AXA GROUP
BINDING CORPORATE RULES

Background

AXA Group is committed to maintaining the privacy of data obtained during its business activities and complying with applicable laws and regulations regarding the processing of Personal Data and Special categories of Data. We require our suppliers to maintain similar standards to ours for the protection of personal data through contractual agreements.

AXA Group has a global Data Privacy Organization/Governance with (i) a Data Privacy governance model approved by Management Committee, (ii) a Group Data Privacy Officer, (iii) a Group Data Privacy Steering Committee, (iv) a worldwide network of Data Privacy Officers coordinated by the Group Data Privacy Officer and (v) a Group Data Privacy Standard, that is embedded in groupwide risk/compliance management.

AXA Group decided to adopt a set of Binding Corporate Rules ("BCR") in order to set up adequate safeguards to ensure that Personal Data is protected while transferred within the AXA Group from an AXA Company based in a Regulated Jurisdiction (as defined in Article I below) to an AXA Company located in another jurisdiction where that transfer is not otherwise permitted by applicable law, and any subsequent onward transfer of that data that is not otherwise permitted by applicable law.

ARTICLE I - DEFINITIONS

As used in the BCR, in its appendices and the Intra Group Agreement, the following terms and expressions, when written with a capital letter, shall have the following meanings set out below:

"**Applicable Law**" refers to all local, national or regional (such as EEA) laws of Regulated Jurisdictions BCR AXA Companies.

"**AXA BCR Steering Committee**" is a committee specifically dedicated to BCR consisting of AXA Group senior management representatives and Data Privacy Officers of selected BCR AXA Companies.

"AXA Companies " means AXA, Société Anonyme with a Board of Directors having its principal offices at 25, avenue Matignon, 75008 Paris, registered on the Commercial Registry of Paris under the number 572 093 920; and (i) any other company controlled by, or controlling AXA, with a company being considered as controlling another: (a) when it holds directly or indirectly a portion of the capital according to it the majority of the voting rights in general meetings of shareholders of this company; (b) when it holds solely the majority of the voting rights in this company by virtue of an agreement concluded with other partners or shareholders and which is not contrary to the interest of the company; (c) when it determines de facto, by voting rights which it holds, the decisions in the general meetings of shareholders of this company; (d) in any event, when it holds, directly or indirectly, a portion of voting rights greater than 40% and when no other partner or shareholder holds directly or indirectly a portion which is greater than its own; (e) when it has the power to direct or cause the direction and management (whether through the ownership of voting shares, by contract or otherwise); (ii) any economic interest group in which AXA and/or one or more other Companies of the AXA Group participates for at least 50% in operating costs; (iii) in the cases where the law applicable to a company limits voting rights or control (such as defined here in above), this company will be deemed to be a

company of the AXA Group, if the voting rights in general shareholders' meetings or the control held by a Company of the AXA Group reaches the maximum amount fixed by said applicable law; and (iv) all AXA Companies constitute the "AXA Group".

"**AXA Employees**" are all the employees of the AXA Companies including directors, trainees, apprentices and assimilated status.

"AXA Group" means, together, AXA SA and all AXA Companies.

"BCR AXA Companies" are (i) all AXA Companies which have signed the Intra-Group Agreement in their capacity either as Data Exporters or as Data Importers; and (ii) enterprises engaged in a joint economic activity with AXA Companies which have signed the Intra-Group Agreement in their capacity either as Data Exporters or as Data Importers.

"BCR Companies Employees" are all the employees of companies engaged in a joint economic activity with AXA Companies which have signed the Intra-Group Agreement in their capacity either as Data Exporters or as Data Importers.

"BCR AXA Hubs" means the main transversal or/and local AXA Companies or other AXA organizations which participate in the implementation of the BCR in collaboration with the GDPO to protect Personal Data within AXA Group and for the transfer of Personal Data from member states of the European Economic Area ("EEA") within EEA and outside EEA.

"Binding Corporate Rules" or **"BCR"** means the present Binding Corporate Rules entered by and between AXA SA and all other BCR AXA Companies.

"Controller" means a BCR AXA Company which, alone or jointly with others, determines the purpose(s), conditions and means of the Processing of Personal Data.

"Coordinating Data Protection Authority" means the French Data Protection Authority (CNIL).

"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.

"Data Exporter" means any Controller located in a Regulated Jurisdiction or Processor located in a Regulated Jurisdiction processing Personal Data on behalf of a Controller which transfers Personal Data outside the Regulated Jurisdiction in which it is located (whether via a Processor or third-party processor or not) and has signed the Intra Group Agreement.

"Data Importer" means any Controller or Processor processing Personal Data on behalf of a Controller who receives Personal Data from the Data Exporter under a Relevant Transfer or Onward Transfer and who has signed the Intra Group Agreement.

"Data Privacy Officer" or **"DPO"** means the person in AXA Companies responsible for coordinating with the GDPO and for ensuring the AXA Companies' compliance with the Binding Corporate Rules and applicable local legal / regulatory requirements.

"Data Subject" means any natural person, who can be identified, directly or indirectly, by means reasonably likely to be used by any natural or legal person, by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

"**European Data Protection Board**" means the body of the Union composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor.

"EEA" or **"European Economic Area"** means the European Economic Area that combines the countries of the European Union and member countries of EFTA (European Free Trade Association). As of February 16th, 2023, EEA includes Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden.

"EEA Data Exporter" means any Controller located in EEA or Processor located in EEA processing Personal Data on behalf of a Controller which transfers Personal Data outside the EEA (whether via a Processor or third-party Processor or not) and has signed the Intra Group Agreement.

"EEA Data Subject" means any Data Subject who was a resident of an EEA member state at the time when his/her Personal Data was collected or whose Personal Data was processed in EEA by a BCR AXA Company within the context of AXA business activities.

"EU Model Clauses" are the standard contractual clauses issued by European Commission which offer sufficient safeguards as required by European Regulation for the transfer of personal data to third countries which do not ensure an adequate level of data protection according to European Commission.

"European Regulation" means the current and future applicable rules and regulations related to data privacy applicable in the EEA countries.

"Group Data Privacy Officer" or **"GDPO"** means the person in charge of the overall supervision of these Binding Corporate Rules through a network of Data Privacy Officers.

"Intra Group Agreement" or **"IGA"** means the BCR agreement as attached in Appendix 1 and any BCR Acceptation agreement (referred to in Schedule 2 of Appendix 1) of the AXA Group Binding Corporate Rules to be signed or signed by BCR AXA Companies.

"Onward Transfer" means the onward transfer of Personal Data previously exported pursuant to a Relevant Transfer:

(i) to another BCR AXA Company that is in a territory which (but for the operation of the BCR) does not offer an adequate level of protection as required by the data privacy law of the relevant Regulated Jurisdiction at the origin of the original Relevant Transfer; and

(ii) which is not subject to any of the permitted derogations or conditions contained in the privacy law in the relevant Regulated Jurisdiction (which may include the consent of the Data Subject, existing contractual protections and/or establishment in a jurisdiction approved by the European Commission under European Regulation).

"Personal Data" means any data relating to an individual (natural person) who is or can be identified either from the data or from the data in conjunction with other information.

"Processing" means any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, separating, crossing, merging, modification, provisioning, usage, disclosure, dissemination, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Processor" means a BCR AXA Company which processes Personal Data on behalf of a Controller.

"**Regulated Jurisdiction**" means any jurisdiction in the EEA and Andorra, Switzerland, Faeroe Islands, Guernsey, Isle of Man, Jersey, Singapore, Turkey, Morocco, the United Kingdom, Brazil, Thailand, China, Abu Dhabi and Hong Kong.

"Regulated Jurisdiction Data Subject" means any Data Subject who was a resident of a Regulated Jurisdiction at the time when his/her Personal Data was collected.

"**Relevant Transfer**" means a transfer of Personal Data (to the extent such Personal Data has not previously been the subject of a Relevant Transfer or Onward Transfer):

(i) from a BCR AXA Company that is a Data Exporter to another BCR AXA Company that is in a territory which (but for the operation of the BCR) does not offer an adequate level of protection as required by the data privacy law of the Regulated Jurisdiction of the Data Exporter; and

(ii) which is not subject to any of the permitted derogations or conditions contained in the privacy law in the relevant Regulated Jurisdiction (which may include the consent of the Data Subject, existing contractual protections and/or establishment in a jurisdiction approved by the European Commission under European Regulation).

"Special categories of Data" means such data as described in Article IV section 2.

"Supervisory Authority" or **"Data Protection Authority"** or **"DPA"** means the administrative authority officially in charge of Personal Data protection in each Regulated Jurisdiction in which AXA Group is present and acts as Data Exporter (for example in France, this authority is the *Commission Nationale de l'Informatique et des Libertés*; in Spain, it is the *Agencia Espanola de Proteccion de Datos*, etc.). For the avoidance of doubt, the term "Supervisory Authority" includes any replacement or successor of a Data Protection Authority.

"Third Party" shall mean any natural or legal person (including AXA Companies/BCR AXA Companies), public authority, agency or any other body other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorized to process the Personal Data of a Data Subject.

ARTICLE II - PURPOSE

The purpose of the BCR is to ensure an adequate level of protection to the Personal Data subject to a Relevant Transfer or Onward Transfer from an AXA Company or a company engaged in a joint economic activity with AXA Companies based in a Regulated Jurisdiction to an AXA Company or a company engaged in a joint economic activity with AXA Companies based in another jurisdiction.

ARTICLE III - SCOPE

1. Geographical scope

AXA Group is present in more than 50 countries and more than 150 000 AXA Employees and distributors of AXA are committed to serving millions of clients.

