DATA PRIVACY POLICY

Contents

I Distribution List

II Version History

III Policy Statement

IV Overview

V Definitions

VI Scope of Coverage

VII Data protection Officer (Grievance Officer)

VIII Employees/Relevant Individuals Obligations & Consequences of Policy Violations

Policy Name	Data Privacy Policy
Version No	2.0
Contact Person	Data Protection Officer (Grievance Officer): Legal Department
Last Review Date	14th June, 2017
Reviewed By	Renucka Naik Senior Director Legal & DPO
Approved By	Bharat Mehta, Executive Vice President Legal

I. Distribution List

Employees and/or Relevant Individuals as defined below of Capgemini Technology Services India Limited, its subsidiaries, its affiliates in India (including non-profit organizations and/or trust), hereinafter "**Capgemini**".

II. Version History

Version	Date	Description
1.0	23.04.2015	Data Privacy Policy released
2.0	14.06.2017	Amendments to the Policy referring to Capgemini Group's adoption and implementation of the Binding Corporate Rules (BCRs). Amendments reinforcing employee/relevant individual's obligations while handling personal data; And consequences of non-compliance with the Policy.

III. Policy Statement

The objective of this Policy is to cultivate organization-wide privacy culture to protect the rights and privacy of individuals; to comply with applicable privacy and data protection legislations by implementing privacy principles and controls in cooperation with the Information Security Management System.

All employees should adhere and comply with this Policy and additionally, specific privacy practices that may be adopted by Capgemini.

IV. Overview

Currently, the Indian Information Technology Act 2000 mandates the secure processing of personal information and prevention of misuse of Information. On April 11, 2011, India's Ministry of Communications and Information Technology passed the Information Technology (Reasonable Security Practices, Procedures and Sensitive Personal Data or Information) Rules which deals with practices and procedures for protection and maintenance of Personal Information.

It is Capgemini Group's policy to comply with the privacy legislation within each jurisdiction in which a Capgemini entity operates. The privacy legislation and/or an individual's right to privacy are different from one jurisdiction to another. Specific privacy practices may be adopted by Capgemini to address the privacy requirements of particular jurisdictions (for e.g. HIPAA, GLBA, PCI-DSS, etc.).

This Privacy Policy of Capgemini ("**Policy**") sets out the rules and procedures relating to the processing of Personal Data in India.

Capgemini Binding Corporate Rules (hereinafter referred to as the "**BCR**s") have been approved by the European Data Protection Authorities to express Capgemini's commitment to establishing and maintaining high standards across the Group for the transfer and processing of Personal Data. Capgemini entities in India are committed to adhere to the BCRs. The BCRs are designed to enable the transfer of Personal Data from Capgemini entities located in the European Union ("EU") to Capgemini affiliate entities located outside of the EU, and in this regard, constitute Capgemini Group's global compliance program. Subject to Indian laws, the BCRs shall govern the transfer/processing of EU personal data.

In addition, Capgemini is implementing a global security and cyber security program to align security practices within the entire Group through the mandatory implementation of 64 security baselines across all its business organisations.

This Policy supersedes any previous communications, representations or agreements, verbal or written, related to the subject matter of this Policy. In case of contradiction between the BCRs and this Policy, this Policy shall prevail.

V. Definitions

Personal Data means **any information** that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

Processing refers to any action performed on Personal Data, such as collecting, recording, organizing, storing, transferring, modifying, using, disclosing, uploading or deleting**.**

Sensitive Personal Data of a person, under the Indian Information Technology Rules 2011, means such Personal Data which consists of information relating to:

- Password;
- Financial Information such as bank account or credit card or debit card or other payment instrument details;
- Physical, physiological and mental health condition;
- Sexual orientation;
- Medical records and history;
- Biometric Information;
- Any other details relating to the above mentioned, provided by any person to Capgemini for providing services;
- Any Information received pursuant to the above mentioned by Capgemini for processing, or storing such Information under a lawful contract or otherwise;
- Provided that any Information that is freely available or accessible in public domain or furnished under the Right to Information Act 2005 or any other law for the time being in force will not be considered to be Sensitive Personal Data.

