POLICY REGARDING THE PROTECTION AND ENHANCEMENT OF PERSONAL DATA

Disclaimer English Translation

Note that this document represents an English translation of the original version " POLITICA IN MATERIA DI PROTEZIONE E VALORIZZAZIONE DEI DATI PERSONALI," originally issued in Italian. The accuracy and conceptual consistency of the English version of this document maynot be ensured. In case of any discrepancies or doubts in the interpretation of the document, official reference must be made to the Italian-language version

[Bologna, 9 november2023]

[Version submitted for examination by the Board of Directors]

[PAGE INTENTIONALLY LEFT BLANK]

Index

1 Introduction

1.1 Document objectives

The Policy on the protection and enhancement of Personal Data (the " ***Data Protection*** **Policy** " or the " **Policy** ") has the objective of defining the general guidelines of the Unipol Group (the " **Group** ") regarding the protection of natural persons with regard to the processing of Personal Data (as defined *below*).

The Policy therefore establishes, with regard to the need to protect Personal Data as part of the Processing carried out by the Group Companies in scope referred to in paragraph 2.2 (the "Companies within the scope "): the Organizational Model (organization and roles, people, culture and skills);

- the Operating Model (processes and rules and documentation);
- the Architectural Model (Personal Data, technologies and tools).

The Policy also consists of an annex which defines the commitments undertaken by the Group - in relation to the specific business model of Unipol and the Companies in scope - towards its customers and all stakeholders, ensuring that the protection granted to the Personal Data available to the Companies in scope is supported by a growing enhancement activity. By "enhancement" of Personal Data, we mean the promotion, development, and enrichment activity of the Group's information assets for the purpose of creating shared value, which should be kept distinct from the "protection" of Personal Data, which has a conservative nature and is aimed at protecting the data subjects from risks to their rights and freedoms.

It should be noted that, unless otherwise specified, the Bodies/Departments/Directorates/Functions mentioned in the Policy refer to those of UnipolSai Assicurazioni S.p.A. ("UnipolSai"), or to the equivalent Bodies/Departments/Directorates/Functions, where present, of the other Companies in scope, even if outsourced.

1.2 Approval and revision of the document

This Policy, drafted/revised with the involvement of all the company structures concerned in order to ensure a clear definition and sharing of objectives, roles and responsibilities, has been approved by the Board of Directors of the Parent Company Unipol Gruppo S.p.A. (" **Unipol** " or the " **Parent Company** "), also in its capacity as Parent Company , in the exercise of its management and coordination activity towards the subsidiaries and in coherence with the Group corporate process regarding the preparation and validation of corporate policies.

Subsequently, the Boards of Directors of the other companies in scope, as part of their responsibilities in terms of *governance* , internal control system and risk management, evaluate and approve the Policy, as applicable, in accordance with their *business model.* .

The Policy will be reviewed and - if necessary - modified whenever there is a need for regulatory updating, interventions by the Supervisory Authority, *business strategies* or changes in the context (significant changes to business processes, significant structural reorganisations, significant changes to the IT platforms used) request it.

The Policy is communicated and made available by the Companies in scope to all interested personnel through adequate communication channels.

2 Reference context

2.1 Regulatoy Reference

On 24 May 2016, Regulation (EU) 2016/679 of the European Parliament and of 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 (the " **GDPR** ") entered into force. It has been directly applicable in all Member States from 25 May 2018.[1]

The GDPR applies to the Processing of Personal Data carried out by (i) companies established in the European Union (whether the Processing takes place in the EU or not), as well as (ii) companies established outside the European Union that offer goods or services to Data Subjects who "are located" in the European Union and/or monitor their behavior within the European Union.

The protection of Personal Data is, to date, regulated in Italy (i) by the GDPR, (ii) by the *Privacy Code* (as defined [2]*below*), as well as (iii) by the Provisions and Guidelines of the Italian Data Protection Authority (as defined *below*) on its direct initiative or in reference to complaints, reports, requests for opinions, presented by citizens, companies, associations,entities [3].

Furthermore, the Working Group established pursuant to art. 29 of Directive 95/46/EC (the " **WP29** ", defined *below*), replaced by the **European Data Protection Committee** , has issued guidelines and guidance documents on the protection of Personal Data in order to provide recommendations and clarifications on application regarding certain provisions of the GDPR.

This Policy is also consistent with and supplements the self-regulation system in force in the Group [4].

2.2 Scope of application

This Policy applies to the Parent Company and to the Group companies under its control with registered offices in Italy (the "Companies in scope"). The Group companies with registered offices in other EU countries adopt their own Personal Data protection policy consistent with this Policy.