The present BCR exclusively apply to Relevant Transfers from Data Exporters located in a Regulated Jurisdiction to Data Importers located in another jurisdiction and Relevant Transfers from Data Importers located in another jurisdiction back to a Data Exporter in a Regulated Jurisdiction following this initial Relevant Transfer, as well as to Onward Transfers, and the recourse against breaches under the Third Party Beneficiary Rights, Complaint and Liability provisions of these BCR (as set out in Articles VII, VIII and IX of these BCR) are limited to Regulated Jurisdiction Data Subjects.

Although BCR AXA Companies may have processes required for BCR implemented everywhere, BCR AXA Companies do not provide BCR guarantees for Personal Data that is not subject to a data privacy law in a Regulated Jurisdiction, i.e. which is not transferred from a Regulated Jurisdiction e.g.:

- If a US-based AXA Company transfers its Personal Data to an India-based AXA Company such transfer and associated processing shall not be subject to the BCR; or

- If a Japan-based AXA Company transfers its Personal Data to a Philippines-based AXA Company, such transfer and associated processing shall not be subject to the BCR.

2. Material scope

a. BCR AXA Companies scope and enforceability towards employees

The present BCR binds all AXA Companies and enterprises engaged in a joint economic activity with AXA Companies which have signed an Intra-Group Agreement setting out and expressing their acceptance of the BCR as listed in Schedule 1 to Appendix 1 or accessing to the Intra-Group Agreement. Each AXA Company or enterprise engaged in a joint economic activity with AXA Companies signing an IGA becomes a BCR AXA Company as of the date of signature or (if later) any effective date set out in the applicable IGA.

In accordance with applicable labour law, the present BCR are made binding and enforceable upon the AXA Employees and BCR Companies Employees of all the BCR AXA Companies through any of the following at each BCR AXA Company:

- through respect of binding AXA internal policies, or
- through respect of a binding collective agreement, or
- through respect of a clause in the employment contract, or
- through any other means suitable to make the BCR binding on AXA Employees or BCR Companies Employees in the respective country.

In accordance with applicable labour law, its own internal rules and employment contracts, each of the BCR AXA Companies may take disciplinary actions towards any of its own AXA Employees or BCR Companies Employees, in particular in the event of:

- breach of these BCR by an AXA Employee or BCR Companies Employees,
- failure to apply the recommendations and advice issued by its Data Privacy Officers (the "DPO") following a compliance review,
- failure to cooperate in verification of BCR compliance carried out by its DPO, or with the relevant authorities responsible for the protection of Personal Data.

b. Personal Data and Processing operations scope

The purpose(s) of the Personal Data transfers and the Processing carried out after the transfers are servicing and facilitating AXA's business activities.

AXA’s areas of expertise are reflected in a range of products and services adapted to the needs of each client in three major business lines: property-casualty insurance, life & savings, and asset management:

- the property-casualty business includes the insurance of property and liability. It covers a broad range of products and services designed for our individual and business clients including assistance services and international insurance for large corporate clients, such as Marine and Aviation.
- our individual and group life insurance business includes both savings and retirement products, on the one hand, and other health and personal protection products, on the other. Savings and retirement products meet the need to set aside capital to finance the future, a special project or retirement. Personal protection covers risks related to an individual's physical integrity, health or life. AXA also offers its individual clients in some countries a simple range of banking services and products that supplement the insurance offering.
- the asset management business involves investing and managing assets for the Group's insurance companies and their clients, as well as for third parties, both retail and institutional clients.

Servicing AXA's business activities includes:

- Visioning (define the enterprise long-term vision, develop the business strategy, manage a strategic initiative, control progress)
- Designing (develop product strategy, establish risk policy, design, develop & launch product, maintain existing product portfolio)
- Distributing (develop distribution strategy, manage and control the distribution networks, execute marketing operations, manage customer relationship, customize an offer, sell, reward sales performances)
- Producing (underwrite, administrate a policy, collect premium, monitor the policy portfolio)
- Servicing (cope with a catastrophe, handle a claim, provide customer services, manage auxiliaries, detect fraud, manage subrogation and recover claim funds from re insurance, manage wreck salvage, control the claims management)
- Manage finance (plan and control finance, manage investment, manage corporate finance, pass operations, manage capital asset, analyse finance, manage cash, manage treasury operations and cash, manage tax, comply with regulation, handle reinsurance)
- Manage information technology (manage it customer relationship, deliver and maintain solutions, deliver & support it services, manage it infrastructure, manage it organization, manage it security)
- Develop & manage human resources (administrate human resource, manage human resource, perform hr communication, manage social partners and work councils)
- Manage purchasing (manage suppliers and contracts, purchase, receive goods and services, manage supplier invoices, approve and validate payments, perform procurement reporting and performance analysis)
- Manage risk (manage financial risk, manage investment risk, manage operational risk, perform projection, calculate risk adjusted profitability)
- Other support functions (perform external communication, legal support, manage improvement and change, internal auditing, central functions)

All types and categories of Personal Data processed by the BCR AXA Companies in the course of their business activities shall fall within the scope of these BCR. Such types and categories shall include Personal Data collected from customers, prospective customers, claimants, AXA Employees or BCR Companies Employees, job applicants, agents, suppliers and other third parties.

The categories of Personal Data processed by the BCR AXA companies required or capable of locally collecting them in accordance with the applicable legislation include:

- Marital status/identity/identification data,
- Professional life,
- Personal life,
- Connection data,
- Location data,
- Social Security Number,
- Economic and financial information
- Offences, convictions, security measures,
- Philosophical, political, religious, trade union, sexual life, health data, racial origin,
- Biometric data,
- Genetic data,
- Death of persons,
- Appreciation of the social difficulties of people,
- Health Insurance data

The BCR cover both automated and manual types of Processing.

The third countries where Relevant Transfers or Onward Transfers take place are listed in the list of BCR AXA Companies available on axa.com.

Below the table that can help understanding the sets of transfers

The type of processing and their purposes	**The categories of data subjects *(e.g., data related to employees, customers, suppliers and other third parties as part of the Group's respective regular business activities***	**The categories of Personal data**	**The third country or countries**
Develop & manage human resources (administrate human resource, manage human resource, perform HR communication, manage social partners and work councils)	AXA Employees or BCR Companies Employees, Job applicants.	'- Marital status /identity/identification data, - Professional life, - Personal life, - Connection data, - Location data, - Social Security Number, - Economic and financial information, - Offences, convictions, security measures, - Philosophical, Political, religious, trade union, sexual life, health data, racial origin, - Biometric data, - Genetic data, - Death of Persons, - Appreciation of the social difficulties of people	The third countries where Relevant Transfers or Onward Transfers take place are listed in the list of BCR AXA companies available on AXA.com

Servicing and facilitating AXA's Business activities.	customers, prospective, customers, claimants, suppliers and other third parties	- Marital status /identity/identification data, - Professional life, - Personal life, - Connection data, - Location data, - Social Security Number, - Economic and financial information, - Offences, convictions, security measures, - Philosophical, Political, religious, trade union, sexual life, health data, racial origin, - Biometric data, - Genetic data, - Death of Persons, - appreciation of the social difficulties of people	The third countries where Relevant Transfers or Onward Transfers take place are listed in the list of BCR AXA companies available on AXA.com.
Assisting and supporting AXA's operations (use of IT applications).	AXA Employees or BCR Companies Employees, agents, suppliers and other third parties.	'- Marital status/identity/identification data, - Connection data, - Location data,	The third countries where Relevant Transfers or Onward Transfers take place are listed in the list of BCR AXA companies available on axa.com.

ARTICLE IV - PROCESSING PRINCIPLES

For any Processing of Personal Data within the scope defined in ARTICLE III - SCOPE, the Processing principles set out hereinafter shall be respected.

1. Main principles

Each of the BCR AXA Companies warrants and covenants that it complies with the obligations required by applicable law and the competent local Data Protection Authority for the original Processing of Personal Data, which is subsequently transferred under a Relevant Transfer or Onward Transfer under the BCR.

Each of the BCR AXA Companies undertakes that the Processing of Personal Data carried out under their control, including data transfers, will continue to be carried out in accordance with the provisions of these BCR and with the following minimum general data protection principles:

- Personal Data must be obtained lawfully, fairly and in a transparent manner, and with the Data Subject's right of information, except if such information is not necessary because of legal exceptions; and must be processed only if the Data Subject has given his or her consent or if the Processing is otherwise allowed by applicable laws.

- Personal Data must be collected only for specified, explicit and legitimate purpose(s) and not further processed in a way incompatible with those purpose(s). Personal Data will only be made available to third parties for those purpose(s) or as otherwise allowed by applicable laws.

- Appropriate controls and technical and organizational procedures must be implemented to ensure security of Personal Data and prevent unauthorized access or disclosure, potential harm which might result from alteration, accidental or unlawful destruction or accidental loss of the data, and against all other unlawful forms of Processing. Having regard to the legal obligations, the good practices and the cost of their implementation, security measures shall be designed to ensure a level of security

appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected.

- Appropriate technical and organizational measures must be taken, both at the time of determination of the means of processing and at the time of the processing itself, to implement data protection principles in an effective manner and to integrate the necessary safeguards by design into the processing in order to meet the requirements of European Regulation and protect the rights of data subjects.

- Appropriate technical and organizational measures must be implemented to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

- Personal Data collected must be accurate, complete for the purpose(s) concerned and, where required, kept up to date.

- Personal Data collected must be minimized, *i.e.* adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are collected and/or further processed.

- Personal Data must not be retained for any longer than necessary for the purpose(s) for which it was obtained unless otherwise required by applicable laws. More information on the relevant data retention periods is available in the data retention policy applicable in each BCR AXA Company.

- Procedures must be implemented to ensure prompt responses to enquiries from Data Subjects to ensure that they can duly exercise their rights of access, rectification, erasure of their Personal Data and rights of restriction and objection to Processing (except where the applicable law provides otherwise) and to withdraw consent when the Processing relies on this legal basis.

