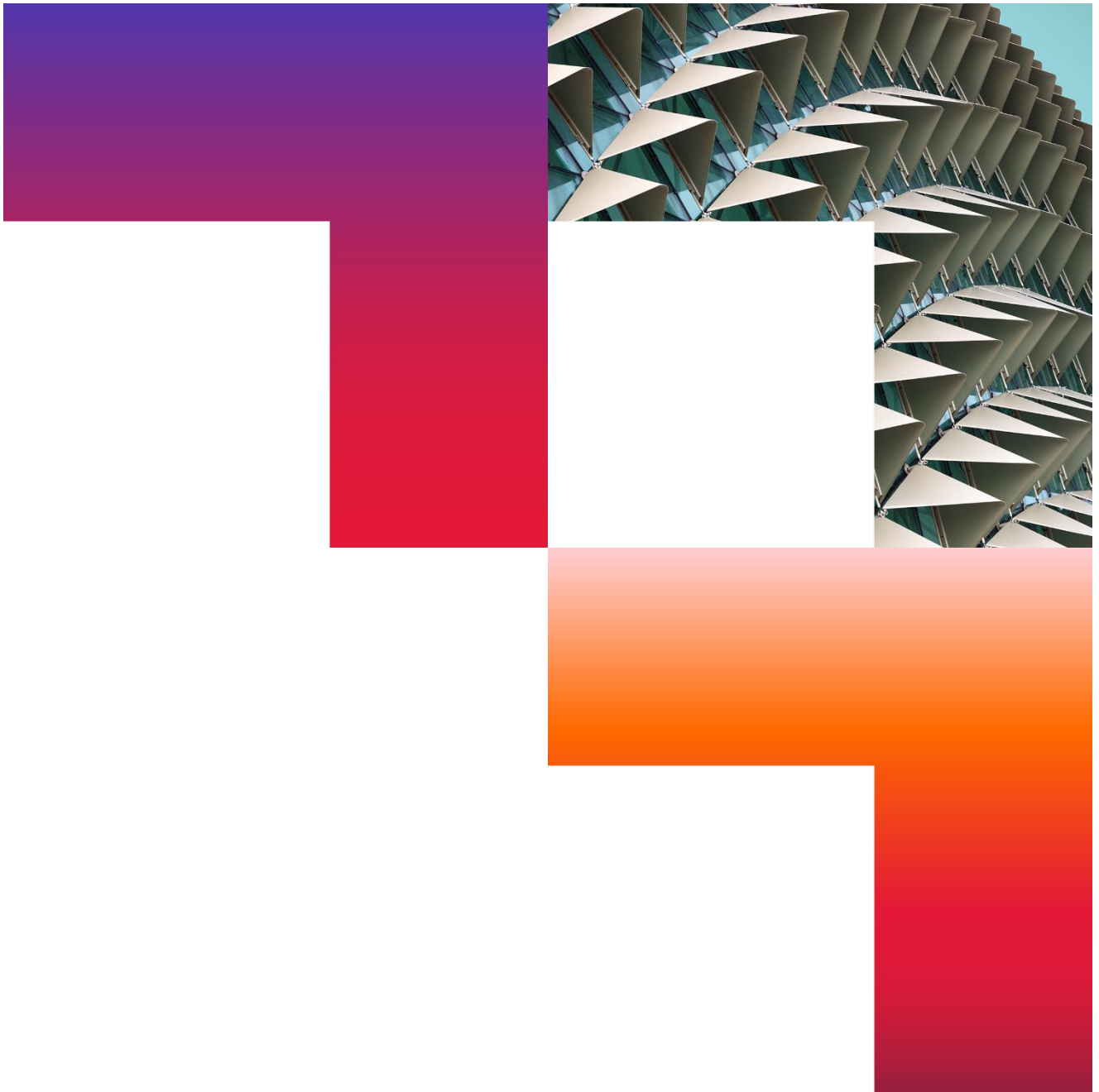




BCR P – CGI – Appendix D CGI Data Subject Request & Complaint Handling Process

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-P, unless otherwise defined hereunder.

