

# Data Privacy Policy

## Version 2.2

2025-01-01

CGI protects the Personal Data that we handle and works closely with its clients and Third-Party Suppliers to address the challenges of the evolving data protection regulatory landscape.

We maintain this Data Privacy Policy detailing our privacy principles, standards and practices and how we protect all Personal Data as part of our operations, whether we Process Personal Data for our own purposes or for the needs of our clients.

Capitalized terms are defined in Appendix 1 hereto.

## Principles

As a global IT and business consulting services organization, CGI is committed to maintaining levels of protection of Personal Data aligned to best practices, the Applicable Data Protection Legislation and CGI's contractual obligations.

CGI collects and/or uses Personal Data for its own needs.

CGI may also handle Personal Data on behalf of and upon instructions of a client, including the technical and organizational measures required to prevent accidental or unlawful destruction, loss, alteration, disclosure or access to the Personal Data. Any commitment regarding these responsibilities and measures must be expressly reflected in any agreements entered between CGI and our clients.

CGI's value proposition includes data protection and data risk exposure prevention. CGI guides and assists its clients on how to manage and protect their Personal Data to meet compliance requirements. Upon a client's instructions, CGI will implement effective security measures to safeguard the Personal Data and avert data breaches.

## Scope and compliance

This Data Privacy Policy forms an integral part of CGI Management Foundation and is binding on all CGI Legal Entities and employees ("CGI Partners") regardless of their location, as well as Third-Party Suppliers engaged by CGI. To the extent permitted by law, any violation of this Data Privacy Policy may result in administrative and/or disciplinary action by CGI (including monetary penalties, suspension, or termination).

CGI Partners acknowledge these requirements and annually confirm acceptance of this Data Privacy Policy as part of their commitment to the Code of Ethics. In addition to this Data Privacy Policy, CGI Partners must also comply with other applicable confidentiality and privacy obligations, including those



set out in Applicable Data Protection Legislation, their employment agreements, CGI's Management Foundation and/or client instructions.

Any Third-Party Supplier that Processes Personal Data on CGI's behalf is required to implement appropriate technical and organizational measures to ensure compliance with the principles and requirements of this Data Privacy Policy. When CGI Processes Personal Data on behalf of a client, any contractual commitments or other obligations of CGI towards its client need to be passed down to all engaged Third-Party Suppliers. Any commitment or obligation must be expressly reflected in agreements entered between CGI and Third-Party Suppliers.

## Which Personal Data categories does CGI Process as part of its operations?

Subject to Applicable Data Protection Legislation, CGI and any Third-Party Supplier may Process the following non-exhaustive list of Personal Data categories:

<p><b>Demographics &amp; Private life information</b></p> <p>(e.g. age, gender, physical traits, date of birth, home address, marital status, memberships, preferences, interests)</p>	<p><b>Location, login, traffic &amp; tracking</b></p> <p>(e.g. IP address, browser fingerprint, logs)</p>	<p><b>Economic &amp; financial</b></p> <p>(e.g., account number, financial health, shares, tax status, salary, financial transactions)</p>
<p><b>Sensitive Personal Data</b></p> <p>(e.g. social security number, biometrics, health information)</p>	<p><b>Identity &amp; contact information</b></p> <p>(e.g. name, email address, telephone number, photo, nationality, ID and passport numbers)</p>	<p><b>Professional life &amp; business information</b></p> <p>(e.g. employer, department, job title, employment history, performances, interviews, degrees and certifications, billing, delivery address)</p>

These categories of Personal Data relate to the following non-exhaustive list of individuals:

- Employment candidates, trainees, and students,
- CGI Partners and former employees, and their relatives,
- Clients' employees and former employees, and their relatives,
- Clients' patients, customers or citizens,
- Prospective clients' employees and customers,
- Visitors of CGI websites,
- Shareholders,
- Third-Party Suppliers' employees and freelancers.

More detailed information is available in the relevant privacy information notices.

