

Public version

Capgemini Binding Corporate Rules

For Controller Activities





Table of Contents

Introduction.....	3
Definitions.....	4
1. Scope of the BCR	6
1.1 Material Scope	6
1.2 Geographical Scope.....	7
2. Bindingness of the BCR.....	7
2.1 Bindingness upon Capgemini Companies.....	7
2.2 Bindingness upon Capgemini Employees	7
3. Data protection principles implementation within Capgemini.....	8
4. Internal and External Processing	11
5. Transparency.....	13
6. Data Subjects’ enforcement rights.....	14
7. Data Subjects’ requests handling procedure	15
8. Capgemini data protection organisation	15
9. Data protection awareness and training	16
10. Privacy by design	16
11. Audits related to the BCR	18
12. Capgemini’s liability in case of a breach of the BCR	18
13. Jurisdiction	18
14. Applicable DP Law and potential conflicts with the BCR	19
15. Transfer impact assessments.....	22
16. Management of of access requests issued by third countries authorities.....	20
17. Cooperation duties	22
18. Easy access to the BCR.....	22
19. Update of the BCR.....	22
Appendix 1 - Capgemini companies bound by the BCR	23
Appendix 2 - Capgemini processing activities	39
Appendix 3 - Capgemini Data Protection Organisation	58
Appendix 4 – Data Subjects Requests Handling Procedure.....	59

Version History

Version History		
Version	Date	Comments
V.1	March 2016	Initial version
V.2	January 2019	Update to comply with new requirements under the General Data Protection Regulation (GDPR)
V. 2.1	March 2023	Update to comply with new requirements
Authors and contributing		
Role	Activity	Comments
Senior legal counsel	Draft	
Group Data Protection Officer (GDPO)	Draft & review	
Document Distribution		
Status	Location	Action/Information
Public	Capgemini website	
Document Reviewed and Approved by		
Role	Responsibility	Comments
Group Data Protection Officer	Review	
Group General Counsel	Approval	
Commission Nationale de l'Informatique et des Libertés (CNIL)	Approval	



Introduction

As a global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organisations to realize their business ambitions through an array of services from strategy to operations. Capgemini therefore processes large amounts of personal data.

Capgemini is committed to protecting all personal data entrusted to it as part of its activities as a Data Controller. As an international group with entities located in more than 40 countries, it is important to Capgemini that information flows freely and securely. Providing an appropriate level of protection to the personal data being transferred within the group, is one of the reasons why Capgemini has chosen to implement these Binding Corporate Rules (**BCR**) which were first approved by the French data protection authority, the CNIL, in March 2016. This is all the more important as legal data protection and legal data security are crucial for each affiliate of Capgemini. The financial and reputational risks are high.

For this very reason, Capgemini's BCR should not be construed as a mere transfer mechanism, but rather as a comprehensive personal data protection framework defining our entire accountability approach to the processing of personal data.

Capgemini's BCR define indeed not only the principles with which it shall comply with when processing personal data but also specify the procedures designed to address Capgemini compliance with applicable data protection laws and in particular with the General Data Protection Regulation 2016/679 (**GDPR**).



Definitions

The terms used in this document are defined as follows:

“Applicable DP Law” means any applicable data protection regulation that may apply and in particular (i) the European Regulation n° 2016/679 relating to the processing of Personal Data (**GDPR**), and (ii) any applicable laws and regulations relating to the processing of Personal Data.

“Binding Corporate Rules” or **“BCR”** means a Data Protection policy which is adhered to by a controller or processor for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity. They comprise this document together with its appendices, and the BCR-P.

“Binding Corporate Rules for Controller Activities” or **“BCR-C”** means the BCR applicable to Capgemini’s activities as a Data Controller, and in particular, where a Capgemini Company acting as Controller Transfers Personal Data to another Capgemini Company acting as Controller or Processor. **“Binding Corporate Rules for Processor Activities”** or **“BCR-P”** means the BCR applicable to Capgemini’s activities as a Data Processor.

“Capgemini Business Contact” means a Capgemini supplier, subcontractor, shareholder, client or partner.

“Capgemini” or **“Group”** means all the entities owned and/or controlled directly or indirectly by Capgemini SE.

“Capgemini Company(ies)” means any entity which is part of the Group and which is bound by the BCR.

“Capgemini Client” means any natural or legal person to which Capgemini provides services to, pursuant to an agreement.

“Capgemini Employee” means any and all current, former or prospective staff member of

Capgemini, including agency workers and interns.

“Data Controller” or **“Controller”** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

“Cybersecurity Organisation” means the global function creating and managing global security policies; and tracking compliance from Business Units and Global Business Lines. The Cybersecurity Organisation is made up of a network of Cybersecurity Officers appointed for each Business Unit.

“Data Protection Impact Assessment” or **“DPIA”** means a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of Personal Data by assessing them and determining the measures to address them.

“Data Protection Officer” or **“DPO”** means the designated Capgemini Employees possessing expert knowledge of data protection law and practices, dedicated to advise, inform, and monitor compliance with the Applicable Law, and who are part of the Data Protection Organisation described in Section 8.

“Data Subject” means any identified or identifiable natural person whose Personal Data is processed.

“EEA Capgemini Company” means any Capgemini Company located in the European Economic Area (or **“EEA”**).

“Non-EEA Capgemini Company” means any Capgemini Company located outside of the EEA.

“Employee Personal Data” means Personal Data relating to a current, former or prospective Capgemini Employee.

“EU Model Clauses” or **“Model Clauses”** » means the contractual clauses issued by the



European Commission to frame data transfers from Controllers established in the EEA to Controllers established outside of the EEA and from Controllers established in the EEA to Processors established outside of the EEA.

“Personal Data” means any information relating to an identified or identifiable natural person (i.e. **“Data Subject”**). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“Processing” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Data Processor” or “Processor” means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

“Personal Data Breach” or “Data Breach” means the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, whether resulting from a security breach or not.

“Service Agreement” means a written agreement between a Controller and Processor whereby the Processor shall provide services to the Controller and which entails the processing of Personal Data by the Processor under the instructions of the Controller.

“General Data Protection Regulation” or “GDPR” means Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

“Intra-Group Agreement” means the legally binding agreement designed to make the BCRs binding upon the Capgemini Companies

“Special Categories of Personal Data” means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

“Supervisory Authority(ies)” or “Data Protection Authority(ies)” means the public authorities responsible for monitoring the application of the GDPR and/or any Applicable Laws.

“Transfer” means the disclosure, transmission or the process of making Personal Data available to any third-party.



1. Scope of the BCR

The BCR apply to and frame all Personal Data transfers within Capgemini and drive the Group's accountability approach. As a result, the BCR constitute the data protection policy defining the applicable data protection principles with which Capgemini shall comply.

Where Applicable DP Law requires a higher level of protection than the commitments defined under the BCR, it will take precedence over the BCR.

1.1 Material Scope

These BCR apply to all Personal Data processed within Capgemini, where Capgemini is acting as Controller. More specifically, these BCR shall apply to and frame the following Transfers of Personal Data:

- From a Capgemini Company acting as Controller to another Capgemini Company acting as Controller;
- From a Capgemini Company acting as Controller to a Capgemini Company acting as Processor.

In practice, where acting as Controller, Capgemini mainly processes the Personal Data of its Employees and Business Contacts. The purposes of such processing are related to human resources, internal and external communication, marketing, compliance, etc.

For a more comprehensive view of Capgemini's processing activities as a Controller, please refer to Appendix 2.



1.2 Geographical Scope

These BCR cover all Personal Data being transferred and further processed within the Group, regardless of the origin of the Personal Data. In practice, this means that the BCR will apply to Personal Data transferred from:

1. An EEA Capgemini Company to another EEA Capgemini Company;
2. An EEA Capgemini Company to a Non-EEA Capgemini Company;
3. A Non-EEA Capgemini Company to an EEA Capgemini Company; and
4. A Non-EEA Capgemini Company to another Non-EEA Capgemini Company.

The Capgemini Companies, bound by the BCR, are listed on the Capgemini [website](#).

2. Bindingness of the BCR

Each Capgemini Company, and its Employees, is legally bound by and required to comply with the BCR.

2.1 Bindingness upon Capgemini Companies

In practice, each entity of Capgemini gives a power of attorney to Capgemini International BV to sign the Intra-group Agreement on its behalf so that each Capgemini entity is effectively bound to comply with the BCR vis-à-vis each other. By signing the Agreement, the Capgemini entity commits to comply with the provisions of the BCR, and to implement them within its own organisation.

As for newly acquired Capgemini entities, located outside the EEA, no Personal Data shall be transferred to them, until they are effectively bound by the BCR according to the above-mentioned mechanism.

2.2 Bindingness upon Capgemini Employees

All Capgemini Employees are bound by the BCR through a specific mention in their employment contracts and/or through the obligation, contained in all employment contracts, to comply with the Group's policies, which include the BCR.

As further detailed in Sections 9 and 16 of the BCR, Capgemini Employees are made aware of the BCR, and the ensuing obligations, through internal communication and training. Capgemini Employees are also made aware of the fact that the non-compliance with the BCR may lead to sanctions according to applicable local laws.



3. Data protection principles implementation within Capgemini

Capgemini is committed to complying with the data protection principles set out in these BCR, irrespective of Applicable DP Law, unless Applicable DP Law is providing more stringent requirements than those set up in the BCR. All these principles are promoted and implemented within Capgemini through a set of privacy by design policies and trainings.

Furthermore, where acting as Controller, Capgemini shall comply with Applicable DP Laws.

3.1 Clear identified purpose

Where acting as Controller, Capgemini shall only process Personal Data for specified, explicit and legitimate purposes and not further process it in a manner that is incompatible with those purposes.

In practice, this means that the purposes of every Processing must be determined and expressly defined prior to the collection of Personal Data. In addition, Capgemini must ensure that Personal Data are not further processed in a way incompatible with the purposes for which they were originally collected.

3.2 Legal basis

Where acting as Controller, Capgemini shall only process Personal Data if one of the following conditions is fulfilled:

1. The Processing is necessary to comply with a legal obligation to which Capgemini is subject. **E.g.** *communicate Personal Data to tax authorities for instance.*
2. The Processing is necessary for the performance of a contract to which the Data Subject is party or to take steps, at the requests of the Data Subject, prior to entering into a contract. **E.g.** *in the case of employment contract for instance, Processing salary information and bank account details is necessary to pay salaries.*
3. The Processing is necessary for the purposes of the legitimate interest pursued by Capgemini or by a third party. **E.g.** *where Capgemini has a legitimate interest in getting to know its clients' preferences to be able to personalise its offers, and ultimately offer services that better meet the needs and expectations of clients.* Where relying on legitimate interest as a legal basis, Capgemini will perform a balancing test to determine whether its legitimate interests are overridden by those of the Data Subjects, or their fundamental rights and freedoms, in circumstances where the Personal Data of such Data Subjects must be protected.
4. The Processing is necessary to protect the vital interests of the Data Subject or of another natural person. **E.g.** *where the Data Subject is physically or legally unable to give his/her consent to the Processing, and his/her safety or health is at stake.*



5. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. **E.g.** *where an officer of a public body competent for investigating a crime asks Capgemini for cooperation in an on-going investigation.*

In practice, Subsections 4) and 5) above are very unlikely to apply to Capgemini.

6. Where none of the above-mentioned legal basis can apply to a situation at stake, Capgemini can seek to obtain the Data Subject's consent. To be valid, such consent shall be freely given, specific, informed and unambiguous.

In practice, this means that Capgemini shall not engage in any data Processing activity if it is not able to demonstrate that one of the above-mentioned conditions is fulfilled.

3.3 Data minimisation

Capgemini shall only collect and further process the Personal Data which is strictly necessary in relation to the purposes defined beforehand.

