

Public version

# Capgemini Binding Corporate Rules

For Controller & Processor Activities





# Table of Contents

Introduction.....	2
Definitions .....	3
1. Scope of the BCR .....	5
1.1 Material Scope .....	5
1.2 Geographical Scope .....	6
2. Bindingness of the BCR .....	6
2.1 Bindingness upon Capgemini Companies .....	6
2.2 Bindingness upon Capgemini Employees .....	6
2.3 Bindingness vis-à-vis Controllers.....	7
3. Data protection principles implementation within Capgemini.....	7
4. Internal and External Processing and Sub-Processing .....	14
5. Transparency.....	16
6. Data Subjects' enforcement rights.....	17
7. Data Subjects' requests handling procedure .....	19
8. Capgemini data protection organisation .....	20
9. Data protection awareness and training .....	20
10. Privacy by design .....	21
11. Audits related to the BCR .....	23
12. Capgemini's liability in case of a breach of the BCR .....	24
13. Jurisdiction.....	25
14. Applicable DP Law and potential conflicts with the BCR .....	25
15. Cooperation duties .....	26
16. Easy access to the BCR.....	27
17. Updates of BCR.....	27
Appendix 1 - Capgemini Processing Activities .....	28
Appendix 2 - Capgemini Data Protection Organisation .....	31
Appendix 3 - Data Subjects Requests Handling Procedure.....	32



# 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 and as a Data Processor. 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.

**"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.

**"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 (decision and from Controllers established in the EEA to Processors established outside of the EEA).

**"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 or personal data and on the free movement of such data.

**“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.

**“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.

**“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, whether acting as Controller or as Processor.



### Controller Activities

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, refer to Appendix 1.

### Processor Activities

Where acting as Processor, Capgemini processes Personal Data on behalf of Controllers and according to their instructions.

Capgemini provides an array of services including consulting services which enhance the performance of organisations based on in-depth knowledge of client industries and processes; application services which devise, develop, implement and maintain IT applications covering integration; application maintenance activities, hosting; and technology and engineering services which provide assistance and support to internal IT teams within client companies; and other managed services which integrate , manage and/or develop either fully or partially, clients’ IT infrastructure systems, transaction services and on demand services and/or business activities.

For a more comprehensive view of Capgemini’s processing activities as a Processor, refer to Appendix 1.



## 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.



## 2.3 Bindingness vis-à-vis Controllers

Where acting as a Processor, Capgemini undertakes to enter into Service Agreements compliant with the requirements set out in article 28 of the GDPR.

In addition, Capgemini commits to complying with the BCR, which shall be made binding on the Capgemini Companies, through a specific reference in the Service Agreement.

In any case, the Controller shall be able to enforce the BCR against any Capgemini Company for breaches of the BCR, it caused, according to the provisions set out in Section 12.

## 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. Where acting as Processor, Capgemini shall notify the Controller if its instructions clearly infringe Applicable DP Law.

### 3.1 Clear identified purpose



#### Controller Activities

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.

#### Processor Activities

Where acting as Processor, Capgemini must strictly comply with the instructions of the Controller, in particular in relation to the reasons for which the Personal Data shall be processed.

**In practice,** this means that Capgemini must comply with the provisions set out in the Service Agreement and must not process the Personal Data for any other purpose, unless expressly authorised by the Controller, and subject to Applicable DP Law.





# 3.2 Legal basis



## Controller Activities

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 contracts 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, 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.

## Processor Activities

Where acting as Processor, Capgemini shall assist the Controller in the implementation of the organisational and technical measures to enable the Controller to comply with the obligation to have a legal basis for processing activities.

**In practice,** Capgemini may need to assist the Controller by implementing mechanisms to obtain Data Subjects' consent on behalf of the Controller. In any case, such support will be subject to negotiations to be captured in the Service Agreement entered into between Capgemini and the Controller.

Capgemini shall not take over the responsibility to determine what is the valid legal basis on behalf of the Controller and what are the appropriate technical and organisational measures to be implemented for the implementation of the consent mechanism.



