CAPGEMINI BINDING CORPORATE RULES

Controller Activities

Public version

Table of Contents

Version History

Version History		
Version	Date	Comments
1.0	2016	Initial version communicated to the CNIL and approved by the CNIL by official letter.
2.0	2018	Complete rewrite of the Binding Corporate Rules
3.0	2023	Updated following Schrems II decision
4.0	2024-2025	Update and reshape of the Binding Corporate Rules, separated into Controller & Processor versions to comply with the requirements of the European Data Protection Board (EDPB) and to ensure better legibility.
Authors and contributing		
Role	Activity	Comments
Nathalie Laneret	Group DPO	
Louise Achache	Senior Data Protection Legal Counsel	
Document Distribution		
Role	Location	Action/Information
CNIL	Paris, France	For Official Review and Approval where relevant.
Group & Local General Counsels, Group Chief Executive Officer	Paris, France	For Official Management Information & Endorsement.
All Employees	All Capgemini Locations	Informed as required by law, upon employment and throughout employment.
Document Reviewed and Approved by		
Role	Responsibility	Comments
Group DPO, Emmanuelle Bartoli	Internal Approver	
CNIL, French Data Protection Authority	Official Reviewer & Approver	Approved by official letter in 2016, Reviewed and confirmed newer versions as per official authority process.

Introduction

As a global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation leveraging cloud, data, AI connectivity, software, digital engineering, and platforms to address the entire breadth of our clients' needs. From advancing the digital consumer experience, to accelerating intelligent industry and transforming enterprise efficiency, we help our clients define the right path forward to a better future.

Capgemini is committed to protecting all personal data entrusted to it as part of its activities. As an international group with entities located in more than 40 countries, it is essential to Capgemini that information flow freely and securely. Providing a strong 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 and further amended in 2019 and 2023 to comply with the General Data Protection Regulation (GDPR) and the European Data Protection Board updated requirements further to the so-called *Schrems II* decision.

More than a mere data transfer mechanism, Capgemini's BCR are our global data protection policy, a comprehensive framework defining our entire accountability approach to the processing of personal data. Capgemini's BCR do not only define the principles with which it shall comply when processing Personal Data, it also specifies the procedures it has implemented to comply with applicable data protection laws and in particular the General Data Protection Regulation 2016/679.

Definitions

The terms used in this document are defined as follows:

"**Adequacy Decision**" means a decision by which the European Commission determines that a country offers an adequate level of data protection, allowing personal data to be transferred freely to such country in compliance with the GDPR.

"**Applicable DP Law**" means any data protection regulation that may apply and in particular (1) the European Regulation n°2016/679 relating to the processing of Personal Data (**GDPR**), and (2) any applicable local laws and regulation relating to the processing of Personal Data.

"**Binding Corporate Rules**" or "**BCR**" means personal data protection policies which are adhered to by a Controller or Processor established on the territory of a Member State 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.

"**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 as Processor.

"**Binding Corporate Rules for Processor Activities**" or "**BCR-P**" means the BCR applicable to Capgemini's activities as a Data Processor.

"**Blue Book**" means Capgemini's book of policies and guidelines specifying a range of commonly adopted principles, values, policies and processes.

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

"**Capgemini Business Contact**" means a supplier, subcontractor, shareholder, client, or partner of Capgemini's.

"**Capgemini Client**" means any natural or legal person to which Capgemini provides services pursuant to an agreement.

"**Capgemini Company(ies)**" means any entity which is part of the Group, and which is bound by Capgemini BCR.

"**Capgemini Employee**" means all current, former, or prospective staff member of Capgemini, including agency workers and interns.

"**Competent Supervisory Authority**" means either the Supervisory Authority of the country where the Data Subject has their habitual residence, place of work or place of the alleged infringement, or the Supervisory Authority of the country where the Data Controller is established.

"**Cybersecurity Organization**" means Capgemini's global function creating and managing global security policies and monitoring compliance from Business Units and Global Business Lines. The Cybersecurity Organization is made up of a network of Cybersecurity Officers appointed for each Business Unit.

"**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.

"**Data exporter**" or "**Exporter**" means the entity transferring the personal data.

"**Data Importer**" or "**Importer**" means the recipient of a data transfer.

"**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.

"**Data Protection Impact Assessment**" or "**DPIA**" means a process to evaluate, in particular, the origin, nature, particularity and severity of a risk associated with a processing of Personal Data. The purpose of a DPIA is to assess and mitigate the risk associated with a processing or set of processing of Personal Data.

"**Data Protection Officer**" or "**DPO**" means the designated Capgemini Employees duly appointed before the competent data protection authority where required and possessing expert knowledge of data protection law and practices, advising, informing, and monitoring compliance with Applicable DP Law, and who are part of the Data Protection Organization described in Section 8 of this document.

"**Data Subject**" means any identified or identifiable natural person whose Personal Data is processed.

"**European Economic Area**" or "**EEA**" means the Member States of the European Union and three countries of the European Free Trade Association.

"**EEA Capgemini Company**" means any Capgemini Company located in the European Economic Area ("**EEA**").

"**Employee Personal Data**" means Personal Data relating to a current, former, or prospective Capgemini Employee.

"**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 Capgemini BCR binding upon Capgemini Companies.

"**Non-EEA Capgemini Company**" means any Capgemini Company located outside of the EEA.

"**Personal Data**" means any information relating to an identified or identifiable natural person ("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, or online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person.

"Personal Data Breach" or "**Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

"**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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

"**Service Agreement**" means a written agreement between a Controller and a 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.

"**Standard Contractual 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.

"**Supervisory Authority(ies)**" or "**Data Protection Authorities**" means an independent public authority which is established by a Member State of the European Union or any other state.

"**Third country**" means a country which has not been recognized by the European Commission as offering an adequate level of data protection.

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

1. Scope of the BCR

Capgemini BCR-C apply to all processing of personal data carried out by Capgemini as a data controller. Capgemini BCR-C frame all transfers of personal data from a Capgemini company acting as data controller to another Capgemini company acting either as controller or as processor. Capgemini companies are responsible for and able to demonstrate that they comply with the BCR-C.

Where local law is more stringent and requires a higher level of protection than the commitments provided under Capgemini BCR-C, it will take precedence over the BCR-C. Capgemini shall comply with applicable local data protection law.

1.1 Material Scope

These BCR-C apply to all personal data processed within Capgemini, where Capgemini is acting as controller. More specifically, these BCR-C 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 a data controller, Capgemini mainly processes the personal data of its employees and business contacts. The purposes of such processing are mainly related to human resources, cybersecurity, internal and external communications, marketing, and compliance.

For a more comprehensive overview of Capgemini's processing activities as a Controller, including the most common data transfers carried out by Capgemini, please refer to Appendix 2.

1.2 Geographical Scope

These BCR-C cover all personal data being transferred and further processed within the group, regardless of the origin of the personal data. The BCR-C cover all transfers of personal data carried out within the group, including onward transfers.

In practice, this means that the BCR-C apply to personal data transferred from:

- An EEA Capgemini company to another EEA Capgemini company
- An EEA Capgemini company to a non-EEA Capgemini company
- A non-EEA Capgemini company to an EEA Capgemini company
- A non-EEA Capgemini company to another non-EEA Capgemini company.

Capgemini companies, bound to comply with these BCR-C are listed under Appendix 1.

2. Bindingness of the BCR-C

All Capgemini companies and their employees are legally bound to comply with these BCR-C.

2.1. Bindingness on Capgemini companies

In practice, each Capgemini entity 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-C. By signing

the intra-group agreement, Capgemini entities commit to comply with the provisions of the BCR-C, and to implement its principles within its own organization.

Where Capgemini creates or acquires new entities, in particular where these are located outside the EEA, no personal data shall be transferred to them until they are fully able to comply with, and effectively bound by the BCR-C according to the above-mentioned mechanism.

2.2. Bindingness upon Capgemini employees

All Capgemini employees are bound to comply with these BCR-C through a specific mention in their employment contract and/or through the obligation, contained in all employments contracts, to comply with Capgemini's policies, which include the BCR.

In practice, an assessment is performed locally to determine how the BCR can be made legally binding on the employees according to applicable law(s). In most cases it consists of adding a provision to the employment contract and/or the to the collective agreement. Information and/or consultation of the competent work councils are also ensured in due course where necessary.

As further detailed in Sections 10 and 17 of the BCR-C, Capgemini employees are made aware of the BCR, and the relevant obligations, through internal communication and training. Capgemini employees are also made aware of the fact that any non-compliance with the BCR shall lead to disciplinary sanctions according to applicable laws.

3. Implementation of data protection principles

Capgemini is committed to complying with and implementing the data protection principles set out in these BCR-C, irrespective of applicable local data protection laws, unless such laws provide more stringent requirements than those provided under these BCR-C.

In practice, this means that as a minimum, Capgemini shall comply with the principles and obligations set out in the BCR. Where applicable local law requires Capgemini to comply with any additional or more stringent principles and/or obligations, Capgemini shall do so.

All the principles and obligations described in the BCR are promoted and implemented within Capgemini through a set of policies, processes, guidelines, and trainings.

3.1. Clear identified purpose

Where acting as controller, Capgemini shall only collect and further 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 objective(s) for which personal data are collected and further processed shall be set before such collection occurs. Where acting as controller, Capgemini might collect and further process personal data for several reasons, including in particular: purposes related to HR (recruitment, workforce management, etc.), Cybersecurity, promoting Capgemini's offerings, etc. As part of the review and approval process, the business owner of every project involving the processing of personal data shall detail the reasons why such data shall be collected and further processed.

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 for the purposes of **the legitimate interest pursued by Capgemini** or by a third party.
   For instance, Capgemini shall rely on legitimate interest as a legal basis when processing the personal data of its employees for security related purposes, to secure its network, assets and/or facilities.
   Where relying on legitimate interest, Capgemini shall perform a balancing test to determine whether its legitimate interests are overridden by those of the individuals whose personal data are processed, or their fundamental rights and freedoms, in circumstances where the personal data of these individuals must be protected.