In practice, this means that when designing a project involving the Processing of Personal Data, Capgemini must determine which Data is strictly necessary to achieve the contemplated purposes. As a result, Capgemini shall not collect and store non-essential Personal Data just to have the possibility to use such Personal Data for a hypothetical purpose which it would define in the future.

3.4 Data quality

Capgemini shall ensure that Personal Data is accurate and kept up to date throughout the lifecycle of the Processing.

In practice, this means that Capgemini must provide Data Subjects with means to request inaccurate Data to be corrected, updated or deleted as detailed in the Data Subjects' requests handling procedure described in Appendix 3. In addition, Capgemini must ensure that it is technically able to delete or rectify the Data upon request of the Data Subjects.



3.5 Data retention limitation

Capgemini must keep Personal Data for no longer than necessary in relation to the purposes for which the Personal Data were collected.

This means that Capgemini must define the data retention period beforehand and according to the purposes of the Processing taking into account and balancing the elements listed below:

- the applicable legal requirements;
- the business needs;
- the interests of the Data Subjects whose Personal Data are processed.

In practice, for each project involving the Processing of Personal Data, Capgemini must put in balance the overall objective of the project and document such assessment.

3.6 Security

Capgemini must implement all the appropriate technical and organisational measures to ensure the security of the Personal Data entrusted to it, and guard against unlawful access, loss, destruction, or alteration of the Personal Data.

In practice, this means that, as a minimum, Capgemini must implement the requirements and good practices defined by the Cybersecurity Organisation. In the event of a Data Breach, Capgemini must document the Breach in a dedicated register and notify it to the relevant management and DPO according to the internal Data Breach procedure. Where the Data Breach is likely to result in a risk to the rights and freedoms of individuals, Capgemini must also notify the relevant Supervisory Authority(ies), subject to Applicable DP Laws, without undue delay and no later than 72 hours after having become aware of the it. In case the Data Breach is likely to result in a high risk to the rights and freedoms of the Data Subjects, Capgemini must notify them.

3.7 Processing of Special Categories of Personal Data

Capgemini shall only process Special Categories of Personal Data when strictly necessary or legally required. When processing Special Categories of Personal Data, Capgemini must implement reinforced technical and organisational measures to ensure the security of the Processing.

3.8 Automated individual decision

Data Subjects have the right not to be subject to a decision based solely on automated Processing, including profiling, which produces legal effects concerning them or significantly affects them. However, this right does not apply if the decision is:

1. Necessary for entering into, or performance of, a contract between the Data Subject and Capgemini;
2. Authorised by Union or Member State law to which Capgemini is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests;
3. Based on the Data Subject's explicit consent.



Capgemini must strive to explain to the Data Subjects the underlying logic of any automated Processing they are subject to.

In practice, this must be done in the information notice which shall be provided to data subjects as stated under Section 6 of these BCR.

4. Internal and External Processing

4.1 Basic obligation – Data Processing Agreement or Clause (“DP Clause”) in the Service Agreement

Capgemini shall rely on Processors either within or outside of the Group only to the extent that such Processor provide sufficient guarantees to implement technical and organisational measures to ensure that the Processing is carried out in compliance with Applicable DP Law and the principles set out in the BCR.

In practice, this means that, when relying on a third party, Capgemini shall enter into a Service Agreement which sets up the conditions under which the processing activities must take place. The Service Agreement shall contain a DP Clause reflecting as a minimum that the Processor must:

- process the Personal Data only on the documented instructions of Capgemini – including with regard to Transfers to a country located outside of the EEA;
- ensure that persons authorised to process the Personal Data have committed themselves to confidentiality;
- implement technical and organisational measures to ensure an appropriate level of protection to the Personal Data;
- only use a sub-Processor with the prior specific or general authorisation of Capgemini and enter into a Service Agreement with the sub-Processor providing the same obligations as the ones described here;
- assist Capgemini for the fulfilment of its obligation to respond to requests from Data Subjects;
- assist Capgemini in ensuring compliance with its obligations in terms of security of the Processing, carrying out DPIAs, reporting Data Breaches;
- at the choice of Capgemini and as agreed in the Service Agreement, to either delete or return the Personal Data after the end of the provision of services relating to the Processing;
- make available to Capgemini all the information necessary to demonstrate compliance with its obligations under the GDPR, and in particular allowing Capgemini to conduct audits;
- report any Data Breach to Capgemini without undue delay.

In any case, where relying on a third party, Capgemini shall carry out an assessment of the data protection and security guarantees which such third party commits to implement and to comply with.

4.2 Additional obligation in case of a data transfer to a third country



In addition to the implementation of the above-mentioned Data Processing Agreement or Clause, where Processing or Sub-processing gives rise to Transfers to third countries, Capgemini must guarantee that an adequate level of protection is provided, as per the requirements defined below.

In practice, this means that where an EEA Capgemini Company acting as Controller transfers Personal Data to a non-EEA Capgemini Company acting either as Controller or as Processor, these BCR shall apply.

Where an EEA Capgemini Company acting as Controller transfers Personal Data to a third party located out of the EEA and acting as Controller or Processor, Capgemini must enter into the relevant EU Model Clauses.

Where a Non-EEA Capgemini Company acting as Controller transfers Personal Data to a third party located in a third country, appropriate framework may need to be implemented to comply with Applicable DP Law, or other legal requirements. In case of such transfer to another Capgemini Company, such transfer can benefit from the BCR and may require additional guarantees to be implemented to comply with Applicable DP Law.

In addition to the obligations detailed herein, where transferring Personal Data from the EEA to a third country which does not benefit from an adequacy decision granted by the European Commission, Capgemini shall further comply with the provisions of Sections 15 & 16 of these BCR.



5. Transparency

Capgemini must provide the Data Subject with all the required information regarding the Processing of his or her Personal Data.

In practice, this means that where Personal Data relating to a Data Subject are collected directly from him or her, Capgemini must provide them with the following information:

- The identity and contact details of the Capgemini Company acting as Controller;
- The contact details of the competent local DPO;
- The purposes of the Processing for which the Personal Data are intended as well as the legal basis for the Processing;
- Where the Processing is based on Capgemini's legitimate interest, the description of the interest pursued by Capgemini;
- The recipients or categories of recipients if any;
- Where applicable, the fact that Capgemini intends to transfer Personal Data outside of the EEA, and the existence or absence of an adequacy decision by the European Commission, or the reference to the appropriate safeguards (i.e. BCR or EU Model Clauses) and how to obtain a copy of them or where they have been made available;
- The period for which Personal Data will be stored, or if it is not possible, the criteria used to determine this period;
- The right for the Data Subject to request access to and rectification or erasure of Personal Data or restriction of Processing or to object to the Processing as well as the right to data portability;
- Where the Processing is based on the consent of the Data Subject, the right to withdraw consent at any time, without affecting the lawfulness of the Processing;
- The right to lodge a complaint before a Supervisory Authority;
- Whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and the possible consequences of failure to provide such Data;
- The existence of automated decision-making, including profiling, and information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

Where the Personal Data have not been obtained directly from the Data Subject, Capgemini shall still provide him or her with the above-mentioned information as well as with the description of the categories of Personal Data and the source of said Personal Data. Capgemini must provide the aforementioned information to the Data Subject within a reasonable period after obtaining the Personal Data. If the Data is used to contact the Data Subject, Capgemini must provide him or her with the information at the time of that first communication.



6. Data Subjects' enforcement rights

Data Subjects can enforce provisions of the BCR on Capgemini, as third-party beneficiaries, as detailed below:

- The data protection principles detailed in Sections 3, 4 and 5;
- The fact that Capgemini grants easy access to the BCR, as detailed in Section 16;
- The rights of access, rectification, erasure, restriction, objection to Processing, and the right not to be subject to decisions solely based on automated Processing granted to Data Subjects, as detailed in Section 5;
- The obligation, for each Capgemini Company, to notify the competent Supervisory Authority as well as the Capgemini headquarters, in case of a conflict between the local legislation and the BCR, as detailed in Section 14;
- The right for Data Subjects to complain through the internal complaint mechanism of Capgemini, as detailed in Section 7;
- The duty for Capgemini to cooperate with the Supervisory Authorities, as detailed in Section 15;
- The rights for Data Subjects to lodge a complaint with the competent Supervisory Authority and/or before the competent courts of law, as detailed in Sections 7 and 13;
- The obligation for each EEA Capgemini Company transferring Personal Data to a Non-EEA Capgemini Company on the basis of the BCR, to accept liability for any breaches of the BCR by the Non-EEA Capgemini Company which received the Personal Data, as detailed in Section 12;
- The fact that in case of a breach of the BCR by a Non-EEA Capgemini Company, it is up to the EEA Capgemini Company which exported the Personal Data to demonstrate that the recipient (i.e. the Non-EEA Capgemini Company) did not breach the BCR, as detailed in Section 12.
- The fact that they may enforce provisions of the BCR as described under this Section.



7. Data Subjects requests handling procedure

Capgemini has set up an internal Data Subjects requests handling procedure, described in Appendix 3, allowing Data Subjects to contact the local DPO either to exercise their rights in relation to the Processing of their Personal Data, or to complain of a breach of the Applicable DP Law.

The Data Subjects requests handling procedure describes to the Data Subjects where and how to express a request and/or complaint, the delays for the reply to the request or complaint, the consequences in case of the rejection of the request or complaint, the consequences if the request or complaint is considered justified, and the right for the Data Subject to lodge a claim before the competent courts or Supervisory Authorities.

8. Capgemini data protection organisation

The Data Protection Officers, part the Data Protection organisation depicted in Appendix 2, monitor the legal compliance to the Applicable DP Law of the Capgemini Company within their scope, advise in all matters that relate to data protection, implement the global data protection program, handle or advise on Data Breaches and have an active relationship with the local Supervisory Authority.

As part of the Legal function, Global, Regional and Local Data Protection Officers are supported in their task by the local legal teams. The Data Protection Officers report quarterly to the local country board or Executive Comity on privacy related matters such as critical Data Breaches, Data Subject Requests, privacy issues in large deals etc.

In addition to this regulatory role, the Group, Regional and Local DPOs act as business facilitators by validating the Capgemini approach to data protection and data security. The Group, Regional and Local DPO also have a key role in helping the business identify new business opportunities by identifying the gap between the strict data privacy legal requirements with which Capgemini must comply and the requirements defined by clients that might warrant additional offers.

In practice, this means that the Data Protection organisation should be consulted in any and all new projects to ensure that such new projects embed data protection constraints in the design phase. In addition, to support the business further the Group DPO will provide templates and procedures to make sure that the data protection constraints are taken into account by default in the different offers and services.

The Data Protection Officer network is completed by a network of Data Protection Champions who represent each Group function and each Global Business Line. Data Protection Champions are not part of the legal organisation but were designated amongst Group Functions and Global Business Lines representatives to ensure that the legal constraints and Group guidance are actually reflected at each level of the organisation. More importantly, the Data Protection Champions liaise with the Data Protection organisation to make sure the program properly integrates business needs and expectations.

Finally, it must be noted that the Data Protection organisation works closely with the Group Cybersecurity Officer and the Cybersecurity Organisation.



9. Data protection awareness and training

Capgemini has adopted and implemented a mandatory data protection training program to ensure that all Capgemini Employees are aware of and understand the key principles and requirements of data protection, as well as these BCR.

The training program, which is defined in a dedicated document internal to Capgemini, is articulated around the following pillars:

- General Training: A common core knowledge describing the applicable principles when Processing Personal Data;
- Practical Training: An overview of the existing applicable policies and processes;
- Functions Training: Tailor-made training designed to address the needs of specific functions (such as HR or marketing for instance).

In addition to the mandatory training, Capgemini is committed to promoting the implementation of data protection principles within the Group's organisation through a set of privacy by design policies and communication actions dedicated to raising awareness among the different Capgemini communities.

10. Privacy by design

Each Capgemini Company is responsible for and able to demonstrate compliance with the BCR and the Applicable DP Law in general.

