



AG2R LA MONDIALE

May 2018

PERSONAL DATA PROTECTION POLICY

Approved by the Executive Committee of La Mondiale
Europartner as of May 2nd, 2018.

TABLE OF CONTENTS

- 1. BACKGROUND 3
 - 1.1. Objectives 3
 - 1.2. Issues 3
 - 1.3. Scope 3
- 2. PRINCIPLES 4
 - 2.1. LA MONDIALE EUROPARTNER: the business-specific context 4
 - 2.2. Fostering a sense of responsibility among the different parties involved 4
 - 2.3. Transparency 4
 - 2.4. Proportionality of protection measures 4
 - 2.5. Support for the business lines 5
- 3. FRAMEWORK AND PRINCIPLES FOR PERSONAL DATA PROTECTION 5
- 4. ROLES AND RESPONSIBILITIES 5
 - 4.1. Data-protection function 5
 - 4.2. Governance and data-quality function 8
 - 4.3. IT systems function 9
 - 4.4. Security function 9
 - 4.5. Legal function 9
 - 4.6. Risk-management, internal-control and compliance function 10
 - 4.7. Internal Audit function 10
 - 4.8. Joint data controllers and processors 10
- 5. GOVERNANCE AND REPORTING 10
 - 5.1. Personal data protection committee 10
- 6. GLOSSARY 11



1. BACKGROUND

1.1. Objectives

This policy note on personal data protection (hereafter termed the “Policy Statement”) sets forth the principles for protection of the personal data of which LA MONDIALE EUROPARTNER S.A. (hereafter, the “Company” or “LA MONDIALE EUROPARTNER”) is recipient. It outlines the organisational structure for data protection and defines the roles and responsibilities of those involved in the processing of personal data. The main aims of personal data protection are to:

- safeguard the rights and privacy of data subjects;
- process their personal data in fairness and transparency;
- apply the regulations and professional best practices.

1.2. Issues

The Company has built itself up in the sole interest of its policyholders, with the ambition of protecting their lives, their relatives and their assets. In the course of its business, it receives information that is private and may contain intimate details.

The confidentiality and security of such information is a **condition of trust** essential to our Company’s activities and development.

The conduct of the Company’s business involves the processing of large quantities of personal data which constitute a major proportion of the stock of information for which it is responsible and a **source of value** both for itself and for the community of its policyholders.

In dealings with its own staff, for purposes of its human-resources management, the Company seeks the highest standards in safeguarding the rights of employees and protecting their information.

Compliance with the regulations and best practices addressing the protection of privacy and of personal data underpins the legitimacy and credibility of our Company, which aims to place the individual at the heart of its economic and social business model.

1.3. Scope

This Policy Statement covers the following:

- LA MONDIALE EUROPARTNER together with its partners and sub-contractors;
- all the Company’s business lines involved in developing and marketing life insurance (assurance-vie) products and endowment policies;
- all persons whose data are processed by this Company, particularly:
 - customers, policyholders, beneficiaries and prospective customers;
 - employees and all other staff;
 - staff in the employment of partners and service providers;
 - directors, business contacts, etc.



2. PRINCIPLES

2.1. LA MONDIALE EUROPARTNER: the business-specific context

The Company complies with the statutory provisions and with the recommendations and decisions of the data-protection supervisory authorities which it falls under (the Grand Duchy of Luxembourg national data-protection commission – CNPD).

We are attentive to the distinctive features of our business which require special conditions for applying the rules, particularly as regards:

- the processing of special data categories addressed by the regulations (particularly health data);
- the use of specific processes for sensitive or specially-protected data (e.g. tax identification number);
- the indirect collection of personal data;
- management of the confidential information of its customers and staff.

2.2. Fostering a sense of responsibility among the different parties involved

The Company institutes a scheme of organisation relying on the skills and accountability of the people involved in the processing of personal data. We foster awareness and provide training in data protection in order to enhance watchfulness and improve the knowledge of everyone concerned.

Directors, who are members of the Executive Committee, each as concerns his/her own remit and jointly for cross-functional processing, guarantee compliance of the processing operations with the rules for the protection of privacy and of the data of internal and external data subjects concerned by the activities they oversee.

2.3. Transparency

The Company adopts a fair and transparent approach to processing personal data. For this purpose, it provides information that is complete, clear and easily accessible regarding the processing it performs and the rights of data subjects over their personal data.

It refrains from disclosing data entrusted to it without previously informing or seeking the agreement of data subjects, except where it is obliged to make such disclosure by law.

It does not collect or process information concerning data subjects without their knowledge or for purposes incompatible with those for which the data was collected.