## With whom does CGI share your Personal Data?

As part of its operations, CGI may disclose Personal Data to CGI Legal Entities, clients and prospects, Third-Party Suppliers, and/or other third parties (including banks and financial advisors, external advisors, and auditors), as well as administrative, judicial, or governmental authorities, state agencies or public bodies in accordance with Applicable Data Protection Legislation.

## How does CGI protect Personal Data Processed for its own needs?

*CGI is responsible for protecting any Personal Data handled as part of its operations.*

As a result, CGI Partners comply with the following core principles:

### 01 Transparency, Fairness and Lawfulness

Personal Data is Processed **lawfully, fairly, and in a transparent manner** in relation to the individual, in accordance with the requirements of this Data Privacy Policy. CGI provides detailed data Processing information to relevant individuals, in an easily understandable and accessible format, through **privacy information notices**.

### 02 Purpose Limitation

Any Processing of Personal Data is preceded by the **identification of the specific purpose for such Processing**, which must be **explicit and legitimate** and in line with what would reasonably be expected by an individual.

### 03 Data Minimization

Personal Data is only collected and used to the extent **required to accomplish the purpose for which it is Processed**. Personal Data must be **adequate, relevant, and limited to what is strictly necessary** in relation to such purpose.

### 04 Accuracy

Collected Personal Data must remain **accurate and up to date**. Reasonable steps must be taken to ensure that any inaccurate Personal Data is erased or rectified without delay including through self-service options for individuals. Adequate means must be provided to individuals to inform CGI of any change to their Personal Data.

### 05 Storage Limitation

**Personal Data must not be kept for longer than strictly necessary** to achieve the purpose for which it is collected. Consequently, CGI must determine the required data retention period in accordance with CGI Records Retention Schedule and Applicable Data Protection Legislation.

### 06 Integrity and Confidentiality

Appropriate technical and organizational measures, as prescribed in CGI's Enterprise Security Management Framework (ESMF), must be implemented to **guard against unlawful access and/or Processing of Personal Data**.

## On which legal basis does CGI Process Personal Data for its own needs?

Most commonly, CGI may Process Personal Data in the following circumstances:

- ✓ When CGI needs to comply with a **legal obligation**.
- ✓ When it is necessary for the **execution of a contract with an individual**.
- ✓ When CGI has a **legitimate interest** in doing so as part of its operations.

There can be some occasions where it becomes necessary for CGI to Process Personal Data to **protect individuals' interests** or with the prior **consent** of the individuals.

## Sensitive Personal Data Processed for CGI's own needs

CGI will not Process Sensitive Personal Data unless one of the following conditions is met:

1. The individual has given their prior consent, or
2. The Processing is required for the purposes of carrying out the obligations and exercising specific rights of CGI or of the individual in the field of employment, social security and social protection law, or
3. If the individual is not able to give their consent (e.g., for medical reasons), the Processing is necessary to protect the vital interests of the individual or another person, or
4. The Processing is required in the context of preventive medicine or medical diagnosis by a health professional under Local Legislation, or
5. The individual has already manifestly placed the relevant Sensitive Personal Data in the public domain, or
6. The Processing is essential for the purpose of establishing, exercising or defending legal claims, unless the individual has an overriding legitimate interest in ensuring that such Sensitive Personal Data is not Processed, or
7. The Processing is explicitly permitted by Local Legislation.

## How does CGI protect clients' Personal Data?

*When CGI Processes clients' Personal Data, CGI ensures that Personal Data is Processed for the client's sole expressed purposes, and according to the client's written instructions, including in respect of duration, set out in the terms and conditions agreed between CGI and the client.*

The client remains solely responsible for ensuring that there is a valid legal basis for the Processing performed by CGI and that the instructions given to CGI in respect of the Processing comply with Applicable Data Protection Legislation, including the retention period to be applied. Nonetheless, CGI will promptly inform the client if, in its opinion, any such instructions contravene Applicable Data Protection Legislation.

Unless otherwise instructed by the client, CGI will apply (as a minimum) CGI's security baseline as prescribed in CGI's Enterprise Security Management Framework (ESMF). Any deviation to this baseline requires relevant risk reviews and the approval of CGI's Privacy and Security teams in accordance with CGI's Management Foundation.