- 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.*

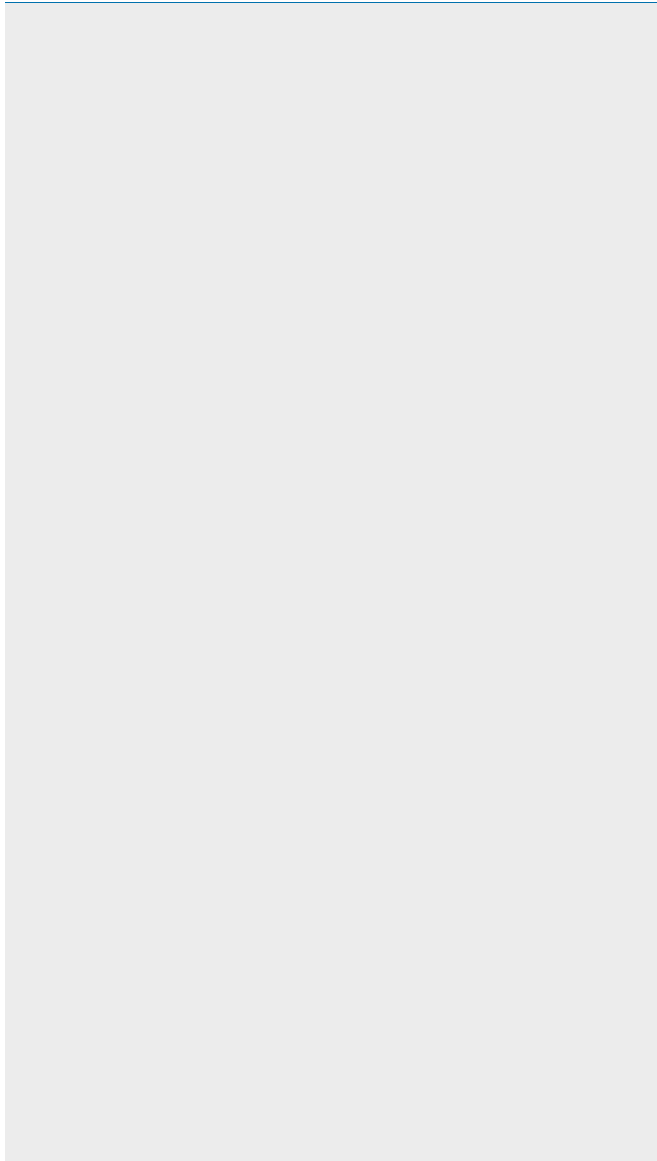
- 5. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

*E.g. where an officer of a public body competent for investigating a crime asks Capgemini for cooperation in an on-going investigation.*

Subsection 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



#### Controller Activities

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



#### Processor Activities

Where acting as Processor, Capgemini must strictly comply with the instructions of the Controller.

In addition, when designing and developing a product or service involving the processing of Personal Data, such service or product should be developed so that it only collects and processes the Personal Data which is necessary



### Controller Activities

**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.



### Processor Activities

for the purpose(s) of the processing, as determined by the Controller.

**In practice,** this means that Capgemini shall cooperate with and support the Controller in limiting the personal data which needs to be collected when designing applications or systems is part of its scope of services. However, this shall not be interpreted as an obligation for Capgemini to determine itself which Personal Data should be collected when acting on behalf of the Controller.

## 3.4 Data quality



### Controller Activities

Where acting as Controller, 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.



### Processor Activities

Where acting as Processor, Capgemini must assist the Controller in complying with its obligation to keep the data accurate and up to date.

This means that Capgemini must update, correct or delete the Personal Data upon request of the Controller insofar as this is technically possible, and in the conditions, agreed between the parties under the Service Agreement. Where the Data has been disclosed to a Capgemini Company acting as sub-Processor, it will be notified of such modifications.

**In practice,** Capgemini is to implement the technical measures necessary to comply with the Controller's instructions regarding any request to update, correct or delete the Personal Data.



## 3.5 Data retention limitation



### Controller Activities

Where acting as Controller, 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.



### Processor Activities

Where acting as Processor, Capgemini must ensure that, pursuant to the provisions of the Service Agreement and according to the Controller's instructions, Personal Data are either deleted or returned to the Controller upon termination and/or upon request of the Controller.

