisations and ensuring you have a full impact assessment of your personal data holdings. This will assist with the risk management process to ensure that your organisation protects against a GDPR breach. Where required, assessments can be structured to address both UK and EU GDPR obligations, supporting multinational organisations with a harmonised and defensible approach to privacy risk management.

Why CGI?

For over 40 years, CGI has helped secure government and commercial clients and delivered some of the most complex technology projects and services. We have over 1,700 cyber security experts globally with one of the largest cyber security practices in the UK helping clients manage complex security challenges with a business-focussed approach, protecting what is most valuable to them. Ensuring organisations are resilient against cyber-attacks and protecting data accordingly has become one of the most important challenges facing senior management.

We understand security from all angles - technology, business, and compliance. Our specialists build cyber security into business to drive agility, efficiency, and competitive advantage. Our services enable innovation and help organisations with privacy and business resilience.

Cyber threats are global, but security requirements and data privacy legislation are different in local markets. For our clients, we are a local security partner who understands the industry and sector environments, but we also have a global view and multi-country experience to be able to defend against future attacks and support the assurance regimes. Whether serving the public or growing the economy in this digital world, CGI gives clients the peace of mind to focus on what's most important to them - protecting citizens and customers and operating with confidence.

1. Service Description

In the information age, the innovative use of information technology continues to drive transformation and efficiency across both public and commercial sectors. The widespread adoption of cloud-based services—including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—has accelerated this progress, resulting in increasing volumes of personal and sensitive data being collected and processed. With this growth comes heightened responsibility for the lawful collection, retention, sharing, and disposal of data, often within complex cloud environments that present additional challenges for the consistent application and oversight of security controls, particularly in the face of an evolving threat landscape. For organisations operating across borders, this complexity is amplified by the need to comply with multiple data protection regimes, including both UK GDPR and EU GDPR, particularly where data is transferred between jurisdictions.

In response to these risks, privacy and data protection legislation has been strengthened globally. The General Data Protection Regulation (GDPR), introduced in 2016, and the UK Data Protection Act 2018 together form the foundation of the UK's data protection framework. These regulations place clear obligations on organisations to protect personal data and to demonstrate accountability in how data is processed. Following the UK's exit from the EU, EU GDPR continues to apply separately to organisations established in the EU or processing the personal data of EU residents, requiring careful consideration of parallel compliance obligations.

The Data Protection Act 2018 provides a comprehensive framework for data protection in the UK, strengthening sanctions for non-compliance and addressing areas beyond EU law, including law enforcement and intelligence processing. It ensures that the rights of individuals are appropriately protected while enabling lawful data use in support of public interest functions. EU GDPR operates alongside national legislation within EU Member States, and organisations with EU operations must ensure that DPIAs reflect any additional local regulatory requirements or supervisory authority expectations.

Organisations must therefore consider UK GDPR and the Data Protection Act 2018 together, particularly in sectors such as health, education, and law enforcement, where sensitive personal data is routinely processed. Both frameworks collectively govern how personal data must be managed throughout its lifecycle. Where EU operations exist, organisations must also align these practices with EU GDPR principles to ensure consistent protection of personal data across all jurisdictions.

The increasing use of cloud services and data-driven solutions has further heightened the relevance of data protection obligations for organisations. Compliance now requires ongoing governance, risk management, and demonstrable controls, rather than one-off implementation activity. This ongoing approach is equally expected by both UK and EU regulators, with DPIAs forming a central component of accountability under each regime.

Key challenges introduced by UK GDPR include:

- Financial penalties of up to 4% of global annual turnover or £17.5 million/€20 million, whichever is higher
- Mandatory breach notification to the relevant supervisory authority within 72 hours
- Extended obligations for both data controllers and data processors
- Expanded territorial scope, including obligations for organisations outside the UK that process UK residents' data
- A broader definition of personal data
- Enhanced rights for individuals, including data portability, accuracy, and erasure
- A requirement to evidence due diligence through ongoing risk management and controls.

These requirements broadly mirror those under EU GDPR, with similar penalty thresholds, breach notification obligations, and accountability expectations enforced by EU supervisory authorities.

