AXA Life Europe dac

Data Privacy Policy

Document Owner	Data Protection Officer
Document Reference	Data Privacy Policy
Version	1.0 2018
Audit Committee Approval Date	April 2018
Next Audit Committee Review Date	No later than 2019

Contents

Page

Context

The Data Protection Acts 1988, the Data Protection (Amendment) Act 2003 (hereinafter referred to as the "DPA") and the European Union General Data Protection Regulation (EU)2016/679 (hereinafter referred to as the "GDPR") impose a number of constraints upon the collection or processing of personal data and sensitive personal data.

Personal data is defined as data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

A data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.

AXA Life Europe DAC (hereaster "ALE" or the "Company") has registered as a data controller for the personal data it holds on its clients and for the HR data that it holds in relation to employees and other individuals holding Pre-approval Controlled Functions and Controlled Functions under the Central Bank of Ireland's Fitness and Probity regime.

AXA Life Europe is also required to adhere to the Code of Practice on Data Protection for the Insurance Sector, which was approved by the Data Protection Commissioner under section 13(2) of the Data Protection Act in August 2008. This Code applies to all personal data held by or on behalf of insurance companies established in the State. This includes data relating to a person who holds policies (or who has applied for or held policies in the past) and any other individual whose claim is being assessed, processed or negotiated under a policy issued by the insurer. The Code of Practice is available on www.dataprotection.ie.

Policy Objectives and Scope

ALE is committed to maintaining the privacy of data obtained in the course of its business activities and to complying with applicable laws and regulations (e.g. GDPR) regarding the processing of Personal and Sensitive Personal Data.

This Data Privacy Policy (the "Policy") aims to ensure that the Company adequately protects the personal and sensitive data of clients and other persons obtained during its business activities, to minimise the risk of breaching applicable data privacy and protection laws (e.g. EU General Data Protection Regulation - GDPR) and to minimise the potential for penalties and damage to the Company's reputation.

This Policy applies to all individuals (employees and contractors) working for the Company.

Failure by any individual to comply with any aspects of this policy will be considered as a serious matter and could lead to action being taken against the employee under the Company's Disciplinary Policy.

General Principles

The Company commits to comply with the following requirements:

- Personal Data[1] must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
- Personal data must be processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- Personal Data collected must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Personal Data collected must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Not collecting unnecessary data (for which we have no business and legal reasons to collect) reduces both Cyber Risk and Data Leakage Risk.
- Personal Data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. For that purpose, the Company has a documented data retention policy that specifies how long data may be retained, how it may be stored, and in which format it may be held. Investment in Data Deletion is cost effective in order to reduce both the capital charge that needs to be held under Solvency II in relation to Cyber Risk and Data Leakage Risk.
- Enquiries from data subjects must be responded to promptly and within applicable legal deadlines.
- The Company shall establish processes and controls in order to ensure that Personal Data from clients is not sold to parties outside the AXA Group.
- The Company shall provide the data subject with transparent information if the data is collected from the data subject or if the data was obtained from elsewhere, including information on how they can exercise their rights.
- Processing of special categories of personal data (revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data in order to uniquely identify a person or data concerning health or sex life and sexual orientation) must have
  (i) explicit consent from the data subject about processing of such personal data for one or more specified purposes, or
  (ii) there must be a positive legal basis for processing of such special categories of personal data recorded for each purpose.
- A data protection impact assessment must be undertaken in relation to all relevant data projects and prior consultation for the processing that would result in a high risk in the absence of mitigation measures.

[1] For this purpose references to "Personal Data" also include "Sensitive Personal Data".

