CAPGEMINI BINDING CORPORATE RULES

Introduction

As one of the world's foremost providers of consulting, technology and outsourcing services to a wide array of clients around the world, Capgemini is committed to protecting privacy and the Personal Data entrusted to it. As an international Group with companies in more than 40 countries, Capgemini needs to ensure that Personal Data flows freely and securely between the Capgemini Companies with an appropriate and uniform level of protection.

Most of the countries where the Group provides services have data protection or privacy laws designed to regulate the collection, use, transfer, storage and disposal of Personal Data. As stated in its Code of Business Ethics and its Data Privacy Policy (**Annex 1** attached), Capgemini is committed to complying with the data protection laws of the countries from where Personal Data is collected and processed. This includes compliance with current and future EU Law.

In addition, clients rely on Capgemini's global organization to operate effectively and competitively while affording protection to their Personal Data. This means that, potentially, at a client's direction or provided there is a legitimate need, client Personal Data may be stored and processed at Capgemini locations and data centers outside of the EEA.

The Binding Corporate Rules together with its Annexes (collectively hereinafter referred to as the "**BCRs**") have been adopted to express Capgemini's commitment to establishing and maintaining high standards across the Group for the transfer and processing of Personal Data by the Capgemini Companies.

The BCRs are designed to cover the flow of Personal Data transferred within the Group (including to countries located outside the EEA) for the Processing purposes described in this document, so as to facilitate a free and secured flow of Personal Data between the Capgemini Companies. The BCRs cover the Personal Data Capgemini processes as a Data Controller (BCR-Controller) and the Personal Data Capgemini processes as a Data Processor (BCR-Processor).

The BCRs are also intended to summarize the measures implemented by Capgemini, as part of its commitment as an accountable company, to demonstrate that Processing of Personal Data by the Capgemini Companies is performed in accordance with EU Law.

In order to give full effectiveness to its commitments, in addition to these BCRs, Capgemini has implemented a comprehensive privacy compliance program comprised of (1) a Global Data Privacy Policy, (2) a Cybersecurity Organization which includes a global network of Data Protection Officers, privacy attorneys and security professionals; (3) privacy and security awareness and trainings for Employees; (4) monitoring of compliance with regulatory and contractual privacy requirements; and (5) security incident response plans.

1. Definitions

In these BCRs, the following terms shall be defined as follows and shall be construed in accordance with EU Law:

"**Applicable Law**" means any data privacy or data protection law, applicable at the time of the processing.

"**Business Contact**" means a Capgemini's supplier, subcontractor, client or alliance partner, whether having an on-going commercial relationship with Capgemini or being a former or potential Business Contact of Capgemini.

"**Capgemini**" or "**Group**" means the entire Group of Capgemini Companies controlled, directly or indirectly, by Cap Gemini SA.

"**Capgemini Company(ies)**" means a company within Capgemini which is controlled directly or indirectly by Cap Gemini SA.

"**Capgemini Data Privacy Policy**" means the global Data Privacy Policy covering all Capgemini Companies activities whether acting as a Data Controller or as a Data Processor and listed in **Annex 1**.

"**BCR-Controller**" means Controller Binding Corporate Rules.

"**Covered Personal Data**" means Personal Data that are included in the scope of the BCRs.

"**Data Controller**" or "**Controller**" means the company that determines the purposes and means of processing the Personal Data.

"**Data Processor**" or **"Processor**" means the company which processes Personal Data on behalf of the Data Controller (whether a Capgemini Processor, i.e. an "**Internal Data Processor**", or a non Capgemini Processor, i.e., an "**External Data Processor**") that may be located within the EEA or outside the EEA.

"**Data Subject**" means the individual to whom the Personal Data relates.

"**DPA**" means Data Protection Authority.

"**DPO**" means Data Protection Officer.

"**EEA**" means the European Economic Area.

"**Employee**" means a Capgemini Company's Employee as well as agency workers.

"**Employee Personal Data**" means the Personal Data of a current, former or prospective Capgemini Employee.

"**EU Law**" means Directive 95/46/EC of the European Parliament and of the Council of October 24th 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive 2002/58/EC of the European Parliament and of the Council of July 12th 2002 concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and any subsequent European Union legislation amending it.

"**BCR-Processor**" means Processor Binding Corporate Rules.

"**Personal Data**" means any information relating to an identified or identifiable natural person ("**Data Subject**"). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Personal Data shall also be understood as Personally Identifiable Information.

"**Processing**" includes the collection, recording, organization, storage, adaptation, retrieval, consultation, use, and disclosure by transmission, dissemination or otherwise and making available, alignment or combination, blocking, erasure or destruction of Personal Data.

"**Security Breach(es)**" means any compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

"**Sensitive Personal Data**" means Personal Data revealing directly or indirectly racial or ethnic origin, political, philosophical or religious beliefs, criminal records, trade union membership, healthcare Personal Data or Personal Data related to sexual life.