Where acting as Controller, Capgemini must keep and maintain, in writing, a record of Processing containing the following information:

- The name and contact details of the Capgemini Company acting as Controller, the DPO, and where applicable the joint Controller;
- The purposes of the Processing;
- A description of the categories of Data Subjects and of the categories of Personal Data;

The categories of recipients to whom the Personal Data have been or will be disclosed including recipients located outside of the EEA;

10.1 Record of Processing



Capgemini must keep and maintain, in writing, a record of Processing containing the following information:

- The name and contact details of the Capgemini Company acting as Controller, the DPO, and where applicable the joint Controller;
- The purposes of the Processing;
- A description of the categories of Data Subjects and of the categories of Personal Data;
- The categories of recipients to whom the Personal Data have been or will be disclosed including recipients located outside of the EEA;
- Where applicable, Transfers of Personal Data to countries located outside the EEA, including the identification of such countries.

Where a Capgemini Company is acting as another Capgemini Company's Processor, it shall also maintain a record of Processing containing the following information:

- The name and contact details of the Capgemini Company acting as the Processor and of each Capgemini Company acting as Controller on behalf of which the Capgemini Company acting as Processor is acting, and the DPO;
- The categories of Processing carried out on behalf of each Capgemini Company acting as Controller;
- Where applicable, the Transfers of Personal Data to countries located outside the EEA, including the identification of such countries and the documentation of suitable safeguards;
- Where possible, a general description of the technical and organizational security measures.

Capgemini shall make the record available to the competent Supervisory Authority upon request.

In practice, to comply with this requirement, Capgemini uses a dedicated tool which allows it to digitally record all Personal Data Processing and extract a complete record of Processing for its Controller's activities.

10.2 Data Protection Impact Assessment

Capgemini must comply with the obligation to carry out Data Protection Impact Assessments where a Personal Data Processing presents risks to the rights and freedoms of a Data Subject.

In practice, this means that Capgemini shall implement a DPIA Policy designed to identify the risks of a Processing and, depending on the severity of such risk, either launch a DPIA or not. The decision to carry out a DPIA will rest on several factors, including the criteria and the lists identified by the Supervisory Authorities.

The DPIA process is described in a DPIA Policy and is articulated around 4 steps:

1. The description of the Processing
2. Assessing the necessity and proportionality of the Processing
3. Risk assessment
4. Risk mitigation.



11. Audits related to the BCR

Capgemini must carry out data protection audits covering all aspects of the BCR on a regular basis and according to our BCR and Data Protection audit program.

The audits shall be carried out either by internal or external qualified and independent auditors according to a schedule developed by the Group DPO on a yearly basis. In addition, the Global, Regional and Local DPOs can request that additional audits be carried out. Such audits may cover specific applications, IT systems or databases that process Personal Data; or may be carried out for an entire geography.

The audit report, including the proposed corrective actions to address and mitigate the risks, must be communicated to the Data Protection organisation and to the top management and shall be made available to the competent Supervisory Authority(ies) upon request.

12. Capgemini's liability in case of a breach of the BCR

Each EEA Capgemini Company exporting Personal Data to a Non-EEA Capgemini Company shall be liable, towards Data Subjects, for any breaches of the BCR caused by the Non-EEA Capgemini Company.

In all other cases ((1) transfers from an EEA Capgemini Company to another EEA Capgemini Company; (2) transfers between two Non-EEA Companies; or (3) transfers from a Non-EEA Company to an EEA Company) each Capgemini Company shall be liable for a breach of the BCR it caused.

Please find the full list of Capgemini Companies, including contact details, under Appendix 1.

In practice, this means that the Capgemini Company identified as bearing the responsibility according to the above-mentioned scheme, must accept responsibility for paying compensation and to remedy the breach where it caused a damage to a Data Subject.

In addition, it shall be up to Capgemini to demonstrate that it did not breach the BCR. In the case of a Transfer between an EEA Capgemini Company and a Non-EEA Capgemini Company, if the alleged breach is blamed on the Non-EEA Capgemini Company, the EEA Capgemini Company must demonstrate that the Non-EEA Capgemini Company did not breach the BCR.

13. Jurisdiction

In case of a breach of any rights guaranteed under the BCR, Capgemini encourages Data Subjects to use the dedicated complaint handling procedure described in Section 7.

However, Data Subjects are also entitled to lodge a complaint before the competent Supervisory Authority – which can either be that of the EU Member State of their habitual residence, place of work or place of the alleged infringement.

In addition, Data Subjects can lodge a complaint before the competent court of law.

Where the Processing is carried out by a Non-EEA Capgemini Company, the Data Subject can lodge a complaint before the competent court of law according to the applicable legislation; unless the Non-EEA Capgemini Company is subject to the GDPR in which case the above provisions shall apply.



14. Applicable DP Law and potential conflicts with the BCR

Where Applicable DP Law requires a higher level of protection for Personal Data, it shall take precedence over the BCR. In any case, Personal Data will be processed in compliance with the Applicable DP Law.

Where a Capgemini Company has reasons to believe that the applicable local legislation prevents it to fulfil its obligations under the BCR, it must inform Capgemini's headquarters as well as the DPO organisation, unless prohibited to do so by a law enforcement authority.

In addition, if a Capgemini Company is subject to local legal requirements having substantial adverse effects on the guarantees provided by the BCR (including binding requests for disclosure of Personal Data), it should notify it to the competent Supervisory Authority, unless prohibited to do so by a law enforcement authority. Capgemini will use its best efforts to alert the competent Supervisory Authority, and will, in any case, provide the Authority, annually, general information regarding the requests for disclosure of Personal Data it received.

Section 16 below provides further information on how Capgemini shall manage any Personal Data access request issued by third countries public authorities.

15. Transfer impact assessments

Capgemini EEA Companies shall only Transfer Personal Data to non-EEA Capgemini Companies established in a third country (i.e. a country located outside of the EEA and which does not benefit from an adequacy decision delivered by the European Commission) pursuant to the BCR where they have assessed that the laws and practices of such third country do not prevent the non-EEA Capgemini Company to which the Personal Data are transferred to from fulfilling its obligations under the BCR.

The assessment of the laws and practices of the third country shall be made under the assumption that laws and practices respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives of public interest.

In practice, where conducting a Transfer Impact Assessment (TIA), Capgemini shall consider:

- (i) The specific circumstances of the Transfer(s) or set of Transfers and of any envisaged onward transfer(s) within the same third country or to another third country, including:
 - a. The purposes for which the data are transferred and processed (e.g. HR, IT support, etc.);
 - b. The types of entities involved in the Transfer;
 - c. The economic sector in which the Transfer or set of Transfers occur;
 - d. The categories and format of the Personal Data transferred;
 - e. The location of the processing including storage; and
 - f. The transmission channels used.
- (ii) The laws and practices of the third country of destination relevant in light of the circumstances of the Transfer, including those requiring to disclose Personal Data to public authorities or authorising access by such authorities and those providing access to these Personal Data during the transfer, as well as the applicable limitations and safeguards.



- (iii) Any relevant contractual, technical or organizational safeguards implemented to supplement the safeguards under the BCR including measures applied during the transmission and to the processing of Personal Data in the country of destination.

Where the TIA reveals that supplementary safeguards must be implemented in addition to those provided under the BCR, the EEA Capgemini Company(ies) and the competent Data Protection Officer(s), shall be notified and involved in the implementation of such safeguards.

Capgemini shall continuously monitor the laws and practices of third countries where Capgemini Companies are established and where Personal Data is transferred pursuant to the BCR, in order to identify any changes that would require the update of the TIAs and the implementation of supplementary safeguards.

Where a non-EEA Capgemini Company has reasons to believe that it has become subject to laws and practices that would prevent it from fulfilling its obligations under the BCR, it shall notify the Group Data Protection Officer, to ensure that any Transfer of Personal Data to the third country where such non-EEA Capgemini Company is established benefits from the appropriate supplementary safeguards. The relevant Data Protection Officer(s) shall support the Capgemini Companies acting as data exporter and data importer to identify and implement the appropriate supplementary measures.

Where a Capgemini Company determines that the BCR can no longer be complied with – even where supplementary measures have been implemented – for a specific Transfer or set of Transfers, or if instructed by the competent Supervisory Authority, it shall suspend such Transfer or set of Transfers until compliance can be achieved. If compliance with the BCR is not restored within one month of suspension, the Transfer or set of Transfers at stake shall end. Personal Data that were transferred prior to the suspension and copies thereof shall be returned or destroyed in their entirety at the choice of the EEA Capgemini Company acting as data exporter.

Capgemini shall document and record TIAs – including the nature of the supplementary safeguards that are selected and implemented. Such documentation shall be made available to the competent Supervisory Authority upon request.

In practice, the assessments of laws and practices of third countries, as well as the specific TIAs conducted for a Transfer or set of Transfers and the supplementary safeguards identified and implemented, as well as all relevant documentation, shall be made available to all Capgemini Data Protection Officers. Thus, enabling Capgemini to ensure compliance with the BCR and consistency in the manner they are implemented throughout the group.



16. Management of access requests issued by third countries public authorities

Where legally permitted, a non-EEA Capgemini Company acting as data importer shall strive to notify the EEA Capgemini Company acting as data exporter and, where possible, the Data Subject(s) involved where it:

- (i) receives a legally binding request issued by a public authority for disclosure of Personal Data transferred pursuant to the BCR
- (ii) becomes aware of any direct access by the public authorities to Personal Data transferred pursuant to the BCR

Such notification shall include all information available to the non-EEA Capgemini Company, including in particular: the personal data request, the requesting authority, the legal basis for the request and the response provided.

Where prohibited from notifying the EEA Capgemini Company acting as data exporter and/or the Data Subjects involved, the non-EEA Capgemini Company acting as data importer shall use its best efforts to obtain a waiver of such prohibition in order to communicate as much information as possible and as soon as possible. It shall document such efforts to be able to demonstrate them upon request from the EEA Capgemini Company acting as data exporter.

Each Capgemini Company monitors and records, monthly, information regarding the requests to access Personal Data issued by public authorities it receives. Such information includes in particular:

- The number of requests
- The types of data requested
- The authority(ies) who issued the request
- Whether the requests have been challenged
- The outcome of such challenged

Capgemini Data Protection Officers shall have access to that information. Information regarding the access requests shall be preserved for as long as necessary and shall be made available to the competent Supervisory Authorities upon request.

Where a Capgemini Company is or becomes prohibited from reporting on the information listed above, it shall notify the Group Data Protection Officer without undue delay.

Capgemini shall systematically review the legality of a request to access or otherwise disclose Personal Data. Capgemini shall challenge such request if, after careful consideration, it determines that there are reasonable grounds to consider that the request is unlawful under applicable law, applicable obligations under international law, and principles of international comity. Capgemini shall, under the same conditions, pursue possibilities of appeal.

Where challenging a request, Capgemini will seek interim measures to suspend the effects of the request until the competent judicial authority has ruled on its merits. Capgemini shall not disclose the Personal Data requested until required to do so under the applicable procedural rules.

Where Capgemini is required to respond to the request, it shall provide the minimum amount of information permissible. In addition, any Transfer or set of Transfers carried out by Capgemini to comply with a request issued by a public authority shall not be massive, disproportionate, or indiscriminate in a manner that would go beyond what is necessary in a democratic society.



17. Cooperation duties

Capgemini must cooperate with the Supervisory Authorities.

In practice, this means that Capgemini shall comply with the advice of the competent Supervisory Authorities and accept to be audited by them upon request.

18. Easy access to the BCR

A public version of the BCR is made available on Capgemini's website as well as on the Capgemini Intranet.