"**Employee**" means a Capgemini current or former employee. As far as it applies to Employees, the Policy covers all stages of the employment cycle including recruitment and selection, promotion, evaluation and training.

"Relevant Individual" means an Employee, contractor and/or any other third party working on Capgemini's behalf and job applicants.

VI. Scope of Coverage

This Policy is applicable to all Personal Data collected, received, possessed, owned, controlled, stored, dealt with or handled by Capgemini in respect of a Relevant Individual.

Personal Data and Information that Capgemini handles for its clients in the context of providing consulting, technology and outsourcing services shall be processed according to the contractual provisions, specific privacy practices agreed upon with each client and the BCR processor, as applicable. This Policy lays emphasis on the obligations of the Relevant Individuals dealing with Personal Data in the course of performance of their duties.

A) Collection of Personal Data by Capgemini

Throughout the course of the relationship with the Relevant Individual, Capgemini needs to collect Personal Data. The type of Information that may be collected includes (but is not limited to), where relevant:

- Basic Information regarding the Relevant Individuals such as name, contact details, address, gender, birth date, marital status, children, parents details, dependent details, photos, photo id proof, pan card, passport, voter ID, aadhar card, life insurance nominees/beneficiaries, fingerprint information, emergency contact details, citizenship, visa, work permit details;
- Recruitment, engagement or training records including cv's, applications, notes of interview, applicant references, qualifications, education records, test results (as applicable);

- Information about the Relevant Individual's medical condition – health and sickness records;
- The terms and conditions of employment/engagement, employment contracts with Capgemini and/or previous employer;
- Performance, conduct and disciplinary records within Capgemini and/or with previous employers; mobility records generated in the course of employment/work with Capgemini;
- Information relating to the Relevant Individual's membership with professional associations or trade unions;
- Leave records (including annual leave, sick leave and maternity leave);
- Financial Information relating to compensation, bonus, pension and benefits, salary, travel expenses, stock options, stock purchase plans, tax rates, taxation, bank account, provident fund account details;
- Information captured as result of monitoring of Capgemini assets, equipment, network owned and/ or provided by Capgemini;
- Any other Information as required by Capgemini.

B) Purposes of collection and processing of Personal Data

Capgemini may collect, process and disclose Personal Data of the Relevant Individual for purposes connected with its business activities including the following purposes, hereinafter the "**Agreed Purposes**":

- Managing the Relevant Individual's employment/ work with Capgemini including deployment/assignment of the individual to specific client projects;
- Record-keeping purposes; Payroll Administration, Payment of the Relevant Individual's salary or invoice; Performance Assessment and Training;
- Compliance with a legal requirement/obligations; health and safety rules and other legal obligations; Administration of benefits, including insurance, provident fund, pension plans; immigration, visa related purposes; Capgemini Group reporting purposes;

- Back ground verification purposes; credit and security checks;
- Operational issues such as promotions, disciplinary activities, grievance procedure handling;
- Audits, investigations, analysis and statistics, for example of various recruitment and employee retention programs;
- IT, Security, Cyber security and Access Controls;
- Disaster recovery plan, crisis management, internal and external communications;
- For any other purposes as Capgemini may deem necessary.

Capgemini only collects uses and discloses Personal Data for purposes that are reasonable and legitimate. Such Personal Data shall be processed in a manner compatible with the Agreed Purposes; unless the Relevant Individuals have consented to it being processed for a different purpose or the use for a different purpose is permitted by applicable law. There may be circumstances, when the Relevant Individual may have volunteered personal information and given explicit/fully informed consent to its processing (for example by submission of a CV).

C) Limited Access to Personal Data

Only those Employees who "need-to-know" or require access to function in their role should have access to Personal Data. Capgemini will not disclose Personal Data to any person outside Capgemini except for the Agreed Purposes, or with the Relevant Individuals' consent, or with a legitimate interest or legal reason for doing so, such as where Capgemini reasonably considers it necessary to do so and where it is permitted by applicable law. In each instance, the disclosed Personal Data will be strictly limited to what is necessary and reasonable to carry out the Agreed Purposes.