**In practice**, this means that Capgemini must implement the necessary technical and organisational measures to make sure that the Personal Data is either deleted or returned to the Controller, as agreed between the parties in the Service Agreement and/or according to the Controller's instructions.



# 3.6 Security



## Controller Activities

Where acting as Controller, 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.



## Processor Activities

Where acting as Processor, Capgemini must implement the appropriate technical and organisational measures, as agreed with the Controller, to ensure a high level of security to the Processing of Personal Data entrusted to it by the Controller.

**In practice,** this means that Capgemini must implement the agreed upon provisions included in the Service Agreement.

In addition, in case of a Data Breach, Capgemini is to notify the Controller without undue delay and shall assist it in addressing the Data Breach, as agreed between the parties in the Service Agreement.



# 3.7 Processing of Special Categories of Personal Data



## Controller Activities

Where acting as Controller, Cappgemini shall only process Special Categories of Personal Data when strictly necessary or legally required.

When processing Special Categories of Personal Data, Cappgemini must implement reinforced technical and organisational measures to ensure the security of the Processing.

## Processor Activities

Where acting as Processor, Cappgemini shall process Special Categories of Personal Data on behalf of the Controller and as per its request.

When processing Special Categories of Personal Data, Cappgemini shall implement any reinforced technical and organisational measures as per the Controller’s instructions, and subject to commercial negotiations, 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 Cappgemini (acting as Controller);
2. Authorised by Union or Member State law to which the Controller (Cappgemini) 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.



## Controller Activities

Cappgemini 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.

## Processor Activities

Cappgemini must follow the instructions of the Controller and strive to enable the Controller to comply with its obligation to inform the Data Subjects.



## 4. Internal and External Processing and Sub-Processing

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

Capgemini shall rely on Processors or Sub-Processors either within or outside of the Group only to the extent that such Processor or Sub-Processors provide sufficient guarantees to implement technical and organisational measures to ensure that the Processing is carried out in compliance with the GDPR 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 or Sub-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.



**Controller Activities**

**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.

**Processor Activities**

**In practice**, where an EEA Capgemini Company acting as Processor on behalf of a Controller established in the EEA intends to transfer Personal Data to a Non-EEA Capgemini Company, the BCR provide an adequate level of protection to the Personal Data transferred.

Where an EEA Capgemini Company acting as Processor on behalf of a Controller established in the EEA intends to transfer Personal Data to a third party located out of the EEA, the parties must enter into the relevant EU Model Clauses.

In any case, where acting as Processor, Capgemini shall make sure that before any such Transfer to a third country takes place, it obtains the Controller prior authorisation.





## 5. Transparency

**Where acting as Controller**, 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.

**Where acting as Processor**, Capgemini must assist the Controller in complying with the obligation to inform the Data Subjects.

**In practice**, this means that Capgemini must provide the Controller with detailed information regarding the Processing, and in particular with the data recipients including the entities to which the personal data may be transferred, in order to enable the Controller to correctly inform the Data Subjects.



## 6. Data Subjects' enforcement rights

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



### Controller Activities

Data Subjects can enforce the following elements of the BCR on Capgemini acting as Controller:

- 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;



### Processor Activities

Data Subjects can enforce the following elements of the BCR directly on Capgemini acting as Processor:

- The duty for Capgemini to respect the instruction of the Controller regarding data Processing, as detailed in Section 2;
- The duty for Capgemini to implement appropriate technical and organisational security measures, as detailed in Sub-Section 3.6;
- The duty to notify the Controller in case of a Personal Data Breach, as detailed in Sub-Section 3.6;
- The duty for Capgemini to only engage sub-processors in compliance with the provisions of article 28 of the GDPR, as detailed in Section 4;
- The duty for Capgemini to cooperate with and assist the Controller in complying with and demonstrating compliance to the GDPR, as detailed in Sections 3 and 15;
- The fact that Capgemini grants easy access to the BCR, as detailed in Section 16;
- The right for Data Subjects to complain through the internal complain mechanism of Capgemini, as detailed in Section 7;
- The duty for Capgemini to cooperate with Supervisory Authorities competent for the Controller, as detailed in Section 15;



## Controller Activities

- 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.