In practice, the body of the public version of the BCR-C is identical to that of the internal version. However, there are some differences in the appendices. More specifically, the public version of the BCR-C is structured as follows:

- The full body of the BCR-C
- Appendix 1 Capgemini companies bound by the BCR
- Appendix 2 Capgemini processing activities
- Appendix 3 Capgemini data protection organization
- Appendix 4 Data Subjects' requests handling procedure – *this version of the procedure was drafted to inform the data subjects on how Capgemini is processing their data subject requests. The internal version of the BCR-C contain another version of the procedure which is meant to support the DPOs and operational to manage data subjects requests.*

In case of a significant update of the BCR, Capgemini shall inform the Employees through a communication on the Intranet. Capgemini shall publish the public version of the BCR on the company's Intranet and conduct a communication campaign to ensure that Capgemini Employees are made aware of their obligations under the BCR.

19. Updates of BCR

Capgemini must communicate an updated list of the Capgemini Companies to its lead Supervisory Authority, the CNIL, once a year.

Where Capgemini chooses to make substantial modifications to the BCR, to reflect new regulatory requirements or changes to its internal organisation for instance, it shall inform the CNIL as well as all the Capgemini Companies.



Appendix 1 – Capgemini companies bound by the BCR

FRANCE	
Capgemini Service SAS SIRET 65 202 579 200 084	11 rue de Tilsitt, 75017 Paris, France dpocapgemini.global@capgemini.com
Capgemini SE SIRET 33 070 384 400 036	11, rue de Tilsitt, 75017 Paris, France dpocapgemini.global@capgemini.com
Capgemini Gouvieux SAS SIRET 42 857 118 600 017	11 rue de Tilsitt, 75017 Paris, France dpocapgemini.global@capgemini.com
Immobilière Les Fontaines SARL SIRET 42 177 631 100 019	11 rue de Tilsitt, 75017 Paris, France dpocapgemini.global@capgemini.com
SCI Paris Etoile SIRET 33 133 855 800 033	11 rue de Tilsitt, 75017 Paris, France dpocapgemini.global@capgemini.com
Capgemini Latin America SAS SIRET 48 760 678 200 018	11 rue de Tilsitt, 75017 Paris, France dpocapgemini.global@capgemini.com
Capgemini Ventures SAS SIRET 44 033 009 000 018	11 rue de Tilsitt, 75017 Paris, France dpocapgemini.global@capgemini.com
Sogeti France 2005 SAS SIRET 48 760 757 400 018	11 rue de Tilsitt, 75017 Paris, France dpocapgemini.global@capgemini.com
Sogeti SAS SIRET 43 432 597 300 031	11 rue de Tilsitt, 75017 Paris, France dpocapgemini.global@capgemini.com
Global Management Treasury Services S.N.C SIRET 44 837 008 000 054	11 rue de Tilsitt, 75017 Paris, France dpocapgemini.global@capgemini.com
Altran Participations SAS SIRET 48 755 097 200 037	11 rue de Tilsitt, 75017 Paris, France dpofrance.fr@capgemini.com
Altran Technology & Engineering Center SAS SIRET 81 745 935 700 023	4 avenue Didier Daurat, 31700 Blagnac, France dpofrance.fr@capgemini.com
Capgemini France SAS SIRET 32 878 178 601 143	145-151 Quai du Président Roosevelt –92130 Issy-les-Moulineaux, France dpofrance.fr@capgemini.com
Capgemini Consulting SAS SIRET 47 976 680 000 060	145-151 Quai du Président Roosevelt –92130 Issy-les-Moulineaux, France dpofrance.fr@capgemini.com
Open Cascade SAS SIRET 42 091 980 500 093	1 place des Frères Montgolfier, 78280 Guyancourt, France dpofrance.fr@capgemini.com
Capgemini Technology Services SAS SIRET 47 976 684 200 724	145-151 Quai du Président Roosevelt –92130 Issy-les-Moulineaux, France dpofrance.fr@capgemini.com
Capgemini Engineering Research & Development SAS SIRET 44 449 577 400 531	145-151 Quai du Président Roosevelt –92130 Issy-les-Moulineaux, France dpofrance.fr@capgemini.com
French Bureau SAS SIRET 82 217 266 400 036	17 rue Bouchardon, 75010 Paris, France dpofrance.fr@capgemini.com
Altran ACT SAS SIRET 81 754 920 300 026	145-151 Quai du Président Roosevelt, 92130 Issy-les-Moulineaux, France dpofrance.fr@capgemini.com



Altran Allemagne SAS SIRET 51 909 304 100 043	76 avenue de Kleber, 75016 Paris, France dpofrance.fr@capgemini.com
Altran Connected Solutions SAS SIRET 49 337 888 900 056	145-151 Quai du Président Roosevelt, 92130 Issy-les-Moulineaux, France dpofrance.fr@capgemini.com
Altran Education Services SAS SIRET 43 203 785 100 115	145-151 Quai du Président Roosevelt, 92130 Issy-les-Moulineaux, France dpofrance.fr@capgemini.com
Altran Lab SAS SIRET 44 939 756 100 043	145-151 Quai du Président Roosevelt, 92130 Issy-les-Moulineaux, France dpofrance.fr@capgemini.com
Altran Prototypes Automobiles SAS SIRET 48 754 969 300 025	145-151 Quai du Président Roosevelt, 92130 Issy-les-Moulineaux, France dpofrance.fr@capgemini.com
Altran Technologies SAS SIRET 70 201 295 600 935	76 avenue Kleber, 75016 Paris, France dpofrance.fr@capgemini.com
Logiquai SAS SIRET 48 755 068 300 030	4 avenue Didier Daurat, 31700 Blagnac, France dpofrance.fr@capgemini.com

North Africa

Capgemini Technology Services Maroc SA 164141	Shore 8 – A – Casanearshore – 1 100, Boulevard Al Qods – Sidi Maârouf - Casablanca, Morocco dpomaroc.fr@capgemini.com
Altran Maroc SARLU 289225	1100 boulevard Al Qods, Casanearshore, Shore 17, Quartier Sidi Maârouf, 20270, Casablanca, Morocco dpomaroc.fr@capgemini.com
Capgemini Egypt LLC 183227	Level 4, Plot 202, 2nd Sector, 5th Settlement New Cairo, Egypt dpo.in@capgemini.com
Altran Telnet Corporation, S.A.	Centre urbain Nord, Immeuble Ennour 1082 Tunis El Mahrajène, Tunisia dpofrance.fr@capgemini.com



UK & Ireland	
Capgemini UK Plc 0943935	No.1 Forge End – Woking GU21 6DB, UK dpocapgemini.uk@capgemini.com
CGS Holdings Limited 02798276	No.1 Forge End – Woking GU21 6DB, UK dpocapgemini.uk@capgemini.com
Capgemini Financial Services UK Limited 03282049	No.1 Forge End – Woking GU21 6DB, UK dpocapgemini.uk@capgemini.com
Sogeti UK Limited 04268004	No.1 Forge End – Woking GU21 6DB, UK dpocapgemini.uk@capgemini.com
Restaurant Application Development International UK Limited 07363730	30 Finsbury Square, London, EC2A 1AG, UK dpocapgemini.uk@capgemini.com
Idean Capgemini Creative Studios UK Limited 06934128	30 Finsbury Square, London, EC2A 1AG, UK dpocapgemini.uk@capgemini.com
IGATE Computer Systems (UK) Limited 02859908	No.1 Forge End – Woking GU21 6DB, UK dpocapgemini.uk@capgemini.com
IGATE Information Services (UK) Limited 04276081	30 Finsbury Square, London, EC2A 1AG, UK dpocapgemini.uk@capgemini.com
Capgemini Ireland Limited 67792	Ground Floor, Metropolitan Building, James Joyce Street, Dublin 1, Ireland dpocapgemini.uk@capgemini.com
Aricent Ireland, Private Limited 546416	C/o Moore Ireland, 3rd Floor, Ulysses House, Foley Street, Ireland dpocapgemini.uk@capgemini.com
Purpose Europe Limited 08340026	Raleigh House 14c Compass Point Business Pk, Stocks Bridge Way, St Ives, Cambridgeshire, PE27 5JL, UK dpocapgemini.uk@capgemini.com
ECSI Consulting Limited 08871329	No.1 Forge End – Woking GU21 6DB, UK dpocapgemini.uk@capgemini.com
Altran UK Limited 03066512	No.1 Forge End – Woking GU21 6DB, UK dpocapgemini.uk@capgemini.com
Altran UK Holding Limited 03066512	No.1 Forge End – Woking GU21 6DB, UK dpocapgemini.uk@capgemini.com
Cambridge Consultants Limited 01036298	Milton Road, Science Park – Unit 29 CB4 0DW, Cambridge, UK dpocapgemini.uk@capgemini.com



Frog Design Group UK Limited 09436565	No.1 Forge End – Woking GU21 6DB, UK dpocapgemini.uk@capgemini.com
Information Risk Management Limited 03612719	No.1 Forge End – Woking GU21 6DB, UK dpocapgemini.uk@capgemini.com
Tessella Limited 01466429	26 The Quadrant, Abingdon Science Park, OX14 3YS, Abingdon, UK dpocapgemini.uk@capgemini.com
Capgemini Certifications UK Limited 08126402	No.1 Forge End – Woking GU21 6DB, UK dpocapgemini.uk@capgemini.com
Aricent Technologies UK, Limited 06140181	30 Finsbury Square, EC2A 1AG London, UK dpocapgemini.uk@capgemini.com

BeNeLux	
Capgemini Nederland BV 30053172	Reykjavikplein 1, 3543 KA Utrecht, The Netherlands dpocapgemini.nl@capgemini.com
Capgemini NV 30067608	Reykjavikplein 1, 3543 KA Utrecht, The Netherlands dpocapgemini.nl@capgemini.com
Capgemini Business Services BV 33030578	Reykjavikplein 1, 3543 KA Utrecht, The Netherlands dpocapgemini.nl@capgemini.com
Capgemini International BV 33268283	Reykjavikplein 1, 3543 KA Utrecht, The Netherlands dpocapgemini.nl@capgemini.com
Capgemini Educational Services BV 30197497	Reykjavikplein 1, 3543 KA Utrecht, The Netherlands dpocapgemini.nl@capgemini.com
Capgemini Sourcing BV 30135992	Reykjavikplein 1, 3543 KA Utrecht, The Netherlands dpocapgemini.nl@capgemini.com
Sogeti Nederland BV 30200252	Lange Dreef 17 – 4131 NJ Vianen – The Netherlands dpocapgemini.nl@capgemini.com
Altran Engineering BV 17122872	59 Automotive Campus, 5708JZ Helmond, The Netherlands dpocapgemini.nl@capgemini.com
Altran International BV 33294562	1 Reykjavikplein, 3543KA, Utrecht, The Netherlands dpocapgemini.nl@capgemini.com
Altran Netherlands BV 34106539	1 Reykjavikplein, 3543KA, Utrecht, The Netherlands dpocapgemini.nl@capgemini.com
Capgemini Belgium SA/NV 0407.184.521	Bessenveldstraat 19 – 1831 Diegem, Belgium dpocapgemini.be@capgemini.com



Sogeti Luxembourg B42610	36 Route de Longwy- 8080 Bertrange – Luxembourg dpocapgemini.lu@capgemini.com
Capgemini Reinsurance International SA 163.854	534 rue de Neudorf, 2220 Luxemburg dpocapgemini.lu@capgemini.com
Altran Luxembourg SA B65221	36 Route de Longwy- 8080 Bertrange – Luxembourg dpocapgemini.lu@capgemini.com