CGI has more than 40 years' experience delivering complex and secure data solutions for government and commercial clients. As a leading provider of cyber security and data protection services in the UK, CGI is well placed to support organisations in meeting their Data Protection Impact Assessment (DPIA) obligations. This includes supporting clients with multinational footprints who must demonstrate compliance with both UK GDPR and EU GDPR in a consistent and auditable manner

As part of CGI's cyber security and data privacy services, we work with clients to identify what data is most valuable, how and where it is processed, and where vulnerabilities may exist, including through data sharing arrangements. While DPIAs were previously considered good practice, UK GDPR mandates their use where processing is likely to result in a high risk to individuals' rights and freedoms. EU GDPR contains equivalent requirements, making DPIAs a critical control for organisations processing EU personal data at scale or engaging in high-risk processing activities.

A DPIA is a structured assessment of specific business processes, applications, or systems. It maps data flows within the organisation and to third-party suppliers, identifies privacy risks, and defines appropriate mitigation measures. Where data flows cross national boundaries, DPIAs also support the identification and management of international data transfer risks under both UK and EU GDPR.

In line with UK GDPR, ISO/IEC 27001, and relevant government security frameworks, CGI's DPIA service will:

- Determine whether a DPIA is required
- Document data flows through workshops and stakeholder engagement
- Identify privacy and information security risks
- Assess and recommend appropriate mitigation measures
- Consider external and emerging data protection factors
- Integrate outcomes into project and operational plans
- Produce a final report including findings, recommendations, and an action plan.

Beyond regulatory compliance, DPIAs deliver additional benefits, including:

- Reducing the likelihood and impact of financial penalties
- Clarifying accountability between data controllers and processors
- Improving readiness for Data Subject Access Requests and erasure requests
- Embedding privacy by design into systems and architectures
- Reducing reputational risk associated with data breaches
- Providing assurance that third-party suppliers manage data appropriately.

For organisations operating internationally, DPIAs also provide confidence that privacy risks are being managed consistently across UK and EU regulatory environments.

2. Data backup and restore

CGI can carry out backup and restore activities in accordance with any specific requirements and in compliance with the Information Assurance Backup / Restore policies as defined in ISO 27001; any information that has been processed as part of an engagement will be stored securely. Where applicable, this information can then be restored from an appropriate back-up, should the need arise.

3. Service Continuity

CGI will agree appropriate service continuity in accordance with any specific requirements, and any conditions that need to be met.

4. Onboarding and Offboarding

4.1. Onboarding

For Specialist Cloud Services, CGI will engage directly with the client to ensure the full scope of the requirements is understood and agreed in advance of any engagement. We will work with senior stakeholders to define the necessary business outcomes and ensure the services are aligned accordingly.

For all services, CGI understands the client's requirements and make on-boarding specific to these needs, using the experience, lessons learnt and methodology from many years of public sector transition experience,

we can quickly align to client joiners, movers and leavers policies and ensure that we have appropriately cleared staff for every engagement.

4.2. Offboarding

Off-boarding is instigated by a client request or after expiration of the service agreement.

4.2.1. Access to data upon exit

Deletion of any virtual machine image and data will occur in line with the service agreement. Any required data will be made available using appropriate media, in line with the data security classification. After client notification that data has been successfully recovered, CGI will purge and destroy client data from any computer or storage device or media that remains part of CGI's estate, with the exception of any data related to a data retention agreement between a client and CGI.

5. Service constraints

CGI will work with you to define and tailor the services to meet your specific requirements. During this definition period, detailed responsibilities will be agreed across the service delivery. Examples of common general constraints are listed below:

Share the existing internal sponsorship and governance for Information Assurance.

Assign or appoint a suitably skilled and empowered person to act as the receiving client.

Provide appropriate access to its policies, processes and standards for the Information Assurance service and other suppliers.

Provide timely information relating to its business plans, goals and projects.

As a main feature of any Service will necessitate an on-going dialogue with client representatives, the most important responsibility of the Contracting Body is to ensure the timely availability of individuals for fact-finding interviews.

6. Service levels

The overall accountability for the relationship with the client lies with CGI’s Executive Sponsor and CGI Account Manager and they will provide strategic governance to the service working closely with the client's Senior Executive team or nominated delivery / engagement contact. The purpose of this team is to ensure that the relationship is collaborative, the service is delivering, as agreed, the governance model is working, and best practice is being applied.

7. Hosting options and locations

CGI has a network of 21 offices across the United Kingdom and Northern Ireland, with our UK members having the capability to deliver as hybrid-workers. Through our engagements we also understand that for some clients it is essential that our members are physically present on their sites, our distributed network of offices makes this possible. Whatever your requirements are the options for hosting and locations will be agreed at contract negotiations.