Personal Data should only be processed if such Processing is based on a legal basis, including, for example, if:

- the Data Subject has given his or her consent; or
- the Processing is necessary for the performance of a contract to which the Data Subject is party or to take steps at the request of the Data Subject prior to entering into a contract; or
- the Processing is necessary for compliance with a legal obligation to which the Controller is subject; or
- the Processing is necessary in order to protect the vital interests of the Data Subject; or
- 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 or in a third party to whom the Personal Data is disclosed; or
- the Processing is necessary for the purpose(s) of the legitimate interests pursued by the Controller or by the Third Party or Parties to whom the Personal Data is disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject.

If the Personal Data Processing is based solely on automated processing of data, including profiling, and produces legal effects concerning him or her or significantly affects him or her, the Data Subjects have the right not to be subject to such a decision, unless such Processing:

- is necessary during the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the Data Subject, has been satisfied or that there are suitable measures to safeguard his or her legitimate interests, such as arrangements allowing him or her to express his or her point of view and to contest the decision; or
- is authorized by a law which also lays down measures to safeguard the Data Subject's legitimate interests; or
- is based on the Data Subject's explicit consent,

provided there are suitable measures to safeguard his or her legitimate interests, such as arrangements allowing him or her to obtain human intervention, to express his or her point of view and to contest the decision.

Each Controller and Processor will maintain a record of all categories of processing activities carried out on Personal Data of EEA Data Subjects and will make the record available, in writing, including in electronic form, to the Coordinating Data Protection Authority and any other relevant Data Protection Authorities upon request. The content of the record shall be in line with what is required by Article 30(1) (for controllers) and Article 30(2) (for processors) of General Data Protection Regulation.

Each Controller will conduct Data Protection Impact Assessments when required for processing operations likely to result in a high risk to the rights and freedoms of EEA Data Subjects. Where a Data Protection Impact Assessment indicates that the processing would result in a high risk in the absence of measures taken by the BCR AXA Company to mitigate the risk, the Coordinating Data Protection Authority or any other relevant Data Protection Authority should be consulted.

For processing activities carried out on Personal Data of EEA Data Subjects, Controller and Processor will enter into contracts with all internal and external processors and must specify the content of such contracts, as set out in Article 28(3) General Data Protection Regulation, including the duty to follow the controller's instructions and implement appropriate technical and organizational measures.

2. Special categories of personal Data

For the purposes of these BCR, Special categories of Data shall include any Personal Data relating to:

- The racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the Data Subject.
- Whether the Data Subject is a member of a trade union.
- The physical or mental health or condition or sex life or sexual orientation of the Data Subject, genetic data, biometric data for the purpose of uniquely identifying a natural person.
- Specific data deemed within Special categories of Data under applicable law and regulation (e.g. medical data).

The list above shall in no event be regarded as setting out exhaustively Special categories of Data as local legislation may include additional categories which shall, in such cases and where applicable, be regarded as Special categories of Data by the Data Exporter and the Data Importer.

Processing of Special categories of Data is prohibited unless:

1. the Data Subject has given its explicit consent to the Processing of those Special categories of Data, and such consent is considered as valid pursuant to the applicable law and regulation; or
2. the Processing is necessary for the purpose(s) of carrying out the obligations and specific rights of the Controller or of the Data Subject in the field of employment law and social security and social protection law in so far as it is authorized by applicable law providing for adequate safeguards; or
3. the 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 consent; or
4. The Processing is carried out in the course of legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the Processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purpose(s) and that the Personal Data is not disclosed to a third party without the consent of the Data Subjects; or
5. The Processing relates to Special categories of Data which has been made public by the Data Subject; or
6. The Processing of Special categories of Data is necessary for the establishment, exercise or defence of legal claims; or
7. The Processing is necessary for reasons of substantial public interest, based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interest of the data subject; or
8. The Processing of the Special categories of Data is required for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards and where those data are processed:
   - by a professional subject to an obligation of secrecy or
   - by another person also subject to an obligation of secrecy; or
9. The Processing is necessary for reasons of public interest in the area of public health on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy.
10. The Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with European Regulation based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interest of the Data Subject.
11. . The Processing of personal data of Data Subjects other than EEA Data Subjects is otherwise permitted under the applicable law of the country of establishment of the Data Exporter.

3. Data related to criminal convictions and offences:

For the purposes of these BCR, Data related to criminal convictions and offences shall include any Personal Data relating to:
- The actual or alleged commission of any criminal conviction and offence by the Data Subject; or
- Any proceedings for an actual or alleged offences to have been committed by the Data Subject, the disposal of such proceedings or the sentence of any courts in such proceedings.

The list above shall in no event be regarded as setting out exhaustively Data related to criminal convictions and offences as local legislation may include additional categories which shall, in such cases and where applicable, be regarded as Data related to criminal convictions and offences by the Data Exporter and the Data Importer.

Processing of Data related to criminal convictions and offences is prohibited unless:

- Processing of personal data of EEA Data Subjects, relating to criminal convictions and offences, is carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.
- Processing of personal data of Data Subjects other than EEA Data Subjects is permitted under the applicable law of the country of establishment of the Data Exporter.

4. Subcontracting with processors

Where Processing is carried out by a subcontractor on a Data Importer's behalf, the latter shall obtain the prior written authorization of the Data Exporter, choose a subcontractor providing sufficient guarantees to implement appropriate technical security measures and organizational easures to ensure the Processing will be carried out in accordance with the BCR, and the Data Importer must ensure that the subcontractor will comply with those measures. The Data Importer who chooses the subcontractor shall ensure that the subcontractor will agree to such technical security measures and organizational measures in writing by executing a contract in line with European Regulation stipulating in particular that the subcontractor shall act only on instructions from the Data Importer.

5. Data transfers

1. Data transfers within the AXA Group and companies engaged in a joint economic activity with AXA Companies

No Personal Data may be transferred to a Data Importer based in a country outside the EEA (or in the case of exports from another Regulated Jurisdiction, that Regulated Jurisdiction), until the Data Exporter has determined that the Data Importer is bound by and comply with:

- these BCR, or,
- other measures which allow the transfer of Personal Data of EEA Data Subjects according to Article 44 to 46 of General Data Protection Regulation, or,
- other measures which allow the transfer of Personal Data of Data Subjects other than EEA Data Subjects according to applicable law (e.g., EU Model Clauses).

As reflected in the concepts of "Relevant Transfer" and "Onward Transfer" the BCR apply only to transfers that are not already covered by other measures which allow the transfers unless otherwise agreed in writing between the Data Exporter and the Data Importer.

2. Data transfers outside the AXA Group and companies engaged in a joint economic activity with AXA Companies

For all transfers to a third-party company outside of the EEA (in the case of exports from the EEA, and otherwise outside of the relevant Regulated Jurisdiction) not bound by this BCR, each Data Importer must undertake to:

- when transferring to a processor, sign a data processing agreement with the third-party processor to provide adequate protection of processed data according to European standards, for instance by using the applicable EU Model Clauses proposed by the European Commission or by any agreement which takes up at least an equivalent obligation; or
- implement all other necessary safeguards required for the transfer of Personal Data of EEA Data Subjects in accordance with Article 44 to 46 of General Data Protection Regulation (e.g., EU Model Clauses), or
- implement all other necessary safeguards required for the transfer of Personal Data of Data Subjects other than EEA Data Subjects in accordance with applicable law (e.g., EU Model Clauses).

6. Data Breach

In the event of a Data Breach of Personal Data of Regulated Jurisdiction Data Subjects, the concerned BCR AXA Companies shall notify the Data Breach without undue delay to the DPO(s) of affected BCR AXA Companies, including to the BCR AXA Companies acting as Controller when BCR AXA Company acting as a Processor becomes aware of a Data Breach and when more than 1 000 Regulated Jurisdiction Data Subjects are concerned also to the GDPO.

If the BCR AXA Companies who are Controller determine that the Data Breach is likely to result in a risk to rights and freedom of natural persons, they need to notify the Data Breach, without undue delay and where feasible, not later than seventy-two (72) hours, after having become aware of the Data Breach to the competent Data Protection Authority.

The BCR AXA Companies who are Controller involved in a Data Breach likely to result in a high risk to the rights and freedoms of the Regulated Jurisdiction Data Subjects shall also directly notify Regulated Jurisdiction Data Subjects.

Any notification of a Data Breach shall be documented and must comprise at least:
- the facts relating to the Data Breach,
- the likely consequences of the Data Breach,
- the remedial action taken to address the Data breach including, where appropriate, measures to mitigate its possible adverse effects.

Such documentation shall be made available to the Coordinating Data Protection Authority and any other relevant Data Protection Authorities upon request.

ARTICLE V - RIGHTS OF INFORMATION, ACCESS, RECTIFICATION, ERASURE AND BLOCKING OF DATA

In the event of a Processing of Personal Data by Data Importer, Regulated Jurisdiction Data Subjects are entitled, upon written request, to:

- obtain a copy of the public facing version of this BCR from AXA internet site, AXA Intranet website, or the DPO, on request and within a reasonable time frame.
- request information about stored Personal Data relating to them, including information relating to how Personal Data had been collected.
- obtain the list of recipients or categories of recipients to which their Personal Data is transferred.