- The Company must maintain a record of processing activities under its responsibility.
- The Company shall ensure that each processor shall maintain a record of all categories of personal data processing activities carried out on its behalf.
- Where processing is to be carried out on behalf of the Company, the Company shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of this Policy and ensure the protection of the rights of the data subject. Any processing activity sub-contracted to third parties by the processor must be agreed in writing and the same standards applied to that processor shall be imposed on the sub-contractor.
- Data protection by design and by default should be the objective. In particular, Personal Data shall be minimised, pseudonymised, or anonymised with appropriate technical and organisational measures being applied, where possible, to ensure privacy by design provisions are applied. Only with these measures can the processing of personal data for scientific or statistical purposes be allowed.
- Personal Data may not be routinely transferred across borders without the written approval of the DPO and implementation of appropriate Personal Data transfer mechanisms.
- The DPO must keep a formal record of any groups of Personal Data that are routinely held or processed outside the country of origin and must ascertain if there are any additional laws or regulations that need to be complied with as a result.
- Personal Data may only be routinely transferred from one legal entity to another with the written approval of the DPO after ensuring that:
    - the applicable laws and regulations for such transfer and the requirements of this Policy are complied with; and in particular:
    - the ownership of the data in question is clear with any restrictions on its use clearly documented and reflected in the written policies and procedures of the recipient entity including appropriate and necessary legal transfer mechanisms.
- When obtaining Personal Data from clients:
    - It must be made clear to the client what the purpose of collecting the data is (e.g. to underwrite their insurance policy) - if this is to be extended to other purposes (e.g. marketing) then this must be disclosed;
    - In line with applicable laws and regulations, the clients should confirm that the data provided is accurate;
        → If the data is provided by a third party, then the client should be given an opportunity to review the data held by AXA and correct it if necessary;
        → If the data is provided by the client orally to AXA staff, the client should have the data taken presented back to them and given the opportunity to correct it if necessary.
    - Staff must not annotate client documents or document any information about the client that has not been provided by the client, is subjective, or has not been substantiated.

- In addition, the Company commits to comply with the AXA Group's Binding Corporate Rules relating to Data Protection as amended from time to time.

Organisation and Governance

The CEO of AXA Life Europe is ultimately responsible for ensuring that the Company establishes policies and procedures consistent with this Policy within his/her business and for meeting applicable legal, regulatory or contractual requirements. This is achieved by means of the Data Privacy Framework.

The Data Privacy Framework follows AXA's model of the "three lines of defence".

Role of the First Line of Defence

Management (the first line of defence) are responsible for ensuring Personal Data handling procedures within their areas of responsibility meet local requirements and are consistent with this Policy.

For the purposes of this Policy, the term Management refers to the following heads of function within the Company:

- Chief Executive Officer,
- Chief Financial Officer,
- Head of Compliance and Legal,
- Chief Risk Officer,
- Head of Actuarial,
- Head of Operations,
- Head of IT,
- HR Business Partner,
- Chief Information Security Officer.

Management decides what, why and how Personal Data is collected and processed. As the representatives of the Company, they are responsible for understanding the applicable regulatory requirements and ensuring that AXA Life Europe's collection, processing, transfer and retention of Personal Data comply with those regulatory requirements and this Policy.

Management should provide the DPO with the necessary information and means to enable him to support them in ensuring AXA Life Europe's compliance with this Policy and local requirements. In particular, the Management should have regular exchanges with the DPO and keep him informed about relevant organisational or other developments that may have an impact on Data Privacy.

Also, the Management should ensure appropriate "tone at the top" communication with respect to awareness of the issues covered by this Policy.

Management must ensure they develop, implement and enforce their own department data protection policies and procedures, indicating levels of confidentiality, access rights and retention requirements.

Management acknowledge their responsibilities in relation to Data Protection by signing a "Data Processor Appointment Letter".

Role of the Second Line of Defence

The DPO is the initial contact person for any Data Privacy matters or issues. The DPO has a joint reporting line to the AXA Group DPO ("GDPO").

The implementation of dual reporting lines means:

- All decisions regarding hiring or changing the DPO must be taken jointly by the local senior management and the GDPO
- DPO's objectives should be set jointly by the local line manager and the GDPO
- All performance appraisal and remuneration decisions (basic salary, incentive payments and equity grants) must be agreed by the local line manager and the GDPO

The DPO is responsible for:

- Developing local Data Privacy Policy and, where applicable, ensuring that any approved exemptions from the AXA Group Data Protection Policy are included in the local Policy;
- Monitoring both local and other relevant Data Privacy related regulations impacting AXA Life Europe and adapting the Company Data Privacy Policy to ensure compliance with regulatory requirements;
- Training and providing consultative advice to all the areas and departments of the Company with regard to Data Privacy matters;
- Coordination with the local Risk, Information Security, Compliance, Legal, HR, Physical Security, Operations, Finance and Internal Audit functions on Data Privacy matters;
- Communication and reporting to the local data protection authority and other relevant regulators, attendance at data protection authority inspections, handling audit submissions and other information submission requirements;
- If required by local regulation, complying with the obligation/ responsibility for supporting and controlling a general data protection register (which has to be created by each Data Controller, containing all data processing applications in use and current information about purpose);
- Collaboration with the unit(s) responsible to manage Data Subject requests (i.e. rights of access, rectification, cancellation and similar requests);
- Support on drafting internal or external confidentiality agreements relating to data,
- Reviewing and monitoring business activities and vendors' contracting/management to ensure compliance with local Data Privacy legislation and AXA Policy requirements;
- Attendance at Data Privacy, Security or similar Committees;
- Coordination and management of responses to incidents involving Personal Data (e.g. unauthorized access or disclosure);