## Processor Activities

- The right for Data Subjects to lodge a complaint before the competent Supervisory Authority and/or before the competent courts of law, as detailed in Sections 7 and 13;
- The obligation for each Capgemini Company exporting Personal Data outside of the EEA, to accept liability for any breaches of the BCR by the sub-processors (internal or external to Capgemini) established outside of the EEA, which received the Personal Data, as detailed in Section 12;
- The fact that it is up to the EEA Capgemini Company, which exported the Personal Data, to demonstrate that the sub-processor located outside of the EEA (i.e. the recipient of the data) did not breach the BCR, as detailed in Section 12;
- Data Subjects can enforce additional elements of the BCR on Capgemini acting as a Processor, if they cannot bring a claim to the Controller because the Controller has factually disappeared or ceased to exist in law or has become insolvent – and no successor entity has assumed the legal obligations of the Controller by contract or by operation of law;
- The duty for Capgemini Companies, and their employees, to respect the BCR as detailed in Section 2;
- The duty for Capgemini to create third-party beneficiary rights for Data Subjects, as detailed in this very Section;
- The data protection principles listed in Sections 3, 4 and 5;
- The obligation to list the Capgemini Companies, as detailed in Section 1 and set out on the Capgemini website;



### Controller Activities



### Processor Activities

- The obligation for each Cappgemini Company to notify the Controller, the competent Supervisory Authority for the Controller, and Cappgemini’s headquarters, in case of a conflict between the local legislation and the BCR, as detailed in Section 14.

## 7. Data Subjects requests handling procedure



### Controller Activities

Where acting as Controller, Cappgemini 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.



### Processor Activities

Where acting as Processor, Cappgemini shall promptly forward any Data Subject request it receives to the Controller without undue delay. Cappgemini shall then await the instructions of the Controller as to how to proceed, unless otherwise agreed between the parties in the Service Agreement.

Although Cappgemini encourages Data Subjects to contact the Controller directly, it still allows them to submit requests and/or complaints through the dedicated internal mechanism described in Appendix 3.



## 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

Where acting as Controller, each Capgemini Company is responsible for and able to demonstrate compliance with the BCR and the Applicable DP Law in general.

Where acting as Processor, Capgemini shall provide the Controller with the necessary information to help them comply with their own obligations.

### 10.1 Record of Processing



#### Controller Activities

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;



#### Processor Activities

Where acting as Processor, Capgemini must keep and maintain, in writing, a record of all categories of Processing activities carried out on behalf of Controllers, containing the following:

- The name and contact details of the Capgemini Company acting as Processor, and of each Controller on behalf of which Capgemini is acting, as well as the DPO;
- The categories of Processing carried out on behalf of the Controller;
- Where applicable Transfers of Personal Data to countries located outside the EEA, including the identification of such countries;



### Controller Activities

- Where applicable, Transfers of Personal Data to countries located outside the EEA, including the identification of such countries.

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

**In practice,** to comply with this requirement, Cappgemini 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.

### Processor Activities

- Where possible, a general description of the technical and organisational measures implemented.

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

**In practice,** to comply with this requirement, Cappgemini uses dedicated tools which allow it to digitally record all Personal Data Processing and extract a complete record of Processing for its Processor’s activities.

## 10.2 Data Protection Impact Assessment



### Controller Activities

Where acting as Controller, Cappgemini 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.

### Processor Activities

Where acting as Processor, Cappgemini is to assist the Controller to comply with its obligation to carry out Data Protection Impact Assessments.



### Controller Activities

**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.



### Processor Activities

**In practice**, this means that Capgemini shall provide the Controller with all relevant information regarding the Processing. In particular, the technical and organisational means used to implement the Processing, the location of the Data, the security measures implemented (physical and technical), and where applicable, details on the sub-Processor(s), etc.

This shall not mean that Capgemini shall conduct the DPIA on behalf of the Controller. Capgemini shall only assist the Controller without committing on the performance of the DPIA *per se*.