2.4. Proportionality of protection measures

The Company adopts a risk-based approach in measuring the risks affecting data subjects. This approach is used to identify appropriate, efficient organisational or technical measures for protecting personal data.



2.5. Support for the business lines

The Company has instituted an organisational scheme and means for supporting and advising the business lines to enable them to fulfil their objectives and develop initiatives while safeguarding the privacy of data subjects concerned by the processing they perform. Our commitment in this respect means that we can propose services suited to our customers in an environment of transparency and trust.

3. FRAMEWORK AND PRINCIPLES FOR PERSONAL DATA PROTECTION

The personal data processing performed by the Company is regulated by the General Data-Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, hereafter the “Regulation”) and by all legislation and/or regulations implementing these provisions.

The Company undertakes to perform only lawful processing grounded in the legal bases provided by the Regulation: the consent of the person concerned, the execution of a contract concluded with that person or the execution of pre-contractual measures taken at that person’s request, the fulfilment of a legal obligation or the legitimate interest pursued by the Company provided the processing does not infringe the rights of individuals.

The Company collects only the data necessary for legitimate, determined purposes, and provides comprehensive information to individuals on the use of and storage times for the data, and concerning their rights.

It safeguards data subjects’ rights over their personal data (right of access, rectification, deletion and portability) and as regards processing (the right of objection or limitation and the right not to be subject to automated decisions).

The Company institutes security measures that are duly proportionate to the sensitivity of the data, having regard to the nature of the processing and the risks incurred by individuals in the event of unavailability of the processing or of a breach of the integrity or confidentiality of the data. It factors these risks in from the process design stage onwards.

Where an external service is used to handle personal data, the Company chooses subcontractors providing sufficient assurances as regards the protection of personal data.

4. ROLES AND RESPONSIBILITIES

4.1. Data-protection function

4.1.1. Data Controller

The data controller is the legal entity determining the purpose and means of processing. This role is principally assumed by the Company, in connection with its operations or the staff it employs. However, the Company may act alone or jointly with other legal entities (see in particular Article 4.8 of this Policy Statement).



4.1.2. General Management

The Chief Executive Officer and all the members of the Executive Committee approve the Policy Statement. The Chief Executive Officer shall see to its implementation.

The CEO determines the respective responsibilities, under the powers delegated, for the material processing of personal data by the Company's departments.

The Chief Executive Officer appoints a data protection officer (hereafter, the "DPO" or "Data Protection Officer") and ensures that this official has sufficient resources to exercise his/her missions as prescribed by the regulations.

The Managing Director approves the personal data protection commitments made known to the data subjects concerned by the processing performed by the Company.

4.1.3. Processing implementation officer

Each Manager institutes within his/her remit the organisational scheme designed to guarantee that the processing of personal data is compliant with this Policy Statement. This is the person responsible for implementing processing covering the activities falling within his/her remit.

The processing implementation officer lies at the origin of the need warranting the introduction of processing. He/she guarantees the compliance of processing, the updating of the relevant documentation and the coordination of stakeholders involved in performing the processing. Implementing processing may involve the action of several stakeholders, particularly the following:

- the project manager or team leader: applies the Business Line management rules and performs operational execution of the processing;
- the Information Systems manager: implements the IT and technical design elements of data processing;
- the Management staff: conduct operations in accordance with the rules and procedures conducive to proper performance of the processing;
- the partner or subcontractor: executes all part of the processing on the Company's behalf.

4.1.4. Personal data protection local officer

Where justified by the nature of the activities and processes used, the processing implementation officer, in consultation with the Data Protection Officer, appoints a local officer to act for the latter in implementing the policy and procedures within his/her remit. The processing implementation officer affords the local officer the time and resources necessary for proper fulfilment of his/her duties.

An appointment of this kind is particularly useful for:

- the digital business scope which covers the data-related activities, governance and quality, customer experience, marketing, digital services and innovation all of which are much concerned with personal data protection;
- the IT Department, in view of the number of functions and individuals in that department that are involved in implementing personal data processing solutions;
- the Human Resources Department, which implements systems for managing information on the Company's staff.

The missions of the personal-data protection local officer and "business-specific data quality and practices" key person may be conferred upon a single person. Where these



missions are assigned to different persons, they shall cooperate where needed concerning the data of natural persons.

The contact details for the personal data protection local officers appointed pursuant to this Article shall be forwarded to the Data Protection Officer.