CGI will, subject to financial, technical, and organizational conditions agreed in writing, provide reasonable assistance to the client to support it in undertaking its obligations under Applicable Data Protection Legislation.

## Privacy by Design and Privacy by default

To ensure that the principles defined in this Data Privacy Policy are effectively considered when CGI Processes Personal Data, CGI will identify and address data protection constraints at the beginning of any new internal project or client opportunity so that the principles contained herein are reflected in the design of the project and appropriately implemented. CGI has therefore implemented Data Privacy and Security review processes, as well as a Privacy by Design Code of Practice and several frameworks (e.g. Responsible Use of Data, Responsible Use of Artificial Intelligence and Responsible Use of Cloud Technology) applicable to all CGI internal projects and client opportunities involving the Processing of Personal Data and assisting each relevant CGI Partner in analyzing and addressing data privacy risks.



As per Applicable Data Protection Legislation, CGI will carry out a data privacy impact assessment for all CGI internal projects where the Personal Data Processing activity is likely to result in a high risk to the rights and freedoms of individuals and determine any corrective measures to be implemented to ensure risks are mitigated.

The CGI Privacy organization reviews and approves the Privacy aspects of proposals and/or services developed for clients, as well as of any CGI Intellectual Property or new internal project, as defined in the CGI Management Foundation. The CGI Partner responsible for the solution, service and/or project retains evidence of compliance with CGI Privacy organization approval requirements.

## What are the rights of individuals and how they can be exercised?

Rights of individuals over their Personal Data differ from one country to another. CGI acts in accordance with Applicable Data Protection Legislation.

Depending on jurisdictions, Applicable Data Protection Legislation may provide individuals with the following rights:

- Have access to their Personal Data and the information on how it is Processed,
- Request the rectification or deletion of any inaccurate or incomplete Personal Data relating to them,
- Revoke consent or object on legitimate grounds to the Processing of their Personal Data, unless such Processing is imposed by law,
- Request restrictions to the Processing where the Personal Data is no longer accurate or necessary, or the Processing is unlawful,
- Not be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects the individuals,
- Receive their Personal Data in a structured, commonly used and machine-readable format, and
- Appoint an individual to exercise their rights upon their death or incapacity.

Individuals who wish to exercise these rights and/or obtain information on the Processing of their Personal Data may send a request as set out in the [“Question and Recourse”](#) section below.

**When CGI Processes Personal Data for its own needs:** CGI communicates any rectification or deletion of Personal Data or restriction of Processing carried out in accordance with Applicable Data Protection Legislation to each recipient to whom the Personal Data has been disclosed unless this proves impossible or involves disproportionate effort. CGI ensures that it handles requests without undue delay in accordance with CGI’s individual rights request process.

**When CGI Processes clients’ Personal Data:** If CGI receives a complaint or request from individuals wishing to exercise their rights, CGI will promptly communicate all relevant information to the client and will expressly indicate to the individual that it is the client’s responsibility to handle such complaint or request. CGI is only responsible for handling complaints or requests in accordance with the client’s instructions.

## How does CGI manage Personal Data breaches?

CGI has a mature, standards-based security incident response and management process designed to handle all phases of a security incident, including incidents with privacy impacts. CGI Partners' responsibilities are clearly defined at all levels. Incident assessment and prioritization standards are followed to ensure appropriate engagement levels and timely resolution.

Incident records are maintained and reported to CGI’s senior management as required. All incidents are managed through CGI’s 24x7 Global Security Operations Centre (SOC), where highly trained, full-time incident response professionals coordinate response efforts. CGI’s Privacy team is immediately engaged in the incident management process whenever Personal Data is suspected or known to be involved.



If CGI reasonably believes that a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed has occurred, CGI will provide security incident notification and status updates to the relevant Data Protection Authority, individuals and/or clients (as the case may be), in accordance with Applicable Data Protection Legislation, as well as CGI's Management Foundation.