## 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.

In addition, where acting as Processor, Capgemini shall agree to be audited by Controllers regarding specific Processing activities carried out on their behalf. The conditions of such audits must be set out in the Service Agreement.





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



## Controller Activities

Where Capgemini is acting as Controller, 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.

**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.

## Processor Activities

Where Capgemini is acting as Processor, the Controller, and in certain cases the Data Subject, as provided under Section 6, can enforce the BCR against any Capgemini Company for breaches it caused.

Where an EEA Capgemini Company transfers Personal Data to a Non-EEA Capgemini Company, the EEA Capgemini Company shall be liable for breaches 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.

**In practice**, this means that, in case of a breach of the BCR, the exporting EEA Capgemini Company must accept responsibility for paying compensation and to remedy the breach of the BCR where such breach caused a damage to the Controller and/or to Data Subjects.

In addition, it shall be up to Capgemini to demonstrate that it 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.



## Controller Activities

Where a Capgemini Company, acting as Controller, 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.



## Processor Activities

Where a Capgemini Company, acting as Processor, has reasons to believe that the applicable local legislation prevents it to fulfil its obligations under the BCR, it must inform the Controller, Capgemini’s headquarters as well as the DPO organisation and the Supervisory Authority competent for the Controller; unless prohibited to do so by a law enforcement authority.

In addition, any legally binding request for disclosure of Personal Data by a law enforcement authority or state security body must be notified to the Controller; unless prohibited.

In any case Capgemini will use its best efforts to alert the competent Supervisory Authority for the Controller as well as its own competent Supervisory Authority and provide them with information regarding the request for disclosure.



# 15. Cooperation duties

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.



## Controller Activities

Where acting as Controller, 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.

## Processor Activities

Where acting as Processor, Capgemini shall cooperate with and assist the Controller to help it comply with their obligations under the Applicable DP Law.

In addition, Capgemini must cooperate with the competent Supervisory Authority(ies) for the Controller, according to the Controller's instructions. In particular, Capgemini must follow the Supervisory Authority(ies)' advice and accept to be audited by them, in relation to the Processing activities performed on behalf of a specific Controller.



## 16. 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.



### Controller Activities

Where acting as Controller, 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.

In case of a significant update of the BCR, Capgemini shall inform the Employees through a communication on the Intranet.



### Processor Activities

Where acting as Processor, Capgemini must ensure that a reference to the BCR is included in Service Agreements, together with a link to the public version of the BCR.

In addition, Capgemini shall send the public version of the BCR to the Controller upon request and/or attach it to the Service Agreement as agreed between the parties.

## 17. 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.

If such changes significantly affect the conditions of the Processing of Personal Data, Capgemini acting as Processor shall duly inform the Controllers.



# Appendix 1 – Capgemini Processing activities



## Where Capgemini is acting as Controller

### ▪ Employee Personal Data

The Binding Corporate Rules cover Capgemini Employee Personal Data, agency workers and other third parties working on Capgemini's behalf as well as job applicants. The Capgemini Employee Personal Data Capgemini may hold may include but is not limited to:

- **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;
- **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.**

Capgemini processes Employee Personal Data exclusively for work-related purposes. Such purposes include but are not limited to the following activities:

- Recruitment, including background checks subject to applicable law;
- Performance assessment and training;
- Pay-roll and administration of other employment-related benefits (including stock options, stock purchase plan, or other corporate plans or benefits);
- Day-to-day management activities, such as deployment on projects, promotion, disciplinary activities, grievance procedure handling;
- Marketing the professional services of consultants to potential Capgemini clients (e.g., by providing details of experience on previous projects);



- Administration of current benefits, including the Capgemini personal pension plan, life insurance scheme, private health insurance scheme;
- Employment analysis, for example, comparing the success of various recruitment and/or Employee retention programs;
- Compliance with health & safety rules and other legal obligations placed on Capgemini as an employer;
  
- 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;
- IT, security, cybersecurity and access control;
- Human Resource Management, Career management and mobility;
- Internal and external communication;
- Disaster recovery plan and crisis management;
- Company resources management;
- Audit and statistics;