8. Security

CGI has invested significant resources to develop an Enterprise Security Management Framework (ESMF) based on recognized industry standards and applicable regulations or legislation such as ISO 27001, ISO27701, NIST, COBIT, CIS, CCPA and GDPR to name but a few. This framework is used across the global organization to protect information assets, technologies, facilities, and CGI members, including the data

managed across the business, and is supported by CGI's security and privacy policies, standards and controls (Security Baseline) which are implemented through our processes, practices, services, solutions and our interactions with any third parties working on behalf of CGI.

Across the CGI business, the technical and organizational measures are defined using a risk-based approach. This considers the nature, scope, context and purposes of processing as well as the risk to the rights and freedoms of natural persons, where CGI is acting as either the data controller or data processor. This ensures a level of security and privacy appropriate to the risk, in situations where CGI holds responsibility and accountability for personal data processing.

CGI's ESMF Security Baseline is the minimum-security standard for all CGI offerings (including cloud-based services) to be applied by both CGI and clients. In some cases, CGI Security or Data Privacy may wish to add additional controls e.g. where sensitive personal data is involved. Where CGI or our clients agree to strengthen the level of security or privacy to consider specific requirements (risks, regulatory requirements, etc.) these additional security or protective measures will be defined within the CGI contracted services, particularly where CGI may be acting as data processor on behalf of a client.

9. Service Pricing and Terms and Conditions

9.1. Pricing

Please refer to the G-Cloud 15 portal for the rates available.

9.2. Terms and Conditions

Please refer to the associated Terms and Conditions Document relevant for this Service including termination by the Buyer or Supplier.

10. Further information

For more information about this or any of our G-Cloud services, please contact us:

Phone: +44 0845 070 7765. Ask to speak to the G-Cloud team.

Email: uk.gen.ccsframeworks@cgi.com, including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.

We will prepare a quotation for you. Once the quotation is agreed upon, we will issue you the necessary documentation (as required by the G-Cloud Framework) and ask you to provide us with a purchase order.

Once we have received your purchase order, the services will be configured to the requirements agreed with invoices issued to you for the services procured. On a monthly basis, we will also complete the mandated management information reports to Government Procurement.

PROPRIETARY AND CONFIDENTIAL

The information in this proposal is submitted on 30 Jan 2026 - Issue 1.0 on behalf of CGI by the following authorised representative:

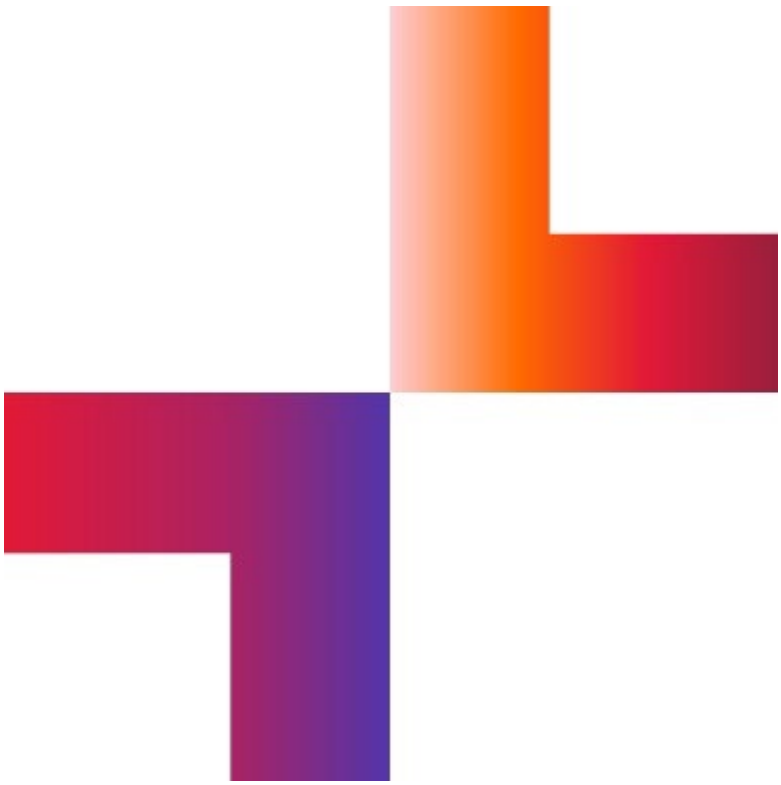
Simon Figg

Frameworks Manager

CGI IT UK Ltd

14th Floor, 20 Fenchurch Street, London, EC3M 3BY

Tel: +44 0845 070 7765



cgi.com/uk