2. **Individuals' whose personal data are processed consented to such processing**. To be valid, such consent shall be freely given, specific, informed, and unambiguous.
   For instance, when collecting personal data directly from individuals to allow them to register for an event, subscribe to a newsletter or download a report, through contact forms on its website, Capgemini shall rely on the individuals' consent.

3. The collection and further processing of personal data is **necessary for the performance of a contract** to which the individual whose personal data are processed is party, or to take steps, at the request of the individual, prior to entering such contract.
   For instance, processing salary information and bank account details is necessary to pay salaries which is part of executing an employment contract.

4. The processing is necessary **to comply with a legal obligation** to which Capgemini is subject.
   For instance, communicating personal data to tax authorities may be required under applicable local law.

   In practice, these 4 legal bases are the ones Capgemini is most likely to rely on when processing personal data.

5. The processing is **necessary to protect the vital interests of the individual** whose personal data are processed or of another individual.
   For instance, where the individual is physically or legally unable to give his/her/their consent to the processing, and his/her/their safety or health is at stake.

6. 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.
   In practice, it is unlikely Capgemini would ever rely on this legal basis.

3.3. Data minimization

Capgemini shall only collect and further process the personal data which is strictly necessary in relation to the purpose(s) defined beforehand.

In practice, this means that Capgemini shall determine, ahead of the processing, which personal data are needed to achieve the objective(s). As a result, Capgemini shall not collect, store, or otherwise process non-essential personal data just so that it could use it for a hypothetical purpose which would be defined 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 process place to determine which data shall be updated or deleted to ensure data quality in the systems remains at the right level. This also means that Capgemini shall provide individuals with means to request inaccurate data to be corrected, updated, or deleted. For instance, Capgemini employees can make changes to their profile through a dedicated dashboard.

3.5. Data retention limitation

Capgemini shall keep personal data for no longer than necessary in relation to the purpose(s) for which the personal data were collected.

This means that Capgemini shall define the data retention period beforehand and according to the purpose(s) of the processing, considering and balancing the following:

- Any applicable/local legal requirement(s)
- The business needs
- The interests of the individuals whose personal data are processed.

In practice, for each project involving the processing of personal data, Capgemini shall determine whether any local law(s) provide data retention requirements and balance the overall objective of the project with the interests of the data subjects. This assessment will allow Capgemini to determine the data retention period related to the relevant processing activity.

3.6. Data security

Capgemini shall implement appropriate technical and organizational 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 shall implement the requirements and good practices defined by its Cybersecurity Organization. Such security measures shall be developed considering the nature of the personal data to be processed and the risks associated with such processing.

In the event of a data breach, Capgemini shall comply with its Cybersecurity Incident Management and Data Breach Notification Policy. The policy indicates all the necessary steps Capgemini must undertake to address incident management requirements, from preparation stage to closure. In particular, Capgemini shall involve the DPO in any incident which may impact personal data and keep records of all such incidents as per regulatory requirements. In practice, such records shall include the facts relating to the incident, its effects and the remedial actions taken, and it shall be made available to the competent supervisory authority upon request. The DPO shall then assess all incidents' severity in light of criteria based on the ENISA (European Union Agency for Cybersecurity) recommendations, and determine all notification and information Capgemini must perform in light of the risks identified:

- when the Data Breach is likely to result in a risk to the rights and freedoms of individuals, Capgemini shall also notify the relevant supervisory authority(ies), subject to applicable data protection law(s), without undue delay and no later than 72 hours after having become aware of it.
- In addition, Capgemini shall notify the data subject(s) without undue delay, when the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons.

Finally, and more specifically, when the Capgemini company importing personal data becomes aware of a Data Breach, it shall notify the Capgemini company exporting the personal data without undue delay.

3.7. Processing of special categories of personal data & data relating to criminal convictions and offences

Capgemini shall only process special categories of personal data – revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic and/or biometric data for the purpose of uniquely identifying an individual, data concerning health or an individual's sex life or sexual orientation – where strictly necessary and/or legally required.

- The individual has given explicit consent to the processing of those personal data for one or more specific purposes.
- The processing of those data is necessary for Capgemini or the individual to comply with an obligation or exercise specific rights in the employment, social security, and social protection law.
- The processing is necessary to protect the vital interests of the individual whose data are processed or of another individual.
- The processing is necessary for the establishment, exercise, or defence of legal claims or whenever courts are acting in their judicial capacity.
- The processing is necessary for reasons of substantial public interest.
- The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health.

In practice, Capgemini shall refrain from processing any special categories of personal data, and/or any personal data relating to criminal convictions and offences, unless one of the conditions listed above is fulfilled.

Special categories of personal data and/or data related to criminal convictions and offenses will only be transferred from the EEA to other countries, where covered by an equivalent level of protection to the one provided under EEA legislation.

3.8. Decision-making based on automated processing

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 affect them. However, this right does not apply if the processing is:

- Necessary to enter into, or the performance of, a contract between the individual and Capgemini.
- Authorized by applicable local law to which Capgemini is subject, and which also lays down suitable measures to safeguard the individual's rights and freedoms and legitimate interests.
- Based on the individual's consent.

In addition, Capgemini shall strive to explain to the individuals the underlying logic of any automated processing affecting them.

In practice, Capgemini shall inform the data subjects through a data protection notice which shall set out the method by which data subjects can contact Capgemini seeking the right to human intervention and/or to contest the decision where applicable.

4. Transparency

Capgemini shall provide data subjects with all the required information regarding the processing of their personal data.

Where personal data relating to individuals are collected directly from them, Capgemini shall, as a minimum, share the following information:

- The identity and contact details of the Capgemini company acting as data controller;
- The contact details of the competent DPO;
- The purpose(s) for which the personal data are processed as well as the legal bas(es) 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 – this is relevant in cases where Capgemini would share ;
- Whether Capgemini intends to transfer personal data outside of the EEA, and the existence or absence of an adequacy decision from the European Commission, or the reference to the appropriate safeguards (such as BCR or Standard Contractual Clauses) and how to obtain a copy of these;

- 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 portability;
- Where the processing is based on the consent of the individual, the right to withdraw consent at any time, without affecting the lawfulness of the processing;
- The right to lodge a complaint before a data protection and/or 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 individual 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 individual.

Where the personal data were not obtained directly from the individual, Capgemini shall still provide them with the above-mentioned information within a reasonable period after obtaining the personal data as well as with the description of the categories of personal data and the source(s) of said personal data. If the data is used to contact the individual, Capgemini shall provide them with the information at the time of that first communication.

In practice, Capgemini make available "data protection" or "privacy" notices to individuals to provide them with the necessary information.

Where collecting personal data directly from individuals for specific purposes, for instance through user-facing applications or tools, Capgemini shall draft and make available customized notices.

Capgemini also drafted and published more general data protection notices such as the one available on its website, which covers a wider array of processing activities including for instance marketing related processing.

5. Data subjects' rights

Individuals whose personal data are collected, used, or otherwise processed by Capgemini can request access to, rectification, or erasure of their data. In addition, data subjects can object to the processing of their data and have the right not to be subject to decisions based solely on automated processing, including profiling. In addition, data subjects can ask for the communication of their personal data in a structured, commonly used, and machine-readable format.

In practice, individuals are informed of their rights through dedicated notices and can exercise their rights by contacting Capgemini according to the process further detailed under Appendix 4.

Data subjects can exercise these rights by contacting the DPO, or another point of contact as may be relevant, following the internal process. Data subjects may also submit a complaint with regards to the processing of their personal data, through this same process.

In addition, individuals have the right to lodge a complaint regarding the processing of their personal data with the competent supervisory authority(ies) and/or before the competent court of law.

In case of any breach of the rights guaranteed and/or obligations provided under the BCR-C, Capgemini encourages individuals to submit a complaint using the dedicated process detailed under Appendix 4. However, individuals are also entitled to lodge a complaint before the competent supervisory authority(ies) – 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, individuals can lodge a complaint before the court of law of the Member State of their habitual residence, place of work or place of the alleged infringement. Where the processing of personal data is carried out by a non-EEA Capgemini company, the individuals may lodge a complaint before the competent court of law as may be provided under applicable local legislation, unless the processing and/or non-EEA Capgemini company is subject to the GDPR, in which case, the above-mentioned provisions shall apply.

Data Subjects have the right to judicial remedies and the right to obtain redress, and, where appropriate, compensation in case of any breach of one of the enforceable elements of the BCR-C, as listed under Section 6.

Data subjects may be represented by a non-profit organization or association to exercise these rights, under the conditions provided by applicable local law.

In practice, in case of a breach of the BCR-C, individuals can submit a complaint to Capgemini directly and/or the competent data protection authority and/or court of law. In addition, individuals may seek remedies, redress, and compensation in case of breach of one of the elements listed under Section 6.