Central Europe	
Capgemini Deutschland Holding GmbH HRB 102576	Potsdamer Platz 5, D-10785 Berlin, Germany dpocapgemini.de@capgemini.com
Capgemini Outsourcing Services GmbH HRB 58881	Balcke-Dürr-Allee 7, 40882 Ratingen, Germany dpocapgemini.de@capgemini.com
Capgemini Deutschland GmbH HRB 98814	Potsdamer Platz 5, D-10785 Berlin, Germany dpocapgemini.de@capgemini.com
Capgemini Deutschland Services GmbH HRB 215542 B	Potsdamer Platz 5, D-10785 Berlin, Germany dpocapgemini.de@capgemini.com
Sogeti Deutschland GmbH HRB 49963	Balcke-Dürr-Allee 7, 40882 Ratingen, Germany dpocapgemini.de@capgemini.com
XL2 GmbH 773865	Potsdamer Platz 5, 10785 Berlin, Germany xl2-dpo.de@capgemini.com
Altran Deutschland SAS & Co. KG HRA 100894	81 Frankfurter Ring 80807, München, Germany dpocapgemini.de@capgemini.com
Altran Service GmbH HRA 89337	81 Frankfurter Ring 80807, München, Germany dpocapgemini.de@capgemini.com
Frog Design Europe GmbH HRB 245808	55 Leopoldstrasse, 80802, München, Germany dpocapgemini.de@capgemini.com
Altran Management SE HRB 103091	Hamburger Allee 2-4, 60486 Frankfurt am Main, Germany dpocapgemini.de@capgemini.com
Aricent Technologies Germany GmbH HRB 32026	Neumeyerstr. 22-50, 90411 Nürnberg, Germany dpocapgemini.de@capgemini.com
Capgemini Consulting Österreich AG FN 194903y	Millennium Tower, 22nd Floor, Handelskai 94-96, 1200 Wien, Austria dpo.request.at@capgemini.com
Altran Austria GmbH FN 287997 a	1 Concept Strasse, A-8101 Gratkom, Austria dpo.request.at@capgemini.com
Capgemini Suisse S.A. CH-290.3.006.037-8	World Trade Center, Leutschenbachstrasse 95, CH 8050 Zurich, Switzerland dpocapgemini.ch@capgemini.com
Capgemini Polska Sp. z.o.o KRS 0000040605	Ul. Żwirki i Wigury 16a, 02092 Warsaw, Poland dprequestpoland.pl@capgemini.com
Altran Polska Sp. z.o.o KRS 0000396882	ul. Towarowa, 00-839 Warszawa, Poland dprequestpoland.pl@capgemini.com



Northern Europe	
Capgemini Sverige AB 556092-3053	Fleminggatan 18 (6th floor), 112 26 Bromma, Sweden dldposweden.se@capgemini.com
Capgemini AB 556447-9763	Fleminggatan 18 (6th floor), 112 26 Bromma, Sweden dldposweden.se@capgemini.com
Sogeti Sverige AB 556631-4687	Svetsarvägen 4, 171 41 Solna, Sweden dldposweden.se@capgemini.com
Altran Sverige AB 556542-2531	37 Södra Hamngatan, SE 411 06 Göteborg, Sweden dldposweden.se@capgemini.com
Aricent Technologies Sweden AB 556786-2866	c/o TMF Sweden AB, Sergels Torg 12, 111 57 Stockholm, Sweden dldposweden.se@capgemini.com
Capgemini Denmark A/S 25606965	Delta Park 40, 2665 Vallensbaeck Strand, Denmark privacy.dk@capgemini.com
Altran Denmark APS 31605466	7 Philip Heymans Alle, C/o Horten Advokatpartnerskab, DK62900 Hellerup, Denmark privacy.dk@capgemini.com
Capgemini Finland Oy 1628142-5	Keilaranta 10 E – 02150 Espoo, Finland dpofinland.fi@capgemini.com
Capgemini Norge A/S 943574537	Karenslyst allé 20, 0213 Oslo, Norway dponorway.no@capgemini.com
Matiq AS 985149437	Abels gate 7, 7030 Trondheim, Norway dponorway.no@capgemini.com

Southern Europe	
Capgemini España S.L M-287781	Calle Puerto de Somport, Edificio Oxxeo, CP 28050, Madrid, Spain protecciondedatos.es@capgemini.com
Agencia de Certification en Innovacion Espanola SLU B-82.271.313	En calle Campezo 1, edificio 4, planta 0, 28022 Madrid, Spain protecciondedatos.es@capgemini.com
Altran Innovacion SLU B-80428972	Avenida Diagonal, 199, 08018 Barcelona, Spain protecciondedatos.es@capgemini.com
Ecosat Airships SL B-47.794.425	C. Nicostrato Vela, 20, 24009 León, Spain protecciondedatos.es@capgemini.com
Aricent Spain SA B-66.541.772	11 Travessera de Gràcia, 5 th Floor, 08021 Barcelona, Spain protecciondedatos.es@capgemini.com
Capgemini Portugal SA 504272179	Av. Colégio Militar, 37 - Torre Colombo Oriente, Piso 10 - 1500-180 Lisboa, Portugal dp.pt@capgemini.com
Capgemini Italia S.p.A 4877961005	Via di Torre Spaccata, 140 - 00169 Roma, Italy dataprivacy.it@capgemini.com



Southern Europe	
CAPGEMINI FINANCE TECH S.R.L. 16239151000	Via di Torre Spaccata, 140 - 00173 Roma, Italy dataprivacy.it@capgemini.com

Eastern Europe	
Lohika LTD 37413934	50 Prakhovykh Simi Str., 01033 Kyiv, Ukraine dpo.ukr@capgemini.com
Altran Slovakia, S.R.O. 46655956	Piešťanská 3, 917 01 Trnava, Slovakia dpoaltrancapgemini.nl@capgemini.com
Altran Romania, S.R.L. 28381169	21 Garii street, Building E - Liberty Technology Park, 3rd floor 400267 Cluj-Napoca, Romania dpoaltrancapgemini.ro@capgemini.com
CAPGEMINI SERVICES ROMANIA S.R.L J40/22612/2007	Gara Herastrau Street, no. 4D, Green Court building, 4th floor Bucharest, Sector 2, Romania dpoaltrancapgemini.ro@capgemini.com
CAPGEMINI CZECH REPUBLIC S.R.O. 260 33 062	5. května 1746/22, 140 00 Praha 4-Nusle, Česko, Czech Republic dpo.cz@capgemini.com
Altran CZ, A.S. B3416	2071 Příkladná, 508 01 Hořice , Czech Republic dpo.cz@capgemini.com
CAPGEMINI MAGYARORSZÁG Kft 13-09-087168	Rétköz utca 5, HU-1118 Budapest, Hungary dpoaltrancapgemini.hu@capgemini.com
RESTAURANT APPLICATION DEVELOPMENT INTERNATIONAL HUNGARY	Árpád fejedelem útja 26-28., 1023 Budapest, Hungary Dpoaltrancapgemini.hu@capgemini.com



APAC	
Capgemini Australia Pty Ltd ACN 092 284 314	Level 7, 77 King Street, Sydney NSW 2000, Australia privacy.au@capgemini.com
WhiteSky Labs Pty Ltd ACN 141 042 382	Suite 1105, 50 Clarence Street, Sydney, NSW 2000 Australia privacy.au@capgemini.com
RXP Services Limited ACN 146 959 917	Level 15, 31 Queen Street, 3000 Melbourne, Victoria, Australia privacy.au@capgemini.com
The Worksmelbourne Agency Pty Ltd ACN 120 388 436	Level 15, 31 Queen Street, 3000 Melbourne, Victoria, Australia privacy.au@capgemini.com
The Workssydney Pty Ltd ACN 102 213 794	Level 15, 31 Queen Street, 3000 Melbourne, Victoria, Australia privacy.au@capgemini.com
NSI Technology Pty Ltd ACN 126 122 272	Level 15, 31 Queen Street, 3000 Melbourne, Victoria, Australia privacy.au@capgemini.com
Daresay Pty Ltd ACN 610 783 312	Level 15, 31 Queen Street, 3000 Melbourne, Victoria, Australia privacy.au@capgemini.com
Acclimation Pty Ltd ACN 152 878 398	Level 7, 77 King Street, NSW 2000 Sydney, Australia privacy.au@capgemini.com
Empired Limited ACN 090 503 843	Level 7, The Quadrant, 1 William Street, Perth WA 6000, Australia privacy.au@capgemini.com
Conducive Pty Ltd ACN 119 878 143	Level 7, The Quadrant, 1 William Street, Perth WA 6000, Australia privacy.au@capgemini.com
Tusk Technologies PTY Ltd ACN 094 777 376	Level 7, The Quadrant, 1 William Street, Perth WA 6000, Australia privacy.au@capgemini.com
OBS PTY Ltd ACN 081 252 922	Level 7, The Quadrant, 1 William Street, Perth WA 6000, Australia privacy.au@capgemini.com
Esavvy PTY Ltd ACN 138 682 148	Level 7, The Quadrant, 1 William Street, Perth WA 6000, Australia privacy.au@capgemini.com
Intergen Business Solutions PTY Ltd ACN 142 682 148	Level 7, The Quadrant, 1 William Street, Perth WA 6000, Australia privacy.au@capgemini.com
Purpose Asia Pacific Pty Ltd ACN 625 798 807	Level 7, The Quadrant, 1 William Street, Perth WA 6000, Australia privacy.au@capgemini.com
Altran Australia Property Limited 602543519	C/o Grant Thornton Australia Limited, Level 17, 383 Kent Street NSW 2000 Sydney, Australia privacy.au@capgemini.com
Capgemini New Zealand Limited (formerly known as Intergen Limited)	Level 4, 80 Willis Street, Wellington, 6011 New Zealand privacy.au@capgemini.com



Intergen ESS Limited	Level 4, 80 Willis Street, Wellington, 6011New Zealand privacy.au@capgemini.com
Capgemini Singapore Pte Ltd 199106419N	Level 32, 12 Marina Boulevard, Marina Bay Financial Centre– Singapore 018982, Singapore dpo.sg@capgemini.com
Capgemini Asia Pacific Ltd 199602754G	Level 32, 12 Marina Boulevard, Marina Bay Financial Centre– Singapore 018982, Singapore dpo.sg@capgemini.com
Liquidhub Pte. Ltd. 201703318C	Level 32, 12 Marina Boulevard, Marina Bay Financial Centre – Singapore 018982, Singapore dpo.sg@capgemini.com
Acclimation PTE. Ltd 201619606D	Level 32, 12 Marina Boulevard, Marina Bay Financial Centre– Singapore 018982, Singapore dpo.sg@capgemini.com
Altran Singapore Private Limited 200106758M	4 Battery Road #25-01 Bank of China Building, 049908 Singapore dpo.sg@capgemini.com
Cambridge Consultants Singapore Private Limited 201230536C	4 Battery Road #25-01 Bank of China Building, 049908 Singapore dpo.sg@capgemini.com
Frog Strategy & Design Private Limited 201333973K	38 Beach Road, #29-11 South Beach Tower, 189767 Singapore dpo.sg@capgemini.com
CAPGEMINI BUSINESS SERVICES (CHINA) LIMITED 440101400083545	6/F Podium, Glory IFC, No. 25 Ronghe Road, 528200 Nanhai District, Foshan City, PRC, China dpo.cn@capgemini.com
CAPGEMINI (CHINA) CO, LTD 310115400049352	Room A256, Floor 2, Building 3, 2250 South Pudong Road, Pilot Free Trade Zone, Shanghai, China dpo.cn@capgemini.com
CAPGEMINI (HANGZHOU) Co., LTD 330100400004425	15F, Building E,Tiantang Software Park, 3 XiDouMen Road, 310012 Hangzhou, Zhe Jiang Province, China dpo.cn@capgemini.com
CAPGEMINI (KUNSHAN) CO., LTD. 320583400050999	NO.1 Jinjie Road, service outsourcing area Huaqiao, Kunshan, Jiangsu Province, China dpo.cn@capgemini.com