Similarly, in the event a Personal Data breach is identified by a Third-Party Supplier engaged by CGI, the Third-Party Supplier must inform CGI as agreed upon in the relevant agreement and in accordance with Applicable Data Protection Legislation.

## Communication and training

CGI continually promotes a data protection culture within its organization. CGI deploys an annual data privacy learning program, regularly updated to reflect technological and legislative changes. Such training is mandatory for all CGI Partners, subcontractors, and freelancers. All CGI leaders must ensure that the CGI Partners reporting to them take the training.

Role specific learning courses adapted to several functions within the organization and security trainings are also available on CGI's learning platform.

Additional information to CGI Partners may also be provided through several channels, including targeted Privacy briefings, webinars, individual meetings, newsletters, 'Know How' sessions, security awareness campaigns, and global annual Data Privacy Day communications.

These provide **CGI Partners' awareness** of the core principles contained in this Data Privacy Policy and associated best practices to help **protect CGI and its stakeholders** against unauthorized access and improper handling of Personal Data

## Audit

CGI integrates into its business-wide internal audit program a review of its compliance with this Data Privacy Policy. The internal audit program defines:

- A schedule under which audits will be carried out,
- The expected scope of the audit, and
- The team responsible for the audit.

The business-wide internal audit program includes verification at delivery, functional, and corporate levels. The audit programs may be revised on a regular basis. However, CGI will perform internal audits on a regular basis through qualified audit teams. Such programs will be initiated by the relevant CGI audit departments for each level.

The results of the audit will be communicated to the CGI Privacy organization and resulting actions will be defined and prioritized, enabling the CGI Privacy organization to determine a schedule for the implementation of corrective and preventive measures.

Competent data protection authorities, as well as clients, may request access to the audit results (in the latter case, subject to contractual obligations, as defined in the Contract Management Framework). Such communication is subject to a confidentiality agreement and audit results do not include any confidential information of other CGI clients or CGI internal business areas. Release of such results are subject to the approval of the CGI Privacy organization and Legal Services.

As part of **CGI's ISO27701:2019 certification**, external auditors independent from CGI act as an additional line of compliance. They provide oversight and assurance of our ISO27701:2019 implementation across the organization and conduct annual audits. The results of such audits are treated as per all audit results, with any recommended corrective and preventive measures being prioritized across all areas of the business.

## CGI Privacy Organization

CGI has designated a Chief Privacy Officer (“CPO”) and a network of Privacy Business Partners who may also be appointed as Data Protection Officers, in accordance with Applicable Data Protection Legislation, and records management specialists. The CGI Privacy organization is further defined on the Privacy page of CGI's corporate intranet.

## Record of Processing activities

CGI maintains a record of Processing activities carried out as part of its operations (the “Data Processing Inventory”). CGI will ensure that any new Processing of Personal Data is recorded in the Data Processing Inventory with relevant information regarding the context of each Processing of Personal Data. CGI will make a record(s) of Processing available to the supervisory authority upon request.

## Updates of the Data Privacy Policy

This Data Privacy Policy may be amended from time to time, as necessary, and CGI will issue relevant communications relating to such changes in due time.

## Questions, requests and recourses

**Questions and requests:** In case of questions related to the interpretation or operation of this Policy, or requests related to your Personal Data Processed by CGI, please:

- send an email to [privacy@cgi.com](mailto:privacy@cgi.com), or
- contact CGI's Chief Privacy Officer in Paris – Carré Michelet, 10-12 Cours Michelet, 92800 Puteaux, France, or
- complete the following [online form](#).



**Independent recourse mechanism:** If you believe that you have evidence of misconduct that could harm CGI, CGI Partners, its clients or shareholders, you should report it using [CGI's Ethics Hotline](#).

CGI seeks to maintain strong relationships with data protection authorities and cooperate with them in any relevant matter, including any audit requests. CGI will also carefully consider recommendations issued by competent data protection authorities in relation to Personal Data Processing carried out by CGI as part of its operations.