#### ▪ **Business Contacts**

Business Contact means a Capgemini supplier, subcontractor, shareholder, client or alliance partner, whether having an on-going commercial relationship with Capgemini or being a former or potential Business Contact of Capgemini. The Personal Data Capgemini may hold about the personnel of its Business Contacts include but is not limited to:

- **Contact details**, such as name, job title, employer, address, telephone numbers, e-mail address, fax numbers;
- **Financial details** relating to invoicing and payment, such as bank account information (when the Business Contact is a natural person);
- **Relevant experience and/or qualifications** (such as for the personnel of subcontractors);
- **Details of business interests and opinions** (such as where information is held in a CRM marketing database).

Capgemini processes Business Contact Personal Data exclusively for business related purposes. Such purposes include but are not limited to the following activities:

- Concluding and performing contracts with Capgemini clients, suppliers, subcontractors or alliance partners;
- Managing Capgemini accounts and records;
- Advertising, marketing and public relations;
- Communicating with Business Contacts;
- Market research;
- Health, Security, Environment and Quality;
- Compliance with legal and regulatory obligations;
- Maintaining certifications;
- Audit and statistics.

As a general rule, Capgemini does not collect, or process Special Categories of Personal Data as defined under EU Law. However, Capgemini may process Special Categories of Personal Data where it is necessary to enable Capgemini to exercise its legal rights, and/or perform its legal obligations, as an employer, in so far as it is strictly required by Applicable Law of the country where the Capgemini Company responsible for the Personal Data is established



As a general rule, Capgemini does not take any individual decisions with significant effect for a Data Subject based solely on automated processing as per article 22 GDPR.



## Where Capgemini is acting as Processor

Capgemini provides its clients with a full range of services in consulting, application services, infrastructure services, business process outsourcing and local professional services.

A Capgemini Company may process a wide variety of Covered Personal Data in the context of providing services to its clients, whether the processing of Personal Data is the main obligation of the service rendered by the Capgemini Company to the client, or whether the processing of Personal Data is ancillary to the execution of another service provided to the client by the Capgemini Company.