Individuals have specific rights regarding the Processing of their Personal Data. When collecting and using Personal Data on behalf of its clients, acting as a Data Processor, CGI must ensure that any request or complaint from individuals in relation to the exercise of their privacy rights is addressed in a timely manner in order to comply with the BCR-P and Applicable Data Protection Legislation. However, this applies only when CGI Processes the requested information.

This document describes how CGI handles a request or complaint from a Data Subject such as a client employee, client end user, subcontractor (**Request**), when CGI acts as a Data Processor (stakeholders, steps and timeline). Conversely, Request received from individuals whose Personal Data is Processed by CGI only on its own behalf as a Data Controller must be handled according to the Privacy Request & Complaint Handling Process (CGI Controller).

I. CONTENT

In most cases, a Request from a Data Subject will cover the following situations:

- Personal Data Processing conditions do not comply with Applicable Data Protection Legislation (e.g., health data not used, stored and encrypted in accordance with local applicable law).
- The Data Subject would like to exercise his/her privacy rights according to Applicable Data Protection Legislation such as the following:
 - o Having access to Personal Data relating to him/her and Processed by CGI on behalf of the client with whom he/she has a relationship;
 - o Obtaining rectification, deletion or suspension of any inaccurate or incomplete Personal Data relating to him/her or which is no longer Processed for a valid or appropriate purpose;
 - o Objecting to the Processing of his/her Personal Data at any time, unless such Processing is required by applicable law, provided that the individual demonstrates he/she has a legitimate ground to object as it pertains to his/her particular situation;
 - o Receiving his/her Personal Data in a structured, commonly used and machine-readable format.

Even if such Data Subject is in direct relationship with CGI's clients, there may be cases where CGI receives a Request directly from the Data Subject and/or is asked by the client to handle the Request on its behalf.

Please refer to the client engagement agreement to check whether specific conditions apply as to the handling of the Request (e.g., interdiction to communicate directly with the individuals, etc.). Please consult your legal contacts for any questions relating to the interpretation of contractual clauses in this respect.

As a consequence, the cost and technical impacts of Requests must be anticipated and addressed at the beginning of each engagement.

II. STEPS AND TIMELINE FOR HANDLING A REQUEST

CGI, acting as a Data Processor, is not responsible for informing Data Subjects on their rights in relation to Personal Data. This is the role of the Data Controller. The procedure below applies when CGI acts as a Data Processor on behalf of a Data Controller.

The BU Leader remains fully accountable for handling such Requests.

Case 1: Data Subject sends his/her Request directly to CGI	
STEPS	ACTIONS
1	Receipt of the Request A CGI Partner who receives a Request in relation to Personal Data that CGI Processes as a Data Processor (e.g., on behalf of clients) must send it promptly to the SBU Privacy Business Partner (SBU PBP) responsible for the country and BU to which the Request is deemed to relate or to privacy@cgi.com in case of any doubt. To find the relevant SBU PBP please consult: https://intranet.ent.cgi.com/browse/priv/global/Documents/GP_Business_Partners_List.pdf A Request sent directly to privacy@cgi.com will be handled directly by the CGI Privacy Team. When necessary, and if no SBU PBP has been specified, the Chief Privacy Officer will transfer the Request to the relevant SBU PBP no later than one working day after receipt. The information provided by the CGI Partner to the SBU PBP must, at a minimum, specify the following information: - Name of the Vice-President, Consulting Services (VPCS) in charge of the client account; - Copy of the Request; - Name of the client to whom the Data Subject relates.
2	Communication of the Request to the client Once it receives such Request, the SBU Privacy Business Partner (SBUPBB), together with the privacy lead (PL), will identify the Vice President, Consulting Services (VPCS) in charge of the client account in order to draft a communication to the client about the Request. The VPCS is exclusively responsible for handling the Request with the support of the CGI Privacy Team. Such communication must be sent to the client, under instruction of the VPCS, no later than two working days after receiving the Request. At the same time, the SBU PBP will ask the VPCS whether CGI actually Processes the Personal Data related to the Request. In any case, since CGI is not the Data Controller, CGI must wait for the client's instructions before handling the Request. Should the client allow CGI to handle the Request on its behalf, the VPCS and the SBU PBP will determine with the client whether the client itself or CGI will acknowledge receipt of the Request and inform the Data Subject of CGI's role in the processing of his/her Request. Unless otherwise expressly instructed by the client, CGI will not have contact with the Data Subject during the entire procedure.
Case 2: Data Subject sends Request to CGI client (the Data Controller)	
STEPS	ACTIONS
1	Receipt of Request When a client sends to CGI a Data Subject's Request regarding the Processing of his/her Personal Data, CGI will acknowledge its receipt of the Request to the client no later than two working days after receiving the latter.