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

"**SBU**" means a Capgemini Group Strategic Business Unit.

2. Scope of the BCRs

2.1 Material Scope

The BCRs cover the Personal Data Capgemini processes as a Data Controller (BCR-Controller) and the Personal Data Capgemini processes as a Data Processor (BCR-Processor). Such Personal Data include Employees' Personal Data processed for work related purposes, as well as well as Business Contacts' Personal Data processed for business related purposes. When acting as a Data Processor, this may also cover any other type of Personal Data as requested by the Data Controller.

2.2 Geographical scope

The BCRs apply to the Capgemini Companies to the extent that they process Covered Personal Data as Data Controllers or as Data Processors. For more information about Capgemini Companies worldwide please click here.

Transfer of Covered Personal Data to Capgemini Companies outside of the EEA is made only to those Capgemini Companies who have adhered to the BCRs by signing an adhesion agreement.

The BCRs reflect EU Law and national data protection laws of EEA countries. In some countries, other national rules might be in some instances more stringent. To the extent these national rules apply to Covered Personal Data, the local legal department of the relevant countries will issue, as appropriate, country-specific guidelines or local policies which will apply in addition to the BCRs. Some particular privacy policies may also be implemented within some Capgemini Business Units or Capgemini Companies. These policies shall refer to the BCRs and will take in account any local laws or regulations that require additional or stricter requirements.

BCR-Controller only apply to Covered Personal Data transferred from the EEA within the Capgemini Group.

As far as BCR-Processor are concerned, the Controller may decide to apply the BCR either 1) to Covered Personal Data processed by a Capgemini Company on the Data Controller's behalf and that is submitted to EU law, or 2) to Covered Personal Data processed by a Capgemini Company on the Data Controller's behalf, whatever the origin of such Personal Data.

3. BCRs and Capgemini Data Privacy Policy implementation

The BCRs and the Capgemini Data Privacy Policy in **Annex 1** shall be binding on all Capgemini Companies and their Employees. Local management of Capgemini Companies and their DPO shall be accountable for local BCR and Capgemini Data Privacy Policy implementation.

The Data Privacy Policy and a public version of the BCRs (translated in local language when required) are available on Capgemini's Intranet and on Capgemini's public website.

This Capgemini Data Privacy Policy encapsulates the principles governing the processing of Personal Data across the Capgemini Group which are based on articles 6 and 7 of Directive 95/46/EC of the European Parliament and of the Council of October 24th 1995 on the protection of individuals with

regard to the processing of personal data and on the free movement of such data. These principles are further developed below.

3.1 Capgemini processes Personal Data in a fair, lawful and transparent manner

When acting as a Data Controller, Capgemini processes Personal Data in compliance with Applicable Law and shall provide all necessary information to the Data Subject and access to his/her Personal Data as required by Applicable Law and in accordance with Capgemini's applicable procedure. This includes enabling that Personal Data is adequate, relevant and not excessive in relation to the purposes for which they are processed, as well as updating, correcting or deleting the Personal Data so that it is accurate and kept up-to-date.

When acting as a Data Processor, Capgemini processes Personal Data in compliance with Applicable Law and the Data Controller's instructions as per the contractual obligations contained in the Service Agreement. Capgemini shall support the Data Controller as it is reasonably necessary to enable the Controller's compliance with data protection law and with data quality, fair processing and transparency principles. Capgemini shall cooperate with and assist the Data Controller within a reasonable time and to the extent reasonably possible. This may include updating, correcting or deleting the Personal Data and informing other Data Processors as per the Data Subject or the Data Controller request so that it is accurate and kept up-to-date. This may also include communicating any useful information to the Data Controller in order to help the later comply with Data Subjects rights, handle complaints or reply to an investigation or an inquiry from the DPAs.

3.2 Capgemini processes Personal Data for limited and defined purposes

When acting as a Data Controller, Capgemini only processes Personal Data for specified, explicit, lawful and legitimate purposes and in compliance with the purpose for which it is originally collected, subject to Applicable Law. Capgemini processes Personal Data (i) with the unambiguous consent of the Data Subject, or (ii) for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract, or (iii) for compliance with a legal obligation to which the Data Controller is subject, or (iv) to protect the vital interests of the Data Subject, or (v) when processing is necessary for the purposes of the legitimate interest of Capgemini or by the third party to whom the data are disclosed, except where such purposes are overridden by the fundamental rights and freedoms of the Data Subject. Personal Data is only disclosed for legitimate and relevant "need-to-know" purposes for business or legal reasons. In each instance, any disclosure of Personal Data is strictly limited to what is necessary and reasonable to comply with the purpose of the processing. Unless in case of business acquisition or divestiture, Capgemini does not sell or trade Personal Data. In addition, subject to Applicable Law, Sensitive Personal Data shall be processed by Capgemini (i) if the Data Subject has given explicit consent, or (ii) processing is necessary for the purposes of carrying out the obligations and specific rights of Capgemini in the field of employment law, or (iii) processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving his/her consent, or (iv) the processing relates to data which are manifestly made public by the Data Subject or is necessary for the establishment, exercise or defense of legal claims.