6. Data subjects' enforcement rights

Data subjects may enforce the following elements of the BCR-C, as third-party beneficiaries:

- The implementation of the data protection principles detailed under Sections 3, 4 & 12 of the BCR-C.
- The obligation for Capgemini to share relevant information with individuals regarding the processing of their personal data, as provided under Section 4; as well as the obligation to provide easy access to the BCR-C, as provided under Section 17.
- Individuals' rights with regards to the processing of their personal data, as provided under Section 5.
- Individuals' right to complain through Capgemini's internal complaint process as provided under Section 5.
- Individuals' rights to lodge a complaint with the competent supervisory authority(ies) and/or before the competent courts of law, as provided under Sections 5.
- The obligation, for each non-EEA Capgemini company importing personal data, to notify the EEA Capgemini exporting such personal data as well as Capgemini's headquarters, in case of a conflict between the applicable local legislation and the BCR-C, as provided under Section 13.
- The obligation, for each Capgemini company importing personal data, to inform the exporting Capgemini entity as well as Capgemini's headquarters, and if legally permitted the data subject, of any requests from a public authority and/or law enforcement agency to access the personal data as provided and further detailed under Section 14.
- The duty for Capgemini to cooperate with the supervisory authorities, as provided under Section 16.
- The obligation for each EEA Capgemini company transferring personal data to a non-EEA Capgemini company, to accept liability for any breaches of the BCR-C by the non-EEA Capgemini company receiving the data, as provided under Section 15.
- The fact that, in case of a breach of the BCR-C by a non-EEA 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-C, as provided under Section 15.
- The obligation for Capgemini to inform data subject of any update of the BCR-C – including with regards to the list of Capgemini companies bound by the BCR-C – as provided under Section 18.
- The obligation of Capgemini to allow data subjects to enforce the elements of the BCR-C listed in this Section as third-party beneficiaries.
- The right for individuals to seek judicial remedies, obtain redress and, where appropriate compensation in case of any breach of the enforceable elements of the BCR-C listed under this Section – as provided under Section 5.

7. Data subjects' requests handling process

Capgemini created a dedicated internal process allowing individuals to submit requests and/or complaints regarding the processing of their personal data and/or any breach of the BCR-C. As further detailed under Appendix 4, individuals can reach out directly to the group, regional and/or local DPO, and/or other point(s) of contact.

The process detailed under Appendix 4 explains to the data subjects where and how to submit a request and/or complaint, the delays for the reply, the consequences in case of 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 supervisory authority(ies) or court(s) of law.

In practice, individuals can submit any request related to the processing of their personal data by contacting a DPO or other point of contact as described under Appendix 4. Capgemini shall first acknowledge receipt of the request and may ask for further information to facilitate the management of the request. Upon review of the request and/or complaint, the DPO and/or other function habilitated to handle requests, it will determine whether and to what extent the request can be addressed and will then respond to the requestor.

Capgemini shall respond to the requestor without undue delay and in any case, no later than 30 days upon receiving the request. Should Capgemini be unable to properly process the request within the 30 days period, it shall notify the requestor. Such notification shall be sent to the requestor within the 30 days period, explaining that the review and processing period could be extend for a further 2 months and detailing the reasons for the extension.

Capgemini shall manage such requests following its internal process.

8. Capgemini's data protection organization

Capgemini has appointed a group data protection office headed by the group data protection officer, as well as regional and local data protection officers, data protection champions and specific points of contacts (SPOCS) as depicted in Appendix 3.

If you wish to contact our Group Data Protection Office, please:

- Email us at: dpocapgemini.global@capgemini.com
- Write to us at the following address: 11 rue de Tilsitt, 75017 Paris, France.

To contact any of our local data protection officers, please fill-out our dedicated contact forms available on our Website.

Data protection officers monitor and ensure the compliance of the Capgemini company(ies) within their scope with applicable local data protection laws as well as with the BCR. DPOs provide support on all matters related to data protection, implement the global data protection program, handle and/or advise on data breaches and maintain an active relationship with the local supervisory authority.

As part of the legal function, DPOs are supported in their mission by their local legal teams. The DPOs report annually to the local country board or executive comity on privacy related matters such as the implementation of the global data protection program, privacy issues which may have occurred in large deals, critical data breaches and/or data subject requests where relevant, etc.

The DPOs act as business partners to support the different functions and operations to ensure they understand and implement the data protection principles and obligations in their day-to-day operations.

In practice, this means that DPOs shall implement a data protection strategy and program to ensure compliance with applicable local law as well as group policies and processes.

- → DPOs shall advise the business where a project involves the collection and further use of personal data to ensure data protection is embedded from the beginning. DPOs shall then review and approve projects involving the processing of personal data. In addition, DPOs shall provide templates, processes, and guidelines to ensure that data protection constraints are considered by default by the business.
- → DPOs shall support in-house lawyers in reviewing and negotiating data processing agreements with clients, providers and/or partners.
- → DPOs shall review and assess data protection risks associated with opportunities and recommend mitigation measures to eliminate or minimize such risks.
- → DPOs shall develop and deliver data protection function-specific trainings.
- → DPOs shall manage data breaches, in cooperation with Cybersecurity and any other relevant stakeholder(s), assessing the severity of the breach, making any required notification(s) and supporting in the implementation of mitigating measures.

→ DPOs shall review and address data subject requests, in cooperation with Group IT, HR and/or any other relevant stakeholder(s).

The DPO network is supported by data protection champions who represent each group function and, where relevant, each global business line (GBL). Data protection champions are appointed as representatives of their function or GBL to ensure that data protection guidelines, processes and procedures are properly implemented throughout the group. Data protection champions play a key role in the data protection organization as they enable DPOs to gain better insight into the operations so as to better support the business with tailored content.

9. Privacy by design

9.1. Record of processing activities

Where acting as controller, Capgemini shall keep and maintain, in writing, a record of processing activities containing the following information:

- The name and contact details of the Capgemini company acting as controller, the competent DPO, and where applicable the joint controller(s).
- The purpose(s) of the processing activities.
- A description of the categories of data subjects and of the categories of personal data processed.
- The categories of recipients to whom the personal data have been or will be disclosed including recipients located outside of the EEA.
- Where applicable, the cross-border transfers of personal data, including the country(ies) of destination as well as the transfer mechanism(s) used to frame such transfers.
- The data retention period.
- A general description of the security measures.

In practice, the business owner of any tool, application or any other project involving the processing of personal data shall create an entry in the register, including all the above-mentioned details. The competent DPO(s) shall then review the entry to ensure that it contains all the necessary information to enable them to assess the compliance of the project at stake with regard to applicable DP laws. Based on their assessment the DPO shall make recommendations to ensure the business owner carries out processing activities in compliance with these BCR-C and with applicable DP laws.

Where acting as a data processor, Capgemini shall also keep and maintain a record of processing activities carried out on behalf of the controller and including:

- The name(s) and contact details of the Capgemini company(ies) acting as processor(s) as well as the name(s) and contact details of each controller(s) on behalf of which they are processing the data.
- The categories of processing carried out on behalf of each controller.
- Where applicable, the cross-border transfer(s) of personal data including the country(ies) of destination as well as the transfer mechanism(s) used to frame such transfers.
- A general description of the security measures.

Capgemini shall make the records of processing available to the competent supervisory authority(ies) upon request.

9.2. Data protection impact assessments

Capgemini shall carry out a data protection impact assessment (DPIA) where a processing activity is likely to result in a high risk to the rights and freedoms of individuals.

Group and/or local DPO shall assess processing activities to determine whether it should be considered "high-risk" using a methodology aligned with the European Data Protection Board's recommendations and with any other local practices and/or guidelines issued by the data protection authority.

Group and/or DPOs shall determine the need to carry out a DPIA for a high-risk processing, considering:

1. The possibility of an undesirable event – e.g., illegitimate, or unauthorized access to the data, modification, or erasure of the data, etc.
2. The likelihood of such undesirable event occurring.
3. The severity of the consequences to the rights and freedoms of the data subjects.

In practice, when reviewing data processing activities, as further described under sub-section 9.1., the group or local DPO shall determine whether the owner needs to initiate a DPIA, answering a questionnaire designed to assess the risks. Group or local DPO shall then review the assessment and make recommendations to mitigate the risks.

Where the DPIA indicates that the processing activity would result in a high risk, and the group or local DPO determines that no measure can be implemented to mitigate such risk, it shall consult the competent supervisory authority. The supervisory authority shall review and assess the processing activity and determine whether Capgemini has properly assessed the risks through the DPIA and that the safeguards Capgemini intends to implement to address the risks are adequate.

10. Training & awareness

10.1. Global mandatory training

Capgemini has created and implemented a mandatory data protection training for all employees. The aim of the mandatory training is to ensure that all Capgemini are aware of and understand data protection key principles and requirements. This mandatory eLearning addresses the following:

- Understanding data protection key principles and requirements
- Data transfers & use of suppliers
- Data breaches management
- Personal data disclosure requests from law enforcement and/or public authorities (as well as any other third parties)

At the end of the training, employees are required to take a test. If they don't obtain a minimum of 80% to the test, they need to retake the entire training. Furthermore, once they have successfully passed the test at the end of the training, employees are prompted to download the BCR to have their training registered as "attended"– including in particular the process that must be followed in case of a request from a third party, public authority or law enforcement agency, to disclose personal data.

Capgemini employees are required to complete the training upon joining the company. Every year, employees shall be required to answer data protection related questions to assess their knowledge. In the event, the employee is not able to answer the questions correctly, they will be required to complete the full training again. In any case, Employees are required to take the full training every three years irrespective of the answers provided to the above-mentioned questionnaire.

10.2. Function-specific trainings & guidelines

In addition to the global mandatory eLearning, the data protection organization creates function-specific guidelines and trainings. The aim is to better support functions with tailored content: to address use cases that are specific to some functions.

In practice, all Capgemini employees regardless of their job description are required to complete the global mandatory data protection eLearning, to ensure they are aware of and understand the principles and obligations provided under the BCR. In addition, data protection officers and data protection champions deliver country and/or function specific trainings.

11. Audits

Capgemini shall carry out protection audits covering all aspects of the BCR on a regular basis. The audits and controls shall especially ensure that the BCR, all related policies, procedures or guidelines adopted within Capgemini ("Data Protection Program") as well as the Applicable Data Protection Laws are implemented, documented, and assessed.

The audits shall be carried out either by internal or external qualified and independent auditors.

Capgemini performs audits of data protection obligations that affect the governance and policy aspects ("Entity Audits"), and data protection obligations that affect the execution of such policies in the actual activities that involve processing personal data ("Activity Audits"). The combination of all these audits makes up the BCR Audits Program.