	As a first step, and no later than five working days after receipt of the Request, CGI must verify the extent to which it can address and handle the Request (complexity, technical aspects, etc.). CGI must refrain from communicating directly with the Data Subject unless otherwise expressly instructed by the client.
--	--

PLEASE NOTE: CGI will refrain as much as possible from communicating with the Data Subject, even if required by the client. If a request for contact is sent to CGI, CGI will first discuss with the client the appropriateness of CGI having direct contact with the Data Subject. If CGI agrees to have direct contact with the Data Subject, CGI must inform the client that the latter retains entire responsibility vis-à-vis the Data Subject for handling in due course his/her Request.

2	Analysis of Data Subject's information The Vice President, Consulting Services (VPCS) and the SBU Privacy Business Partner (SBU PBP) will ensure they have all of the necessary information from the client and the Data Subject to address his/her Request. The VPCS must fully cooperate with the SBU PBP to obtain all of the relevant information in order to properly address the Request, including: first name, last name, approximate date the data was collected, and a description of the context in which the data was collected (if possible). Notably, the gathering of such information must be limited to what is currently available within CGI. No additional information will be collected.
3	Handling of the Request For the following steps, please note that CGI will handle the Request either by responding to the client <u>or</u> to the Data Subject when duly authorized by the client. Any communication with the Data Subject, as authorized by the client, will be first reviewed and validated by the client.
4	Analysis of information for handling the Request - The VPCS and the SBU PBP must examine the information provided by the client and Data Subject within eight working days after receiving the Request to determine both of the following: (i) They have appropriate information to handle the Request. (ii) The client deems the Request to be reasonable (e.g., as opposed to one that lacks proof of the Data Subject's identity, is excessive, repetitive or manifestly unfounded, is unlawfully submitted on behalf of others, etc.). ❖ Insufficient information on Data Subject - Where information provided by the Data Subject is not sufficient to handle the Request, the VPCS will request the Data Subject or the client to provide additional information within two working days. Where the Request is too complex and subject to prior approval of the client, the timeline of the response may be extended up to 2 months. Please note that such an extension is exceptional and possible only if CGI can demonstrate that the Request is truly complex. The extension must be communicated to the Data Subject within 20 working days from receipt of the request, with explanation of the reasons for the delay.

	❖ Request deemed illegitimate - When the VPCS and SBU PBP surmise, upon a first analysis, that the Request may not be reasonable, they must document their findings and notify the client. Guidance for assessing the legitimacy of the Request is provided in sections III and IV of this process. If the client decides the Request should be further investigated, CGI will request the Data Subject or the Client to provide more explanation as to why he/she intends to exercise his/her rights within 10 working days after receiving the Request. - If the client believes that, based on the additional elements, the Request can be handled, the VPCS and SBU PBP must address the Request within the above mentioned 15 working days. - If the client decides the Request is not reasonable, the VPCS and SBU PBP must reply to the client or Data Subject no later than 15 working days after receiving the additional information. The response must include the reason for not taking an action and the possibility of the Data Subject lodging a complaint with a Supervisory Authority and seeking a judicial remedy. The wording of the response must be validated by the Chief Privacy Officer, VPCS and client.
--	---

Please note the intermediary timelines are designed to ensure that CGI meets the global deadline to respond. Such intermediary timelines may be adapted given the complexity of the request. However, **the global deadline cannot be extended**.