When Capgemini works with third parties which may have access to Personal Data in the course of providing their services, Capgemini contractually requires third party to process Personal Data only on

Capgemini's instructions and consistent with Capgemini's Data Privacy policies and Data Protection laws.

D. Disclosure and Transfer of Personal Data

Capgemini may, from time to time, disclose and/or transfer the Relevant Individuals' Personal Data to third parties (including but not limited) listed below:

- Group Companies, affiliate companies and/or other business associates, Capgemini's insurers and banks;
- External and internal auditors;
- Medical practitioners appointed by Capgemini;
- Administrator of Capgemini's mandatory provident fund scheme;
- Third parties who are involved in a merger, acquisition or due diligence exercise associated with Capgemini;
- External companies or third-party service providers Capgemini engages to perform Services on the Company's behalf;
- Third Parties providing certain information technology and data processing services to enable business operations;
- The applicable regulators, governmental bodies, tax authorities or other industry recognised bodies as required by any applicable law or guidelines of any applicable jurisdiction; and
- To any other party as deemed necessary by Capgemini.

Notwithstanding anything contained elsewhere, any Personal or Sensitive Personal Data may be disclosed by Capgemini to any third party as required by a Court of Law or any other regulatory or any other law enforcement agency established under a statute, as per the prevailing law without the Relevant Individual's consent.

As Capgemini is part of a larger group of companies operating internationally, it may transfer Personal Data for the Agreed Purposes described above to its own operations, or to other subsidiaries or affiliated

companies located in other jurisdictions. Such transfer is justified on the basis that there is a "need-to-know" and it is reasonable and legitimate to allow Capgemini companies and businesses to operate effectively and competitively. Personal information is only transferred to another country, including within the Capgemini Group, in particular only in as far as a reasonable level of data protection is assured in the recipient country

When using external data processers or transferring personal data to external third parties, Capgemini shall enter into agreements with appropriate contractual clauses for protection of Personal Data and confidentiality including requirements to process the Personal Data only in accordance with instructions from Capgemini and to take appropriate technical and organisational measures to ensure that there is no unauthorised or unlawful processing or accidental loss or destruction of or damage to Personal Data.

E. Retention and Deletion of Personal Data

It is Capgemini's policy to retain certain Personal Data of the Relevant Individuals when they cease to be employed/ engaged by Capgemini. This Personal Data may be required for Capgemini's legal and business purposes, including any residual activities relating to the employment/engagement, including for example, provision of references, processing of applications for re-employment/re-engagement, matters relating to retirement benefits (if applicable) and allowing Capgemini to fulfil any of its contractual or statutory obligations.

All Personal Data of the Relevant Individuals may be retained for periods as prescribed under law or as per Capgemini policy from the date the Relevant Individuals cease to be employed/engaged by Capgemini. The Personal Data may be retained for a longer period if there is a subsisting reason that obliges Capgemini to do so, or the Personal Data is necessary for Capgemini to fulfil contractual or legal obligations. Once Capgemini no longer requires the

Personal Data, it is destroyed appropriately and securely or anonymized in accordance with the law.

F. Security of Personal Data

Capgemini takes reasonable security measures to protect Personal Data against loss, misuse, unauthorized or accidental access, disclosure, alteration and destruction. Capgemini has implemented policies and maintains appropriate technical, physical, and organizational measures and follows industry practices and standards in adopting procedures and implementing systems designed for securing and protecting Personal Data from unauthorized access, improper use, disclosure and alteration.

G. Accuracy of Personal Data

Capgemini aims to keep all Personal Data as accurate, correct, up-to-date, reliable and complete as possible. However, the accuracy depends to a large extent on the data the Relevant Individuals provide. An Individual may access much of his Personal Information online using various "self-service" HR applications deployed in Capgemini. As such, Relevant Individuals must, agree to:

- Provide Capgemini with accurate, not misleading, updated and complete Personal Data of the Relevant Individuals and/or any relevant person (including their consents to such disclosures to Capgemini); and
- Up-date Capgemini as and when such Personal Data provided earlier becomes incorrect or out of date, by providing new details.