In practice, Capgemini shall carry out 3 types of data protection audits:

- **Level 1 - Local stakeholders are responsible for the auditing of their local activities.**
  - The Local DPO must perform an annual self-assessment of their Data Protection Program.
  - The Local DPO is also responsible for the auditing of the local stakeholders (central functions and/or GBL) which can be audited by them or a third-party mandated by them, against their responsibilities under the BCR and Capgemini's Data Protection Program.
  - Finally, the Local DPO shall audit the local activities (engagement, supplier and/or controller activities) to verify the implementation of the Data Protection Program.

- **Level 2 – The Group Data Protection Officer is responsible for the auditing of the local activities.**
  - The Group DPO shall audit the Local DPO's Data Protection Program to ensure compliance with Group-mandated BCR.
  - The Group DPO is also responsible for the auditing of local activities and/or global activities which may impact local compliance (engagements, suppliers, controller activities).
  - The Level 2 audits may be carried out by external qualified and independent auditors.

- **Level 3 – Capgemini's Group Internal Audit** is responsible for the auditing of both local & global DPOs, Global Business Lines (GBL) and/or central functions against the Blue Book and the BCR.

As part of our commitment to implementing strict control mechanisms and considering the diverse locations and structures of our company, our BCR Audits Program is designed to encompass all areas, year after year, within a maximum period of five years. This ensures that every aspect of our operations is represented and audited within this timeframe.

The audit reports, including the proposed corrective actions to address and mitigate the risks, shall be communicated to the data protection organization – and in particular the competent local DPO(s) – and to the top management and shall be made available to the competent supervisory(ies) authority(ies) upon request.

12. Use of internal or external processors

12.1. Data processing agreements or data protection clauses

Capgemini shall rely on data processors, either within or outside of the group, only to the extent that such processor provides sufficient guarantees to implement technical and organizational measures to ensure that the processing is carried out in compliance with applicable local data protection law.

When relying on another Capgemini company (internal processor) or on a third-party provider (external processor) to process personal data, Capgemini shall enter into a data processing agreement (DPA) or data protection clause which provides the conditions under which the processor shall process the personal data. As minimum, the DPA or data protection clause shall provide that the processor must:

- Process the personal data only on the documented instructions of Capgemini – including with regards to data transfers to countries located outside of the EEA.
- Ensure that persons authorized to process the personal data have committed themselves to an obligation of confidentiality.
- Implement technical and organizational measures to ensure an appropriate level of protection to the personal data.
- Only use a sub-processor with the prior specific or general authorization of Capgemini and enter into an agreement with such 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 under the DPA or data protection clause, to either delete or return the personal data after the end of the provision of services.
- Make available to Capgemini all the information necessary to demonstrate compliance with its obligations under applicable data protection law, and in particular the GDPR, and allowing for data protection audits.
- Report any data breach without undue delay.

In practice, before relying on any external processor, Capgemini shall:

1. Carry out a data protection & cybersecurity due diligence to assess providers maturity and ensure personal data shall be processed in a secure way.
   Capgemini has drafted dedicated questionnaires allowing this assessment to be performed. Providers are required to complete such questionnaire, allowing Capgemini to determine their level of data protection maturity as well as that of the services they would deliver.

2. Enter into an agreement, containing a DPA or data protection clause providing the conditions under which the provider shall process personal data on behalf of Capgemini.
   Capgemini has drafted DPA templates to address different scenarios – depending on the qualification of the parties (Controller/Controller, Controller/Processor, etc.). Irrespective of the whether Capgemini relies on such template, Capgemini shall review and negotiate all DPAs to ensure providers only access, collect or otherwise process personal data in compliance with applicable data protection law.

12.2. Additional obligations in case of transfers to third countries

In addition to the implementation of the above-mentioned DPA or data protection clause, where the use of a data processor involves cross-border transfer(s) of personal data, Capgemini shall ensure that an adequate level of protection is provided, as per the requirements detailed below.

In practice, it 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-C shall apply.
- Where an EEA Capgemini company acting as controller transfers personal data to a third party located outside of the EEA and acting as controller or processor, Capgemini shall enter the relevant modules of the Standard Contractual Clauses approved by the European Commission.
- Where a non-EEA Capgemini company acting as controller transfers personal data to a Capgemini company or to a third party located in a country which is not considered as providing an adequate level of protection by applicable data protection law, Capgemini shall implement any safeguard as may be required by such applicable law, on top of these BCR-C.

In addition, where transferring personal data from the EEA to a country which does not benefit from an adequacy decision granted by the European Commission, Capgemini shall further comply with the provisions of Sections 13 of these BCR-C.

13. Transfer impact assessments

Capgemini EEA companies shall only transfer personal data to non-EEA Capgemini companies or to third parties – i.e., data importers – located in a country which does not benefit from an adequacy decision delivered by the European Commission, where they have assessed that the laws and practices of such country do not prevent the data importer from fulfilling its obligations under the BCR.

This assessment, shall be made under the assumption that the laws and practice of the country where personal data are transferred, respect the essence of the fundamental rights and freedoms of individuals and do not exceed what is necessary and proportionate in a democratic society to safeguard objectives of public interest.

In practice, where conducting a transfer impact assessment (TIA), Capgemini shall consider:

1. The specific circumstances of the transfer or set of transfers and of any envisaged onward transfer(s) within the same country or to another country, including:
    - The purpose(s) for which the data are transferred and further processed (e.g. HR, IT support, etc.)
    - The types of entities involved in the transfer.
    - The economic sector of the data importer and the data exporter and in which the transfer occurs.
    - The category(ies) and format of the personal data transferred.
    - The location of the processing including storage, and
    - The transmission channels used.

2. The laws and practices of the country of destination, relevant in light of the circumstances of the transfer, including those requiring disclosing personal data to public authorities or authorizing access by such authorities and those providing access to these personal data during the transfer, as well as the applicable limitations and safeguards.

3. Any relevant contractual, technical, or organizational safeguards implemented to supplement the safeguards under the BCR-C including measures applied during the transmission and the processing of personal data in the country of destination.

Where the TIA reveals that supplementary safeguards must be implemented, on top those provided by the BCR-C, the EEA Capgemini Company(ies) transferring the data and their DPO(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-C, to identify any changes that would require updating the TIA(s) and the implementation of supplementary safeguards.

Where a non-EEA Capgemini company importing personal data has reasons to believe that it has become subject to laws and practices that would prevent it from fulfilling its obligations under the BCR-C, it shall notify the group data protection office, to ensure that appropriate additional safeguards are implemented to secure the transfer(s).

Similarly, where a Capgemini company exporting personal data has reasons to believe that a Capgemini company acting as importer can no longer fulfill its obligations under the BCR-C, it shall notify the group data protection office to ensure that appropriate additional safeguards are implemented to secure the transfer(s).

Competent local DPO(s) shall support Capgemini companies acting as exporter and importer to identify and implement the appropriate supplementary measures to ensure data transfers comply with applicable local laws and these BCR-C.

Where a Capgemini company determines that the BCR-C can no longer be complied with – even after supplementary measures have been implemented – for a specific transfer or set of transfers, or if instructed by a competent supervisory authority to do so, it shall suspend such transfer or set of transfers at stake – as well as all transfers for which the same assessment and reasoning would lead to a similar result – until compliance can be achieved or the transfer is ended. If compliance with the BCR-C 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 Capgemini company acting as data exporter.

Capgemini shall document and record TIAs – including the nature of the supplementary safeguards implemented to secure the transfer. Such documentation shall be made available to the competent supervisory authority(ies) 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 – including cases where supplementary measures could not be put in place, shall be made available to all Capgemini DPOs. Thus, enabling Capgemini to ensure compliance with the BCR-C and consistency in the manner they are implemented throughout the group.

14. Management of access requests from public authorities

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.

In practice, Capgemini employees are instructed to transfer any personal data disclosure request they might receive to their local legal department for review.

Where challenging a request, Capgemini shall 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 by the authority until expressly 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 from a public or law enforcement authority shall not be massive, disproportionate, or indiscriminate in a manner that would go beyond what is necessary in a democratic society.

Where legally permitted, the Capgemini company acting as data importer shall promptly notify the Capgemini company acting as data exporter, and, where possible, the data subject(s) involved, where it:

1. Receives a legally binding request issued by a public authority for the disclosure of personal data transferred under the BCR-C.
2. Becomes aware of any direct access by a public authority to personal data transferred under the BCR-C.

Such notification shall include all information available to the Capgemini company acting as data importer, and in particular: the personal data requested, the requesting authority, the legal basis for the request and the response provided.

Where prohibited from notifying the data exporter and/or the data subject(s) involved, the data importer shall use its best efforts to obtain a waiver of such prohibition 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 data exporter.

In practice, all Capgemini companies are required to monitor and record, monthly, information regarding any public and/or law enforcement authorities' requests to access personal data they may have received. Such reporting includes in particular:

- The number of requests.
- The type(s) of data requested.
- The authority(ies) that issued the request(s).
- Whether requests have been challenged.
- The outcome.

Local and regional DPOs record this information and share it with group data protection office. The information shall be accessible to all regional and local DPOs, preserved for as long as necessary and shall be made available to 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 office without undue delay.

15. Capgemini's liability in case of breach of the BCR-C

Each EEA Capgemini company exporting personal data to a non-EEA Capgemini company shall be liable, towards the data subjects, for any breaches of the BCR-C caused by the non-EEA Capgemini company.

In all other cases – (1) transfers from an EEA Capgemini to another EEA Capgemini company, (2) transfers between two non-EEA Capgemini companies, or (3) transfers from a non-EEA Capgemini company to an EEA Capgemini company – each Capgemini company shall be liable for a breach of the BCR-C it caused.

