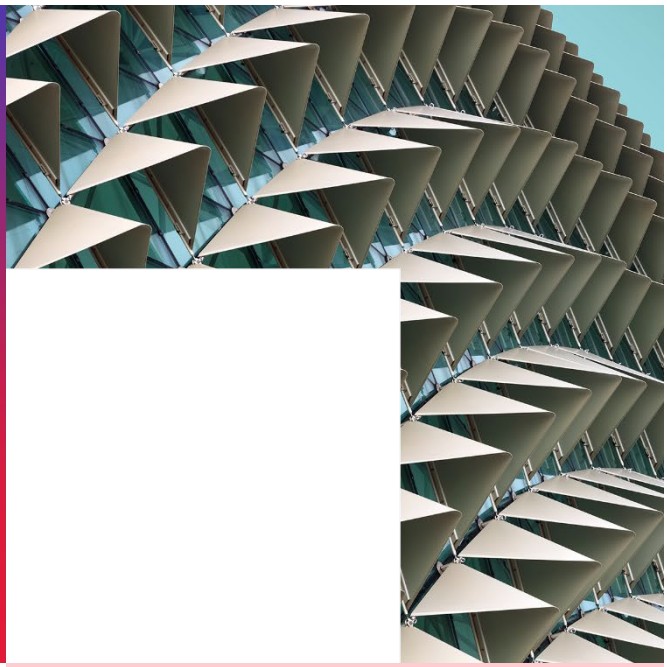


BCR C – CGI – Appendix G Privacy Impact Assessment Standard

1. PURPOSE

The adoption of the BCR-C by CGI and the commitment from CGI Entities to comply with the BCR-C demonstrate that CGI intends to provide a high level of protection to the Personal Data it Processes.

This document describes how a CGI Entity, as a Data Controller, shall implement a Privacy Impact Assessment procedure mainly as a preventative measure to ensure that its Processing of Personal Data aligns with the Applicable Data Protection Legislation and best practices. It has been developed with reference to the current guidance published by the Supervisory Authorities and international standard organizations.

This procedure shall enable CGI to:

- Identify which Processing is likely to present a high risk for the protection of Personal Data;
- Assess the level of compliance of the Processing it implements with the Applicable Data Protection Legislation;
- Assess the level of risk on individuals' rights associated with the Processing (severity, likelihood);
- Determine the corrective measures to be implemented in order to ensure that Personal Data is Processed with risks that are mitigated and performed in compliance with applicable laws;
- Approve or reject the Processing considering the residual risks.

2. DEFINITIONS

The terms used herein with capital letters have the same meaning as in the BCR-C.

Privacy Impact Assessment (PIA) or Data Protection Impact Assessment (DPIA): is the overall process of identifying, analyzing, evaluating, consulting, communicating and planning the treatment/management of potential privacy impacts with regard to the Processing of Personal Data.

3. SCOPE

Where CGI is the Data Controller, CGI will perform a PIA for new and existing Processing:

a) where there is a high risk to the rights and freedoms of individuals, and
b) where the Processing has not already been covered by another PIA, as it reflects a similar set of Processing instructions; or
c) to address the impact of a technology product for which CGI has the IP, if commercially expedient;
d) where CGI's internal policies dictate that in order to address the risk and assure compliance with the Applicable Data Protection Legislation a PIA is required.

These criteria are detailed further in Appendix A.

When acting as a Data Processor, CGI may be required by its clients to cooperate and provide relevant information to enable the client to conduct a Privacy Impact Assessment. CGI shall provide its clients with all relevant information it has **while making sure that it does not provide legal advice in the performance of the impact assessment which shall remain the client's sole responsibility**. The guidance in this procedure may also be applied where CGI contributes to a client driven Privacy Impact Assessments where CGI is, or will be, a Data Processor. In this case, it is important to keep in mind that performing a DPIA is a project *per se* requiring time and resources. Consequently, the related cost must be discussed with the client.

4. METHODOLOGY

❖ AT WHAT POINT(S) IN THE PROJECT LIFECYCLE WILL CGI PERFORM A PIA?

The PIA is one of the essential elements of the principles of Privacy by Design and Default. It encompasses the system development, the operation and the supporting manual processes.

It is a requirement that the risks and mitigations are identified and addressed before the Processing begins.

However, also:

a) it is an industry accepted principle that the earlier within the lifecycle that requirements are identified then the more cost effective is their implementation;

b) to more accurately cost a project, the mitigations must be considered before significant financial commitment is made to the project therefore the initial PIA must be performed as early in the project lifecycle as possible, and reviewed at key points, e.g. at proposal time, project startup time, as part of system design, before solution sign off and implementation;

c) a PIA must evolve with the system and processes. It is not a one-off exercise so it must be revisited if there is a change to the privacy risk profile; e.g., a change to the data collected, introduction of different technology, a change of use of the data, disclosure to different people.