- Adopting and implementing detailed requirements or guidelines to ensure the compliant handling of specific matters as deemed necessary, such as:
    - Marketing activities. Whether the AXA companies can use Personal Data for marketing activities. Right of Data Subject to opt out of receiving such material;
    - Sensitive Personal Data. Greater emphasis on whether and how to process/manage Sensitive Personal Data: e.g. access to sensitive medical data;
    - Information of clients, employees and other data subjects;
    - Complaints procedure. Detailed guidance as to how clients, employees and other data subjects can exercise any rights they may have under local law to complain about the way their Personal Data is being handled.
- Inclusion in project and process sign-off procedures and providing Data Privacy sign-off when satisfied that each project or process is compliant with the Policy and applicable local requirements;
- Ensuring on a regular basis that data processing applications and processes are compliant with local Data Privacy legislation and AXA Policy requirements, notably through establishing and ensuring execution of a privacy control plan;
- Participating as a Peer DPO to the Data Privacy Assurance on-site reviews (travels funded centrally);
- Writing, reviewing and implementing of common deliverables as agreed with GDPO;
- Fulfilling DPO role in the identification and maintenance of an inventory of Personal Data repositories across information systems as per the data classification policy;
- Keeping Management informed about their responsibilities with regard to Data Privacy and this Policy.
- The DPO shall be given appropriate support from the AXA company's Management, Legal, Compliance, Human Resources and IT.

Role of the Third Line of Defence

Internal Audit (the third line of defence) provides independent assurance on the effectiveness of the Data Privacy Framework.

Control and Reporting Procedures

The Company must conduct an annual maturity level self-assessment against the AXA Data Protection Policy. The GDPO provides a maturity level self-assessment questionnaire for this purpose.

The Company's DPO shall submit the annual maturity level self-assessment against the AXA Group Data Privacy Policy to:

- the Company's Executive Committee;
- the GDPO by 31st March for the preceding year
- the Audit Committee (in the form of a summary of the results of the assessment)

The DPO shall exchange on a regular basis with the Operational Risk Management Function in order to ensure that their risk assessment is consistent with Operational Risk Management's risk scenarios.

Refer also to the reporting requirements under the section "Obligation to report breaches".

Training

For this Policy to be fully effective, all staff within the Company must be aware of the requirements in relation to Data Protection insofar as they are relevant to their day-to-day responsibilities. To this end, the Company shall maintain a list of all staff within the organisation who have permanent or regular access to personal data in the course of their employment.

The Company shall ensure that all staff follow training relevant to their level of involvement in processing personal data:

- Staff who have access to personal data on a permanent or regular basis shall receive half-yearly classroom-based training in relation to data protection;
- All other staff shall receive annual training on data protection, either via e-Learning or classroom-based.

Obligation to report breaches

Under GDPR, the Company is obliged to notify the Data Protection Commissioner within 72 hours of becoming aware of a loss of personal data for which it is responsible. Examples include loss of personal data through loss of a portable device (laptop), misaddressing of e-mails or a "leak" from the organisation.

The Company must also notify the affected Data Subjects.

Where an employee is aware of a data breach or suspects a data breach has occurred, he/she must notify the Data Protection Officer immediately. The Data Protection Officer for AXA Life Europe is:

Steven Taggart
Email: steven.taggart@axa-lifeinvest.com
Tel: 014711351

A summary of all data protection breaches occurring in the period shall also be reported to the Company's Audit Committee on a quarterly basis. Serious breaches (affecting more than 1000 data subjects) should be notified at the earliest possible opportunity to the Audit Committee and also to the GDPO.

Owner of this Policy

The Company's DPO is responsible for maintaining this Policy and ensuring it remains relevant and consistent with applicable data protection regulations. The Policy should be reviewed on an annual basis, and significant changes should be proposed to the Company Audit Committee for approval.