- obtain information regarding the purpose(s) of the collection of their Personal Data and of their transfer.
- obtain the rectification of their Personal Data without undue delay, when it is inaccurate.
- object to the Processing of their Personal Data on grounds relating to their particular situation unless otherwise provided by applicable laws.
- request for the erasure of their Personal Data without undue delay if legally possible and on the grounds specified under European Regulation.
- obtain the restriction of processing in accordance with European Regulation
- obtain any other information which would be required under applicable local law,
- obtain a notification regarding rectification or erasure or restrictions of their Personal Data;
- object to decisions based solely on automated processing, including profiling.
- obtain the right to portability of their Personal Data: they have the right to receive the Personal Data they have provided to BCR AXA Companies in a suitable format and have the right to transfer that data to another data controller without BCR AXA Companies interfering (only where the Processing is based on the performance of a contract or their consent);
- request BCR AXA Companies' cooperation with competent Data Protection Authorities relating to compliance with this Article.

in each case, this applies only to the extent permitted by the data privacy laws of the Regulated Jurisdiction where the Regulated Jurisdiction Data Subject was resident at the time his/her personal data was collected or where his/her Personal Data was processed by BCR AXA Company within the context of AXA business activities.

ARTICLE VI - ACTIONS FOR BCR IMPLEMENTATION

1. Training program

BCR AXA Companies undertake to implement, at least every two (2) years, up-to-date training programs on the protection of Personal Data for AXA Employees or BCR Companies Employees involved in the Processing of Personal Data and development of tools used to process Personal Data about the principles contained in this BCR.

The general principles for training and awareness will be elaborated centrally and practical examples will be shared, while the final development and implementation of the training and awareness sessions (e-learning, face-to-face…) will be performed by each BCR AXA Company in line with applicable laws and processes.

Each BCR AXA Company shall define how it carries out the control of the level of training successfully completed. In addition, each BCR AXA Company will determine the periodicity of training refreshers, the training on the protection of Personal Data of newly hired AXA Employees or BCR Companies Employees as part of their induction session upon joining a BCR AXA Company, as well as the training especially devoted to AXA Employees or BCR Companies Employees who are more intimately involved with critical aspects of Personal Data. Such training program shall cover procedures of managing requests for access to Personal Data by public authorities.

2. BCR governance

The ***AXA BCR Steering Committee:***

- Approves scope.
- Approves approaches.
- Approves documents.
- Arbitrates potential resource conflicts.

The governance structure might be subject to evolution and change, for example because of potential future legal/regulatory or structural changes within AXA Group. The GDPO have a duty to report all the changes in the BCR, without undue delay, to all BCR members. Such future changes will be decided ***by the AXA BCR Steering Committee*** specifically dedicated to BCR consisting of Group Senior Management Representatives and Data Privacy Officers of selected BCR AXA Companies such as GDPO, Data Privacy Assurance Officers and some BCR AXA Companies representatives/DPOs.

Before any changes are decided, all BCR AXA Companies will have the chance to give their input to the changes in a consultation process. In case of conflicts, the BCR Steering Committee, together with the BCR AXA Company in question will do its best to solve this conflict in order to ensure that the respective BCR AXA Company can remain covered by the BCR.

The BCR AXA Companies agree that the BCR governance structure is subject to the decisions of the ***AXA BCR Steering Committee*** and that they will comply with all evolutions and modifications brought to this structure resulting from decisions of this Committee (subject to the previous consultation process described above and potential legal and regulatory restrictions).

The BCR AXA Companies agree that non-substantial changes may be adopted in a decision by the ***AXA BCR Steering Committee*** without the need to consult with any of the BCR AXA Companies.

The GDPO is responsible for overseeing the implementation of BCR through a network of DPOs.

BCR AXA Hubs may be created in the future to support the implementation of the BCR in collaboration with the GDPO, for example by overseeing the respect of and compliance with the BCR by the BCR AXA Companies within their scope.

Each BCR AXA Company will appoint a DPO, responsible for coordinating with the GDPO for ensuring such BCR AXA Companies' compliance with BCR. For this purpose, the DPO may be appointed by the holding company of a consolidated subgroup (e.g. AXA France, AXA UK, AXA Germany) to be the DPO of some or all its consolidated subsidiaries.

The DPO is the initial contact person on any data privacy matters or issues for advises and controls. The DPOs should be able to report on data privacy to highest management level including if any questions or problems arise during the performance of their duties.

The DPO being the second line of defense supports the senior and business management by means of developing and implementing procedures, safeguards and controls designed to ensure meeting local requirements and consistency with this BCR, notably with respect to:

- Processing principles
- Actions for BCR implementation
- Third party beneficiary rights
- Complaints
- Mutual assistance and cooperation with data protection authorities.

The DPO should not have any tasks that could result in conflict of interests. The DPO should not oversee carrying out data protection impact assessments, neither should they be in charge of carrying out the BCR audits if such situations can result in a conflict of interests. However, the DPO can assist the BCR AXA Companies, and advice the DPOs for such tasks. BCR AXA Companies should seek DPOs' advice for these tasks.

The GDPO will provide knowledge transfer between the BCR AXA Companies to allow both improvements of local privacy programs and to foster a consistent approach - where appropriate - to Group privacy objectives while allowing for necessary local differences due to legal or other local requirements.

The GDPO, in conjunction with Group IT, Compliance, Audit or others may further develop training, monitoring and reporting requirements across the AXA Group to ensure appropriate compliance with BCR is achieved. This reporting will not replace local requirements if the local legal issues require supplemental measures.

Where appropriate, Regional Data Privacy Officers may be appointed ("RDPO") and Data Privacy governance model replicated for the region. The RDPO has the role of promoting the BCR within the BCR AXA Companies in the region and is coordinating between the DPOs in the region and the GDPO.

3. Responsibilities for the BCR and BCR Compliance Check Program

In relation to the present BCR, the following shall generally apply.

The senior and business management, being the first line of defense, are responsible for ensuring Personal Data processing is compliant with the BCR.

The AXA Group's Data Privacy Officers are the second line of defense. The second line advises the Senior and Business Management on the BCR and related control requirements. They

complete the BCR compliance check program on an annual basis. The BCR compliance check program is detailed in Appendix 2, coverage is detailed in the BCR compliance questionnaire.

Internal Audit, being the third line of defense, provides independent assurance on the effectiveness of the BCR. The third line is responsible for determining the audit plan, conducting internal audits, and verifies effectiveness of the second and first lines within the normal 5 years internal audit cycle. Internal Audit is also responsible for determining the audits frequency, which is at least every 5 years. Employees belonging to Internal Audit are guaranteed independence as to the performance of their duties related to the audits conducted.

External and Data Protection Authorities audits provide additional independent assurance on the effectiveness of the BCR. External auditors may be entrusted by second- or third-line functions to perform audits (e.g. on providers) under their supervision to ensure the adequate quality of the audit. External auditors shall be subject to appropriate confidentiality and security undertakings.

The BCR compliance check program covers all significant aspects of the BCR including methods of ensuring that corrective actions will take place. Therefore, if there are indications of non-compliance of a BCR member (for example, following internal or external audit or BCR compliance check program findings), the BCR compliance check program ensures the verifications of compliance with the BCR. The result of the BCR compliance check program and relevant audit reports – internal, external and from Data Protection Authorities – will be communicated to the GDPO and the DPO of any affected BCR AXA Company, who will report to the local board or its relevant sub-committee such as local audit committee, as well as on an annual basis to Group Audit Committee (which is subcommittee of board of directors and with members from board of directors of AXA SA) .

The results of the BCR compliance check program and relevant audit reports - internal, external and from Data Protection Authorities - will be maintained in a form that Data Protection Authorities located in the EEA may access them if they utilize their audit right set out below.

Each Data Exporter shall permit the local DPA to audit the relevant BCR AXA Companies in order that the DPA may obtain the information necessary to demonstrate BCR AXA Companies compliance with the BCR. Each such audit shall be subject to the same scope and subject to the same conditions as where the local DPA audits the Data Exporter under the data privacy law of the DPA's Regulated Jurisdiction. Each such audit shall not be required to the extent such request contravenes Applicable Law or regulation and the BCR AXA Companies waive no defenses and/or rights available to that BCR AXA Company.

A BCR AXA Company shall not be required to disclose anything that does not relate to compliance with the BCR in response to requests from the DPA, and shall not be required to disclose any privileged or third party confidential information unless permitted to do so by the relevant third parties, and shall not be required to disclose the AXA's own commercially sensitive information unless it is impossible to separate those elements relating to compliance with the BCR from those containing the AXA's own commercially sensitive information.

4. BCR access and disclosure to Regulated Jurisdiction Data Subjects

The informing of Regulated Jurisdiction Data Subjects which do not have access to AXA's Intranet website such as clients, assimilated individuals (claimants, victims of accidents, and other beneficiaries of an insurance policy who did not subscribe to it), job applicants and suppliers about the BCR is affected by publishing the public facing BCR version on AXA's public Internet website. The public facing BCR version is the BCR without its Appendices.

The informing of Regulated Jurisdiction Data Subjects which have access to AXA's Intranet website such as AXA Employees and assimilated individuals (agents, representatives…) about the BCR is affected by publishing the public facing BCR version on AXA's Intranet website.

Additional optional ways of informing clients, providers, AXA Employees and BCR Companies Employees at each BCR AXA Company may include providing information to clients within a letter/notice about several subjects, providing information to clients through an agency – e.g. through agent access to intranet, and providing information to AXA Employees and BCR Companies Employees through works councils or other competent employee representative bodies. It is not possible (as excessively difficult and costly) to send a dedicated letter to all clients in many cases, such as claimants, victims of accidents, or beneficiaries of policy who are not insured or subscribing to it.

ARTICLE VII - THIRD PARTY BENEFICIARY RIGHTS

It is the intent of all the Data Exporters to grant Regulated Jurisdiction Data Subjects third party beneficiary rights under these BCR in respect of Relevant Transfers and Onward Transfers. Accordingly, it is expressly acknowledged and accepted by each Data Exporter that Regulated Jurisdiction Data Subjects shall be entitled to exercise their rights in respect of Relevant Transfers and Onward Transfers pursuant to the provisions of Articles IV.1, IV.2, IV.4, IV 5, V, VII, VIII, IX, X, XIII.4 and XIV of these BCR and that failure by any Data Exporter to comply with its obligations under these Articles in these circumstances shall potentially give rise to remedy and, where appropriate and to the extent provided by applicable law, compensation rights (as the case may be in consideration of the breach committed and the damage suffered) for the Regulated Jurisdiction Data Subject affected. Each BCR AXA Company expressly acknowledges and accepts that data subjects may be represented by a not-for-profit body, organisation or association under the conditions set out in European Regulation.

