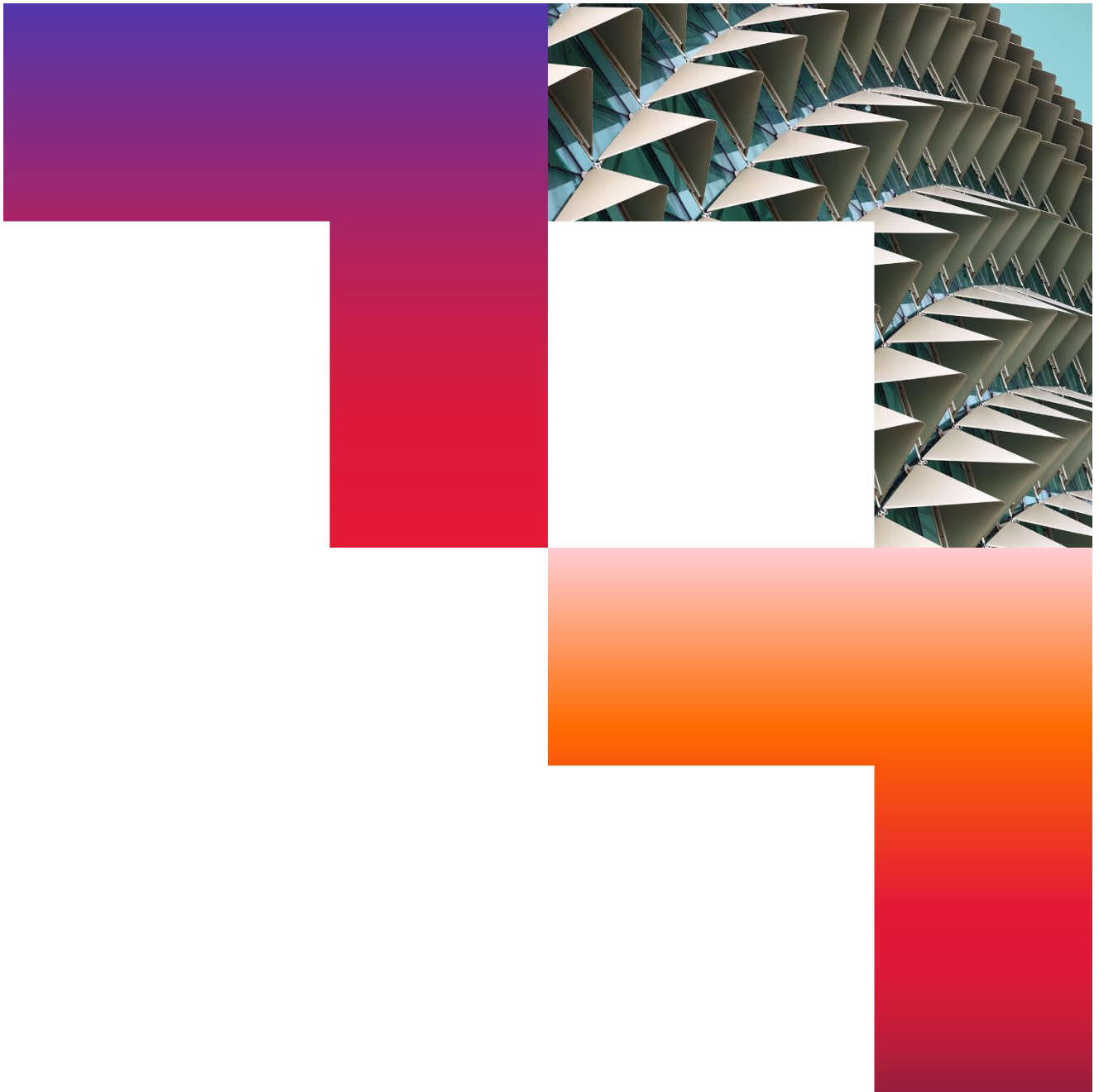




BCR C – CGI – Appendix D CGI Data Subject Request & Complaint Handling Process

CGI

As a preliminary remark, please note that definitions for specific terms with capital letters as used in this document can be found in the BCR-C, unless otherwise defined hereunder.

Individuals whose Personal Data are collected and used by CGI, in particular CGI Partners, clients/employees of CGI's clients, have specific rights regarding the collection and use of their Personal Data. When collecting and using Personal Data on its own behalf (i.e. as a Data Controller), CGI must ensure that any request or complaint (**Request**) from a Data Subject (i.e. an individual) in relation to the exercise of their privacy rights (**Requestor**) is addressed in a timely manner in order to comply with the BCR-C and Applicable Data Protection Legislation.

This document describes how CGI handles a Data Subject's Request when CGI acts as a Data Controller (stakeholders, steps and timeline). Conversely, Requests received from individuals whose Personal Data is Processed by CGI only on behalf of one of CGI's clients must be handled according to the Privacy Request & Complaint Handling Process for CGI as Data Processor.