❖ WHO WILL BE RESPONSIBLE AND INVOLVED IN THE PIA?

An appropriately skilled person responsible for conducting the PIA must be identified and appointed by the Project Manager. Appropriate skills include organizational skills, risk management skills, understanding of Privacy and information security.

The person accountable for signing off the PIA will be:

- For local and regional projects - the Business Unit Leader with final approval by the SBU President.
- For regional projects – the SBU President.
- For Corporate projects - Corporate Services Leader.

Stakeholders will be engaged in the PIA as necessary depending on their potential contribution, influence and the impact of the system and may include:

- impacted business teams e.g. HR, legal, information security, finance, communications and internal audit;
- the CIO Office;
- internal and external sub-contractors and business partners;
- system specialists including architects and designers, database administrators, physical and technical security specialists, computer or network administrators, application operators, computer or network operators;
- CGI Privacy Team.

Responsibilities are further described in Appendix B – PIA RACI.

5. SCALABILITY

- Individuals' rights apply in full irrespective of the level of risk in the Processing. Organizations are required to modulate their data protection compliance (e.g. performance of a PIA) according to the level of risk that their Personal Data Processing operations pose to the fundamental rights and freedoms of individuals.

- The required compliance and accountability measures must take into account **the nature, scope, context and purposes of the Processing**, i.e. a risk-based approach where the mitigations are linked to the specifics of a particular Processing operation.

- To that end, the Data Processing Inventory Tool help the project owner to evaluate risks and identifies the requirement to perform a full PIA and, within the PIA, the Assessor/PIA Coordinator must align the compliance measures to the level of risk.