Where a transfer between two non-EEA Capgemini companies constitutes an onward transfer, the EEA Capgemini company which first initiated the transfer shall be liable towards data subjects, for any breaches of the BCR-C caused by either one of the non-EEA companies.

The list of Capgemini companies is provided under Appendix 1. Individuals may exercise their data protection rights and/or submit a complaint through Capgemini's dedicated process described under Section 7 and Appendix 4.

In practice, this means that the Capgemini company identified as bearing 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. Data subjects submit requests or complaints by reaching out to the competent DPO(s) through the dedicated process.

If a non-EEA Capgemini company violates the BCR-C, courts, or other judicial authorities in the EEA shall have jurisdiction, and data subjects shall have the rights and remedies against the liable EEA Capgemini company (i.e. the EEA Capgemini which transferred the personal data to a non-EEA Capgemini company) as if the violation had been caused by the latter in the Member State in which it is based.

In addition, it is up to Capgemini to demonstrate that it did not breach the BCR-C. In 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 actually breach the BCR-C.

16. Non-compliance with the BCR-C

Should a Capgemini company acting as data importer become unable to comply with the BCR-C for whatever reason, it shall inform the Capgemini company(ies) acting as the data exporter. Should a Capgemini company acting as data exporter become aware of a breach and/or inability by the Capgemini company acting as data importer to comply with the of the BCR-C, it must suspend the transfer.

The Capgemini company acting as data importer shall, at the choice of the Capgemini company acting as data exporter, immediately return or delete the personal data – including any copies thereof - that has been transferred under the BCR-C in its entirety, where:

- The data exporter has suspended the transfer, and compliance with the BCR-C has not been restored within a reasonable period, and in any event within one month of suspension, or
- The data importer is in substantial or persistent breach of the BCR-C, or
- The data importer fails to comply with a binding decision of a competent court or competent supervisory authority regarding its obligations under the BCR-C.

Where the Capgemini company acting as data exporter required the Capgemini company acting as data importer to delete the data, the Capgemini company acting as data importer shall further certify the deletion of the data to the Capgemini company acting as data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with the BCR-C.

Where local laws applicable to the Capgemini company acting as data importer prohibit the return or deletion of the transferred personal data, it shall commit to continue ensuring compliance with the BCR-C and will only process the data to the extent and for as long as required under that local law.

17. Cooperation with the supervisory authorities

Capgemini shall cooperate with the supervisory authorities.

In practice, this means that Capgemini shall comply with the advice and/or decision of the competent supervisory authorities and accept to be audited, and/or to be inspected by them (if necessary on-site) and/or to share documentation with them upon their request.

Any dispute related to the competent supervisory authority's exercise of supervision of compliance with the BCR-C will be resolved by the courts of the Member State of that supervisory authority, in accordance with that Member State's procedural law, and Capgemini companies agree to submit themselves to the jurisdiction of these courts.

18. Easy access to the BCR

The public version of the BCR-C is available on Capgemini's website as well as on Capgemini's Intranet.

The public version of the BCR-C contains all the elements of the internal version of the BCR-C, except for the following appendices, which are confidential documents which cannot be shared outside of the organization:

- The BCR Intra-group agreement
- Capgemini's data subjects' requests handling policy
- Group, regional and local DPO job description
- Capgemini's mandatory data protection eLearning
- Capgemini's data protection audit policy
- Management of personal data disclosure requests

The latest version of the BCR-C shall be made available to all Capgemini employees. In case of a significant update of the BCR-C, Capgemini shall inform its employees, launching a dedicated communication campaign to ensure employees are aware of and understand their obligations and rights under the BCR-C. In addition, Capgemini's mandatory data protection eLearning includes references to the BCR-C and employees are required to download and read the BCR-C upon completion of the training.

19. BCR updates

Capgemini shall keep the BCR-C up to date, in particular to reflect any regulatory changes, including recommendations from the European Data Protection Board.

The group data protection office is in charge of updating the BCR-C – including maintaining the list of Capgemini companies. The group data protection office shall share any update of the BCR-C with the Capgemini companies and their respective DPOs without undue delay. As such, the group data protection office shall provide the necessary information to the data subjects and/or the supervisory authorities.

Should Capgemini make any substantial change to the BCR-C, it shall first reach out to its lead supervisory authority, the CNIL, and provide an explanation of such changes.

Once a year, Capgemini shall communicate to the CNIL, any modifications made to the BCR-C, including an updated list of Capgemini companies. Such communication shall also include a confirmation regarding the group's assets.

20. Termination

Should any Capgemini company, acting as data importer, cease to be bound by the BCR-C, it shall either keep, return, or delete the personal data transferred under the BCR-C.

The decision to allow the former Capgemini company to keep the personal data shall be taken by the group data protection office. Should the former Capgemini company be allowed to keep the personal data, it shall commit to process such data in compliance with all applicable data protection requirements, including the GDPR.

Appendix 1 – List of entities bound by the BCR-C

Country	Name / Legal form	Registration number	Registered address
Argentina	**Capgemini Argentina SA**	1.613.291 Inspeccion General de Justicia	Avenida Presidente Roque Sáenz Peña 615, Piso 2º, Edificio Bencich C1035AAB Buenos Aires Argentina
Australia	**The WorksSydney Pty Ltd**	ACN 102 213 794	Level 10, 420 George Street, Sydney, NSW 2000 Australia
Australia	**Purpose Asia Pacific Pty Ltd**	ACN 625 798 807	Level 10, 420 George Street, Sydney, NSW 2000 Australia
Australia	**Capgemini Australia Pty Ltd**	ACN 092 284 314	Level 10, 420 George Street, Sydney, NSW 2000 Australia
Austria	**Capgemini Consulting Osterreich AG**	FN 194903y Handelsgericht Wien	Millenium Tower Handelskai 94-96, 22. Stock 1200 Wien Austria
Belgium	**Capgemini Belgium NV/SA**	0407.184.521 Brussels	Hermeslaan 9, 1831 Machelen Belgium
Brazil	**RADI Software Do Brasil Ltda**	11.855.485/0001-11	Rua Alexandre Dumas, No. 1711, 1st floor, unit 101, Chácara Santo Antônio, Zip Code 04717-004, City of São Paulo, State of São Paulo Brazil
Brazil	**Purpose Campaigns Do Brasil Ltda**	35231013042	RUA CUBATAO 472 SAO PAULO CITY- SP Brazil
Brazil	**Capgemini Brasil Ltda**	65.599.953\0001-63	ALAMEDA GRAJAÚ, 60, 14º ANDAR Alphaville, Cidade de Barueri 06454-050 BARUERI, ALPHAVILLE São Paulo Brazil
Canada	**Microsys Technologies Inc**	001909086	3710 Nashua Drive, Suite 1 L4V 1M5 Mississauga Canada

Canada	**Capgemini Solutions Canada Inc.**	860883149NP002	44 Chipman Hill, 10th Floor, P.O. Box 7289 Station "A", E2L 4S6 Saint John New Brunswick Canada
Canada	**Société en Commandite Capgemini Québec - Capgemini Québec LP**	NEZ 3367034736	1100 boul. René-Lévesque Ouest, Suite 1110 H3B 4N4 Montréal Québec Canada
Canada	**Capgemini Canada Inc**	610099	44 Chipman Hill, 10th Floor, P.O. Box 7289 Station "A", E2L 4S6 Saint John New Brunswick Canada
China	**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
China	**Altran (Shanghai) Information & Technologies Company Limited**	913101153125083000	The 3rd floor, Building 1, No. 400 Fangchun Road, Pilot Free Trade Zone 201203 Shanghai China
China	**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
China	**Sicon Design Technologies (Shanghai) Company Limited**	9131011509422053X2	700 Shangfeng Road, Unit 8, Room 301A, Pudong 200120 Shanghai China
China	**Capgemini (Hangzhou) Co Ltd**	330100400004425	15F, Building E,Tiantang Software Park, 3 XiDouMen Road 310012 Hangzhou Zhe Jiang Province China
China	**Capgemini Business Services (China) Limited**	440101400083545	6/F Podium, Glory IFC No. 25 Ronghe Road 528200 Nanhai District, Foshan City China
China	**Capgemini (China) Co Ltd**	310115400049352	Room A256, Floor 2, Building 3, 2250 South Pudong Road, China (Shanghai) Pilot Free Trade Zone China

China	**Capgemini (KunShan) Co Ltd**	320583400050999	NO.1 Jinjie Road, service outsourcing area Huaqiao, Kunshan Jiangsu Province China
China_HK	**Altran China Limited**	876293	Suites 1202-04, Tower 2, The Gateway, 25 Canton Road, TST, Kowloon Hong Kong China
China_HK	**Capgemini Hong Kong Ltd**	536651	Suites 4101-02, 41/F., One Island East, Taikoo Place, 18 Westlands Road, Quarry Bay, Hong Kong, China
Colombia	**Capgemini Colombia SAS**	2197990	Cra 7 No.71 - 72 Torre B Piso 9 Bogota DC Colombia
Costa_Rica	**Capgemini Costa Rica SRL (formerly Rivet Logic Costa SRL)**	NUMERO DE CERTIFICACION: RNPDIGITAL-1423520-2022	San José, Escazú, Guachipelín, 400 meters north of Construplaza, Edificio Latitud Norte, 3rd floor, Quatro Legal Office
Czech_Republic	**Capgemini Czech Republic SRO**	260 33 062	5. května 1746/22 CZ-140 00 Praha 4 Czech Republic
Denmark	**Capgemini Danmark AS**	25606965	Delta Park 40 2665 Vallensbaeck Strand Denmark
Denmark	**Capgemini Services Danmark ApS**	43792067	Delta Park 40 2665 Vallensbaeck Strand Denmark
Egypt	**Capgemini Egypt LLC**	183227	Plot 202 - Sector 2, Fifth Settlement, New Cairo, Cairo 12477, Egypt
Finland	**Capgemini Finland Oy**	1628142-5	Keilaranta 10 E 02150 Espoo Finland
France	**Knowledge Expert SAS**	841 323 736 RCS THONON LES BAINS	77 T Impasse du Clou 74500 Evian les Bains France
France	**Open Cascade SAS**	RCS: 420 919 805 RCS NANTERRE SIRET: 420 919 805 00093	145-151 Quai du Président Roosevelt 92130 ISSY- LES-MOULINEAUX France
France	**Capgemini Engineering Allemagne SAS [France] (formerly Altran Allemagne)**	519 093 041 RCS PARIS SIRET: 519 093 041 00043	76 avenue Kléber 75016 Paris France