When acting as a Data Processor, Capgemini only processes Personal Data in compliance with the Data Controller's instructions and shall not further process it for a different client or purpose, except with the express consent of the Data Controller and subject to Applicable Law. In case Capgemini cannot process Personal Data in compliance with the Data Controller's instructions, it shall promptly inform the Data Controller of its inability to comply, in which case the Data Controller is entitled to terminate

the transfer of Personal Data and terminate the contractual relationship to the extent related to the processing of Personal Data, subject to contractual terms and Applicable Law. Similarly if the processing conditions are changed, Capgemini shall inform the Data Controller in a timely fashion so that it has the possibility to object to the change or to terminate the contract before the implementation of the change. When processing Personal Data, Capgemini uses processes and tools that integrate privacy from their inception (privacy-by-design) and performs privacy impact assessments as required by Applicable Law.

3.3 Capgemini processes Personal Data for a limited duration

When acting as a Data Controller, Capgemini only retains Personal Data in a form which permits identification of a Data Subject for as long as is necessary for the purpose(s) for which it is processed, in accordance with local laws.

When acting as a Data Processor, Capgemini only processes Personal Data in compliance with the instructions of the Data Controller, including storage duration. This may include the performance of a task carried out in the public interest or in the exercise of the official authority vested in Capgemini or in a third party to whom the Personal Data are disclosed. In this respect, at the end of the processing, Personal Data and the copies thereof can be either returned to the Data Controller, anonymized or can be destroyed appropriately and securely, and the corresponding instruction shall be communicated to other Data Processors. When Capgemini destroys the Personal Data, it shall certify to the Data Controller that it has done so, subject however to local law requirements and security and back-up obligations. In case local law prevents Capgemini from returning or destroying all or part of the Personal Data, Capgemini shall accordingly inform the Data Controller and warrants that it will ensure confidentiality of the Personal Data transferred and will no longer actively process the Personal Data.

3.4 Capgemini processes Personal Data securely

As a general rule, and unless otherwise requested by the client, Capgemini applies the same level of security to Personal Data it processes as a Data Processor and Personal Data it processes as a Data Controller.

Capgemini applies and maintains appropriate technical, physical, and organizational measures to protect Personal Data, and follows industry practices and standards in adopting procedures and implementing systems designed to prevent unauthorized access to Personal Data and to avoid its accidental loss, damage or destruction.

Capgemini shall report Security Breaches to the authorities and/or the Data Subjects as per Applicable Law if it becomes aware that the security, confidentiality or integrity of the Personal Data has been compromised.

When acting as a Data Processor, Capgemini complies with the security and organizational measures which at least meet the requirements of the Data Controller's Applicable Law and the provisions of the Service Agreement. Capgemini shall promptly inform the Data Controller of any Security Breach and shall ensure that its Processors are bound by equivalent obligations.

3.5 Capgemini works with sub-processors in a responsible manner

Capgemini shall only use Capgemini Processors located outside the EEA who have signed the BCRs and the Data Privacy Policy and are bound by an intercompany agreement and a statement of work. When

using External Data Processors, Capgemini shall enter into appropriate agreements that require that the Personal Data is stored and processed in accordance with EU Applicable Law and as per the Data Controller's instructions.

When using External Data Processors located outside of the EEA, Capgemini shall enter into the standard contractual clauses for the transfer of Personal Data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

When acting as a Data Processor, Capgemini shall ensure that sub-processing of Personal Data to Capgemini Processors or to External Data Processors in the course of providing services is performed with the consent and at the direction of the Data Controller and is strictly relevant to the processing activities. Such processing shall be made under a written agreement to enable that such External Data Processor be bound by obligations equivalent to those imposed on the Data Processor under the Service Agreement and the principles contained in the BCR. In addition, when transferring Personal Data to External Data Sub-Processors located outside of the EEA, Capgemini shall enter into appropriate ad-hoc agreements with these Data Processors that require that the Personal Data is stored and processed in accordance with EU Applicable Law and as per Data Controller's instructions.

4. Capgemini Data Privacy Governance Structure

In order to protect its information and those of its clients and to counter security risks, Capgemini has launched a global "Cybersecurity and Information Protection" (or CySIP) program with the objective of establishing a homogeneous and mandatory security level for all entities of the Capgemini Group. Data protection, data privacy and confidentiality are at the core of the CySIP program.

As part of CySIP, in relation to data privacy matters, Capgemini has put in place a global data privacy governance structure led by the Group DPO who is in charge of overseeing the entire Group privacy compliance program, including advising on data privacy issues, monitoring the application of the BCRs and the Capgemini Data Privacy Policy by the Capgemini Companies, and organizing global awareness campaigns and monitoring their implementation. The local DPO oversees the local implementation of the BCRs, the Capgemini Data Privacy Policy and all related awareness initiatives. He/she acts as the Group DPO local delegate and serves as a single point of contact with the local DPA.