Altran (Xi'an) Technologies, Company Limited 91610131MA6UQKMU7U	5th FL, A11 Building, No.156 Tian Gu 8 Road, Software New Town of Hi-tech Development Zone. Xi'an China dpo.cn@capgemini.com
Altran (Beijing) Technologies, Company Limited 91110108078535347A	Room 132008, 17th FL, Building C, Tower 1 of Wangjing SOHO, No. 1 Futong East Road, Chaoyang District 100020 Beijing, China dpo.cn@capgemini.com
Altran (Shanghai) Information & Technologies, Company Limited 913101153125083000	The 3rd floor, Building 1, No. 400 Fangchun Road, Pilot Free Trade Zone 201203 Shanghai, China dpo.cn@capgemini.com
Altran Shanghai, Limited 91310000695752806Q	Room B33, the 7th floor, No. 1359 Zhonghua Road, Huangpu district 200001 Shanghai, China dpo.cn@capgemini.com
Frog Business Consultancy (Shanghai), Company Limited 91310000666008500P	373-381 South Suzhou Road, Room 407P01, Huangpu, 200040 Shanghai, China dpo.cn@capgemini.com
Sicon Design Technologies (Shanghai), Company Limited 9131011509422053X2	700 Shangfeng Road, Unit 8, Room 301A, Pudong, 200120 Shanghai, China dpo.cn@capgemini.com
Capgemini Hong Kong Ltd 536651	Suites 4101-02 & 4111-12, 41/F., One Island East, Taikoo Place, 18 Westlands Road, Quarry Bay, Hong Kong privacy.apac@capgemini.com
ITBCONSULT HONGKONG LIMITED 63804140	Room 1905, 19/F., West Tower, Shun Tak Centre, 168-200 Connaught Road Central, Hong Kong privacy.apac@capgemini.com
Altran China Limited 876293	Suites 1202-04, Tower 2, The Gateway, 25 Canton Road, TST, Kowloon, Hong Kong China privacy.apac@capgemini.com
Capgemini Vietnam Co. Ltd 411043001695	Centre Point Building, 106 Nguyen Van Troi, Ward 8, Phu Nhuan District, Ho Chi Minh City, Vietnam privacy.apac@capgemini.com



Capgemini Saudi Ltd 1024341133776	Centria Mall Office Tower, Suite 506, 5th floor, Prince Muhammad ibn Abdulaziz Road / Olaya Street, Al Olaya District, 12241-6055 Riyadh Kingdom of Saudi Arabia dpo.sa@capgemini.com
Altran Middle East Private Plc 1010430493	Al Oyal, Kingdom Tower, 25 th floor, 11351 Riyadh, Saudi Arabia privacy.apac@capgemini.com
Altran Middle East FZ-LLC 502709	1803-1804 Al Thuraya Tower 1, PO Box 502709 Dubai Media City, United Arab Emirates privacy.apac@capgemini.com
Altran Israel Limited 514792282	7 Rival Street, 6777840, Tel-Aviv Yafo, Israël privacy.apac@capgemini.com
Capgemini Japan K.K 0104-02-035069	Level 23, Otemachi Financial City North Tower, 1-9-5 Otemachi, Chiyoda-ku, 100-0004 Tokyo, Japan dpo.jp@capgemini.com
Altran Engineering Solutions Japan Limited 0104-01-126631	2-15-1 Kounan 28F Shinagawa Intercity Tower A, Minato-ku 108-6028 Tokyo, Japan dpo.jp@capgemini.com
Altran Japan Limited 0104-01-080476	1-23-1 Toranomom, Toranomom Hills Mori Tower, 22 nd Floor, Minato-ku 105-6322 Tokyo, Japan dpo.jp@capgemini.com
Cambridge Consultants Japan Inc. 9-0104-01-126095	3-1-3 Minamiaoyama, 6F Spline Aoyama Tokyu Building, Minato-ku, 107-0062 Tokyo, Japan dpo.jp@capgemini.com
Capgemini Philippines Corp CS200714668	12th Floor, 10 West Campus, McKinley West, Fort Bonifacio, Taguig City, Philippines privacy.apac@capgemini.com
Whitesky Labs (Philippines) Inc. CS201410583	3304 Robinsons Equitable Building, 4 ADB Avenue, Ortigas, Manila, Philippines privacy.apac@capgemini.com
Whitesky Labs (Philippines) N° 2 Inc. CS201913590	3304 Robinsons Equitable Building, 4 ADB Avenue, Ortigas, Manila, Philippines privacy.apac@capgemini.com
Multibook Asia Pacific Inc. CS201405679	7 th floor, Tower 2 Insular Life Corporate Centre, Insular Life Drive, Filinvest Corporate City, Alabang, 1781 Muntinlupa City, Philippines privacy.apac@capgemini.com
Capgemini Services Malaysia SDN BHD 201101031070	Suite 15-01, G Tower, 199 Jalan Tun Razak, 50400 Kuala Lumpur, Malaysia privacy.apac@capgemini.com



Aricent Technologies Malaysia SDN BHD 201801002823	Jalan Raja Chulan, Plaza See Hoy Chan, Suite 6.01, 6 th floor, 50200 Kuala Lumpur, Malaysia privacy.apac@capgemini.com
Capgemini Technology Services India Limited U85110PN1993PLC145950	No. 14, Rajiv Gandhi Infotech Park, Hinjewadi Phase-III, MIDC-SEZ, Village Man, Taluka Mulshi, Pune 411057, Maharashtra – India dpo.in@capgemini.com
Capgemini IT Solutions India Private Limited U74995MH2018FTC330429	5th Floor Part A, Block IV, Plot IT-3 IT-4, Airoli Knowledge Park, TTC Industrial Area, MIDC, Airoli, 400708 Navi Mumbai, Maharashtra, India dpo.in@capgemini.com
Leading Purpose Campaigns (India) Private Limited U74999DL2018FTC329926	1 st Floor, D3 Soami Nagar, New Delhi, DI 110017, India dpo.in@capgemini.com
Aricent Technologies (Holdings) Limited U72100DL2006PLC149728	5 Jain mandir marg (Annexe), Cannaught Place, 110001 DELHI, India dpo.in@capgemini.com
Altran Technologies India Private Limited U74140KA1996ULT068492	SEZ Bellandur Village – RMZ Ecospace, Block 9B Pritech Park, 2 nd floor Varthur Hobli, 560103 Bangalore, India dpo.in@capgemini.com
Global Edge Software Limited U85110KA1992PLC013114	Mysore Road, Global Village – RVCE Post 560059 Bangalore, India dpo.in@capgemini.com
Pan Asia Solutions 98-0688854	Suite 206, SIT Business Center, NG Tower, Cyber City Ebene, Mauritius privacy.apac@capgemini.com
Capgemini Services (Thailand) Co. LTD	8 Wework, T-One Building, 20th Floor, Soi Sukhumvit 40, Sukhumvit Road, Khlong Toei District, Phra Khanong Sub-District, Bangkok, THAILAND privacy.apac@capgemini.com



North America	
Capgemini North America, Inc. 3509818	c/o Corporation Service Company, 251 Little Falls Drive, 19808 Wilmington, Delaware, USA dataprivacyoffice.nar@capgemini.com
Capgemini America, Inc 0100245598	c/o Corporation Service Company Priceton South Corporate Ctr., Ste. 160, 100 Charles Ewing Blvd.08628 Ewing, New Jersey, USA dataprivacyoffice.nar@capgemini.com
Capgemini Business Services USA LLC 5010627	c/o Corporation Services Company, 251 Little Falls Drive 19808 Wilmington, Delaware, USA dataprivacyoffice.nar@capgemini.com
Capgemini Technologies LLC 3529062	c/o Corporation Services Company, 251 Little Falls Drive 19808 Wilmington, Delaware, USA dataprivacyoffice.nar@capgemini.com
Capgemini Government Solutions LLC 3584244	c/o Corporation Services Company, 251 Little Falls Drive 19808 Wilmington, Delaware, USA dataprivacyoffice.nar@capgemini.com
Restaurant Application Development International LLC 4805345	c/o Corporation Services Company, 251 Little Falls Drive 19808 Wilmington, Delaware, USA dataprivacyoffice.nar@capgemini.com
Annik Inc P07000081250	1201 Hays Street, 32301 Tallahassee, County of Leon, Florida 33771, USA dataprivacyoffice.nar@capgemini.com
Purpose Global PBC 5045539	c/o Corporation Services Company, 251 Little Falls Drive 19808 Wilmington, Delaware, USA dataprivacyoffice.nar@capgemini.com
Purpose Campaigns LLC 3971119	c/o Corporation Services Company, 251 Little Falls Drive 19808 Wilmington, Delaware, USA dataprivacyoffice.nar@capgemini.com
Variq Corporation	Corporation service company, 112 North Curry Street, Carson City, NV 89703, USA dataprivacyoffice.nar@capgemini.com
Altran Engineering Solution Inc. 800653319	40600 Ann Arbor Road E, Suite 201, MI 48170-4675 Plymouth, USA dataprivacyoffice.nar@capgemini.com
Cambridge Consultants Inc. 867390	745 Atlantic Avenue #6, MA 02111 Boston, USA dataprivacyoffice.nar@capgemini.com
Capgemini Canada Inc 610099	44 Chipman Hill, 10th Floor, Station "A", Saint John NB E2L 4S6, Canada dataprivacyoffice.nar@capgemini.com



Capgemini Solutions Canada, Inc 860883149NP002	44 Chipman Hill, Suite 1000, Saint John NB E2L 2A9, Canada dataprivacyoffice.nar@capgemini.com
Inergi LP N/A.	200 University Avenue, Suite 1100 – Toronto, ON, Canada M5H 3C6 dataprivacyoffice.nar@capgemini.com
Inergi Inc. 515460	44 Chipman Hill, Suite 1000, Saint John NB E2L 2A9, Canada dataprivacyoffice.nar@capgemini.com
New Horizon System Solutions LP N/A.	700 University Avenue, Suite 1100, Toronto, ON, Canada M5G 1X6 dataprivacyoffice.nar@capgemini.com
New Horizon System Solutions Inc. 1459267	700 University Avenue, Suite 1100, Toronto, ON, Canada M5G 1X6 dataprivacyoffice.nar@capgemini.com
Société en Commandite Capgemini Québec – Capgemini Québec Limited Partnership (LP) NEZ 3367034736	1100 boul. René-Lévesque Ouest, Suite 1110 - Montreal, Québec, Canada H3B 4N4 dataprivacyoffice.nar@capgemini.com
Gestion Capgemini Quebec Inc. 1167041293	C/O WW Place Ville Marie LP, 3 place Ville Marie, Suite 400, QC H3B 2E3 Montreal, Canada dataprivacyoffice.nar@capgemini.com
Microsys Technologies Inc. 001909086	3710 Nashua Drive, Unit 1, L4V 1M5 Mississauga, Canada dataprivacyoffice.nar@capgemini.com



LATAM	
Capgemini Argentina SA 1.613.291	Avenida Presidente Roque Sáenz Peña 615, Piso 2º, Edificio Bencich, C1035AAB, Buenos Aires, Argentina protecciondatospersonales.ar@capgemini.com
Capgemini Business Services Brasil – Assessoria Empresarial Ltda 09.165.392/0001-13	Avenida John Dalton, 301, Lote 2, Block C, Edifício 4, CEP 13069-330, Campinas, São Paulo, Brazil dpobrasil.br@capgemini.com
Capgemini Brasil S.A. 65.599.953\0001-63	Alameda Araguaia, nº 1.930, Alphaville, Cidade de Barueri, State of São Paulo, Zip Code 06455-000, Brazil dpobrasil.br@capgemini.com
RADI Software do Brasil Ltda 11.855.485/0001-11	Rua Alexandre Dumas, No. 1711, 1 st floor, unit 101, Chácara Santo Antônio, Zip Code 04717-004, City of São Paulo, State of São Paulo, Brazil dpobrasil.br@capgemini.com
Purpose Campaigns Brazil Ltda 35231013042	Rua Cubatao 472 Sala 07 Vila Mariana Sao Paulo, SP 04013-001, Brazil dpobrasil.br@capgemini.com
Capgemini Colombia SAS 2197990	Avenida Chile, Carrera 7 No. 71-72 Torre B, oficina 1541. Bogotá DC, Colombia dpo.mx@capgemini.com
Capgemini Costa Rica SRL	San José, Escazú, Guachipelín, 400 meters north of Construplaza, Edificio Latitud Norte, 3rd floor, Quatro Legal Office dpo.mx@capgemini.com
Capgemini Business Services Guatemala SA No.77886 Folio 548 Book 171 of Companies	15 Avenida 5-00 Zona 13, Edificio World Technology Center Torre Sur Nivel 11, Ciudad de Guatemala, Guatemala privacy.gt@capgemini.com
Capgemini Mexico, S. de R.L. de C.V 219759	Av. Santa Fe 440, Piso 8, Colonia Cuajimalpa Morelos, Delegacion Cuajimalpa, 05348 Mexico, D.F., Mexico dpo.mx@capgemini.com



Appendix 2 – Capgemini Processing activities

The table copied below describes the key data Transfers carried out by Capgemini and covered by the BCR where Capgemini acts as a Data Controller. The list below is intended to be as complete as possible but shall not be construed as being exhaustive and will be updated where necessary.