France	**Logiqual SAS**	487 550 683 RCS TOULOUSE SIRET: 487 550 683 00030	4 avenue Didier Daurat 31700 Blagnac France
France	**Capgemini France SAS**	328 781 786 RCS NANTERRE SIRET: 328 781 786 01143	145-151 Quai du Président Roosevelt 92130 ISSY- LES-MOULINEAUX France
France	**Sogeti SAS**	434 325 973 RCS PARIS SIRET: 434 325 973 00031	11, rue de Tilsitt 75017 PARIS France
France	**Altran Lab SAS**	449 397 561 RCS NANTERRE SIRET: 449 397 561 00043	145-151 Quai du Président Roosevelt 92130 Issy-les-Moulineaux France
France	**Altran Technology & Engineering Center SAS**	817 459 357 RCS TOULOUSE SIRET: 817 459 357 00023	4 avenue Didier Daurat 31700 Blagnac France
France	**Altran Prototypes Automobiles SAS**	487 549 693 RCS NANTERRE SIRET: 487 549 693 00025	145-151 Quai du Président Roosevelt 92130 Issy-les-Moulineaux France
France	**Altran Technologies SAS**	702 012 956 RCS PARIS SIRET Paris: 702 012 956 00935 SIRET Issy: 702 012 956 00943	76 avenue Kléber 75016 Paris France
France	**Capgemini Engineering ACT SAS (formerly Altran ACT)**	817 459 209 RCS NANTERRE SIRET: 817 549 203 00026	145-151 Quai du Président Roosevelt 92130 Issy-les-Moulineaux France
France	**Global Management Treasury Services SNC**	448 370 080 RCS PARIS SIRET: 448 370 080 00054	11 rue de Tilsitt 75017 Paris France
France	**Capgemini SE**	330 703 844 RCS PARIS SIRET : 330 703 844 00036	11, rue de Tilsitt 75017 PARIS France
France	**Capgemini Service SAS**	652 025 792 RCS PARIS SIRET: 652 025 792 00084	11, rue de Tilsitt 75017 PARIS France
France	**Capgemini Gouvieux SAS**	428571186 RCS PARIS SIRET: 428571186 00017	11, rue de Tilsitt 75017 PARIS France
France	**Immobilière Les Fontaines SARL**	421 776 311 RCS PARIS SIRET: 421 776 311 00019	11, rue de Tilsitt 75017 PARIS France
France	**SCI Paris Etoile**	331 338 558 R.C.S PARIS SIRET: 331 338 558 00033	11, rue de Tilsitt 75017 PARIS France

France	**Capgemini Latin America SAS**	487 606 782 RCS PARIS SIRET: 487 606 782 00018	11, rue de Tilsitt 75017 PARIS France
France	**Capgemini Ventures SAS**	440 330 090 RCS PARIS SIRET: 440 330 090 00018	11, rue de Tilsitt 75017 PARIS France
France	**Capgemini Technology Services SAS**	479 766 842 RCS NANTERRE SIRET: 479 766 842 00724	145-151 Quai du Président Roosevelt 92130 ISSY- LES-MOULINEAUX France
France	**Capgemini Consulting SAS**	479766800 RCS NANTERRE SIRET: 479 766 800 00060	145-151 Quai du Président Roosevelt 92130 ISSY- LES-MOULINEAUX France
France	**Capgemini Engineering Research and Development SAS**	444495774 RCS NANTERRE SIRET: 444 495 774 00531	145-151 Quai du Président Roosevelt 92130 ISSY- LES-MOULINEAUX France
Germany	**Capgemini Engineering Deutschland SAS & Co KG (formerly Altran Deutschland SAS & Co KG)**	HRA 100894	81 Frankfurter Ring 80807 München Germany
Germany	**Capgemini Deutschland Holding Gmbh**	HRB 102576 Amtsgericht Berlin-Charlotttenburg	Potsdamer Platz 5 10785 Berlin Germany
Germany	**Capgemini Deutschland Services Gmbh**	HRB 215542 B Amtsgericht Berlin-Charlottenburg	Potsdamer Platz 5 10785 Berlin Germany
Germany	**Capgemini Engineering Service GmbH (formerly Altran Service GmbH)**	HRA 89337	81 Frankfurter Ring 80807 München Germany
Germany	**XL2 Gmbh**	HRB 773865 Amtsgericht Stuttgart	Potsdamer Platz 5 10785 Berlin Germany
Germany	**Capgemini Deutschland Gmbh**	HRB 98814 Amtsgericht Berlin-Charlottenburg	Potsdamer Platz 5 10785 Berlin Germany

Germany	**Capgemini Outsourcing Services Gmbh**	HRB 58881 Amtsgericht Düsseldorf	Balcke-Dürr-Allee 7 40882 Ratingen Germany
Greece	**HDL Design House Greece Private Company**	N° 134685604000	1, Plateia Dimokratias, Thessaloniki, 54629 (floor 6, office no. 610) Greece
Guatemala	**Capgemini Business Services Guatemala SA**	Company Patent - No.77886 Folio 548 Book 171 of Companies	15, avenida 5-00 Zona 13 Edifico World Technology Center Torre Sur Nivel 11 Ciudad de Guatemala Guatemala
Hungary	**Restaurant Application Development International Hungary**	Tax number: 23528480-2-09 EU tax number: HU23528480 Company registration number: 09-09-035337	028 Debrecen, Tüzér utca 4. A. ép. 2. em., Magyarország / H-4028 Debrecen, Tüzér Street 4. A building 2nd floor, Hungary
Hungary	**Capgemini Magyarorszag Kft**	13-09-087168 Pest County Registry Court	Rétköz utca 5 HU-1118 Budapest Hungary
India	**Capgemini IT Solutions India Pte Ltd**	CIN No. 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
India	**Leading Purpose Campaigns (India) Pte Ltd**	U74999DL2018FTC329926	FIRST FLOOR D-3 SOAMI NAGAR 110017 DELHI NEW DELHI India
India	**Capgemini Technology Services India Limited**	U85110PN1993PLC145950	No. 14, Rajiv Gandhi Infotech Park Hinjewadi Phase-III, MIDC-SEZ, Village Man, Taluka Mulshi, 411057 PUNE, Maharashtra India
Ireland	**Capgemini Ireland Ltd**	67792	Ground Floor, Metropolitan Building, James Joyce Street, Dublin 1 Ireland
Israel	**Altran Israel Limited**	514792282	7 Rival Street 6777840 Tel-Aviv-Yafo Israel

Italy	**Knowledge Expert SRL**	6988270820	Via Mariano Stabile 160 90139 Palermo Italy
Italy	**Capgemini Italia SPA**	4877961005	Via di Torre Spaccata, 140 00173 Roma Italy
Italy	**Capgemini Finance Tech SRL**	16239151000	Via di Torre Spaccata, 140 00173 Roma Italy
Japan	**Cambridge Consultants Japan Incorporated**	9-0104-01-126095	6F Spline Aoyama Tokyu Building, 3-1-3 Minamiaoyama, Minato-ku, 107-0062 Tokyo Japan
Japan	**Capgemini Japan KK**	0104-02-035069	Toranomon Hills Mori Tower, 1-23-1 Toranomon, Minato-ku, Tokyo
Japan	**BTC Corporation [Japan]**	0100－01－193831	Mita 43MT Bld, 3-13-16 Mita, Minato-ku, Tokyo
Luxembourg	**Capgemini Reinsurance International SA**	163.854 RCS Luxemburg	534 rue de Neudorf 2220 Luxembourg Grand-Duché de Luxembourg
Luxembourg	**Sogeti Luxembourg SA**	B42610	36 Route de Longwy 8080 Bertrange Grand-Duché de Luxembourg
Malaysia	**Capgemini Services Malaysia Sdn Bhd**	201101031070 (959205-M)	Suite 15-01,G Tower, 199 Jalan Tun Razak 50400 Kuala Lumpur Malaysia
Mexico	**Capgemini Mexico S De RL De CV**	219759	Av. Santa Fe No. 428, Torre 3, Piso 15, Colonia Santa Fe Cuajimalpa, Alcaldía Cuajimalpa, Ciudad de México, 05348 Mexico
Morocco	**Altran Maroc SARLU**	IF N°14457667 RC N°289225	1100 boulevard Al Qods, Casanearshore, Shore 17, Quartier Sidi Mâarouf 20270 Casablanca Morocco
Morocco	**MG2 Engineering SA**	IF N° 26143419 RC N°412549	1100 boulevard Al Qods, Casanearshore, Shore 12, Quartier Sidi Mâarouf 20270 Casablanca Morocco
Morocco	**Capgemini Technology Services Maroc SA**	164141	Shore 8 - A - Casanearshore 1100, Boulevard Al Qods - Sidi Maarouf Casablanca Morocco
New_Zealand	**Capgemini New Zealand Ltd**	1128855	Level 4, 80 Willis Street Wellington, 6011 New Zealand

