AXA GROUP
BINDING CORPORATE RULES

Background

AXA Group is committed to maintaining the privacy of data obtained in the course of its business activities and complying with applicable laws and regulations regarding the processing of Personal Data and Special categories of Data.

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.

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:

"**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; (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 all 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 in order 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 into 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.

"Data Breach" means a breach of security leading to the accidental, or unlawful destruction, loss, alteration, unauthorised 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, in particular 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 2012, EEA includes Austria, Belgium, Bulgaria, 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, Sweden, and the United Kingdom.

"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.

"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 either to a Relevant Transfer or to a transfer into the EU-U.S. Privacy Shield, in each case:

(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, enrolment in the EU-U.S. Privacy Shield 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 and Jersey.

"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, enrolment in the EU-U.S. Privacy Shield 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 (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 based in a Regulated Jurisdiction to an AXA Company 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, 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 Singapore-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 AXA Employees

The present BCR binds all 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 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 of all of 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 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, in particular in the event of:

- breach of these BCR by an AXA Employee,
- 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, analyze 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, 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.

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 in particular 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 actually 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 are 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 in order 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 in order 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 in the course of 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 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 to the coordinating Data Protection Authority and any other relevant Data Protection Authorities upon request.

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.

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 commission or alleged commission of any criminal conviction and offence by the Data Subject; or
- Any proceedings for an offence committed or alleged 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 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, on the basis of 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 is otherwise permitted under the applicable law of the country of establishment of the Data Exporter.

3. 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 measures 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.

4. Data transfers

1. Data transfers within the AXA Group

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 these BCR, or,
- by other measures which allow the transfer of Personal Data 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

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
- to undertake all other necessary safeguards required for the transfer of Personal Data in accordance with applicable law (e.g., EU Model Clauses).

5. Data Breach

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

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,

in each case save to the extent permitted by the data privacy law in the Regulated Jurisdiction in which the Regulated Jurisdiction Data Subject was resident at the time his/her personal data was collected.

ARTICLE VI - ACTIONS FOR BCR IMPLEMENTATION

1. Training program

BCR AXA Companies undertake to implement training programs on the protection of Personal Data for AXA Employees involved in the Processing of Personal Data and development of tools used to process Personal Data with regard to 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 as part of their induction session upon joining a BCR AXA Company, as well as the training especially devoted to AXA Employees who are more intimately involved with critical aspects of Personal Data.

2. 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 effected by publishing the public facing BCR version on AXA's public Internet website.

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 effected by publishing the public facing BCR version on AXA's Intranet website.

Additional optional ways of informing clients, providers and AXA 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 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, XII.3 and XIII 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.

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.

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, it has the right to lodge a complaint before the relevant Data Protection Authority and/or the competent jurisdictions of the country as per above paragraph.

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

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

Unless it proves particularly difficult to find the necessary information to conduct the investigation, complaints must be investigated within one (1) month of the date on which the complaint is lodged. In case of particular difficulty and taking into account 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.

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, as the case may be, 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 as a result 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 as a result 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 Data Importer 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. 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 take action 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 of 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 in order 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 their 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,
- 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.

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.

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

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. 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 on the requests it received.

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.

ARTICLE XI - 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 into 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 DPA (the CNIL) and each BCR AXA Company; or (ii) the IGA it has entered into has been terminated under the conditions defined in the IGA.

ARTICLE XII - 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 XIII - UPDATE OF THE RULES

The GDPO shall ensure regular review and update of the BCR, for example as a consequence 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 others 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 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.