6. THE PIA PROCESS

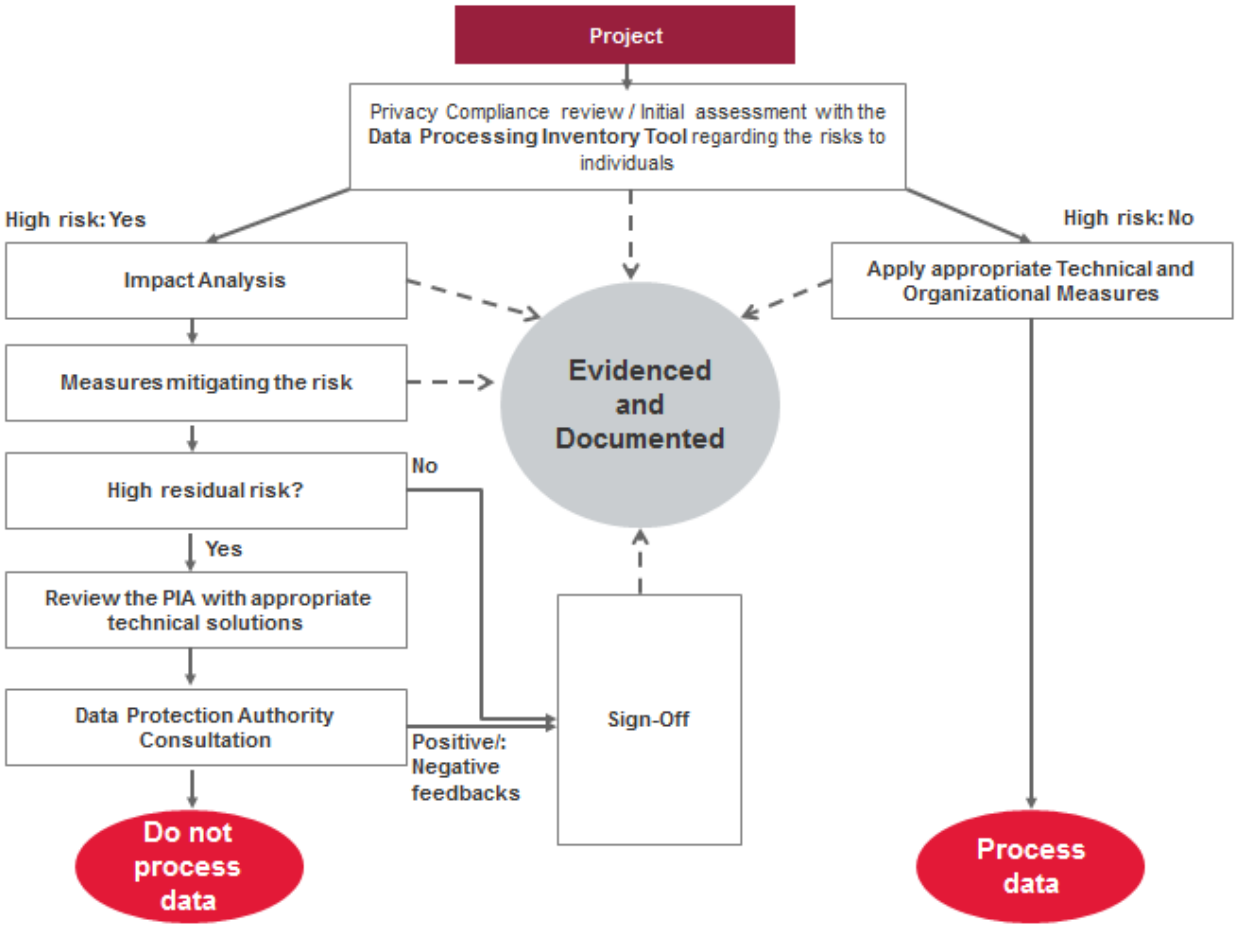


Figure 1: PIA process overview.

The PIA and associated documentation will include:

i. a technical and functional description of the Processing and data flows;
ii. an identification of the benefits the Processing will bring;
iii. a comparison of the Processing against the GDPR privacy requirements;
iv. an analysis of the privacy risk;
v. the risks mitigation plan;
vi. sign-off of the PIA by the responsible Business Unit or Corporate Services Leader;
vii. a record of the conduct and outcome of the PIA.

The outcome of the PIA will indicate if the Processing may occur given the residual risks. If there are high residual risks, even once the mitigating measures are applied, the Chief Privacy Officer must be consulted and then CGI may choose to either a) deny permission for the Processing or b) consult with the Supervisory Authority to seek its advice.

In such circumstances the Processing may not occur until Supervisory Authority positive feedback is received.

❖ MONITORING COMPLIANCE WITH PIA

Compliance is addressed as part of CGI's 3 lines of defense (see CGI Data Privacy Audit Process). In addition to the Business Unit controls, that compliance regime identifies areas of scope for a Privacy Audit specifically:

a) 'Planning of Personal Data Management', which includes compliance to this Privacy Impact Assessment Procedure; and
b) 'Embed Data Privacy into the Operations', to assure that the mitigations identified in the PIA are implemented and effective.

❖ PUBLICIZING THE OUTCOMES

Where CGI acts as a Data Controller, it will make readily available to Data Subjects the information as specified in the Transparency section of the BCR-C.

CGI will hold the PIA documentation confidential, but available to the Supervisory Authority on request.

❖ PIA DOCUMENT TEMPLATE

To ensure consistency of approach to the PIA, CGI provides a template to support performance of the PIA. This template must be used with minimal tailoring and only with the prior approval of CGI Privacy Team.

APPENDIX A: CRITERIA TO TRIGGER A PIA

PIAs are required when there is a "High Risk" to the rights and freedoms of individuals i.e. where Personal Data Processing could lead to "physical, material or non-material damage".

A non-exhaustive list of examples of "physical, material or non-material damage" and of Processing activities that could result in such damage, and therefore introduce risk, includes:

- Discrimination or stigmatisation;
- Reputation damage ;
- Bodily harm;
- Damage to earning power and financial loss ;
- Identity theft / fraud;
- Loss of liberty or freedom of movement ;
- Loss of confidentiality of Personal Data ;
- Chilling effect on freedom of speech, association, etc.;
- Personal, family, workplace or social fear, embarrassment, apprehension or anxiety;
- Curtailing of personal choice or intrusion into private life;
- Unauthorized reversal of pseudonymisation;
- Individuals deprived of rights and freedoms, or prevented from exercising control over their data
- Any other significant economic or social disadvantage.

Where the initial risk assessment indicates there is a likelihood of any of these risks materializing, the Processing must be referred to CGI Privacy Team who will determine, based on guidelines, whether a PIA is required.

- Processing Sensitive Personal Data, including data on racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership; genetic data; biometric data, health data; data concerning sex life; or data on criminal convictions and offences or related security measures, being understood that the Processing of Personal Data relating to criminal convictions and offences shall be prohibited, unless authorised by EEA or Member State law;
- Profiling where personal aspects are evaluated to create or use personal profiles (e.g. analyze or predict work performance, economic situation, health, personal preferences or interests, reliability or behavior, location or movements); or other systematic and extensive evaluation of personal aspects based on automated processing on which decisions are based that produce legal effects such as exclusion or discrimination;
- Processing children's and vulnerable persons' Personal Data;
- Processing large amounts of Personal Data affecting large numbers of individuals;
- Monitoring behaviors or activities, particularly online activity, attendance.
- Processing using new technologies such deep learning, AI, etc. (e.g. that trigger unknown personal & social consequences)
- Systematic monitoring of a publicly accessible area.