2.3 Definitions and terminology

Top Management	The Chief Executive Officer, and/or the General Manager (where appointed)and, with reference to Unipol and the insurance companies of the Group based in Italy, the senior management who carry out management superintendence tasks (i.e. the Managers with strategic responsibilities identified for the purposes of applying the supervisory regulations regarding intragroup operations).
Other Companies	Group subsidiaries with registered office in Italy, other than Arca Vita SpA (" Arca **Vita** ") and its Italian subsidiaries , which have not entered into a

[1] The GDPR repealed previous regulations on this subject, i.e. Directive 95/46/EC of 24 October 1995, "on the protection of individuals with regard to the processing of personal data and on the free movement of such data"; as a result, national regulations issued in application of this Directive also had to be amended, at least in parts that conflicted with the GDPR

[2] The Privacy Code was revised with Legislative Decree 10 August 2018, n. 101, implementing the art. 13 of the Delegation Law of 25 October 2017, n. 163. Legislative Decree 10 August 2018, n. 101 repealed the parts of the Code in conflict with the GDPR.

[3] The provisions contained in Provisions of the Data Protection Authority issued before 25 May 2018 which are not in conflict with the provisions of the GDPR have remained in force, sometimes through new provisions aimed at expressly clarifying the provisions compatible with the new regulatory framework.

[4] In particular, the Policy is integrated by the Group Policy on *Data Governance* , the Information Security Policy and the Sustainability Policy .

	service agreement with the Privacy Function
Area Risk	The fundamental Risk Management function of Unipol and UnipolSai, as well as the similar functions of the other companies within the perimeter, even if outsourced.
Audit	The fundamental Audit function of Unipol and UnipolSai, as well as the similar functions of the other companies within the perimeter, even if outsourced.
Supervisory Authority or Data Protection Authority	The Italian Supervisory Authority for the protection of personal data.
Special categories of Personal Data	Personal data (as defined below) that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. Genetic data, biometric data intended to uniquely identify a natural person, data relating to health as well as data revealing the person's sexual orientation are also considered to belong to this category.
***Privacy* Code**	Legislative Decree 30 June 2003, n. 196 " *Code regarding the protection of personal data* " as amended by the legislative decree of 10 August 2018, n. 101, containing " *Provisions for the adaptation of national legislation to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016* ".
European Data Protection Board (*European Data Protection Board* o EDPB)	The European Data Protection Board (EDPB) replaces the WP29 (or Article 29 Working Party on Data Protection). It is established under Article 68 of the GDPR and is composed of the head of a supervisory authority from each Member State and the European Data Protection Supervisor, or their respective representatives.
Compliance and Anti-Money Laundering	For the scope of compliance activities, the fundamental Compliance function of Unipol and UnipolSai, as well as the similar structures of the other Companies in scope, even if outsourced. For the scope of anti-money laundering activities, the function referred to in (i) Chapter II of IVASS Regulation no. 44 of 12 February 2019 or (ii) Chapter II of the Bank of Italy Provision of 26 March 2019 of Unipol and UnipolSai, as well as the similar structures of the other companies within the perimeter, even if outsourced.
Consent of the Data Subject	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.(art. 4 GDPR)
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. (art. 4 GDPR)
Common data	Personal Data other than data belonging to the Special Categories of Personal Data (as defined) and Personal Data relating to criminal

	convictions and offences. They are data with a level of criticality that tends to be lower than the risks to the rights and freedoms of the interested parties. By way of example: personal data, contact details, bank references, contractual, work, salary data, other Personal Data that can be traced back to the person such as, for example, the vehicle license plate number, etc.
Personal Data	Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (*cfr*. art. 4 del GDPR).
Privacy Officer	The Chief Executive Officer, the General Manager (if the Chief Executive Officer is not present), or in the absence of the Chief Executive Officer/General Manager, the person identified by the Board of Directors and vested with the necessary powers; this officer is appointed by the Board of Directors to supervise the implementation of the guidelines defined by the Board of Directors, overseeing the planning, implementation and management of the internal control and privacy risk management system and constantly verifying its adequacy and effectiveness.
DPIA or *Data Protection Impact Assessment*	Impact assessment on the protection of Personal Data.
DPO or Group DPO or *Data Protection Officer*	Unipol Gruppo has established a Group DPO, which carries out the relevant activities for Unipol and for the other Companies in scope, according to a *risk-based approach*. Subsidiaries with registered office in another European Union country appoint their own DPO, where necessary or deemed appropriate, who coordinates with the Group DPO on issues of general relevance.
GDPR (*General Data Protection Regulation*)	European Union Regulation 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation).
Unipol Group (or Group)	Unipol Gruppo SpA and its subsidiaries.
Authorized Persons	Natural persons authorized to carry out Processing operations by the Data Controller or Processor. Each employee of each Company within the perimeter s an Authorized person for the Processing of Personal Data.
Data Subject	The identified or identifiable natural person to whom the Personal Data refers.