It is expressly specified that the rights granted to Third Parties as set out above are strictly limited to Regulated Jurisdiction Data Subjects in respect of Relevant transfers and Onward Transfers and shall in no event be extended or be interpreted as extending to non-Regulated Jurisdiction Data Subjects or other transfers of personal data.

ARTICLE VIII - COMPLAINT

A responsibility as a BCR AXA Company is to have an internal complaint handling process. In the event of a dispute, Regulated Jurisdiction Data Subjects may lodge, in accordance with the relevant local procedure, a complaint about any unlawful or inappropriate Processing of their Personal Data that is incompatible with these BCR in any fashion, to:

- the Data Privacy Officer,
- the relevant Data Protection Authority which will either be the Data Protection Authority in the Regulated Jurisdiction of his or her habitual residence when the Personal Data involved in the complaint was collected or place of the alleged infringement, and
- the competent jurisdictions of an EEA country at Data Subject's choice: the Data Subject can choose to act before the courts of the EEA country in which the Data Exporter has an establishment or before the courts of the EEA country where the Data Subject has his or her habitual residence when the Personal Data involved in the complaint was collected.

If a complaint is rejected, the Regulated Jurisdiction Data Subjects must be provided with clear and comprehensible reasons for this decision.

When a complaint is found to be justified, remedial actions must be taken to rectify the issue. This might include changing practices or procedures that led to the improper Personal Data handling.

The number of complaints which have been timely handled and the number of complaints which have not been timely handled are annually reported to GDPO and locally, in order to take actions to reduce number of complaints not answered timely.

Each BCR AXA Company will have on its internet website practical tools allowing Regulated Jurisdiction Data Subjects to lodge their complaints including at least a postal address, and at least one of below:

- Web link to a complaint form
- Email address.
- Telephone number.

Unless it proves particularly difficult to find the necessary information to conduct the investigation, complaints must be investigated and an answer to the Regulated Jurisdiction Data Subjects must be provided by the Data Privacy Officer or complaints responsible department, without undue delay and in any event within one (1) month of the date on which the complaint is lodged. In case of difficulty and considering the complexity and number of the requests, that one (1) month period may be extended at maximum by two (2) further months, in which case, Regulated Jurisdiction Data Subjects will be informed accordingly.
For avoidance of doubt, it is understood that if the Regulated Jurisdiction Data Subject is not satisfied by the replies of the Data Privacy Officer or complaints responsible department or in case of unjustified delay in the answer, the Regulated Jurisdiction Data Subject has the right to lodge a complaint before the relevant Data Protection Authority and/or the competent jurisdictions of the country. The rights are not dependent on the Regulated Jurisdiction Data Subject having used a BCR AXA Company's internal complaint handling process.

ARTICLE IX - LIABILITY

1. General Position

Each BCR AXA Company shall bear the sole responsibility for the breaches of the BCR which fall under its responsibility towards other BCR AXA Companies, competent Regulated Jurisdiction Data Protection Authorities and Regulated Jurisdiction Data Subjects in each case, to the extent provided under applicable law and regulation.

To the extent provided under applicable law and regulation and subject to Articles IX(2) and IX(3), each Data Exporter is individually liable for any harm a Regulated Jurisdiction Data Subject may suffer due to any breach of the BCR committed by itself or by a Data Importer having received the Personal Data transferred from a Regulated Jurisdiction pursuant to a Relevant Transfer or Onward Transfer originating from the related Data Exporter.

To the extent provided under applicable law and regulation and subject to Articles IX(2) and IX(3), where EEA Data Subject Personal Data originates from an EEA Data Exporter, each EEA Data Exporter is individually liable for any harm an EEA Data Subject may suffer due to any breach of the BCR committed by itself or by a Data Importer having received the Personal Data transferred from the EEA pursuant to a Relevant Transfer or Onward Transfer originating from the related EEA Data Exporter.

Subject to Articles IX (2) and (3), each BCR AXA Company shall be responsible for the loss or damage because of its own breach of the BCR to the extent provided under applicable law and regulation. No BCR AXA Company shall be liable for the breach committed by any other BCR AXA

Company, except in the case of a breach by Data Importer where the Data Exporter may compensate the Regulated Jurisdiction Data Subject first (subject to Articles IX(2) and (3)), and then seek reimbursement from the Data Importer; e.g. if a Data Importer is in breach with BCR and the Data Exporter pays damages to the Regulated Jurisdiction Data Subject with regards to such breach, then the Data Importer shall be bound to reimburse the Data Exporter. Similarly, if a Data Exporter is in breach with BCR and the Data Importer pays damages to the Regulated Jurisdiction Data Subject with regards to such breach, then the Data Exporter shall be bound to reimburse the Data Importer.

The Data Exporter whose liability is incurred because of a breach by a Data Importer may take the necessary actions to remedy these acts by the Data Importers and, in consideration of the breach and of the damage suffered by the Regulated Jurisdiction Data Subject, to pay compensation to the Regulated Jurisdiction Data Subject in accordance with the applicable law and local standards. Thereafter, Data Exporter may seek recourse against the Data Importer for the breach of the BCR. The Data Exporter may be either partially or fully exonerated if it can prove that it is not responsible for the cause of such harm.

A Regulated Jurisdiction Data Subject is entitled to appropriate compensation for damages caused by a violation of the BCR relating to Personal Data transferred by the Data Exporter in consideration of the breach in accordance with the applicable law and local standards and in accordance with the (proven) damage suffered. In that case, it will be the responsibility of the Data Exporter to prove that the Data Importer was not responsible for the breach of the BCR giving rise to those damages, or that no such breach took place. Upon receipt of a Regulated Jurisdiction Data Subject's complaint with respect to a violation of the BCR, the applicable BCR AXA Company assists and transparently informs the Regulated Jurisdiction Data Subject and undertake to redirect the Regulated Jurisdiction Data Subject to the BCR AXA Company at the cause of the violation. To the extent permitted by applicable jurisdiction, a Regulated Jurisdiction Data Subject is entitled to bring the claim before the Data Protection Authority or the competent jurisdictions of the country in which the Data Exporter is based. Where the latter is not based in the EEA but processes EEA Data Subject Personal Data in the EEA, the competent jurisdiction shall be in the country where such processing takes place. Where EEA Data Subject Personal Data originates from an EEA Data Exporter, the competent jurisdiction shall be the place of establishment of the first EEA Data Exporter.

2. Additional Provisions where Data Importer is a Controller

The following provisions apply only in circumstances where a Data Importer is acting as a Controller and set out the only circumstances when a claim may be brought by a Regulated Jurisdiction Data Subject against such a Data Importer.

In situations where complaints are lodged alleging that the Data Importer has failed in its obligations of the BCR, the Regulated Jurisdiction Data Subject must first request that the relevant Data Exporter take reasonable steps in order to investigate the case and (if there is a breach) remedy the damage resulting from the alleged breach and suffered by the Regulated Jurisdiction Data Subject and to assert its rights against the Data Importer breaching the BCR. Should the Data Exporter fail to take such steps within a reasonable time (normally 1 month), the Regulated Jurisdiction Data Subject shall then be entitled to assert its rights against the Data Importer directly. A Regulated Jurisdiction Data Subject is also entitled to act directly against a Data Exporter who has failed to make reasonable efforts to determine whether the Data Importer is capable of satisfying its obligations under these BCR to the extent provided for and in accordance with applicable law.

3. Additional Provisions where Data Importer is a Processor

The following provisions apply only in circumstances where a Data Importer is acting as a Processor and set out the only circumstances when a claim may be brought by a Regulated Jurisdiction Data Subject against such a Data Importer or its sub-processor.

If a Regulated Jurisdiction Data Subject is not able to bring a claim for compensation against the Data Exporter, arising out of a breach by the Data Importer or his sub-processor of any of their obligations under this BCR, because the Data Exporter has factually disappeared or ceased to exist in law or has become insolvent, the Data Importer agrees that the Regulated Jurisdiction Data Subject may issue a claim against the Data Importer as if it were the Data Exporter, unless any successor entity has assumed the entire legal obligations of the Data Exporter by contract or by operation of law, in which case the Regulated Jurisdiction Data Subject can enforce its rights against such entity. The Data Importer may not rely on a breach by a sub-processor of its obligations to avoid its own liabilities.

If a Regulated Jurisdiction Data Subject is not able to bring a claim against the Data Exporter or the Data Importer, arising out of a breach by a sub-processor BCR AXA Company of any of their obligations under this BCR because both the Data Exporter and the Data Importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor BCR AXA Company agrees that the Regulated Jurisdiction Data Subject may issue a claim against the data sub-processor BCR AXA Company with regard to its own processing operations as if it were the Data Exporter or the Data Importer, unless any successor entity has assumed the entire legal obligations of the Data Exporter or Data Importer by contract or by operation of law, in which case the Regulated Jurisdiction Data Subject can enforce its rights against such entity. The liability of the sub-processor BCR AXA Company shall be limited to its own Personal Data Processing operation.