Additionally risk may arise where:

- a new “kind” of Personal Data Processing operation is introduced where no PIA has been conducted (e.g. “Big Data”); or
- significant time (2 years) has elapsed since the Processing was initiated and the initial PIA was performed; or
- Processing operations were initiated before the current BCR-C, and this procedure, were adopted; or
- there are risks to individual’s rights (and ultimately to CGI’s business) arising from :
    - unjustifiable or excessive collection of Personal Data;
    - use or storage of inaccurate or out-dated data;
    - inappropriate use or misuse of Personal Data, including:
        a) use of Personal Data beyond individuals’ reasonable expectations by matching or combination of different Processing operations;
        b) unusual use of Personal Data beyond societal norms, where any reasonable individual in this context would object; or
        c) unjustifiable inference or decision-making, which the organization cannot objectively defend;
    - lost or stolen Personal Data or destruction and alteration of Personal Data.
    - unjustifiable or unauthorized access, transfer, sharing or publishing of Personal Data.
    - Accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data.
    - The Processing operation aims at preventing individuals from exercising a right or using a service or a contract

However, the initial risk assessment could reveal that the need for a PIA has to be challenged. In particular where:

a) following the initial risk assessment the Processing is demonstrably similar to a set of operations for which a current, recent PIA exists then the responsible Business Unit or Corporate Services Leader, in consultation with the Data Protection Officer, may record the decision and rationale for not duplicating the risk assessment (i.e. the PIA);
b) the Processing utilizes a technology product for which a relevant PIA has been performed and provided to CGI which completely covers the circumstances of the products implementation within CGI. In other cases such a PIA may form, by adoption of the relevant mitigations, a significant contribution to a full PIA performed by the assessor.

APPENDIX B: PIA RACI (RESPONSIBLE; ACCOUNTABLE; CONSULTED; INFORMED)

PIA process - RACI							
R = Responsible A = Accountable C = Consulted I = Informed	Project Manager	Assessor/ PIA coordinator	Business Owner*	CGI Privacy Team	CIO	Other Stakeholders (please specify)	Notes: * may be SBU, BU or Corporate Services Leader holding legal responsibility
Performs DPIA Screening	A / R		I	I			
Assess outcome of DPIA screening	A / R		C	C			
Appoint Assessor	A / R	C	I				
Lead & Document DPIA	A	R					
DPIA participation	A / C	R	C	C	C	C	
Approve DPIA outcome	C	C	A / R	C	C	I	*Other local law may require formal approval.

COMMUNICATION

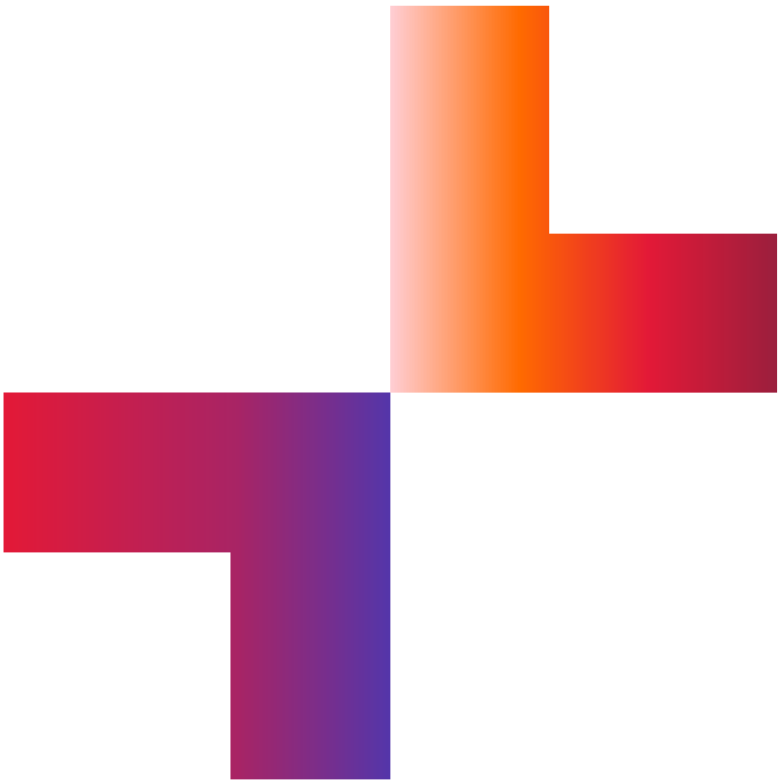
All requests regarding this process should be addressed to privacy@cgi.com.

REFERENCES

POLICY OWNER	APPROVING AUTHORITY
Chief Privacy Officer	Chief Privacy Officer

REVISION HISTORY

VERSION	DATE	DESCRIPTION
1.0		Initial Version
1.1	01.2020	Review – No Changes
1.2	03.2021	Title change CDPO to CPO
1.3	11.2022	Annual Review – No changes
1.4	03-2025	Annual Review – Textual changes; update of the contact email
1.5	06-2026	Annual review – No changes



cgi.com