I. STEPS AND TIMELINE FOR HANDLING A REQUEST

Any Request must be sent by email to privacy@cgi.com. The country and business unit (**BU**) where the Requestor resides must be clearly specified in the Request.

The CGI Privacy Team centralizes all the Requests and appoints the person responsible for managing and coordinating the response (**Request Handler**). The CGI Privacy Team will also determine the other stakeholders that needs to be involved in the process.

STEPS	ACTIONS
Warning: the Request Handler must make sure that the Request is handled <u>within one (1) month maximum</u>, except as otherwise provided below. Each of the steps described below must be taken in the most expedient time to make sure that the one month timeline is respected. CGI may be held liable for not complying with such timing.	
1	Receipt of the Request Once it receives a Request, the CGI Privacy Team will send a receipt of acknowledgement to the Requestor in the most expedient time and where possible within a week after receiving the Request from the Requestor. By default, the Request Handler is the SBU PBP responsible for the country and BU where the Request has been issued. The CGI Privacy Team may appoint a different Request Handler, in particular if no country or BU has been specified.
2	Analysis of the Request The Request Handler will examine the information provided to determine the following: • he/she has appropriate information for handling the Request. • he/she deems the Request to be legitimate and reasonable (e.g., as opposed to one that lacks proof of the Requestor's identity, is excessive, repetitive or manifestly unfounded, is unlawfully submitted on behalf of others, etc.). To the extent possible, the Request Handler will obtain as much information as possible to properly address the Request. As a minimum, he/she will obtain the following information: - First name, last name - Contact details - Scope of request

	- Approximate date the Data was collected and description of the context in which the Data was collected (if possible). Where legally permitted, the Request Handler will obtain and verify a proof of identity from the Requestor to determine whether the Requestor is the individual to whom the Personal Data relates.
3	Handling of the Request ❖ Insufficient information provided by the Requestor Where information provided by the Requestor is not sufficient to handle the Request, the Request Handler must send a request for additional information to the Requestor. Where the Request is complex and requires disproportionate efforts or in case of multiple Requests, the timeline of the response may be extended up to two months in total. Such an extension is exceptional and is possible only if the Request Handler can demonstrate that the Request is truly complex. Where the Request Handler intends to apply such extension, a prior approval from the CGI Privacy Team is needed. In this case, the extension must be communicated to the Requestor within one month from receipt of the Request, with explanation of the reasons for the delay. ❖ Legitimate Request Where information available from the Requestor is sufficient and the Request is deemed legitimate, the Request Handler must take the following steps: - Contact the single points of contact (SPOCs) from the relevant Corporate Services and/or operations teams handling the data at stake to find the information requested in the Request in the most expedient time and to the extent possible within six working days after receiving the Request. SPOCs must collect and send the relevant information in relation to the Request to the Request Handler. - Edit the information received from the SPOCs to ensure it concerns only the Requestor and strictly meets the scope of the Request (no extra set of data should be communicated). - Validate with local Legal Personal Data to be communicated and the adequate format for the communication, and respond to the Requestor. ❖ Request deemed illegitimate If the Request Handler surmises that the Request may not be legitimate, he/she must not immediately close the case at stake. The Request Handler must reply to the Requestor in the most expedient time after receiving the Request, asking the Requestor to provide further explanation as to why he/she intends to exercise his/her rights. - If after receiving the additional information from the Requestor, <u>the Request is deemed legitimate</u>, the Request Handler must make sure that he/she responds to the Request in the most expedient time according to the steps defined above for legitimate Requests. - If after receiving the additional information from the Requestor, the Request Handler deems that <u>the Request is not legitimate</u>, the Request Handler must document why he/she considers the request/complaint manifestly unfounded or excessive and must reply to the Requestor. The Request Handler must specify its decision in the most expedient time. Guidance for assessing the legitimacy of the Request is provided in sections II and III of this process. The response must include the reason for not taking an action. The wording of such response must be validated by the Chief Privacy Officer.

4	Complaint about request/complaint response In the case of a complaint from a Requestor about how his/her Request has been addressed, whether before or after a response has been given, the Request Handler must ensure that he/she shares the matter with the Chief Privacy Officer, in the most expedient time after receiving the complaint. The Chief Privacy Officer must decide about the next steps to take.
5	Request's logs (reception date of the Request, response date, etc.) must be monitored by the Request Handler according to the CGI Privacy Team's instructions.
Cooperation with Chief Privacy Officer For each of the above steps, where it considers that it is necessary, the Request Handler must be ready to cooperate with the Chief Privacy Officer by providing the latter with any relevant information in relation to the matter. The Chief Privacy Officer must then provide guidance as to how to handle the case by taking into account the local circumstances . The Chief Privacy Officer's guidance is binding.	