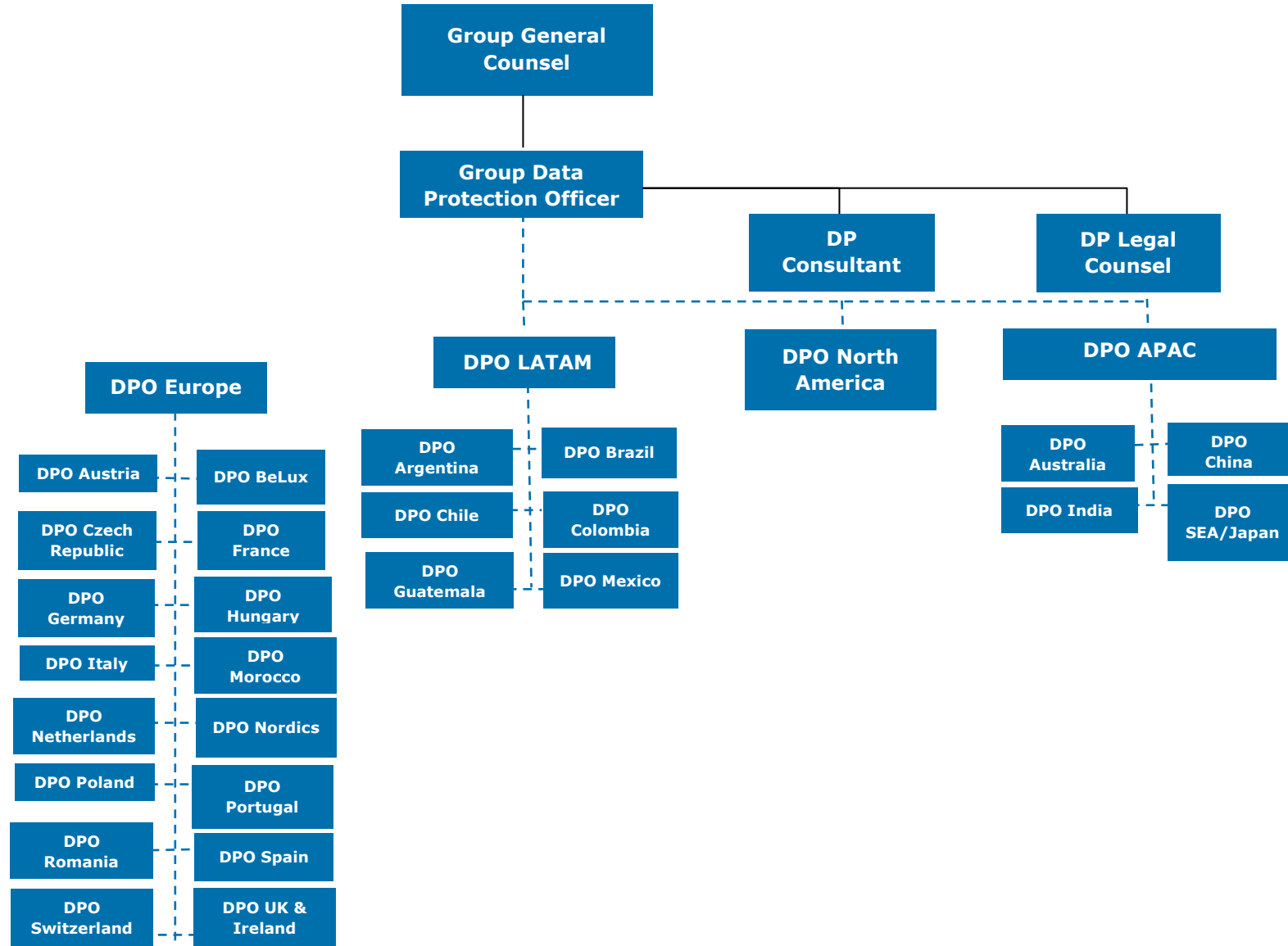
Covered Personal Data in relation to Capgemini's activities a Data Processor may include Personal Data as listed in point 2.1 above as well as any other type of Personal Data as requested by the Data Controller.

As per client instructions, Covered Personal Data may also include Special Categories of Personal Data.

# Appendix 2 – Capgemini Data Protection Organisation



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







# Appendix 3 – 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 personal 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:



<b>Access your Personal Data</b>	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.
<b>Request the deletion of your Personal Data</b>	In some cases, you can request that Capgemini delete your Personal Data.
<b>Request the rectification of your Personal Data</b>	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.
<b>Object to the processing of your Personal Data</b>	In some cases, you are entitled to ask Capgemini not to process your personal data.
<b>Request the restriction of the processing of your Personal Data</b>	In some cases, you can ask Capgemini to limit the processing of your Personal Data for some purposes and subject to certain conditions.
<b>Withdraw your consent to the processing of your Personal Data</b>	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.
<b>Right to data portability</b>	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.
<b>Submit a complaint</b>	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: [d pocapgemini.global@capgemini.com](mailto:d pocapgemini.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:

 <p><b>Access your Personal Data</b></p>	<p>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.</p>
<p><b>Request the deletion of your Personal Data</b></p>	<p>If the request is justified, the Data Protection Office dealing with your request shall instruct the relevant function(s) to delete your Personal Data.</p>
<p><b>Request the rectification of your Personal Data</b></p>	<p>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.</p>

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.



## Where Capgemini is acting as Processor

Where Capgemini is processing Personal Data on behalf of a data Controller, Capgemini strongly encourages you to submit your request directly to the Controller.

In any case, if Capgemini receives a request directly, it shall notify the data Controller without undue delay according to the terms and conditions agreed between Capgemini and the Controller.

Should Capgemini be instructed by the Controller to handle your request directly, Capgemini shall follow the above-mentioned procedure in close coordination with the data controller.



## About Capgemini

---

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 world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2017 global revenues of EUR 12.8 billion.

Learn more about us at [www.capgemini.com](http://www.capgemini.com)

**This document contains information that may be privileged or confidential and is the property of the Capgemini Group. Copyright © 2018 Capgemini. All rights reserved.**