Role of the personal data protection local officer

The local officer possesses an overall vision of the activities and processes within his/her Department enabling him/her to:

- disseminate the data-protection principles and rules within his/her Department;
- foster awareness among the stakeholders within his/her Department of the personal data protection issues;
- provide a first level of response and advice on best practices in personal data protection within his/her Department;
- contribute to implementing data-protection measures;
- alert the Data Protection Officer (DPO) and the processing implementation officer in the event of any non-compliance with the personal data protection rules and/or measures.

4.1.5. Data Protection Officer (DPO)

With regard to data processing operations and the number and nature of personal data items that are to be collected and processed by the Company, the appointment of a Personal-Data Protection Officer is required.

Data Protection Officer's duties

The scope of this Officer's functions is laid down by the Regulation, which provides that:

- he/she is involved appropriately and in a timely fashion in all issues relating to personal data protection;
- he/she is supplied with the resources necessary to carry out his missions and to keep his/her knowledge up to date;
- he/she may access the data and processes;
- he/she receives no instructions concerning the exercise of his missions and cannot be relieved of his duties or penalised for the exercise of his missions;
- he/she reports directly to management;
- he/she may be contacted directly by the data subjects concerned by the processing;
- he/she is required to observe professional secrecy or is bound by a confidentiality obligation as regards the exercise of his missions;
- he/she may not exercise any other missions or tasks that may generate a conflict of interest.

Data Protection Officer's missions

The regulations also lay down a mission remit which takes the following form in our Company:

- √ Informative and advisory missions:

The Data Protection Officer (DPO), supported by the IT Department (as concerns the



issues of Information Systems compliance), the Communication Department and the Human Resources Department, contributes to instituting information campaigns, raising awareness, and training Company staff in order to foster a personal data protection culture and enable the acquisition of specific skills required in the activities in which they are relevant.

The Data Protection Officer advises the Departments, officers and relevant stakeholders within Information Systems on the implementation of personal data processing, whether for projects to upgrade the IT systems or for operations of all kinds involving the collection, transfer, storage or use of personal data. Within this remit, the Data Protection Officer makes all recommendations to Information Systems stakeholders with the aim of achieving a higher standard of legal compliance for processing impacting personal data.

He/she conducts, or performs an advisory role in, impact analyses relating to personal data protection.

√ Supervisory missions:

He/she monitors the implementation of personal data protection regulatory provisions by the Company and its subcontractors [processors], particularly by relying on the existing internal-control function.

He/she is authorised to take all initiatives for conducting checks, and the departments under supervision cooperate in their performance. He/she reports the findings from these checks to the managers concerned and to General Management.

√ Missions as contact person to the supervisory authority:

The DPO is designated to the supervisory authority with which he/she cooperates; he/she is that authority's contact, including for consultations prior to performing processing that entails risk to data subjects.

He/she receives and investigates complaints from data subjects relating to any processing of personal data and cooperates with the CNPD in investigating and following up complaints referred to the Authority.

4.2. Governance and data-quality function

The general data policy defined for the Company applies to personal data. The Chief Data Officer (CDO) in charge of implementing this policy is responsible for data quality and governance. Accordingly, he/she factors the compliance requirements specific to personal data into the organisational scheme he/she implements.

The Data Protection Officer is involved in the work supervised by the CDO where it is of relevance to personal data, and he attends any steering bodies, committees or groups set up to oversee the systems for data quality and governance.

The Data Protection Officer informs the CDO of changes in the regulations and recommendations issued by the supervisory authority, and of any project or initiative may have a bearing on data governance.



4.3. IT systems function

This function is tasked with developing, integrating and operating the automated processing systems. It is under the responsibility of the Information Systems Department, and it designs and implements an organisational scheme and IT solutions, whether internal or subcontracted, that are compliant with the principles and requirements of the regulations and of this Policy Statement, namely:

- the risk-based approach and the factoring-in of risks to privacy and personal data upstream of projects and when making decisions over solutions;
- the use of design and development methods that adhere to the principles of privacy by design;
- the definition and implementation of methods and solutions for development and operation that adhere by default to the primacy of privacy for data subjects whose data is managed (privacy by default);
- the implementation of organisational and technical solutions to assure appropriate standards of security and availability, and to safeguard the rights in personal data (right of access, objection, deletion, portability and limitation);
- compliance with the rules governing data transfers outside the European Union.

4.4. Security function

The Company implements security and continuity policies and procedures that guarantee the availability, integrity and confidentiality of personal data.

The Information Systems Department supervises the implementation of these measures. Basing itself on risk analyses, it makes security measures proportionate to the degree of sensitivity of the processing by reference to the threats to which data subjects would be exposed in the event of a breach of data confidentiality.