Purpose	Categories of data	Data Subjects	Countries where data is transferred
<p>Recruitment, including background checks subject to applicable law</p>	<ul style="list-style-type: none"> ▪ Contact details, such as name, date of birth, gender, age, address, telephone numbers, email address, number of children, citizenship, ID details, visa details, work permit details, emergency contact details, dependents details, marital status, life insurance beneficiaries, pictures or images; ▪ Financial information relating to compensation, benefits and pension arrangements, such as details of salary, bank account, tax codes, travel expenses, stock options, stock purchase plan; ▪ Recruitment information, such as CV, application form, notes of interviews, applicant references (if recorded), qualifications, test results (if applicable); ▪ Professional experience information, such as professional resume, qualifications, details of projects Employees have worked on, training records, mobility records; ▪ Photos 	<p>Candidates</p>	<p>Countries in which Capgemini is established</p>



Purpose	Categories of data	Data Subjects	Countries where data is transferred
<p>Performance assessment and training</p>	<ul style="list-style-type: none"> ▪ Contact details, such as name, date of birth, gender, age, address, telephone numbers, email address, number of children, citizenship, ID details, visa details, work permit details, emergency contact details, dependents details, marital status, life insurance beneficiaries, pictures or images; ▪ Training information; ▪ Performance assessment including year end evaluation 	<p>Employees</p>	<p>Countries in which Capgemini is established</p>



Purpose	Categories of data	Data Subjects	Countries where data is transferred
<p>Pay-roll and administration of other employment-related benefits (including stock options, stock purchase plan, or other corporate plans or benefits)</p>	<ul style="list-style-type: none"> ▪ Contact details, such as name, date of birth, gender, age, address, telephone numbers, email address, number of children, citizenship, ID details, visa details, work permit details, emergency contact details, dependents details, marital status, life insurance beneficiaries, pictures or images; ▪ Financial information relating to compensation, benefits and pension arrangements, such as details of salary, bank account, tax codes, travel expenses, stock options, stock purchase plan; ▪ Employment administration information, such as employment and career history, grades, managers, employment contract details, absence records, safety records, health and sickness records, accident reports, personal development reviews, driving license details and associated documents, skills records, government issued identification numbers 	<p>Employees Third party consultants</p>	<p>Countries in which Capgemini is established</p>



<p>Day-to-day management activities, such as deployment of staff on projects, promotion, disciplinary activities, grievance procedure handling</p>	<ul style="list-style-type: none"> ▪ Contact details, such as name, date of birth, gender, age, address, telephone numbers, email address, number of children, citizenship, ID details, visa details, work permit details, emergency contact details, dependents details, marital status, life insurance beneficiaries, pictures or images; ▪ Employment administration information, such as employment and career history, grades, managers, employment contract details, absence records, safety records, health and sickness records, accident reports, personal development reviews, driving license details and associated documents, skills records, government issued identification numbers; ▪ Professional experience information, such as professional resume, qualifications, details of projects Employees have worked on, training records, mobility records; ▪ Details of Employees' whereabouts in the Capgemini location to the extent recorded by Capgemini electronic card access systems; ▪ Details of IT and connection data to the Capgemini IT systems 	<p>Employees</p>	<p>Any country where Capgemini is established</p>
<p>Marketing the professional services of consultants to potential</p>	<ul style="list-style-type: none"> ▪ Contact details, such as name, date of birth, gender, age, address, telephone numbers, email address, number of 	<p>Employees Consultants</p>	<p>In all countries in which Capgemini is established</p>



Purpose	Categories of data	Data Subjects	Countries where data is transferred
<p>Capgemini clients (e.g., by providing details of experience on previous projects)</p>	<p>children, citizenship, ID details, visa details, work permit details, emergency contact details, dependents details, marital status, life insurance beneficiaries, pictures or images;</p> <ul style="list-style-type: none"> ▪ Recruitment information, such as CV, application form, notes of interviews, applicant references (if recorded), qualifications, test results (if applicable); ▪ Employment administration information, such as employment and career history, grades, managers, employment contract details, absence records, safety records, health and sickness records, accident reports, personal development reviews, driving license details and associated documents, skills records, government issued identification numbers; ▪ Professional experience information, such as professional resume, qualifications, details of projects Employees have worked on, training records, mobility records; ▪ Photos. 		



Purpose	Categories of data	Data Subjects	Countries where data is transferred
<p>Administration of current benefits, including the Capgemini personal pension plan, life insurance scheme, private health insurance scheme</p>	<ul style="list-style-type: none"> ▪ Contact details, such as name, date of birth, gender, age, address, telephone numbers, email address, number of children, citizenship, ID details, visa details, work permit details, emergency contact details, dependents details, marital status, life insurance beneficiaries, pictures or images; ▪ Financial information relating to compensation, benefits and pension arrangements, such as details of salary, bank account, tax codes, travel expenses, stock options, stock purchase plan; ▪ Employment administration information, such as employment and career history, grades, managers, employment contract details, absence records, safety records, health and sickness records, accident reports, personal development reviews, driving license details and associated documents, skills records, government issued identification numbers 	<p>Employees</p>	<p>Countries in which Capgemini is established</p>



Purpose	Categories of data	Data Subjects	Countries where data is transferred
<p>Employment analysis, for example, comparing the success of various recruitment and/or Employee retention programs</p>	<ul style="list-style-type: none"> ▪ Recruitment information, such as CV, application form, notes of interviews, applicant references (if recorded), qualifications, test results (if applicable); ▪ Employment administration information, such as employment and career history, grades, managers, employment contract details, absence records, safety records, health and sickness records, accident reports, personal development reviews, driving license details and associated documents, skills records, government issued identification numbers; ▪ Professional experience information, such as professional resume, qualifications, details of projects Employees have worked on, training records, mobility records 	<p>Employees Candidates</p>	<p>India</p>



Purpose	Categories of data	Data Subjects	Countries where data is transferred
<p>Compliance with health & safety rules and other legal obligations placed on Capgemini as an employer</p>	<ul style="list-style-type: none"> ▪ Contact details, such as name, date of birth, gender, age, address, telephone numbers, email address, number of children, citizenship, ID details, visa details, work permit details, emergency contact details, dependents details, marital status, life insurance beneficiaries, pictures or images; ▪ Employment administration information, such as employment and career history, grades, managers, employment contract details, absence records, safety records, health and sickness records, accident reports, personal development reviews, driving license details and associated documents, skills records, government issued identification numbers; ▪ Professional experience information, such as professional resume, qualifications, details of projects Employees have worked on, training records, mobility records. 	<p>Employees</p>	<p>Countries in which Capgemini is established</p>



<p>Where necessary, processing designed to enable Capgemini to exercise its legal rights, and/or perform its legal obligations, as an employer, in so far as it is required by Applicable Law of the country where the Capgemini Company responsible for the Personal Data is established</p>	<ul style="list-style-type: none"> ▪ Contact details, such as name, date of birth, gender, age, address, telephone numbers, email address, number of children, citizenship, ID details, visa details, work permit details, emergency contact details, dependents details, marital status, life insurance beneficiaries, pictures or images; ▪ Financial information relating to compensation, benefits and pension arrangements, such as details of salary, bank account, tax codes, travel expenses, stock options, stock purchase plan; ▪ Recruitment information, such as CV, application form, notes of interviews, applicant references (if recorded), qualifications, test results (if applicable); ▪ Employment administration information, such as employment and career history, grades, managers, employment contract details, absence records, safety records, health and sickness records, accident reports, personal development reviews, driving license details and associated documents, skills records, government issued identification numbers; ▪ Professional experience information, such as professional resume, qualifications, details of projects Employees have worked on, training records, mobility records; 	<p>Employees Consultants</p>	<p>Countries in which Capgemini is established</p>
--	--	----------------------------------	--



Purpose	Categories of data	Data Subjects	Countries where data is transferred
	<ul style="list-style-type: none"> ▪ Details of Employees’ whereabouts in the Capgemini location to the extent recorded by Capgemini electronic card access systems; ▪ Details of IT and connection data to the Capgemini IT systems. 		



<p>Human Resource Management, Career management and mobility</p>	<ul style="list-style-type: none"> ▪ Contact details, such as name, date of birth, gender, age, address, telephone numbers, email address, number of children, citizenship, ID details, visa details, work permit details, emergency contact details, dependents details, marital status, life insurance beneficiaries, pictures or images; ▪ Financial information relating to compensation, benefits and pension arrangements, such as details of salary, bank account, tax codes, travel expenses, stock options, stock purchase plan; ▪ Recruitment information, such as CV, application form, notes of interviews, applicant references (if recorded), qualifications, test results (if applicable); ▪ Employment administration information, such as employment and career history, grades, managers, employment contract details, absence records, safety records, health and sickness records, accident reports, personal development reviews, driving license details and associated documents, skills records, government issued identification numbers; ▪ Professional experience information, such as professional resume, qualifications, details of projects Employees have worked on, training records, mobility records 	<p>Employees Candidates</p>	<p>Countries in which Capgemini is established</p>
---	---	---------------------------------	--



Purpose	Categories of data	Data Subjects	Countries where data is transferred
Internal and external communication	<ul style="list-style-type: none"> ▪ Contact details, such as name, address, telephone numbers, email address; ▪ Photos 	Employees	Countries in which Capgemini is established



Purpose	Categories of data	Data Subjects	Countries where data is transferred
<p>Disaster recovery plan and crisis management</p>	<ul style="list-style-type: none"> ▪ Contact details, such as name, date of birth, gender, age, address, telephone numbers, email address, number of children, citizenship, ID details, visa details, work permit details, emergency contact details, dependents details, marital status, life insurance beneficiaries, pictures or images; ▪ Employment administration information, such as employment and career history, grades, managers, employment contract details, absence records, safety records, health and sickness records, accident reports, personal development reviews, driving license details and associated documents, skills records, government issued identification numbers; ▪ Details of Employees' whereabouts in the Capgemini location to the extent recorded by Capgemini electronic card access systems; ▪ Details of IT and connection data to the Capgemini IT systems; ▪ Photos. 	<p>Employees Employees' relatives</p>	<p>Countries in which Capgemini is established</p>



<p>Audit and statistics</p>	<ul style="list-style-type: none"> ▪ Contact details, such as name, date of birth, gender, age, address, telephone numbers, email address, number of children, citizenship, ID details, visa details, work permit details, emergency contact details, dependents details, marital status, life insurance beneficiaries, pictures or images; ▪ Financial information relating to compensation, benefits and pension arrangements, such as details of salary, bank account, tax codes, travel expenses, stock options, stock purchase plan; ▪ Recruitment information, such as CV, application form, notes of interviews, applicant references (if recorded), qualifications, test results (if applicable); ▪ Employment administration information, such as employment and career history, grades, managers, employment contract details, absence records, safety records, health and sickness records, accident reports, personal development reviews, driving license details and associated documents, skills records, government issued identification numbers; ▪ Professional experience information, such as professional resume, qualifications, details of projects Employees have worked on, training records, mobility records; 	<p>Employees Candidates Clients contacts details Suppliers contacts details</p>	<p>India</p>
------------------------------------	--	---	--------------