5. Data Subject Rights

Data Subjects can exercise their rights according to the procedure available through the Capgemini Intranet and Internet local website as further detailed in **Annex 2**. When Applicable Law provides for higher protection, the local DPO shall ensure that the highest level of protection as per Applicable Law shall apply to the Data Subject.

Any inquiries by Data Subjects on the BCRs should be directed to the local DPO (and if necessary the Group DPO) who will work towards answering the Data Subject's inquiries satisfactorily, subject however to the terms of the Service Agreement when Capgemini is acting as a Data Processor.

Data Subjects can send an inquiry preferably in writing via e-mail to **privacy@capgemini.com** (or local equivalent). Such contact information is available on the Capgemini Companies websites.

5.1 Data Subjects Rights Procedure

Within the Group, a specific procedure is in place at local level and available on the local intranet, to enable the exercise of the rights of access, opposition, correction and/or deletion of Data Subjects. Each right request is handled according to the local procedure in place. In coordination with the Group DPO, local DPOs shall always be at the disposal of the Data Controller and the Data Subject to provide assistance.

When acting as a Data Controller, the local DPO shall respond to the Data Subject within a reasonable time, but no longer than two (2) months and as per Applicable Law. If the right request is rejected or if the Data Subject is not satisfied with the reply, he/she shall have the right to lodge a complaint according to article 5.2 of the BCRs.

When acting as a Data Processor, the local DPO will act in compliance with the Service Agreement executed with the Data Controller. Service Agreements generally provide that the Data Controller reserves the right of responding to the right requests of Data Subjects and require Capgemini to refer any right request to the Data Controller, in lieu of responding directly to the Data Subjects. If the Service Agreement does not contain any provision related to the handling of Data Subjects rights, by default, the local DPO shall refer the right request to the Data Controller. If Capgemini has to respond directly, it shall respond to the Data Subject within a reasonable time and as per Applicable Law. If the right request is rejected or if the Data Subject is not satisfied with the reply, he/she shall have the right to lodge a complaint according to article 5.2 of the BCRs.

5.2 Complaint Procedure

The complaint procedure shall be applicable if the Data Subject considers that the Data Subjects Rights Procedure has been unsuccessful or if the Data Subject considers that his/her data privacy rights have been violated.

The complaints shall be dealt with by the local DPO. When a complaint is registered, it shall be handled within a reasonable time, but no longer than two (2) months and as per Applicable Law.

If a local DPO fails to solve a complaint of a Data Subject at local level, the complaint procedure can be appealed by the Data Subject to the Group DPO, who shall respond within a reasonable time, but no longer than two (2) months and as per Applicable Law.

When acting as a Data Processor, the DPO shall handle a Data Subject complaint only in the case where the Data Subject is not able to bring a complaint against the Data Controller because the Data Controller has factually disappeared or ceased to exist in law or has become insolvent and no successor entity has assumed the entire legal obligations of the former Data Controller by contract or by operation of law. Resolution of a complaint is always subject to technical constraints and to the provisions of the Service Agreement with the Data Controller. If the Service Agreement does not contain any provision related to the handling of complaints, by default, the local DPO shall refer the complaint without delay to the Data Controller.

6. Liability

6.1 Liability towards the Data Subjects

The BCRs give rights to Data Subjects to enforce the rules as third-party beneficiaries. In case the Data Subject has suffered a damage due to non-compliance by a Capgemini Company with the BCRs, such Data Subject is entitled to bring the case either to the DPA or to the courts of the EEA where the Data Controller is located or to the courts of the EEA where Capgemini's parent company is located (France).

However, if a Capgemini Company has disappeared and its liabilities have not been taken over by a successor, the relevant DPA and local courts shall be those of the EEA country where the Data Processor or its headquarters are located. If the latter solution is not applicable, the DPA and the local courts of the country of residence of the Data Subject shall be competent.

When the Data Subject can establish facts confirming that he/she has suffered direct damage exclusively as a result of a breach of the BCRs, the Capgemini Company that transferred the Covered Personal Data outside of the EEA to a Capgemini Company located outside of the EEA accepts that it would need to prove that the Capgemini Company located outside of the EEA is not responsible for the breach of the BCRs giving rise to such damages. When it can bring such evidence, its liability will be automatically discharged.

The Capgemini Company that transferred the Personal Data outside of the EEA shall take reasonable and necessary action to remedy the acts of the Capgemini Company located outside of the EEA taken in violation of the BCRs and to compensate the direct damages suffered by Data Subjects exclusively resulting from such violation.

When acting as a Data Processor, the Capgemini Company that transferred the Covered Personal Data outside of the EEA shall take reasonable and necessary action to remedy the acts of the Capgemini Company located outside of the EEA or of the External Sub-Processor located outside of the EEA taken in violation of the BCR-Processor and to compensate the direct damages suffered by Data Subjects exclusively resulting from such alleged violation.