ARTICLE X - MUTUAL ASSISTANCE AND COOPERATION WITH DATA PROTECTION AUTHORITIES

1. Cooperation with the Data Protection Authorities

The BCR AXA Companies will cooperate with the competent Data Protection Authority on any issues regarding the interpretation of the BCR, to the extent consistent with applicable law, regulations and without waiving any defences and/or rights of appeal available to the Controller:

- by making the necessary personnel available for dialogue with the Data Protection Authorities and accepting the Data Protection Authorities to audit and to inspect, including where necessary, on-site the BCR AXA Companies
- by actively reviewing, considering any decisions made by the Data Protection Authorities and the views of the European Data Protection Board in respect of the BCR,
- by communicating any material changes to the BCR to their respective Data Protection Authorities,
- by answering requests for information or complaints from the Data Protection Authorities
- by applying relevant recommendations or advice from their competent Data Protection Authorities relating to compliance by the BCR AXA Companies to the BCR.

BCR AXA Companies agree to abide by a formal decision of the competent Data Protection Authority regarding the interpretation and application of these BCR, to the extent consistent with applicable law, or regulations and without waiving any defences and/or rights of appeal available to the Controller.

When Regulated Jurisdiction is within the EEA, any dispute related to the competent Data Protection Authorities' exercise of supervision of compliance with the BCR will be resolved by the courts of the EEA member state of that competent Data Protection Authority in accordance with that member state's procedural law.

2. Relationship between applicable laws and the BCRs

BCR AXA Companies must always comply with applicable local laws. Where there is no data protection law, Personal Data will be processed according to the BCR. Where local law provides for a higher level of protection for Personal Data than the BCR, then local law will be followed. Where local law provides for a lower level of protection for Personal Data than the BCR, the BCR will be followed.

In the event a BCR AXA Company has reason to believe that the applicable legal/regulatory requirements prevent the BCR AXA Company from complying with the BCR, the BCR AXA Company shall promptly inform its DPO, and the DPO shall inform the Data Exporter DPO and the GDPO and the BCR AXA Company shall comply with Article X (4) below.

To the extent certain parts of these BCRs conflict with applicable legal/regulatory requirements, the applicable legal/regulatory requirements shall prevail until the respective conflicts have been resolved in a manner appropriately consistent with all applicable legal requirements. GDPO and/or DPO may contact the competent Data Protection Authority to discuss potential solutions.

3. Request for disclosure from law enforcement bodies

The Data Importer will promptly notify the Data Exporter and, where possible, the Data Subject (if necessary with the help of the Data Exporter) if it receives a legally binding request for disclosure of Personal Data by a law enforcement authority or state security body, likely to have adverse effect on the guarantees provided by the BCR or if it becomes aware of any direct access by public authorities to Personal Data transferred pursuant to the BCR in accordance with the laws of the country of destination; such notification will include all information available to the Data Importer. In case of legal binding request, this notification shall include the Personal Data requested, the requesting authority, the legal basis for the request and the response provided.

When a BCR AXA Company receives a legally binding request for disclosure of Personal Data by a law enforcement authority or state security body, likely to have adverse effect on the guarantees provided by the BCR, the competent Data Protection Authority shall be informed by the DPO or the GDPO, unless otherwise prohibited under applicable local laws. The information to the DPA must comprise information about the data requested, the requesting body and the legal basis for the disclosure. Where notification of requests for disclosure is prohibited under applicable local laws, the requested BCR AXA Company will use its best efforts to waive this prohibition and will document its best efforts to be able to demonstrate them upon request of the Data Exporter.

If, despite its best efforts the prohibition cannot be waived, the requested BCR AXA Company must provide annual general information to the competent Data Protection Authority and the Data Exporter on the requests it received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If the Data Importer is or becomes partially or completely prohibited from providing the Data Exporter with the aforementioned information, it will, without undue delay, inform the Data Exporter accordingly.

The Data Importer shall preserve the abovementioned information for as long as the Personal Data are subject to the safeguards provided by the BCR and shall make it available to the competent Data Protection Authority upon request.

The Data Importer will review the legality of the request for disclosure, whether it remains within the powers granted to the requesting public authority, and will challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law, and principles of international comity. The Data Importer will, under the same conditions, pursue possibilities of appeal. When challenging a request, the Data Importer will seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the Personal Data requested until required to do so under the applicable procedural rules. The Data Importer will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Data Exporter. It will also make it available to the Competent Data Protection Authority upon request.

The Data Importer will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request. In any case, disclosure of Personal Data by a BCR AXA Company to any public authority must comply with the processing principles detailed in article IV and cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

4. Local laws and practices affecting compliance with the BCR

The Data Importer and Data Exporter warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the Processing of the Personal Data by the Data Importer, including any requirements to disclose Personal Data or measures authorising access by public authorities, prevent the Data Importer from fulfilling its obligations under these BCR. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these BCR.

The Data Importer and Data Exporter declare that in providing the warranty in the first paragraph of Article X (4), they have taken due account of the following elements:

- the specific circumstances of the Relevant Transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended Onward Transfers; the type of entities involved in the Relevant Transfer or Onward Transfer (e.g. Data Exporter and Data Importer) ; the purpose of Processing; the categories and format of the transferred Personal Data; the economic sector in which the Relevant Transfer or Onward Transfer occurs; the location of the Processing, including storage location of the data transferred;
- the laws and practices of the third country of destination relevant in light of the specific circumstances of the Relevant Transfer or Onward Transfer – including those requiring the disclosure of data to public authorities or authorising access by such authorities, and those providing for access to these data during the transit between the country of the Data Exporter and the country of the Data Importer, and the applicable limitations and safeguards;

- any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these BCR, including measures applied during transmission and to the Processing of the Personal Data in the country of destination.

The Data Importer warrants that, in carrying out the assessment under the second paragraph of Article X (4), it has made its best efforts to provide the Data Exporter with relevant information and agrees that it will continue to cooperate with the Data Exporter in ensuring compliance with these BCR.

Where any safeguards in addition to those envisaged under the BCR should be put in place, the concerned BCR AXA Companies, and their Data Privacy officer will be informed and involved in such assessment. The concerned BCR AXA Companies shall document appropriately such assessment and the supplementary measures selected and implemented.

The Data Importer and Data Exporter agree to document the assessment under the second paragraph of Article X (4) and make it available to the competent Data Protection Authority on request.
The Data Importer agrees to notify the Data Exporter promptly if, after having agreed to these BCR and for the duration of the BCR, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under the first paragraph of Article X (4), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in the first paragraph of Article X (4). Where the Data Importer and the Data Exporter are both Processors, the Data Exporter shall forward the notification to the Controller. This information should also be provided to the liable BCR AXA Company, if different from the aforementioned Data Exporter.

Following a notification pursuant to the previous paragraph , or if the Data Exporter otherwise has reason to believe that the Data Importer can no longer fulfil its obligations under these BCR, the Data Exporter along with the liable BCR AXA Company if different, shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the Data Exporter and/or Data Importer to address the situation and comply with the BCR, and where the Data Importer and the Data Exporter are both Processors, if appropriate in consultation with the Controller. The Data Exporter, along with the liable BCR AXA Company if different, shall suspend the Relevant Transfer if it considers that no appropriate safeguards for such Relevant Transfer, and all Relevant Transfers for which the same assessment and reasoning would lead to a similar result, can be ensured, or if instructed by the Controller where the Data Importer and the Data Exporter are both Processors or the competent Data Protection Authority to do so, until compliance is again ensured or the transfer is ended. In this case, the Data Exporter shall be entitled to suspend the Relevant Transfer, insofar as it concerns the Processing of Personal Data under these BCR and shall discuss with the Data Importer to determine and implement the appropriate safeguards for the Relevant Transfer. Following such a suspension, the Data Exporter has to end the transfer or set of transfers if the BCR cannot be complied with and compliance with the BCR is not restored within one month of suspension. In this case, Personal Data that have been transferred prior to the suspension, and any copies thereof, should, at the choice of the Data Exporter, be returned to it or destroyed in their entirety.

In case of deletion, the Data Importer should certify the deletion of the data to the Data Exporter. In case of local laws applicable to the Data Importer that prohibit the return or deletion of the transferred personal data, the Data Importer should warrant that it will continue to ensure compliance with the BCR and will only process the data to the extent and for as long as required under that local law.

Data Exporter or the liable BCR AXA Company, if different, will, in that case, inform all other BCR AXA Companies through the BCR Steering Committee of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of transfers is carried out by any other BCR AXA Companies or, where effective supplementary measures could not be put in place, the transfers at stake are suspended or ended.

Data Exporter undertakes to monitor, on an ongoing basis, and where appropriate in collaboration with Data Importer, developments in the third countries to which the Data Exporter has transferred Personal Data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

ARTICLE XI - NON-COMPLIANCE WITH BCR

No Relevant Transfer or Onward Transfer shall be made to a BCR AXA Company unless the BCR AXA Company is effectively bound by the BCR and can deliver compliance or can rely on other measures which allow the transfer of Personal Data according to applicable law (e.g., EU Model Clauses).

The Data Importer should promptly inform the Data Exporter if it is unable to comply with the BCR, for whatever reason, including the situations further described under ARTICLE X -above.

Where the Data importer is in breach of the BCR or unable to comply with them, the Data Exporter should suspend the Relevant Transfer or Onward Transfer.

The Data Importer should, at the choice of the Data Exporter, immediately return or delete the Personal Data that has been transferred under the BCR in its entirety, where:

- the Data Exporter has suspended the Relevant Transfer or Onward Transfer, and compliance with this BCR is not restored within a reasonable time, and in any event within one month of suspension; or
- the Data Importer is in substantial or persistent breach of the BCR; or
- the Data Importer fails to comply with a binding decision of a competent court or competent Data Protection Authority regarding its obligations under the BCR.

The same commitments should apply to any copies of the Personal Data. The Data Importer should certify the deletion of the data to the data exporter. Until the Personal Data is deleted or returned, the Data Importer should continue to ensure compliance with the BCR.

In case of local laws applicable to the Data Importer that prohibit the return or deletion of the transferred Personal Data, the Data Importer should warrant that it will continue to ensure compliance with the BCR and will only process the Personal Data to the extent and for as long as required under that local law.