Purpose	Categories of data	Data Subjects	Countries where data is transferred
	<ul style="list-style-type: none"> ▪ Details of Employees’ whereabouts in the Capgemini location to the extent recorded by Capgemini electronic card access systems; ▪ Details of IT and connection data to the Capgemini IT systems 		
Third-parties suppliers management	<ul style="list-style-type: none"> ▪ Contact details, such as name, address, telephone numbers, email address 	Employees Third parties’ employees	Countries in which Capgemini is established
Leakage Prevention	<ul style="list-style-type: none"> ▪ Contact details, such as name, address, telephone numbers, email address; ▪ Details of IT and connection data to the Capgemini IT systems 	Employees	Countries in which Capgemini is established
Scan Network Traffic for Malicious Activity	<ul style="list-style-type: none"> ▪ Details of IT and connection data to the Capgemini IT systems 	Employees	Countries in which Capgemini is established
Protecting Systems, Network, Infrastructure & Computers	<ul style="list-style-type: none"> ▪ Contact details, such as name, address, telephone numbers, email address; ▪ Details of IT and connection data to the Capgemini IT systems 	Employees	Countries in which Capgemini is established



Purpose	Categories of data	Data Subjects	Countries where data is transferred
Identity Access Management	<ul style="list-style-type: none"> ▪ Contact details, such as name, address, telephone numbers, email address; ▪ Details of IT and connection data to the Capgemini IT systems 	Employees	Countries in which Capgemini is established
BYOD Program Management	<ul style="list-style-type: none"> ▪ Contact details, such as name, address, telephone numbers, email address; ▪ Employment administration information, such as employment and career history, grades, managers, employment contract details, absence records, safety records, health and sickness records, accident reports, personal development reviews, driving license details and associated documents, skills records, government issued identification numbers; ▪ Details of IT and connection data to the Capgemini IT systems 	Employees	Countries in which Capgemini is established
Incident & Event Management (Logging, Remediation, Correction, etc.)	<ul style="list-style-type: none"> ▪ Contact details, such as name, address, telephone numbers, email address; ▪ Details of IT and connection data to the Capgemini IT systems 	Employees	Countries in which Capgemini is established

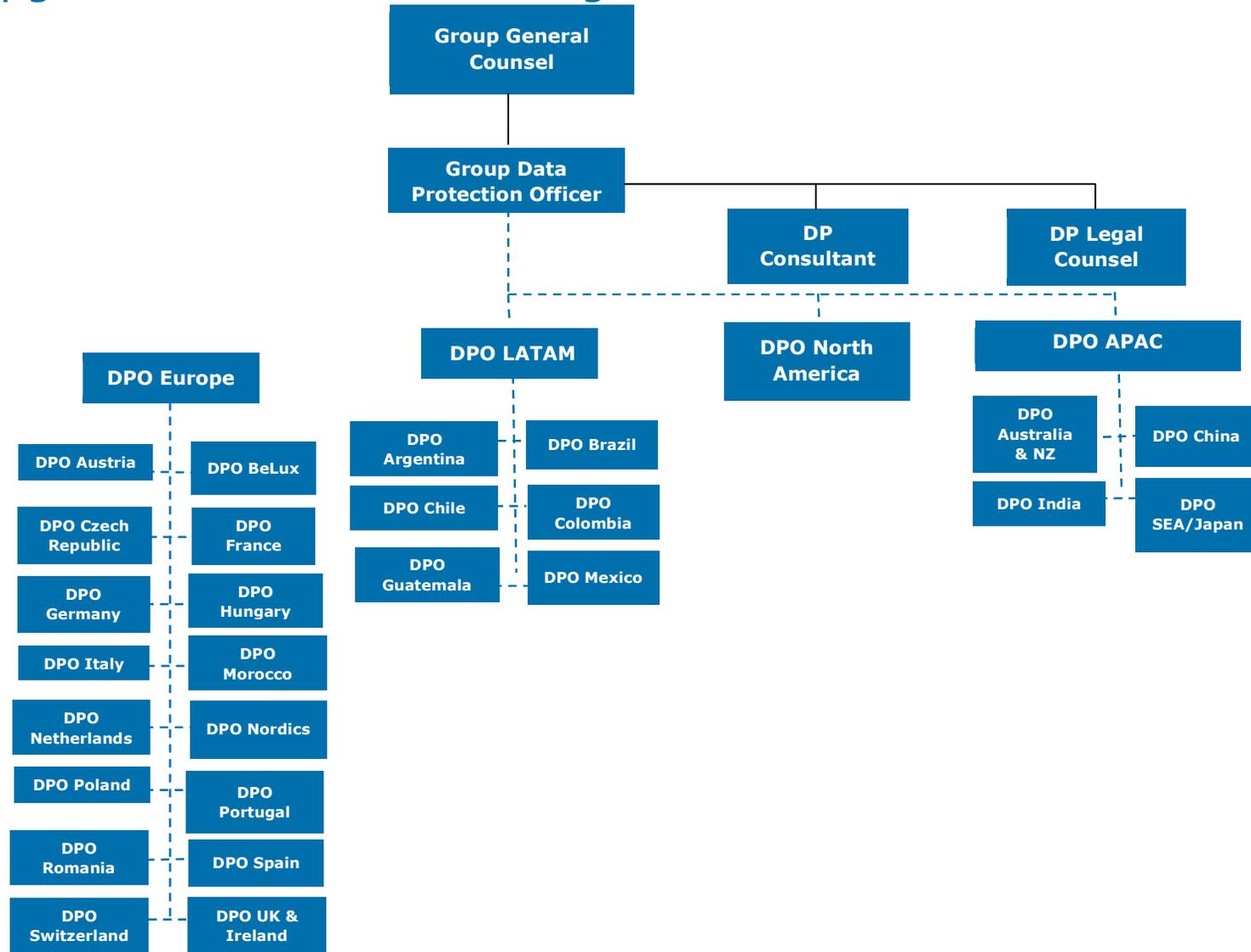


Purpose	Categories of data	Data Subjects	Countries where data is transferred
Forensics Investigation	<ul style="list-style-type: none"> ▪ Contact details, such as name, address, telephone numbers, email address; ▪ Details of IT and connection data to the Capgemini IT systems 	Employees	Countries in which Capgemini is established



Appendix 3 – Capgemini Data Protection Organisation

Data Protection Champions GBLs / Sales / Delivery / FS / Group Functions





Appendix 4 – Data Subjects’ Requests Handling Procedure

This procedure shall be published on all Capgemini websites and adapted to include any relevant local legal requirement.

The aim of this document is to explain to individuals whose Personal Data are processed by Capgemini (“Data Subjects”) how to exercise their rights.

As we care about your privacy, we want you to be aware of how and why we may collect and further process your Personal Data, and in particular, what are your rights and how to exercise them.



Key data protection notions

“**Personal data**” does not only refer to information related to your private life but encompasses any and all information which enables to identify you either directly or indirectly.

“**Processing**” means any operation which is performed on Personal Data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, combination, restriction, erasure or destruction.

“**Controller**” means the natural or legal person which determines the purposes and means of the processing of Personal Data.

“**Processor**” means the natural or legal person which processes Personal Data on behalf of the controller.

“**Purpose**” means the reason(s) why the controller needs to collect and further process the Personal Data.

Capgemini Service SAS and/or affiliates of Capgemini SE (together referred to as “**Capgemini**”) collect(s) and further process(es) your Personal Data as a Controller or as a Processor on behalf of a Controller. In any case, you can contact Capgemini – following the procedure described hereunder – to exercise your data protection rights.



What are your rights?

As a Data Subject, you can request to exercise the following rights in relation to the Personal Data concerning you that Capgemini collects and further processes:



Access your Personal Data	You can ask Capgemini confirmation as to whether or not Personal Data concerning you are being processed, and where that is the case, you can request access to your Personal Data.
Request the deletion of your Personal Data	In some cases, you can request that Capgemini delete your Personal Data.
Request the rectification of your Personal Data	You can ask Capgemini to rectify inaccurate Personal Data concerning you. This means that you can also request that Capgemini updates or completes your Personal Data.
Object to the processing of your Personal Data	In some cases, you are entitled to ask Capgemini not to process your personal data.
Request the restriction of the processing of your Personal Data	In some cases, you can ask Capgemini to limit the processing of your Personal Data for some purposes and subject to certain conditions.
Withdraw your consent to the processing of your Personal Data	You can withdraw your consent to the processing of your Personal Data even if you had initially granted such consent for Capgemini to process the Personal Data.
Right to data portability	In some cases, you can ask Capgemini to provide you with your Personal Data in a structured, commonly used and machine-readable format; and/or to transmit those data to another controller.
Submit a complaint	You can also submit a complaint if you consider that Capgemini is infringing applicable data protection regulation(s) or the BCR.



Please note that these rights may be limited in some situations under applicable law. For instance, if granting you access to your Personal Data would reveal Personal Data about another individual; or if you ask Capgemini to delete your Personal Data while it is required by law to keep it.

How to exercise your rights?

To exercise your rights, or if you have any questions or concerns related to our data protection policies, please contact us:

- By emailing us at the following address: dpocapgemini.global@capgemini.com
Please note that where relevant the Global Data Protection Office shall transmit your request to the local DPO;
- By writing to us at one of our offices which addresses you can find at the following link: <https://www.capgemini.com/fr-fr/nous-contacter/#undefined>
- By contacting by phone one the Capgemini office of your country.

In order to allow us to address your request, please provide us with the following information:



- **Your full name***
- Your status (employee, applicant, etc.)
- **Your email address or other preferred means of communication***
- Identity verification: you may be asked to provide suitable identification documentation
- Country / Region
- **The nature of your request***

** Without this information, Capgemini will not be able to address your request.*

How will Capgemini handle your request?

Your request will be submitted to the competent Data Protection Officer depending on the Capgemini entity you will be addressing the request to. You will then receive an email acknowledging the receipt of your request. Capgemini shall strive to address your request without undue delay, and no later than 1 month after acknowledging receipt of your request. If your request is particularly complex, or if you sent several requests, the time for a response can be extended by a further 2 months. We would inform you of any such extension within a month after receiving your request.

If you choose to submit your request through electronic means, and unless you request otherwise, Capgemini shall provide you with the information in a commonly used electronic format.

Even though we strongly encourage you to follow this process to submit your request, please note that you can also file a complaint with a Supervisory Authority; and/or seek judicial remedy in court.



How will Capgemini address your request?

Once Capgemini has processed your request internally, you will be informed – through the preferred means of communication you indicated – and receive the information relevant to your request. Please find in the table below how Capgemini addresses Data Subjects' most common requests:



Access your Personal Data	Capgemini shall first confirm to you whether or not it is processing your Personal Data; if that is the case, it will provide you with a copy of your Personal Data and all the relevant information on the processing.
Request the deletion of your Personal Data	If the request is justified, the Data Protection Officer dealing with your request shall instruct the relevant function(s) to delete your Personal Data.
Request the rectification of your Personal Data	The Data Protection Officer dealing with your request shall instruct the relevant function(s) to rectify your Personal Data; and you shall receive confirmation that your Personal Data has been rectified or updated.

Please note that upon receiving your request, the competent Data Protection Officer shall perform a first assessment to determine whether:

- Capgemini needs further information to handle your request:

or

- your request cannot be handled. In this case, we would explain the reasoning behind our conclusion.



About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 340,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2021 global revenues of €18 billion.

Get The Future You Want | www.capgemini.com

This document contains information that may be privileged or confidential and is the property of the Capgemini Group.
Copyright © 2022 Capgemini. All rights reserved.