In case the Data Controller has disappeared and its liabilities have not been taken over by a successor, the relevant DPA and local courts shall be those of the EEA country where the Capgemini Company is located or to the courts of the EEA where Capgemini's parent company is located (France). If the latter solution is not applicable, the DPA and the local courts of the country of residence of the Data Subject shall be competent.

The EEA Capgemini Company shall not be entitled to rely on such violation by the non-EEA Sub-Processor to avoid liability vis-à-vis the Data Subjects.

The Data Subject third-party beneficiary rights cover only the following obligations of the Data Processor in terms of BCR-Processor compliance: obligation to respect the BCR-Processor and to enable for the exercise of third-party beneficiary rights, liability for compensation and remediation of breaches, burden of proof on the Data Processor, easy access to the BCR-Processor for the Data Subject, existence of a complaint procedure, obligation to cooperate with the DPA and with the Data Controller, description of the data privacy principles, provision of a list of entities bound by the BCR-Processor, obligation of transparency when national legislation prevents the Group from complying with the BCR-Processor.

6.2 Liability towards the Data Controller

This paragraph is only applicable to the BCR-Processor. The BCR-Processor shall be included in the Service Agreement with the Data Controller.

The Capgemini Company that transferred the Personal Data outside of the EEA to another Capgemini Company located outside of the EEA or an External Data Processor located outside of the EEA, shall be liable to the Data Controller for direct damages resulting exclusively from the violation of the BCR-Processor as per the provisions of the Service Agreement and subject to the following paragraphs.

The Capgemini Company that transferred the personal Data outside of the EEA shall not be entitled to rely on a breach of its obligations by the Capgemini Company located outside of the EEA or an External Data Processor located outside of the EEA to avoid its liabilities vis-à-vis the Data Controller. All Data Controllers shall have the right to enforce the BCRs against any Capgemini Company for breaches they caused.

In such case, the Capgemini Company that transferred the Personal Data outside of the EEA to another Capgemini Company located outside of the EEA or an External Data Processor located outside of the EEA accepts that, when the Data Controller can establish facts confirming it has suffered direct damage exclusively as result of a breach of the BCR-Processor, Capgemini would need to prove that it is not, and that the External Data Processor is not responsible for the breach of the BCR-Processor giving rise to such damages. When Capgemini can bring such evidence, its liability will be automatically discharged.

In addition, the Capgemini Company that transferred the Personal Data outside of the EEA to another Capgemini Company located outside of the EEA or an External Data Processor located outside of the EEA agrees to take the necessary actions to enable that the actions giving rise to the breach of the BCR-Processor are remedied by the Capgemini Company located outside of the EEA or the External Data Processor located outside of the EEA.

7. Audit

Where required by Applicable Law or where requested by a DPA, Capgemini agrees that audits may be performed directly by the DPAs and commits to cooperate with the DPAs.

8. Capgemini Employees' Responsibilities – Awareness and Training

Every Capgemini Employee shall comply with the provisions of the BCRs.

Employees are informed that whenever they come to deal with Personal Data, they have a responsibility to comply with Applicable Law concerning data privacy, the BCRs and the Capgemini Data Privacy Policy and that they must process and treat all such Covered Personal Data accordingly.

Additional local initiatives may also ensure that Employees receive all the necessary information and updates.

Failure to comply with the BCRs and the Capgemini Data Privacy Policy can expose both Employees and/or Capgemini Companies to damages, criminal fines and other penalties. As a result, it is expected

that all Employees comply with the BCRs and the Capgemini Data Privacy Policy. Employees are informed that any non-compliance with these policies will be taken extremely seriously and may lead to appropriate disciplinary actions, subject to local laws.

9. Applicable Law – Conflict of Rules

The Capgemini Companies shall process Covered Personal Data in accordance with the BCRs and with Applicable Law. The BCRs will be interpreted in accordance with EU Law and the laws of the country where the Capgemini Company responsible for the transfer of Personal Data is established.

Any conflict between these BCRs and a binding legal requirement in another jurisdiction that prevents or hinders compliance with this BCRs must be brought to the attention of the Group DPO as soon as possible who will render a decision after consulting with the relevant DPA, if necessary.

For BCR-Processor, if a Capgemini Company has reasons to believe that the existing or future legislation applicable to it may prevents it from fulfilling the instructions received from the Data Controller or its obligations under the BCR or Service Agreement, it will promptly notify this to the Data Controller which is entitled to suspend the transfer of data and/or terminate the Service Agreement, to the Capgemini Company responsible for the transfer of Personal Data and to the DPA competent for the Data Controller.

Any legally binding request for disclosure of Personal Data by a law enforcement authority shall be communicated to the Data Controller. In any case, the request for disclosure will be put on hold and the DPA competent for the Data Controller and the lead DPA for the BCRs shall be clearly informed about it. However, if in specific cases suspension and/or notification are prohibited, the Capgemini Company will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so. If the Capgemini Company, despite having used its best efforts, is not in a position to notify the competent DPAs, Capgemini shall annually provide general information on the requests of disclosure of Personal Data by a law enforcement authority to the competent DPAs.

