



General Data Protection Regulation (GDPR) Compliance Assessment

Contracting body

30 Jan 2026

Issue 2.0

Table of contents

1.	Service Description	4
2.	Data backup and restore	5
3.	Service Continuity	5
4.	Onboarding and Offboarding	5
4.1.	Onboarding	5
4.2.	Offboarding	5
5.	Service constraints	5
6.	Service levels	6
7.	Hosting options and locations	6
8.	Security	6
9.	Service Pricing and Terms and Conditions	6
9.1.	Pricing	6
9.2.	Terms and Conditions	7
10.	Further information	7
PROPRIETARY AND CONFIDENTIAL		8

Service Definition overview

Creative use of information technology continues to drive innovation and operational effectiveness 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 data being collected and processed. With this growth comes clear responsibilities for the lawful collection, retention, sharing, and disposal of data. Much of this data is processed within cloud environments, where the consistent application and oversight of recognised security controls can be challenging, particularly in the context of an evolving threat landscape.

As part of CGI's cyber security information and data privacy services, we work with clients to identify current compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 18), by conducting assessments and assurance activity to identify what data and information is most valuable, where and how it is held, what data could be vulnerable through sharing and identifying any remediation actions that should be taken to continue to protect the data and information processed.

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. Our 'GDPR Compliance Assessment' builds on this solid background by amplifying our security management capabilities and dovetailing with our comprehensive suite of related Cyber Services.

CGI Cyber Security has significant in-house GDPR expertise and has undertaken this form of security leadership for a wide range of organisations, ranging from highly sensitive government organisations, through regulated industries, to large commercial enterprises and technology-oriented entrepreneurial businesses.

1. Service Description

CGI has an established and tested methodology for undertaking technical security assessments analyses. This adapts an enterprise architecture approach to the information security domain, and it leverages our extensive experience in undertaking security assessments for UK Government and CNI clients. ISO/IEC 27000 and 27701, ISF, COBIT, CAF and ITIL standards and frameworks are combined with national and local regulatory requirements and good practice guidance for the domain under analysis.

The UK General Data Protection Regulation (UK GDPR), together with the Data Protection Act 2018, has far-reaching implications for the management of personal data within both public and commercial organisations. These requirements demand demonstrable accountability, effective governance, and ongoing management of privacy risks.

Some of these challenges are:

- Financial penalties of up to £17.5 million or 4% of global annual turnover, whichever is higher.
- Mandatory notification of personal data breaches to the Information Commissioner's Office within 72 hours where required.
- Extended and clarified obligations for both data controllers and data processors, including in cloud-based service models.
- Expanded territorial scope where organisations process UK residents' personal data.
- A broader definition of personal data and strengthened individual rights.
- Enhanced rights relating to data portability, accuracy, and erasure.
- A requirement to evidence due diligence through continuous risk management and appropriate technical and organisational controls.

CGI's comprehensive data privacy review enables organisations to understand their current compliance posture and determine whether additional support is required to meet UK GDPR obligations or to prepare for alignment with ISO/IEC 27001 and ISO/IEC 27701 certifications.

The reviews will be completed through a series of structured interviews, documentation review (policies, procedures, and data protection registrations) and understanding relevant systems controls and technical capabilities, working with our clients' teams to assess the procedural and IT controls in place.

The method hinges on development of the 'As-Is' and 'To-Be' views of the data privacy state, with the to-be view being driven by UK GDPR and the Data Protection Act 2018. A gap analysis, accounting for programmatic constraints then develops a portfolio of prioritised improvements that will inform development of a strategy and roadmap to close the gaps.

CGI will deliver the following:

- Documentation of the as-is (current) privacy / data protection state.
- Identification of individuals with responsibility and accountability for the protection of privacy information.
- Identification of processes and systems that process personal and sensitive information.
- Identification and documentation of privacy data protection controls relevant to meeting the regulatory and legislative requirements for the protection of privacy data and for mitigating the risks of a breach to privacy information.
- A populated risk model to underpin the findings and recommendations of the review.
- Documentation of the to-be (target) privacy state. This will include a defined set of processes for the protection of privacy information, covering:
 - Identification of individuals with responsibility and accountability for the protection of privacy information.
 - Recommended procedural and technical controls.
 - Draft privacy strategy and outline policy documentation.
- A recommended roadmap and supporting plan to achieve the 'target state'. The roadmap will set out a coherent programme of improvements to achieve the 'to-be' state.
- A Data Privacy Review Report that will document the analysis undertaken and decisions made during the course of the review.

CGI adopts a collaborative approach throughout the engagement. Validation workshops are used to confirm findings and agree deliverables, ensuring organisations are equipped with clear, actionable information to manage privacy risks effectively. The resulting strategy and roadmap support prioritised, confidence-based risk reduction activities that can be progressed without delay.

2. Data backup and restore

CGI can carry out backup and restore activities in accordance with any specific requirements and in compliance with the IA 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 takes into account 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 take into account 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 contained in this document is confidential to CGI and/or CGI group companies. This document shall not be reproduced in any form or by any mechanical or electronic means, including electronic archival systems, or submitted to a generative AI tool without the prior written approval of CGI. The receiving party may use this document and the information contained in it for the purpose of evaluating CGI's proposal only. Any personal data included in this document must not be replicated, stored or distributed beyond the immediate recipient or used for any purpose other than evaluating the document.

This proposal is subject to contract and shall not be binding unless and until execution by CGI and Contracting body of a final agreement to the proposal, containing the terms and conditions that will govern the relationship between the parties. Any final agreement is conditional (inter alia) upon due diligence and customary business investigations by CGI. The results of such due diligence and/or investigations may impact upon content of this proposal, including the business structure, business terms and financial arrangements.

If you have received this document by mistake, note that the reading, the reproduction or the distribution of this document is strictly forbidden. You are hereby requested to inform us by telephone at +44 0845 070 7765 and to return this document by special delivery marked for the attention of Simon Figg.

Except where indicated otherwise, all names, trademarks, logos and brands (registered or not) referred to in this document are the property of a company in the CGI group or its licensors.

The information in this proposal is submitted on 30 Jan 2026 - Issue 2.0 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