Norway	**Capgemini Norge AS**	943 574 537	Karenslyst Allé 20 0278 Oslo Norway
Norway	**Matiq AS**	985 149 437	Abels gate 7 7030 TRONDHEIM Norway
Philippines	**Whitesky Labs (Philippines) Inc**	CS201410583 Metro Manila, Philippines	3304 ROBINSONS EQUITABLE BUILDING 4 ADB AVENUE ORTIGAS MANILA Philippines
Philippines	**Capgemini Digital Services Philippines Corp**	CS201405679	7th Floor, Tower 2 Insular Life Corporate Centre, Insular Life Drive, Filinvest Corporate City, Alabang, 1781 Muntinlupa City, Philippines
Philippines	**Capgemini Philippines Corp**	CS200714668	12 Floor, 10 West Campus, McKinely West, Fort Bonifacio, Taguig City, Philippines
Poland	**Capgemini Polska SP Zoo**	KRS 0000040605 District Court for Warsaw, XIIth Commercial Division of the National Court Register	Ul. Żwirki i Wigury 16a 02-092 Warsaw Poland
Portugal	**Capgemini Portugal SA**	504272179	Av. Colégio Militar, Torre Colombo, Piso 10 Lisboa Portugal
Romania	**Capgemini Services Romania SRL**	J40/22612/2007 Bucharest Trade Registry	Gara Herastrau Street, no. 4D Green Court building, 4th floor Bucharest, Sector 2 Romania
Saudi_Arabia	**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

Serbia	**PRIVREDNO DRUŠTVO HDL DESIGN HOUSE ZA INŽENJERING I KONSALTING EXPORT-IMPORT DRUŠTVO SA OGRANIČENOM ODGOVORNOŠĆU BEOGRAD (VRAČAR) [Serbia]**	17376667	Golsvortijeva 35, Beograd, Serbia
Singapore	**Altran (Singapore) Pte Ltd**	200106758M	4 Battery Road, #25-01 Bank of China Building 049908 Singapore Singapore
Singapore	**Liquidhub Pte Ltd**	Registration Number : 201703318C	12 Marina Boulevard # 32 - 02 Marina Bay Financial Centre 018982 Singapore
Singapore	**Cambridge Consultants (Singapore), Private Limited**	201230536C	4 Battery Road, #25-01 Bank of China Building 049908 Singapore Singapore
Singapore	**Capgemini Asia Pacific Pte Ltd**	199602754G	12 Marina Boulevard # 32 - 02 Marina Bay Financial Centre 018982 Singapore
Singapore	**Capgemini Singapore Pte Ltd**	199106419N	12 Marina Boulevard # 32 - 02 Marina Bay Financial Centre 018982 Singapore
Slovakia	**Altran Slovakia SRO**	46655956	Piešťanská 3 917 01 Trnava Slovakia
Spain	**Ecosat Airships SL**	B-47794425	Calle Nicostrato Vela, 20 24009 León Spain
Spain	**ACIE Agencia de Certification Espanola SLU**	B-82271313	En calle Campezo 1, edificio 4, planta 0 28022 Madrid Spain
Spain	**Capgemini Espana SL**	Tomo 27.544; Folio 54; Hoja M-287781 Registro Mercantil de Madrid	Calle Puerto de Somport, Edificio Oxxeo, CP 28050 Madrid Spain
Sweden	**Capgemini Engineering Sverige AB (formerly Altran Sverige)**	556542-2531	37 Södra Hamngatan SE 411 06 Göteborg Sweden
Sweden	**Sogeti Sverige AB**	556631-4687 Stockholm	Svetsarvägen 4 171 41 Solna Sweden

Sweden	**Capgemini AB**	556447-9763 Stockholm	Flemingatan 18, 112 26 Stockholm Sweden
Sweden	**Capgemini Sverige AB**	556092-3053 Stockholm	Flemingatan 18, 112 26 Stockholm Sweden
Switzerland	**Knowledge Expert SA**	CHE-114.807.854	9 rue de la Gabelle 1227 Carouges (GE) Switzerland
Switzerland	**Capgemini Suisse SA**	CHE-106.108.52 Handelsregister des Kantons Zürich	World Trade Center Leutschenbachstrasse 95 8050 Zurich Switzerland
The_Netherlands	**Capgemini Semiconnext Platform BV**	865742030	"Reykjavikplein 1 3543 KA Utrecht The Netherlands "
The_Netherlands	**Altran Netherlands BV**	34106539	1Reykjavikplein 3543KA Utrecht The Netherlands
The_Netherlands	**Altran International BV**	33294562	1 Reykjavikplein 3543KA Utrecht The Netherlands
The_Netherlands	**Sogeti Nederland BV**	30200252 Kamer van Koophandel Midden-Nederland (Utrecht)	Lange Dreef 17 4131 NJ Vianen The Netherlands
The_Netherlands	**Capgemini NV**	30067608 Utrecht	Reykjavikplein 1 3543 KA Utrecht The Netherlands
The_Netherlands	**Capgemini Business Services BV**	33030578 Utrecht	Reykjavikplein 1 3543 KA Utrecht The Netherlands
The_Netherlands	**Knowledge Expert BV**	85051232	Lange Viestraat 2B 3511 BK Utrecht The Netherlands
The_Netherlands	**Capgemini International BV**	33268283 Utrecht	Reykjavikplein 1 3543 KA Utrecht The Netherlands
The_Netherlands	**Capgemini Nederland BV**	30053172 Utrecht	Reykjavikplein 1 3543 KA Utrecht The Netherlands
The_Netherlands	**Capgemini Sourcing BV**	30135992 Utrecht	Reykjavikplein 1 3543 KA Utrecht The Netherlands
The_Netherlands	**Capgemini Educational Services BV**	30197497 Utrecht	Reykjavikplein 1 3543 KA Utrecht The Netherlands

Tunisia	**Altran Telnet Corporation SA**	Identifiant unique 1062046P Ancien numéro d'enregistrement B2455592008 (à noter : Selon la nouvelle loi relative au registre national des entreprises, le matricule fiscal sera l'identifiant unique annulant et remplaçant ainsi le numéro d'immatriculation au registre de commerce.)	Centre urbain Nord, Immeuble Ennour 1082 Tunis El Mahrajène Tunisia
Tunisia	**KE Tunisie SARL**	Identifiant unique 1760466T Ancien numéro d'enregistrement C0182112022 (à noter : Selon la nouvelle loi relative au registre national des entreprises, le matricule fiscal sera l'identifiant unique annulant et remplaçant ainsi le numéro d'immatriculation au registre de commerce.)	Rue du Lac Lochness, Immeuble Fajr, RDC, 1053 Les Berges du Lac, Tunis Tunisia
UAE	**Altran Middle East FZ-LLC**	17595	1803-1804 Al Thuraya Tower 1, PO Box 502709 Dubai Media City United Arab Emirates
UK	**Quorsus Limited**	11521293	1 Forge End GU21 6DB Woking United Kingdom
UK	**Altran UK Holding Ltd**	03066512	1 Forge End GU21 6DB Woking United Kingdom
UK	**Information Risk Management Ltd**	03612719	1 Forge End GU21 6DB Woking United Kingdom
UK	**23RED Ltd**	3974936	1 Forge End GU21 6DB Woking United Kingdom

UK	**Cambridge Consultants Ltd**	01036298	Milton Road, Science Park - Unit 29 CB4 0DW Cambridge United Kingdom
UK	**Purpose Europe Ltd**	8340026	Raleigh House 14C Compass Point Business PK Stocks Bridge Way PE27 5JL ST Ives, Cambridgeshire, United Kingdom
UK	**CGS Holdings Ltd**	02798276 England & Wales	No. 1 Forge End, Woking GU21 6DB, Surrey United Kingdom
UK	**Capgemini UK PLC**	943935 England & Wales	No. 1 Forge End, Woking GU21 6DB, Surrey United Kingdom
Ukraine	**Lohika LTD, LLC**	37413934	50 Prakhovykh Simi Str. 01033 Kyiv Ukraine
USA	**Annik Inc**	Registration Number in Florida : P07000081250	Corporation Service Company 1201 Hays Street 32301 Tallahassee, County of Leon, Florida United States of America
USA	**VariQ Corporation**	Employer identification number (EIN) / Tax Identification Number : 13-4269151 (Nevada)	Corporation service company 112 North Curry street Carson city, NV 89703 United States of America
USA	**Altran Engineering Solutions Inc**	800653319	40600 Ann Arbor Road E, Suite 201 MI 48170-4675 Plymouth USA
USA	**Cambridge Consultants Inc**	000867390	745 Atlantic Ave. 6th floor MA 02111 Boston USA Email Eve 28.09.22 : 2 Drydock Avenue Suite 1210 Boston, MA 02210
USA	**Capgemini VariQ JV LLC**	11267185	Corporation Service Company 100 Shockoe Slip, 2nd Floor Richmond, VA 23219 United States of America
USA	**Purpose Global PBC**	5045539	c/o Corporation Services Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America
USA	**Purpose Campaigns LLC**	3971119	c/o Corporation Services Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America

USA	**Capgemini North America Inc**	Registration number in Delaware: 3509818	c/o Corporation Service Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America
USA	**Capgemini America Inc**	Registration Number in NewJersey: 0100245598	c/o Corporation Service Company Priceton South Corporate Ctr., Ste. 160, 100 Charles Ewing Blvd., 08628 Ewing, New Jersey United States of America
USA	**Capgemini Government Solutions LLC**	Registration Number in Delaware: 3584244	c/o Corporation Services Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America
USA	**Capgemini Technologies LLC**	Registration number in Delaware- 3529062	c/o Corporation Services Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America
USA	**Capgemini Business Services USA LLC**	Registration Number in Delaware: 5010627	c/o Corporation Services Company 251 Little Falls Drive 19808 Wilmington, Delaware United States of America
VietNam	**Capgemini Services Vietnam Limited Liability Company (formerly Aodigy Vietnam Limited Liability Company)**	401966898	150-156 Nguyen Van Linh, Vinh Trung Ward, Thanh Khe District, Da Nang City, Vietnam
VietNam	**Capgemini Vietnam Co Ltd**	411043001695	Centre Point Building, 106 Nguyen Van Troi, Ward 8, Phu Nhuan District, Ho Chi Minh City Vietnam
VietNam	**Công Ty THNN Bigtree Technology & Consulting Vietnam**	107650321	Floor 7, No. 444 Hoang Hoa Tham, Thuy Khue Ward, Tay Ho District, Hanoi, Vietnam
Thailand	**Capgemini Services (Thailand) Co Ltd**	N° 105557076173	8 Wework, T-One Building, 20th Floor, Soi Sukhumvit 40, Sukhumvit Road, Khlong Toei District, Phra Khanong Sub-District, Bangkok THAILAND