10. Cooperation with Data Protection Authorities

Capgemini will cooperate with the DPAs and undertakes to respond to the DPAs within a reasonable timeframe on any request related to the BCRs and their implementation. Under the BCR-Processor, Capgemini will cooperate with the DPAs of the Data Controller. The Capgemini Companies will cooperate with each other as necessary to respond to requests by the DPAs.

The Capgemini Companies will abide by the advice of the DPAs on issues related to the interpretation of the BCRs.

Annex 1: The Capgemini Data Privacy Policy

As one of the world's foremost providers of consulting, technology and outsourcing services to a wide array of clients around the world and providing services in more than 40 countries, Capgemini is committed to protecting privacy and the Personal Data entrusted to it, whether acting as a Data Controller or as a Data Processor (see Definitions at the end of document).

Most of the countries where Capgemini provides services have data protection or privacy laws designed to regulate and safeguard the collection, use, transfer, storage and disposal of Personal Data. As stated in its Code of Business Ethics, Capgemini is committed to complying with the data protection and privacy laws of the countries where Personal Data is collected and processed.

In order to give full effectiveness to its commitments, Capgemini is implementing a comprehensive privacy compliance program in addition to this Capgemini Data Privacy Policy, which is comprised of the following elements:

- A global Cybersecurity and Information Protection organization which includes:
  - Data Protection Officers
  - Privacy lawyers
  - Cybersecurity professionals
- Privacy awareness and training:
  - Privacy and security awareness training for Employees
  - Confidentiality reminders for Employees
  - Account-specific privacy and security training
  - Work group or industry-specific privacy and security training
  - Periodic privacy and security awareness interventions
- Monitoring of compliance with regulatory and contractual privacy requirements:
  - Internal audits
  - Client audits
  - Compliance to framework standards' best practices (such as ISO)
  - Data Protection Officers quality reviews
- A Global Security Incident Response Process and client-specific incident response plans
- Binding Corporate Rules for Data Controller and Data Processor roles.

This Capgemini Data Privacy Policy encapsulates the principles governing the processing of Personal Data across the entire Group. Compliance with this Policy is mandatory for all Capgemini Companies, Capgemini Business Units and Employees collecting and/or processing Personal Data.

This Capgemini Data Privacy Policy applies to all processing activities of Capgemini, whether acting as a Data Controller or as a Data Processor.

1. Capgemini processes Personal Data in a fair, lawful and transparent manner

Capgemini processes Personal Data in compliance with Applicable Law and the Data Controller's instructions (when applicable).

When acting as Data Controller, subject to Applicable Law, Capgemini shall provide all relevant information to the Data Subject in compliance with fair processing and transparency principles.

When acting as a Data Processor, Capgemini shall assist the Data Controller in doing the same.

This includes respecting the Data Subject's rights by updating, correcting or deleting the Personal Data accordingly so that it is accurate and where necessary kept up-to-date in accordance with Capgemini's applicable procedure.

2. Capgemini processes Personal Data for limited and defined purposes

Capgemini only processes Personal Data in compliance with the purpose for which it is originally collected and in compliance with the Data Controller's instructions (when applicable).

Subject to Applicable Law, Capgemini shall not process Personal Data for other purposes, except with the consent of the Data Subject or the Data Controller.

Personal Data is only disclosed for legitimate and relevant "need-to-know" purposes for business or legal reasons. In each instance, any disclosure of Personal Data is strictly limited to what is necessary and reasonable to comply with the purpose of the processing.

Capgemini is committed to use processes and tools that integrate privacy from their inception (privacy-by-design).

3. Capgemini processes Personal Data for a limited duration

In accordance with Applicable Law, Capgemini's internal rules and the Data Controller's instructions (when applicable), Capgemini only processes Personal Data for as long as it is necessary for the purpose(s) for which it is processed.

At the end of the processing, Capgemini shall archive, anonymize or destroy the Personal Data, and otherwise follow the Data Controller's instructions (when applicable).

4. Capgemini processes Personal Data securely

As a general rule and unless otherwise required by the client, Capgemini applies the same standard level of security to Personal Data it processes as a Data Controller and Personal Data it processes as a Data Processor.

Capgemini applies and maintains appropriate technical, physical, and organizational measures to protect Personal Data against unauthorized access and to avoid its accidental loss, damage, destruction or other unlawful form of processing.

These measures follow industry practices and standards and are aimed at establishing a level of security appropriate to the risks represented by the processing and the nature of the Personal Data to be protected.

Capgemini shall report any serious Security Breach to the authorities and/or the Data Subject and/or the Data Controller as per Applicable Law or contractual provisions if it becomes aware that the security, confidentiality or integrity of the Personal Data has been compromised.