II. CASES WHERE CGI IS ENTITLED TO REFUSE TO ADDRESS A REQUEST

A. GENERAL REQUEST

Although CGI is committed to handling Requests efficiently, under certain circumstances defined below CGI may be entitled not to address a Request.

CGI can oppose a Request if accessing tsuch Request would imply that any of the following information would be shared with the Requestor:

- Information covered by legal privilege, to the extent permitted by applicable EEA/Member State law.
- Information/Personal Data regarding other individuals (unless the request/complaint regarding other individuals is deemed acceptable under applicable law, e.g. requests with respect to children or deceased persons or requests for which a reasonable effort on the Personal Data would limit the risk for the third parties' Personal Data).
- Information that CGI is legally forbidden to communicate.
- Information CGI is Processing during the course of an ongoing investigation or pending litigation, to the extent permitted by applicable law.

Where there is a conflict of privacy (e.g., data relates to several individuals), Personal Data must be redacted before it is shared with the Requestor.

B. REQUEST TO OPPOSE OR DELETE PERSONAL DATA

In addition, in the case of a Request to stop the further Processing of his/her Personal Data and/or to ask for the deletion of his/her Personal Data, CGI may refuse such a Request where there is a legal obligation or overriding legitimate interest for CGI. This shall be assessed on a case by case basis and referred to the Chief Privacy Officer for a final decision before the Requestor is informed.

III. CHECKLIST FOR ASSESSING A REQUEST

Upon receipt of a Request, the Request Handler must complete the form below, which intends to (i) document any request/complaint received and (ii) make a relevant assessment of the request/complaint. The questions to be addressed depend on the nature of the request/complaint.

Question to be addressed	Answer (provide explanation regarding the Request)	Assessment (determine the risks raised by the Request and explain how it can be handled and/or why it cannot be handled)
What is the nature of the Request? (e.g., access, deletion, opposition, rectification, portability, complaint)		
Is there enough information to identify the Requestor (e.g., proof of identity)?		
Is there enough information about the scope of the Request (e.g., geographical and material scope)?		
Does the Requestor already have possession or easy access to the requested Data (e.g., through CGI systems)?		
Does the Request include information that is not in a clear format for communication to the Requestor? If yes, make sure you explain the codes so that the information can be understood.		
Has the Requestor sent a similar Request recently (e.g., last quarter)?		
Is it technically possible to address the Request (given, in particular, the volume of Data at stake)?		
Are third parties involved in the Processing of the Requestor's Personal Data within the scope of the request/complaint?		
Would handling the Request imply that third-party Personal Data would need to be		

Question to be addressed	Answer (provide explanation regarding the Request)	Assessment (determine the risks raised by the Request and explain how it can be handled and/or why it cannot be handled)
communicated to the Requestor? If yes, is it possible to extract only the Personal Data of the Requestor, with reasonable efforts and without a risk to third-party Personal Data?		

IV. HOW TO COMMUNICATE WITH THE REQUESTOR

When communicating with the Requestor, it is especially important to demonstrate that CGI is willing to cooperate and that addressing the Request in a timely manner is essential.

The information provided to Requestor must be accurate and strictly limited to (i) what the Requestor has requested and (ii) the list of information that may be provided by a Data Controller according to Applicable Data Protection Legislation.

Always keep in mind that an improperly handled request/complaint may result in a claim before a Supervisory Authority.

The Request Handler must pay particular attention to meeting the one month deadline to handle any Request it may receive.

Where a Request is incomplete, CGI must make sure that it is returned to the Requestor without presenting the request for additional information or for justification of the legitimacy of the Request in a negative manner. In other words, **CGI must not anticipate its final assessment of the matter and must therefore not share any preliminary analysis with the Requestor.**

CGI must not delay the further handling of a Request unless it lacks necessary information.

As a general rule, CGI must not impose fees for a reasonable Request. However, in some circumstances to the extent permitted by applicable law and within the limit of the national authorized maximum, reasonable fees may be imposed provided that the Requestor is informed about the fees in advance.

V. COMMUNICATION

All requests regarding this process should be addressed to privacy@cgi.com. Requests/complaints will be kept by the CGI Privacy Team for a maximum of five years.

VI. REFERENCES

POLICY OWNER	APPROVING AUTHORITY
Chief Privacy Officer	Chief Privacy Officer

VII. REVISION HISTORY

VERSION	DATE	DESCRIPTION
1.0		Initial Version
1.1	01.2020	Review – No Changes
1.2	03.2021	Title change Chief Data Protection Officer to Chief Privacy Officer
1.3	11-2022	Annual Review – No Changes
1.4	03-2025	Annual Review – minor textual changes and update of the contact email
1.5	06-2026	Annual review – No changes