ARTICLE XII - EFFECTIVE DATE AND TERM OF THE BCR

The BCR shall come into force on the 15th of January 2014 for an unlimited period of time.

The BCR shall become enforceable upon each BCR AXA Company on the effective date of the IGA it enters with regards to these BCR. The BCR shall cease to be enforceable upon a designated BCR AXA Company as soon as either (i) the BCR are terminated by written notice by GDPO to the Coordinating Data Protection Authority and each BCR AXA Company; or (ii) the IGA it has entered has been terminated under the conditions defined in the IGA. In both cases, it shall be agreed in writing between the Data Exporter and Data Importer, for each Relevant Transfer, whether the Data Importer ceasing to be bound by the BCR may keep, return or delete the Personal Data subject to such Relevant Transfer or Onward Transfer, including any copies of the Personal Data. If agreed that Personal Data is kept by Data Importer ceasing to be bound by the BCR, such Data Importer will remain liable to maintain protection regarding transfers of Personal Data to third countries or international organisations in accordance with Chapter V General Data Protection Regulation, either pursuant to an adequacy decision of the EU

Commission, an appropriate safeguard such as EU Model Clauses approved by the EU Commission or derogations to specific situations.

In case of deletion, the Data Importer should certify the deletion of the data to the Data Exporter. In case of local laws applicable to the Data Importer that prohibit the return or deletion of the transferred personal data, the Data Importer should warrant that it will continue to ensure compliance with the BCR and will only process the data to the extent and for as long as required under that local law.

ARTICLE XIII - APPLICABLE LAW – Jurisdiction

1. Governing Law

This BCR (including any BCR Agreements) shall be governed by and construed in accordance with French law.

2. Dispute arising between the Data Importer and the Data Exporter.

Any dispute arising between the Data Importer and the Data Exporter under this BCR Agreement shall be settled by the competent jurisdiction of the country of the Data Exporter unless otherwise provided by local laws.

3. Other disputes between BCR AXA Companies

Any other dispute arising between the BCR AXA Companies under the BCR (including any BCR Agreements) shall be settled by the courts of Paris of competent jurisdiction unless otherwise provided by a mandatory requirement of applicable laws.

4. Disputes with Regulated Jurisdiction Data Subjects

To the extent permitted by applicable jurisdiction and the third-party rights provisions of this BCR, a Regulated Jurisdiction Data Subject is entitled to bring a claim against a BCR AXA Company either.

(i) before the competent jurisdictions of the country of an EEA country at Data Subject's choice: the Data Subject can choose to act before the courts of the EEA country in which the Data Exporter has an establishment or before the courts of the EEA country where the Data Subject has his or her habitual residence when the Personal Data involved in the complaint was collected.

(ii) the courts of Paris.

ARTICLE XIV - UPDATE OF THE RULES

The GDPO shall ensure regular review and update of the BCR, for example because of major changes in the corporate structure and in the regulatory environment.

All BCR AXA Companies expressly acknowledge and agree that:

- Substantial modifications to these BCRs, which significantly increase the obligations of the BCR AXA Companies, may be adopted in a decision by the ***AXA BCR Steering Committee*** after one (1) month consultation by email of the BCR AXA Companies through the DPOs emails known by the GDPO; and

- Non-substantial modifications to these BCR, which are all other modifications, may be adopted in a decision by the ***AXA BCR Steering Committee*** without the need to consult with any of the BCR AXA Companies.

The GDPO will be in charge of listing the BCR AXA Companies and to keep track of and record any updates to the BCR and the BCR AXA Companies. The GDPO shall communicate such list of updated BCR AXA Companies and any material changes to the BCR to the Coordinating Data Protection Authority every year and, in addition, any other relevant Data Protection Authorities upon request. The GDPO shall promptly communicate any changes which would materially affect the level of protection offered by the BCR or significantly affect the BCR to the Coordinating Data Protection Authority. The DPO shall communicate such updated public facing version of the BCR to Regulated Jurisdiction Data Subject upon request and shall ensure the public facing version of the BCR and list of BCR AXA Companies is up to date. . The GDPO shall also inform the Coordinating Data Protection Authority every year, where applicable, of absence of changes made to the BCR, and with the renewal of the asset confirmation required in the BCR application form.

The public facing version of the BCR and the list of BCR AXA Companies and contact details of BCR AXA Companies and their DPOs or privacy professionals are available on axa.com, being understood that BCR AXA Companies' DPO or privacy professional may be directly contacted for any question or complaint related to a Relevant Transfer.

LIST OF APPENDICES:

Appendix 1: BCR Agreement
Appendix 2: Compliance Check Program
Appendix 3: Data Protection Corporate Agreement

APPENDIX 1

INTRA GROUP AGREEMENT
FOR THE ESTABLISHMENT OF CORPORATE BINDING RULES
FOR THE TRANSFER OF PERSONAL DATA WITHIN THE AXA GROUP

This Intra Group Agreement for the establishment of Binding Corporate Rules (hereinafter the "**BCR Agreement**") is entered into on [●] (hereinafter "Effective Date") by and between

(1) **AXA SA**, a joint stock corporation incorporated under the laws of France, having its registered office at 25, avenue Matignon – 75008 PARIS France, registered with the Registry of Commerce and Companies of Paris under number 572 093 920,

represented by [●], acted as [●], duly empowered for purposes hereof,

hereinafter referred to as the "**AXA SA**";

AND

(2) **The BCR AXA Companies listed in Schedule 1**

AND

(3) **Any Acceding BCR AXA Company**

AXA SA and the AXA Companies listed in Schedule 1 are hereinafter collectively referred to as the "**BCR AXA Companies**" and individually as a "Party".

RECITALS

WHEREAS, due to the nature of their businesses, the companies of the AXA Group are required to process Personal Data and various types of Personal Data processes are implemented;

WHEREAS, due to the international nature of the AXA Group, Personal Data collected and processed by AXA Companies based in the EEA may be transferred to AXA Companies or enterprises engaged in a joint economic activity with AXA Companies located outside the EEA;

WHEREAS, it has become necessary for the AXA Companies and companies engaged in a joint economic activity with AXA Companies to ensure seamless and secured flows of data between themselves whilst maintaining an adequate level of protection in accordance with applicable laws and regulations;

WHEREAS, the BCR AXA Companies consider that the establishment of Binding Corporate Rules for the transfer of Personal Data between themselves and other AXA Companies or companies engaged in a joint economic activity with AXA Companies which may, from time to time, express their intention to participate in the Binding Corporate Rules of AXA as promulgated by the GDPO from time to time (the "**BCR**"), can help in achieving this purpose; and

WHEREAS, the BCR AXA Companies have created a set of BCR which they wish to make binding between themselves.

IT HAS BEEN AGREED AS FOLLOWS:

1. DEFINITIONS

All capitalised or defined terms in this BCR Agreement shall have the meaning assigned to it in the BCR.

2. PURPOSE

The purpose of this BCR Agreement is to establish between the BCR AXA Companies as well as any Acceding BCR AXA Company, a set of BCR defining the rules according to which Personal Data transferred from a BCR AXA Company located in the EEA to a BCR AXA Company located outside the EEA shall be processed.

This BCR Agreement also sets out the conditions under which any AXA Company or any company engaged in a joint economic activity with AXA Companies can accede to the BCR.

3. BINDING NATURE OF THE BCR

Each of the BCR AXA Companies hereby expressly acknowledges and accepts that it will comply with the rules and principles set out in the BCR (as amended from time to time in accordance with their terms) and expressly accepts to be bound by the entirety of the terms of the BCR during the entire term of its participation in the BCR.

Accordingly, each BCR AXA Company undertakes to process Personal Data in accordance with the terms of the BCR and to submit to all the obligations set out in the BCR.

4. PARTIES TO THE BCR

4.1. All BCR AXA Companies shall be parties to the BCR from the effective date of this Agreement.

4.2. Any AXA Company or any company engaged in a joint economic activity with AXA Companies (the "**Acceding BCR AXA Company**") may (acting by one or more duly authorised representatives in accordance with its articles, statutes and/or constitution) accede to the BCR by signing an IntraGroup Agreement for the Acceptation of the AXA Binding Corporate Rules (the "**BCR Acceptation Agreement**") in materially the same form as set out in Schedule 2.

4.3. For this purpose, each of the BCR AXA Company hereby expressly grants AXA S.A. the right and power to represent it individually for the sole purpose of signing, on its behalf, the necessary BCR Acceptation Agreement to allow the Acceding BCR AXA Company to accede to the BCR.

4.4. The right and power granted above to AXA S.A by the BCR AXA Companies is expressly and exclusively limited to the signature of BCR Acceptation Agreements and shall not be interpreted as granting AXA S.A. any further right or power of representation of the BCR AXA Companies. Such right and power shall not have any influence on the liability of each BCR AXA Company with regards to the BCR.

4.5. Upon the signature of the necessary BCR Acceptation Agreement as set out in Section 4.2 above, the relevant Acceding BCR AXA Company shall, with effect on and from the date specified in the BCR Acceptation Agreement be bound by the terms of the BCR and possess the same

rights and obligations as if it had been an original party to the BCR and to this BCR Agreement and that Acceding BCR AXA Company shall immediately become a BCR AXA Company.

5. LIABILITY

In accordance with, and subject to, the terms of Article IX of the BCR, the BCR AXA Companies acknowledge and accept that:

- Each BCR AXA Company shall bear the sole responsibility for the breaches of the BCR which fall under its responsibility, towards, as the case may be, other BCR AXA Companies, competent Regulated Jurisdiction Data Protection Authorities and Regulated Jurisdiction Data Subjects. If the Data Exporter is not based in the EEA but processes EEA Data Subject Personal Data in the EEA, the competent jurisdiction shall be in the country where such processing takes place. Where EEA Data Subject Personal Data originates from an EEA Data Exporter, the competent jurisdiction shall be the place of establishment of the first EEA Data Exporter.