5. Capgemini works with Data Processors in a responsible manner

Subject to Applicable Law, when using Internal or External Data Processor, Capgemini shall enter into appropriate agreements that require that Personal Data is stored and processed in accordance with Applicable Law, including applying appropriate security measures.

When Capgemini acts as a Data Processor, the same shall apply in addition to the Data Controller's instructions.

Definitions of the Data Privacy Policy

"**Applicable Law**" means any data privacy or data protection law, applicable at the time of the processing.

"**Capgemini Business Unit**" means a Capgemini business organization. A Capgemini Business Unit can be part of a Capgemini Company or span several Capgemini Companies located in different countries, inside and/or outside of the EEA.

"**Capgemini**" or "**Group**" means the entire Group of Capgemini Companies controlled, directly or indirectly, by Cap Gemini SA.

"**Capgemini Company(ies)**" means any company within Capgemini which is controlled directly or indirectly by Cap Gemini SA.

"**Data Controller**" means the company that determines the purposes and means of processing the Personal Data.

"**Data Processor**" means the company which processes Personal Data on behalf of the Data Controller (whether a Capgemini Processor, i.e. an "**Internal Data Processor**", or a non Capgemini Processor, i.e. an "**External Data Processor**") that may be located within the EEA or outside the EEA.

"**Data Subject**" means the individual to whom the Personal Data relates.

"**Employee**" means a Capgemini Company's Employee as well as agency workers.

"**Personal Data**" means any information relating to an identified or identifiable natural person ("**Data Subject**"). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Personal Data shall also be understood as Personally Identifiable Information.

"**Processing**" includes the collection, recording, organization, storage, adaptation, retrieval, consultation, use, and disclosure by transmission, dissemination or otherwise and making available, alignment or combination, blocking, erasure or destruction of Personal Data.

"**Security Breach(es)**" means any compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

For any question, contact Nathalie Laneret, Group Data Protection Officer at: nathalie.laneret@capgemini.com

Annex 2: DATA SUBJECT RIGHT REQUEST AND COMPLAINT PROCEDURE

As one of the world's foremost providers of consulting, technology and outsourcing services to a wide array of clients around the world and providing services in more than 40 countries, Capgemini ("**We**") is committed to protecting privacy and the Personal Data entrusted to it, whether acting as a Data Controller or as a Data Processor (see Definitions at the end of document). The purpose of this Data Subject Right Request and Complaint Procedure ("**Procedure**") is to describe the process by which a Data Subject ("**You**"), can submit a Data Subject Right Request concerning your Personal Data that is processed by Capgemini, or submit a Data Subject Complaint regarding the processing of your Personal Data. In any case you can also contact directly your local Data Protection Authority or a competent court.

1. What are your rights as a Data Subject?

Under Applicable Law and subject to certain exemptions You have the right to access your Personal Data, the right to have it rectified, the right to oppose processing or the right to have it destroyed and no longer processed. If You wish to exercise these rights You may submit an Inquiry according to the two processes described below:

1.1. **The Data Subject Right Request Procedure:** if You have any concern or question regarding your Personal Data.

1.2. **The Data Subject Complaint Procedure:** if you are dissatisfied with Capgemini's response to your Data Subject Right Request or any other matter concerning your Personal Data.

We are committed to handle all Inquiries with the same highest level of quality, and to engage positively to resolve any Inquiry satisfactorily.

2. Who is entitled to submit an Inquiry?

2.1. **Direct Inquiry:** You can submit an Inquiry to Capgemini if You are the individual to whom the Personal Data relates (i.e. the Data Subject), for instance an actual or former Employee, a customer or a shareholder of Capgemini.

2.2. **Indirect Inquiry:** You can also submit an Inquiry via a third party such as a lawyer. In this case, You must provide appropriate evidence that the third party making the Inquiry is entitled to act on your behalf, as per Applicable Law.

Warning - Attempting to obtain Personal Data to which You are not entitled may be unlawful under Applicable Law.

3. What is the scope of Covered Personal Data?

Personal Data covered by this Procedure include all Personal Data processed by a Capgemini Company acting as a Data Controller (whether such Personal Data is processed internally by a Capgemini entity acting as a Data Processor or by an external Data Processor).

When acting as a Data Processor, We only Process Personal Data according to the instructions contractually specified by the Data Controller. In these instances, only the Data Controller is able to respond to your Data Subject Right Request or Data Subject Complaint.

4. What are the prior verifications?

4.1. **Verification of your identity:** To safeguard your Personal Data from unauthorized access, prior to processing your Inquiry, You will be required to provide Capgemini with an official form of identification (e.g., passport, driver's license, etc), to verify your identity as per Applicable Law. Without proper identification your Inquiry cannot be processed.

4.2. **Verification of the completeness of your Inquiry:** Inquiries that are incomplete or inaccurate and/or for which identification has not been possible, will be put on hold until You are able to provide Capgemini with the required information.