That Department periodically reassesses the effectiveness of the measures applied and adapts them to take account of the changing pattern of risks and the latest data-protection developments.

It oversees both measurements of the impact on privacy and the management of security incidents, particularly where personal data breaches are notified.

4.5. Legal function

The Legal Department assures the security of the Company's commitments to protection of personal data through the drafting and validation of contracts, agreements and informative material.

That Department advises the DPO on managing claims and complaints, and in dealings with the CNPD.

The Legal Department handles disputes and litigation arising from the application of the regulations. In this context, it handles relations with the legal professions and represents our interests before the courts of law and the CNPD in the event of proceedings that may lead to sanctions.



4.6. Risk-management, internal-control and compliance function

The management of risks to personal data is aligned with the policy and falls within the scheme of organisation for managing the Company's operating risks and for its compliance.

The Data Protection Officer reports to the Risk Management Committee on the management of these risks. For purposes of personal data protection, risk management is designed to gauge the risks incurred to the privacy of data subjects.

The Company's internal controllers and the operating risk officers (CRO) survey and measure the risks and monitor the implementation of risk-abatement actions; those officials report on the management of risks, as well as declaring and investigating related incidents. They take part in analyses of privacy impacts conducted in accordance with the regulations for risk-bearing processing.

The risk-management scheme for personal data protection also falls under management of the non-compliance risk, in coordination with the Company's compliance function.

4.7. Internal Audit function

The internal audit team interviews the Data Protection Officer annually. That team includes in its audit programme tasks designed to gauge personal data protection within the Company.

4.8. Joint data controllers and processors

Where the Company jointly determines the processing purposes and means jointly with another Data Controller, they have joint responsibility for processing. In these circumstances, the Company institutes agreements providing transparent definition of the respective obligations of the parties in order to ensure compliance with regulatory requirements, with particular reference to the exercise of the data subject's rights, as well as defining the parties' respective obligations to disclose information of which data subjects must be made aware.

When the Company needs to outsource processing, it has exclusive recourse to processors providing sufficient assurances that appropriate technical and organisational measures are deployed to ensure that the processing meets the requirements of the Regulation and of this Policy Statement, and safeguards the data subject's rights.

5. GOVERNANCE AND REPORTING

5.1. Personal data protection committee

The Company puts in place a monitoring and exchange forum focusing on personal data protection.



Participants:

- The member of the Management Committee tasked with the protection of personal data;
- Data Protection Officer;
- Chief Risk and Actuarial Officer;
- Chief Data Officer (CDO) or the latter's key person;
- Chief Legal Officer;
- Chief Processing Implementation Officers;
- IT Director.

Frequency:

Half-yearly

Purpose:

- Describing and sharing the overall state of personal data protection within the Company (presenting relevant indicators);
- Acquainting themselves with audit and control findings, and monitoring the implementation of actions designed for improvement;
- Monitoring the training plan and awareness-raising actions.

Reports of these activities are submitted at the meetings of the Management Committee and Risk Management Committee.

6. GLOSSARY

Personal data: any data relating to an identified or identifiable natural person (hereafter termed a "data subject"). An "identifiable natural person" is deemed to denote any natural person who can be identified directly or indirectly, particularly by reference to an identifier such as a name, an identification number, location data, an on-line identifier or one or more specific elements inherent in that person's physical, physiological, genetic, psychic, economic, cultural or social identity.

Sensitive data: any data concerning racial or ethnic origin, political opinions, religious or philosophical convictions or trade-union membership, and also genetic or biometric data, or data concerning health or sex life are considered sensitive data.

Processing: any operation or set of operations performed or not performed using automated processes and applied to personal data or data sets, such as collection, recording, organisation, structuring, storage, adaptation or modification, extraction, consultation, use, disclosure by transmission, dissemination or any other means for making data available, matching or interconnection, limitation, erasure or destruction.

Data Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing. Where the purposes and means of such processing are determined by European Union or Member State legislation, the data controller may be appointed, or the specific criteria for to its appointment may be provided, by European Union or Member State legislation.



Processor: the natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

Recipient: the natural person or entity, public authority, agency or other body to which personal data are disclosed, regardless of whether the recipient is a third party. However, public authorities to which personal data may be disclosed in connection with a special enquiry mission compliant with European Union law or the law of a Member State are not considered to be recipients; the processing of such data by the public authorities in question complies with the rules applicable for data protection taking account of the purpose of the processing.

Personal data breach: 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.

Supervisory authority: an independent public authority instituted by a Member State; for Luxembourg, this authority is the national data-protection commission (CNPD).

Profiling: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