I. Monitoring of Relevant Individuals' use of company network resources

Capgemini may, from time to time, monitor the Relevant Individual's use of company premises, property and network resources (including computer systems, e-mails, phone calls, and internet) primarily for following purposes:

(i) facilitating business, securing personnel and property of Capgemini; For example, some of the locations are equipped with surveillance cameras.

(ii) maintaining a stable network environment for communications within Capgemini, and communications with external parties;

(iii) responding to any legal processes or to investigate any suspected breach of Relevant Individual's obligations under this Policy or other Capgemini's policies or applicable law; and

(iv) providing information to the Capgemini's management to ensure the proper utilization of Capgemini's resources.

This section is not meant to suggest that all employees will in fact be monitored or their actions subject to constant surveillance. It is meant to notify the fact that monitoring may occur and may result in the collection of personal information (e.g. through the use of company network resources). When using company equipment or resources, employees should not have any expectation of privacy with respect to their use of such equipment or resources.

VII. Data Protection Officer (Grievance Officer)

Any questions, discrepancies, and grievances of the Relevant Individuals with respect to processing of Personal Data may be made to the Capgemini Data Protection Officer (Grievance Officer) at dpo.in@capgemini.com whose name and contact details are available on Talent. http://talent.capgemini.com/in/pages/supportfunctions/legal/data_privacy/

The Grievance Officer shall redress the grievances of the Relevant Individuals expeditiously and in any event within the period prescribed under law. In case of any queries regarding the content, interpretation, implications of this Policy/BCR's, the Relevant Individuals may contact the Grievance Officer.

Notwithstanding the above, Capgemini reserves the right to decline to process any such request which may jeopardize the security and confidentiality of the Personal Data of others, as well as requests which are impractical or not made in good faith, or the circumstances as provided for under the law permitting Capgemini to refuse such request(s).

VIII. Employees/Relevant Individuals Obligations & Consequences of Violations

Every Capgemini Employee/Relevant Individual, who deals with or comes into contact with Personal Data regardless of its origin (EU or non EU originated data), shall have a responsibility to comply with the applicable law concerning data privacy, this Policy, the BCRs and specific privacy practices. The Employee/Relevant Individual should seek advice in the event of any ambiguity while dealing with Personal Data or in understanding this Policy and the BCRs.

The Employee/Relevant Individual shall be diligent and extend caution while dealing with Personal Data of others, in the course of performance of his/her duties and shall also, at all times:

(i) Prevent any un-authorized person from having access to any computer systems processing Personal Data, and especially: (a) un-authorized reading, copying, alteration, deletion or removal of data; (b) un-authorized data input, disclosure, uploading, transmission/transfer of Personal Data;

(ii) Abide by Capgemini internal logical and physical security policies and procedures;

(iii) Ensure that authorized users of a data-processing system can access only the Personal Data to which their access right refers;

(iv) Keep a record of which personal data have been communicated, when and to whom; Not provide any Personal Data to any third party without first consulting with his/her Manager or the Human Resources Department;

(v) Ensure that Personal Data processed on behalf of a third party (client) can be processed only in the manner prescribed by such third party;

(vi) Ensure that, during communication of Personal Data and transfer of storage media, the data cannot be read, copied or erased without authorization;

(vii) Immediately, on becoming aware report and notify any vulnerabilities and privacy related breach/security breaches (including potential risks).

(viii) Attend mandatory and voluntary trainings on security and data privacy including e-learnings and online sessions.

Failure to comply with the Policy/ the BCRs and applicable laws may have serious consequences and can expose both Capgemini and the Employee/Relevant Individual to damages, criminal fines and penalties. It is important to note that any non-compliance with this Policy/BCRs is taken very seriously by Capgemini and may lead to initiation of appropriate disciplinary actions including but not limited to Employee dismissal or Relevant Individual termination.

Note:

1. Capgemini reserves the right, to amend this Policy from time to time.