Warning - In order to facilitate the search of your Personal Data, please specify and detail as much as possible your Inquiry. In certain instances, Capgemini may charge fees to cover administrative costs.

5. Will You be charged a fee for your Inquiry?

In certain instances and subject to Applicable Law, We may determine that due to the complexity of your Inquiry and the effort required to address it properly, a fee may be required. The amount of the fee shall be reasonable, subject to the complexity of the Inquiry. If a fee is required, You will be notified of the amount and payment options.

6. When will You receive a response to your Inquiry?

First, We will acknowledge receipt of your Inquiry and inform You that it is being processed. The processing of your Inquiry and the delivery of the results will be provided within two (2) months (or a shorter delay as per Applicable Law) from the date your Inquiry is complete.

7. How can You submit your Inquiry?

7.1. **Concerning a Data Subject Right Request:** You may submit your Data Subject Right Request preferably online on the Capgemini website, by email [email address of local DPO] or by post [mail address of local DPO].

7.2. **Concerning a Data Subject Complaint:** You may submit your Data Subject Complaint preferably in writing to your local DPO by email [email address of local DPO] or by post [mail address of local DPO].

8. Who handles your Inquiry?

Your Inquiry will be handled by the appropriate local DPO. If You have not provided sufficient information in your Inquiry to enable us to locate your Personal Data, the local DPO will inform You of what further information is required to process your Inquiry.

Warning - In order for your Inquiry to be dealt with in due time, we recommend You submit an Inquiry only to the local DPO of the Capgemini Company of the country where You live.

9. What if You are not satisfied with Capgemini's response?

If You are not satisfied with Capgemini's response to your Data Subject Complaint, You may submit in writing and by email an Appeal to the Group DPO. A response to your Appeal will be provided to You by the Capgemini DPO and within two (2) months (or a shorter delay as per Applicable Law) from the date your Appeal has been submitted.

If You are not satisfied with the response to your Appeal, You may contact your national Data Protection Authority or the competent court.

Definitions of the Data Subject Right Request and Complaint Procedures

"**Appeal**" means the escalation process of a response to a Data Subject Complaint.

"**Applicable Law**" means any data privacy or data protection law, applicable at the time of the Processing.

"**BCRs**" means Capgemini's Binding Corporate Rules for Controller and Processor.

"**Capgemini**" or "**Group**" means the entire Group of Capgemini Companies controlled, directly or indirectly, by Cap Gemini SA.

"**Capgemini Company(ies)**" means any company within Capgemini which is controlled directly or indirectly by Cap Gemini SA.

"**Covered Personal Data"** means Personal Data that are included in the scope of the BCRs.

"**Data Controller**" means the company that determines the purposes and means of Processing the Personal Data.

"**Data Processor**" means the company which Processes Personal Data on behalf of the Data Controller that may be located within the EEA or outside the EEA.

"**Data Subject(s)**" means the individual(s) to whom the Personal Data relates. It can be an Employee of Capgemini, a former Employee, a trainee, an applicant, a provider, a customer, the user of a service handled by Capgemini for a client, a prospect or every individual subject of any Personal Data processed by Capgemini.

"**Data Subject Complaint(s)**" means the right for a Data Subject to submit a complaint if he/she considers that the rights afforded by Applicable Law and the BCRs to him/her have not been respected.

"**Data Subject Complaint Procedure**" means the procedure enabling a Data Subject to submit a Data Subject Complaint if he/she considers that the rights afforded by Applicable Law and the BCRs to him/her have not been respected.

"**Data Subject Right Request(s)**" refers to the right for a Data Subject to submit a right request for access ("**Access Request**"), rectification ("**Rectification Request**"), blocking ("**Blocking Request**") or deletion ("**Deletion Request**"), as per the BCRs and Applicable Law.

"**Data Subject Right Request Procedure**" means the procedure enabling a Data Subject to submit a Data Subject Right Request in order to exercise the individual rights afforded to him/her by Applicable Law and the BCRs.

"**DPO**" means Data Protection Officer.

"**EEA**" means the European Economic Area formed by the European Union member states as well as Norway, Iceland and Lichtenstein.

"**Employee(s)**" means a Capgemini Company's employee as well as agency workers.

"**EU Law**" means Directive 95/46/EC of the European Parliament and of the Council of October 24th 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive 2002/58/EC of the European Parliament and of the Council of July 12th 2002 concerning the processing of Personal Data and the protection of privacy in the electronic communications sector and any subsequent European Union legislation amending it.

"**Inquiry(ies)**" means Data Subject Right Request(s) and/or Data Subject Complaint(s).

"**Personal Data**" means any information relating to an identified or identifiable natural person ("**Data Subject**"). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Personal Data shall also be understood as Personally Identifiable Information.

"**Processing**" includes the collection, recording, organization, storage, adaptation, retrieval, consultation, use, and disclosure by transmission, dissemination or otherwise and making available, alignment or combination, blocking, erasure or destruction of Personal Data.