If you have any question or request related to your Personal Data that is not addressed by CGI in accordance with Applicable Data Protection Legislation or require assistance from any competent data protection authority, you may submit a complaint or reach out to the relevant authority. Below are useful resources:

- ↻ [Canada](#)
- ↻ [EU/European Economic Area](#)
- ↻ [Federal Trade Commission \(FTC\)](#)
- ↻ [India](#)
- ↻ [Malaysia](#)
- ↻ [Philippines](#)
- ↻ [Quebec](#)
- ↻ [Swiss Federal Data Protection and Information Commissioner](#)
- ↻ [UK Information Commissioner's Office \(ICO\) or Gibraltar Regulatory Authority \(GRA\)](#)

**Data Protection Review Court:** As per the EU-U.S. Data Privacy Framework (EU-U.S. DPF), validated by the European Commission on July 10, 2023, the Data Protection Review Court is the second level of a two-level redress mechanism that provides for the review of qualifying complaints by individuals, filed through appropriate public authorities in designated foreign countries or regional economic integration organizations, alleging certain violations of United States law concerning United States, signals intelligence activities.

## Policy owner

CGI's Chief Privacy Officer

## Approving authority

CGI Executive Management Committee

## Effective Date

January 1<sup>st</sup>, 2025

# Revision history

Version	Date	Author	Description
1.0	2017-10-16	Data Privacy	Original Policy Document
1.1	2018-01-09	Data Privacy	Style Changes
1.2	2021-01-01	Data Privacy	Updated to reflect upcoming Binding Corporate Rules requirements and California Consumer Privacy Act
2.0	2021-10-01	Data Privacy	Updated to reflect Binding Corporate Rules
2.1	2023-12-11	Data Privacy	Added EU-US data privacy framework (DPF), the UK extension and the Swiss-US DPF, add Section 14 Question and Recourse from External Policy, plus alignment between external and internal versions.
2.2	2024-12-19	Data Privacy	Updates to reflect CGI Partners terminology, annual review of CGI's Binding Corporate Rules, new legislative changes, merge between external and internal versions of the Data Privacy Policy and reference to CGI Responsible Use of Data, AI and Cloud technology frameworks.

# Appendix 1

## Privacy Glossary

For the purposes of this Data Privacy Policy, the following terms with associated definitions are used:

Terms	Definitions
<b>Applicable Data Protection Legislation</b>	All laws that are applicable to the Processing of Personal Data, including, without limitation and as applicable: (i) the European Data Protection Regulation 2016/679 (General Data Protection Regulation, “GDPR”) relating to the Processing of Personal Data, (ii) any applicable Local Legislation.
<b>BCR</b>	Binding Corporate Rules as detailed in Appendix 2 <a href="#">“Transfer of Personal Data”</a> .
<b>CGI Legal Entities</b>	All legal entities controlled directly or indirectly by CGI Inc., excluding CGI Federal Inc. and its subsidiaries.
<b>CGI Partner(s)</b>	Employee(s) of CGI Legal Entities.
<b>CPO</b>	Chief Privacy Officer as detailed in Section <a href="#">“CGI Privacy Organization”</a> .
<b>Data Controller</b>	Any entity that determines the purposes and means of Processing Personal Data. The client is the Data Controller when CGI Processes Personal Data on its behalf as part of a client project. CGI may act as Data Controller when implementing for its own needs, a new internal solution Processing Personal Data.
<b>Data Processor</b>	Any entity acting on behalf of and under instructions from a Data Controller. CGI is a Data Processor when Processing Personal Data on its clients’ behalf.
<b>DPF</b>	Data Privacy Framework as detailed in Appendix 2 <a href="#">“Transfer of Personal Data”</a> .
<b>Local Legislation</b>	All laws applicable in geographies where CGI operates, including without limitation: data protection, security, employment, industry sectors and consumers legislation.
<b>Personal Data</b>	Any information relating to an individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal Data includes Sensitive Personal Data.
<b>Process, Processing or Processed</b>	Any operation or set of operations performed on Personal Data, whether or not by automated means, such as collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, consulting (including remote access), using, disclosing by transmitting, disseminating, or otherwise making available, aligning, or combining, restricting, erasing, or destroying.
<b>Sensitive Personal Data</b>	Specific categories of Personal Data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person’s sex life or sexual orientation, as well as criminal records.
<b>Third-Party Supplier</b>	Any third party engaged by CGI or providing goods and/or services to CGI, including suppliers, contractors, subcontractors, and freelancers.
<b>Transfer</b>	Sending of Personal Data to another CGI Legal Entity or any other party or making the Personal Data accessible by it, where the other CGI Legal Entity or party is not located in the same country, province, or geographical area, as detailed in Appendix 2 <a href="#">“Transfer of Personal Data”</a> .