Appendix 2 – Capgemini processing activities & main transfers

The table copied below describes the key data processing activities 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
Recruitment, including background checks subject to applicable law	▪ **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, candidate 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**	Candidates	Countries in which Capgemini is established

Purpose	Categories of data	Data Subjects	Countries where data is transferred
Performance assessment and training	▪ **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	Employees	Countries in which Capgemini is established
Pay-roll and administration of other employment-related benefits (including stock options, stock purchase plan, or other corporate plans or benefits)	▪ **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	Employees Third party consultants	Countries in which Capgemini is established

Purpose	Categories of data	Data Subjects	Countries where data is transferred
Day-to-day management activities, such as deployment of staffon projects, promotion, disciplinary activities, grievance procedure handling	▪ **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	Employees	Any country where Capgemini is established

Purpose	Categories of data	Data Subjects	Countries where data is transferred
Marketing the professional services of consultants to potential Capgemini clients (e.g., by providing details of experience on previous projects)	▪ **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; ▪ **Recruitment information**, such as CV, application form, notes of interviews, candidate 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.**	Employees Consultants	In all countries in which Capgemini is established

Purpose	Categories of data	Data Subjects	Countries where data is transferred
Administration of current benefits, including the Capgemini personal pension plan, life insurance scheme, private health insurance scheme	▪ **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	Employees	Countries in which Capgemini is established

Purpose	Categories of data	Data Subjects	Countries where data is transferred
Employment analysis, for example, comparing the success of various recruitment and/or Employee retention programs	▪ **Recruitment information**, such as CV, application form, notes of interviews, candidate 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	Employees Candidates	India

Purpose	Categories of data	Data Subjects	Countries where data is transferred
Compliance with health & safety rules and other legal obligations placed on Capgemini as an employer	▪ **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.	Employees	Countries in which Capgemini is established

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	▪ **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, candidate 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.	Employees Consultants	Countries in which Capgemini is established
Human Resource Management, Career management and mobility	▪ **Contact details**, such as name, date of birth, gender, age, address, telephone numbers, email	Employees	Countries in which Capgemini is established

Purpose	Categories of data	Data Subjects	Countries where data is transferred
	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, candidate 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	Candidates	
Internal and external communication	▪ **Contact details**, such as name, address, telephone numbers, email address; ▪ **Photos**	Employees	Countries in which Capgemini is established

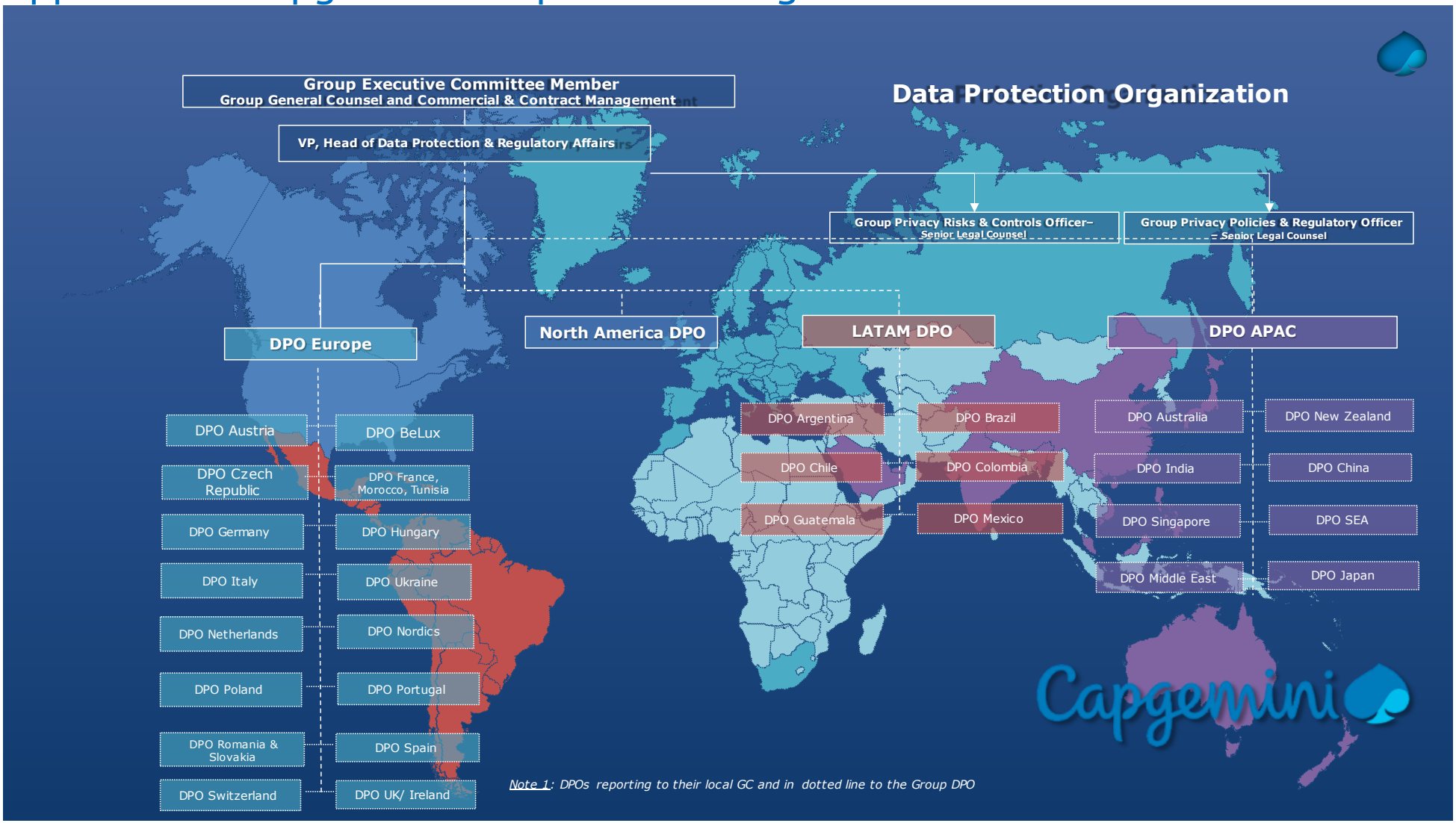
Purpose	Categories of data	Data Subjects	Countries where data is transferred
Disaster recovery plan and crisis management	▪ **Contact details**, such as name, date of birth, gender, age, address, telephone numbers, email address, number of children, citizenship, ID details, visa details, work permit 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.**	Employees Employees' relatives	Countries in which Capgemini is established

Audit and statistics	▪ **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, candidate 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	Employees Candidates Clients contacts details Suppliers contacts details	India

Purpose	Categories of data	Data Subjects	Countries where data is transferred
Third-parties suppliers management	▪ **Contact details**, such as name, address, telephone numbers, email address	Employees Third parties' employees	Countries in which Capgemini is established
Leakage Prevention	▪ **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	▪ **Details of IT and connection data** to the Capgemini IT systems	Employees	Countries in which Capgemini is established
Protecting Systems, Network, Infrastructure & Computers	▪ **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
Identity Access Management	▪ **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
BYOD Program Management	▪ **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.)**	▪ **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
Forensics Investigation	▪ **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



Appendix 4 - How to exercise your data protection rights?

Key data protection notions

Personal data	Any information which can be used to identify an individual, directly or indirectly when used in combination with others.
Processing	Any operation performed on personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, restructuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, combination, restriction, erasure, or destruction
Controller	The natural or legal person which determines the purposes and means of the processing of personal data.
Processor	The natural or legal personal which processes personal data on behalf of the controller.
Purpose	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.

Please note that you can also file a complaint with a Supervisory Authority, and/or seek judicial remedy in court.

What are your rights?

You can request to exercise the following rights in relation to the personal data concerning you that Capgemini collects and further processes:

Access	You can ask Capgemini whether personal data concerning you are being processed, and where that is the case, you can request access to such personal data.
Erasure	In some cases, you can request that Capgemini delete your personal data
Rectification	You can ask Capgemini to rectify, update or complete your personal data.
Objection	In some cases, you can ask Capgemini not to process your personal data.
Restriction	In some cases, you can ask Capgemini to limit the processing of your personal data to some purposes and subject to certain conditions
Withdraw consent	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.
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.
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.

Contact us

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

Using our dedicated contact form

By email

By mail

Full list of Capgemini offices available on our website.

By phone

Full list of Capgemini offices available on our website.

To allow us to properly address your request, please share 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 address your request?

Capgemini shall review and assess your request or complaint and address it without undue delay.

Acknowledgement of receipt

Review of your request by competent local DPO

Answering your request

- Within 30 days of receipt of the request
- Possibility to extend response timeframe by another 2 months in case of complexity/multiple requests

Addressing & closing your request

If you submitted your request via electronic means, Capgemini shall provide the information you requested in a commonly used electronic format.

Should Capgemini be unable to or refuse to respond favorably to your request, it shall provide details explaining its decision as well as a reminder that you can go before the competent court of law and/or Supervisory authority.

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 360,000 team members 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 2022 global revenues of €22 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.

Choose an item. Copyright © 2023 Capgemini. All rights reserved.