Cooperation with the Chief Privacy Officer

For each of the above steps and where necessary to appropriately handle the case, the VPCS and the SBU Privacy Business Partner shall be ready to cooperate with the Chief Privacy Officer by providing the latter with any relevant information in relation to the matter and inform the Client of the handling of the procedure. The Chief Privacy Officer's guidance shall be binding. However, the Chief Privacy Officer shall prevent from entering into contact directly with the Data Subject, unless expressly required by the Client, the VPCS or the SBU Privacy Business Partner.

III. CASES WHERE CGI IS ENTITLED TO REFUSE TO MEET A REQUEST

Although CGI is committed to Data Subject Request efficiently, irrespective of the channel through the Request is submitted, under certain circumstances as defined below, CGI may be entitled not to accept a Request from a Data Subject or client.

CGI can reject a Request from a client or Data Subject if accessing the Request would imply the following information would be shared:

- Information covered by legal privilege, to the extent permitted by applicable EEA/Member State law;
- Information/Personal Data regarding other Data Subjects;
- Information that CGI is legally forbidden to communicate;
- Information CGI is Processing during the course of an ongoing investigation or pending litigation procedure.

Where there is a conflict of privacy, data may be redacted before it is shared with the client or Data Subject.

Request to oppose or delete Personal Data

If a Request is received from a client regarding a Data Subject who is opposed to the further Processing of his/her Personal Data and/or is requesting the deletion of his/her Personal Data, CGI may refuse to grant the Request if legal obligations prevent CGI from doing so or where CGI has an overriding legitimate interest. This must be assessed on a case by case basis and referred to the Chief Privacy Officer for a final decision before the client or Data Subject is informed.

IV. CHECKLIST FOR ASSESSING A REQUEST

Upon receipt of a Request, either directly from the Data Subject or from the client, and subject to the above mentioned provisions and steps, the Vice-President, Consulting Services (VPCS) and the SBU Privacy Business Partner (SBU PBP) must complete the following form, which intends to (i) document any Request received and (ii) make a relevant assessment of the Request.

The questions to be addressed depend on the nature of the request.

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) – with the support of the CGI Privacy Team
Do I have authorization to handle the Request on behalf of the client?		
What is the nature of the Request? (access, deletion, opposition, rectification, portability)		
Does the client consider the Data Subject's Request to be reasonable?		
Is it technically possible to address the Data Subject's Request (given, in particular, the volume of data at stake)?		
Is there enough information to identify the Data Subject?		
Is there enough information regarding the scope of the Request? (geographical and material scope)?		
Does the Data Subject already have possession or easy access to the requested data?		
Does the Request include information that is not in a		

clear format for Data Subjects? If yes, make sure you explain the codes so that the information can be understood.		
Are third parties involved in the Processing of Data Subjects' Personal Data within the scope of the Request?		
Would the handling of the Request imply that third parties' Personal Data would need to be communicated to the Data Subject? 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?		

V. HOW TO COMMUNICATE WITH A DATA SUBJECT WHEN REQUESTED BY THE DATA CONTROLLER

If the client requires CGI to handle a Request on its behalf, the following rules will apply when CGI communicates with the Data Subject. Under no circumstances will CGI communicate directly with the Data Subject, if it has not received the client's prior approval.

When communicating with the Data Subject, it is particularly important for CGI to demonstrate that it is willing to cooperate and that addressing the Request in a timely manner is essential.

The information to be provided to Data Subjects must be accurate and limited to (i) what the Data Subject 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 a Data Subject's Request that is improperly handled may result in a claim before a Supervisory Authority.

The Vice-President, Consulting Services (VPCS) and SBU Privacy Business Partner (SBU PBP) must pay particular attention to the deadlines mentioned above.

Where a Request is incomplete, CGI must return it to the Data Subject 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 the final assessment of the matter and share any preliminary analysis with the Data Subject.

CGI must not delay 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 EEA/Member State law and within the limit of the national authorized maximum, reasonable fees may be imposed provided the client is informed about such fees in advance.

VI. 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.

VII. REFERENCES

POLICY OWNER	APPROVING AUTHORITY
Chief Privacy Officer	Chief Privacy Officer

VIII. 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/Intranet link
1.5	06-2026	Annual review – No changes