- Each Data Exporter is individually liable for any harm a Regulated Jurisdiction Data Subject may suffer due to any breach of the BCR committed by itself or by a Data Importer having received the Personal Data transferred from a Regulated Jurisdiction pursuant to a Relevant Transfer or Onward Transfer originating from the related Data Exporter. Where EEA Data Subject Personal Data originates from an EEA Data Exporter, each EEA Data Exporter is individually liable for any harm an EEA Data Subject may suffer due to any breach of the BCR committed by itself or by a Data Importer having received the Personal Data transferred from the EEA pursuant to a Relevant Transfer or Onward Transfer originating from the related EEA Data Exporter.

- Each BCR AXA Company shall be responsible for the loss or damage as a result of its own breach of the BCR. No BCR AXA Company shall be liable for the breach committed by any other BCR AXA Company, except in the case of a breach by Data Importer where the Data Exporter may compensate the Regulated Jurisdiction Data Subject first and then seek reimbursement from the Data Importer.

Nothing in this agreement or the BCR shall make a BCR AXA Company liable to Regulated Jurisdiction Data Subjects for losses or damages which the Regulated Jurisdiction Data Subject could not have recovered under the provisions of the data privacy law in Regulated Jurisdiction in which the Regulated Jurisdiction Data Subject resided at the time Personal Data was collected about him/her.

6. TERMINATION

This BCR Agreement shall remain in effect as long as the BCRs themselves remain in effect and for so long as at least two (2) BCR AXA Companies remain parties to this BCR Agreement.

Any BCR AXA Company shall be entitled to terminate its participation to the BCR and this BCR Agreement by giving at least six (6) months' written notice to the GDPO.

Any BCR AXA Company which either terminates its participation to the BCR as set out above or ceases to be a member of the AXA Group shall thereupon cease to be a party to the BCR, but shall remain liable for all obligations under the BCR to which it became subject up to the date when it ceased to be a party to the BCR.

7. SIGNATURE PROCESS

This BCR Agreement may be executed in a digital format which means that the signature may be delivered by facsimile transmission or by e-mail delivery of a ".pdf" format data file, such signature shall create a valid and binding obligation of the party executing (or on whose behalf such signature is executed) with the same force and effect as if such facsimile or ".pdf" signature page were an original thereof.

Drawn up in [Number of BCR AXA Companies] counterparts,

[INCLUDE SIGNATURE PAGES FOR EACH BCR AXA Company]

SCHEDULE 1 TO APPENDIX 1: LIST OF COMPANIES PARTY TO THE BCR AGREEMENT

Please find the list of AXA BCR Companies in axa.com.

SCHEDULE 2 TO APPENDIX 1: TEMPLATE OF BCR ACCEPTATION AGREEMENT

INTRA GROUP AGREEMENT
ACCEPTATION OF THE AXA BINDING CORPORATE RULES

This Intra Group Agreement of acceptation of the AXA Binding Corporate Rules (hereinafter "**BCR Acceptation Agreement**") is entered into on [●] (hereinafter "Effective Date") by and between

(1) **AXA SA**, a joint stock corporation incorporated under the laws of France, having its registered office at 25, avenue Matignon – 75008 PARIS France, registered with the Registry of Commerce and Companies of Paris under number 572 093 920,

represented by [●], acted as [●], duly empowered for purposes hereof,

hereinafter referred to as the "**AXA SA**";

AND

(2) **AXA [Insert name of BCR AXA Company/Companies],** having its registered office at [●] with the Registry of Commerce and Companies of [●] under number [●]

represented by [●], acted as [●], duly empowered for purposes hereof,

hereinafter referred to as the "**Acceding BCR AXA Company**";

AXA [Insert name of Acceding BCR AXA Company] and AXA SA are hereinafter collectively referred to as the "Parties" and individually as a "Party".

RECITALS

WHEREAS within AXA Group and companies engaged in a joint economic activity with AXA Companies, various types of Personal Data processes are implemented and Personal Data is transferred to AXA Companies or companies engaged in a joint economic activity with AXA Companies located outside the EEA.

WHEREAS, a number of the AXA Companies and companies engaged in a joint economic activity with AXA Companies (the BCR AXA Companies) have established a set of Binding Corporate Rules for the transfer of Personal Data from AXA Companies or companies engaged in a joint economic activity with AXA Companies located in the EEA to AXA Companies or companies engaged in a joint economic activity with AXA Companies located outside the EEA (the "**BCR**");

WHEREAS, the Acceding BCR AXA Company wishes to be able to benefit from the BCR;

WHEREAS, AXA S.A. has been granted the right and power by the BCR AXA Companies to enter into BCR Acceptation Agreements with AXA Companies, on their behalf, to allow the accession of BCR AXA Companies to the BCR;

IT HAS BEEN AGREED AS FOLLOWS:

1. DEFINITIONS

All capitalised or defined terms in this BCR Acceptation Agreement shall have the meaning assigned to it in the BCR or in the BCR Agreement.

2. PURPOSE

The purpose of this BCR Acceptation Agreement is to establish the Acceding BCR AXA Company as a party to the BCR and to the BCR Agreement.

3. BINDING NATURE OF THE BCR

The Acceding BCR AXA Company hereby expressly acknowledges and accepts that it will comply with the rules, principles, rights and obligations set out in the BCR and of the BCR Agreement and expressly accepts to be bound by the entirety of the terms of the BCR and of the BCR Agreement during the entire term of its participation to the BCR and the BCR Agreement.

Accordingly, the Acceding BCR AXA Company becomes, as of the effective date of this BCR Acceptation Agreement, a BCR AXA Company and undertakes to process Personal Data in accordance with the terms of the BCR and to submit to all the obligations set out in the BCR and the BCR Agreement.

4. PARTIES TO THE BCR AND TO THE BCR AGREEMENT

The Acceding BCR AXA Company hereby expressly grant AXA S.A. the right and power to represent it for the sole purpose of signing, on its behalf, the necessary BCR Acceptation Agreement to allow BCR AXA Companies to accede to the BCR.

The right and power granted above to AXA S.A. by the Acceding BCR AXA Company is expressly and exclusively limited to the signature of BCR Acceptation Agreements and shall not be interpreted as granting AXA S.A. any further right or power of representation of the Acceding BCR AXA Company. Such right and power shall not have any influence on the liability of each BCR AXA Company with regards to the BCR.

5. LIABILITY

In accordance with, and subject to, the terms of the BCR and of the BCR Agreement, the Acceding BCR AXA Company acknowledges and accepts that:

- Each BCR AXA Company shall bear the sole responsibility for the breaches of the BCR which fall under its responsibility, towards other BCR AXA Companies, competent Regulated Jurisdiction Data Protection Authorities and Regulated Jurisdiction Data Subjects. If the Data Exporter is not based in the EEA but processes EEA Data Subject Personal Data in the EEA, the competent jurisdiction shall be in the country where such processing takes place. Where EEA Data Subject Personal Data originates from an EEA Data Exporter, the competent jurisdiction shall be the place of establishment of the first EEA Data Exporter.

- Each Data Exporter is individually liable for any harm a Regulated Jurisdiction Data Subject may suffer due to any breach of the BCR committed by itself or by a Data Importer having received the Personal Data transferred from a Regulated Jurisdiction pursuant to a Relevant Transfer or Onward Transfer originating from the related Data Exporter. Where EEA Data Subject Personal Data originates from an EEA Data Exporter, each EEA Data Exporter is individually liable for any harm an EEA Data Subject may suffer due to any breach of the BCR committed by itself or by a Data Importer having received the Personal Data transferred from the EEA pursuant to a Relevant Transfer or Onward Transfer originating from the related EEA Data Exporter.

- Each BCR AXA Company shall be responsible for the loss or damage as a result of its own breach of the BCR. No BCR AXA Company shall be liable for the breach committed by any other BCR AXA Company, except in the case of a breach by Data Importer where the Data Exporter may compensate the Regulated Jurisdiction Data Subject first and then seek reimbursement from the Data Importer.

Nothing in this agreement or the BCR shall make a BCR AXA Company liable to Regulated Jurisdiction Data Subjects for losses or damages which the Regulated Jurisdiction Data Subject could not have recovered under the provisions of the data privacy law in Regulated Jurisdiction in which the Regulated Jurisdiction Data Subject resided at the time Personal Data was collected about him/her.

6. TERMINATION

This BCR Acceptation Agreement shall remain in effect if the BCRs themselves remain in effect unless terminated in advance by one of the Parties with at least six (6) months' written notice to the GDPO. Any BCR AXA Company which ceases to be a member of the AXA Group shall thereupon cease to be a party to the BCR and to the BCR Agreement but shall remain liable for all obligations under the BCR and the BCR Agreement to which it became subject up to the date when it ceased to be a party to the BCR and the BCR Agreement.

7. MISCELLANEOUS

AXA S.A. shall be authorized to transfer all or part of its rights and obligations hereunder to any entity of its choice within the AXA Group located in the EEA.

8. SIGNATURE PROCESS

This BCR Acceptation Agreement may be executed in a numeric format which means that the signature may be delivered by facsimile transmission or by e-mail delivery of a ".pdf" format data file, such signature shall create a valid and binding obligation of the party executing (or on whose behalf such signature is executed) with the same force and effect as if such facsimile or ".pdf" signature page were an original thereof.

Drawn up in two counterparts,

For **AXA SA**	For **Acceding BCR AXA Company**
Name :	Name :
Title :	Title :
Place:	Place:
Signature :	Signature :

Stamp :	Stamp :

APPENDIX 2: COMPLIANCE CHECK PROGRAM

The document is not public and is made available to each BCR AXA Company and relevant Supervisory Authorities.