## Appendix 2

# Transfer of Personal Data

Any Transfer of Personal Data must take place in accordance with Applicable Data Protection Legislation and the provisions of this Appendix 2.

### 1) TRANSFER WITHIN CGI

A CGI Legal Entity involved in a Transfer must ensure that appropriate technical and organizational measures commensurate with any Processing risks are implemented in accordance with this Data Privacy Policy and CGI's security policies, processes, and standards. These appropriate technical and organizational measures must be agreed and set out in a data processing agreement or any equivalent.

#### (I) BINDING CORPORATE RULES

CGI may only Transfer Personal Data of individuals in the EU in accordance with Applicable Data Protection Legislation and CGI's Binding Corporate Rules ("BCR"), approved by the French Data protection authority on July 22, 2021, as they may be amended. BCR are applicable to all CGI Legal Entities listed in the BCR and each participating CGI Legal Entity is responsible for demonstrating its compliance with the BCR. All CGI Partners are bound by the BCR.

To learn more about our BCR, please consult CGI's corporate intranet, its [public facing website](#) and the [Register of the European Data Protection Board](#).

#### (II) EU-US DATA PRIVACY FRAMEWORK (DPF), THE UK EXTENSION AND THE SWISS-US DPF

As per the approval granted by the US Department of Commerce, the following CGI Legal Entities are self-certified under EU-US Data Privacy Frameworks ("DPF"), the UK Extension, and the Swiss-US DPF:

- CGI Technologies and Solutions Inc.
- CGI Information Systems and Management Consultants (New York) Inc.
- CGI Group Holdings USA Inc.
- Accounts Receivable Automated Solutions Inc.

These DPF provide the above-mentioned CGI Legal Entities with reliable mechanisms for Personal Data Transfers to the United States from the European Union, the United Kingdom and Switzerland while ensuring data protection that is consistent with EU, UK and Swiss Applicable Data Protection Legislation.

CGI complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. CGI has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. CGI has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF.

If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles will take precedence.

To learn more about the Data Privacy Framework (DPF) Program, and to view our certification, please visit <https://www.dataprivacyframework.gov/>.

The Federal Trade Commission has jurisdiction over CGI's compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).

In the context of an onward Transfer, CGI is responsible for the processing of Personal Data it receives under the DPF Principles and subsequently Transfers to a Third-Party Supplier acting as an agent on its behalf. CGI remains liable under the DPF Principles if any Third-Party Supplier engaged by CGI processes such Personal Data in a manner inconsistent with the DPF Principles, unless CGI proves that it is not responsible for the event giving rise to the damage.

Individuals may, under certain conditions, invoke binding arbitration for complaints regarding DPF compliance not resolved by any of the other DPF mechanisms as detailed in the [DPF ANNEX I](#).

## **2) TRANSFER TO THIRD PARTIES**

On a regular basis, CGI conducts due diligence and third-party privacy and security risks assessments with Third-Party Suppliers engaged by CGI, to establish their corporate capabilities and maturity with respect to security and data protection.

Whenever CGI relies on Third-Party Suppliers to process Personal Data, CGI ensures that such Third-Party Suppliers provide an adequate level of protection to the Personal Data they process as per Applicable Data Protection Legislation.

\*\*\*