Model for the protection of Personal Data	Set of organisational, management/operational and technological choices made by the Group to ensure adequate protection of the Personal Data processed by the Parent Company and its subsidiaries.
Regular and systematic monitoring	"Regular" refers to monitoring activity that takes place continuously or at set intervals for a specific period of time; recurring or repeated at constant intervals; or that takes place on a constant basis or at regular intervals. "Systematic" refers to monitoring activities that are managed by the system; predefined, organised or methodical; which takes place as part of an overall data collection plan; carried out as part of a strategy. For example, the following are activities that can involve regular and systematic monitoring of Data Subjects: the provision of telecommunications services; marketing activities on the analysis of data collected; profiling and scoring; location tracking; loyalty programmes; etc
***Privacy* Regulation**	The GDPR, the *Privacy Code,* the Provisions of the Data Protection Authority and in general all external legislation regarding the protection of natural persons with regard to the processing of Personal Data.
Privacy Lab	A dedicated portal on the Group *intranet aimed at disseminating privacy-related matters* to all internal and external subjects (employees, agents and their collaborators). It contains, for example, the documentation on the *Privacy Regulations* , the information and consent models in force, the documentation relating to *privacy issues* for some specific sectors of the Group ,for the agency network, etc.
Process Owner	The Chief/Director or, if not present, the acting Manager of the Area/Department/Function responsible for the Processing, or appointed delegate.
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 .(art. 4 del GDPR).
Privacy Contact	An Internal role in the Areas/Departments/Functions of UnipolSai Assicurazioni and the Companies in service (as defined) which, as part of his/her responsibilities, provides support to the Process Owner on all matters related to application of the Privacy Regulations, as well as for the effective governance of privacy risk. With reference to UnipolSai, this means the Privacy Contact designated in the main company Areas/Departments/Functions. For the Companies in service, it refers to the designated Privacy Contact for each Company. The Privacy Contact cannot be the same as the Privacy Officer, who, within

	its own attributions, designates the Privacy Contact and oversees its work.
Data Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller. The Data Processor is a third party (i.e. service provider) that performs one or more Personal Data Processes for which the Company in scope is the Data Controller. Insurance intermediaries, operating on behalf of the Group pursuant to art. 109, paragraph 2, letters "a", "d" and "f" "of the Private Insurance Code, are considered Data Processors.
Privacy *risk*	As part of non-compliance risk, it is the risk of incurring judicial or administrative sanctions, financial losses, or reputational damage as a result of the violation of Privacy Regulations.
ICT	Set of ICT systems used for business processes involving the reception, storage, processing, transmission, and use of data (e.g., application software, email).
Company *in service*	Group subsidiaries that have entered into a service agreement with the Privacy Function of UnipolSai.
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 the Processing of Personal Data. Each Company within the scope is a Data Controller of Personal Data and must designate a Privacy Officer (as defined) to oversee the correct application of Privacy Regulation.
Processing	Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination otherwise making available, alignment or combination, restriction, erasure or destruction. (art. 4 del GDPR).
Large-scale treatment	Processing of a significant amount of Personal Data at a regional, national or supranational level and which could affect a large number of Data Subjects and which potentially presents a high risk [5].

[5] L'EDPB, in order to establish whether processing is carried out on a large scale, recommends taking into account the following factors: the number of subjects affected by the processing, in absolute terms or expressed as a percentage of the reference population; the volume of data and/or the different types of data being processed; the duration, or persistence, of the Processing activity; the geographical scope of the Processing activity.

3 Guidelines on personal data protection

3.1 Introduction

The GDPR required a real change in philosophy: a formalistic system was abandoned, based on formal rules, analytically defined obligations and clearly outlined minimum security measures, in favor of a Personal Data governance system based on a high degree of accountability of the Data Controller, who must guarantee and be able to demonstrate compliance with the GDPR. This burden of proof consists in the adoption of technical and organisational measures whose adequacy must be assessed on the basis of the specific characteristics of the Personal Data Processing (nature, scope, context and purpose of the Processing), as well as the risks to the rights and freedoms of the Data Subjects (Articles 5 and 24 of the GDPR).

The GDPR has introduced important innovations regarding the protection of Personal Data; however, some provisions already envisaged in previous legislation have been confirmed . Below is a summary of the aspects (i) unchanged or marginally changed and (ii) new, compared to the previous regulations.

Figure 1: Provisions unchanged or marginally changed and New provisions

3.2 Provisions unchanged or changed marginally

Below are the main regulatory obligations that have remained unchanged, with particular attention to those that have changed only marginally; with reference to the description of the newly introduced aspects, see paragraphs 3.3 and 3.4 below.

Principles applicable to the Processing of Personal Data

The definitions and general principles established by the previous legislation remain substantially unchanged.

Personal Data are:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency”);

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (“purpose limitation”);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”);
- 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 (“accuracy”);
- 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 (“storage limitation”);
- processed in a manner 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 (“integrity and confidentiality”).

Privacy Policy

The general rules regarding the Privacy policy to be provided to Data Subjects, envisaged in previous regulations, have been substantially confirmed. Expanded content of the Privacy Policy is envisaged (ref. paragraph 3.4.2.2), establishing, in particular, that the Data Controller adopts appropriate measures to provide the Data Subject with information and communications also related to exercise of their rights in concise, transparent, intelligible and easily accessible form, using simple and clear language and as suited as possible to the reference recipients so that they are easily understandable, especially when the information is specifically addressed to minors. The information may be provided in writing or by other means, including electronically.

Consent and other legal bases legitimizing the processing

Express consent of the Data Subject to the Processing of their data for one or more specific purposes, to ensure lawfulness of the Processing , it must be, in all cases, free, specific, informed and unequivocal; tacit or presumed consent is not permitted.

Processing is also lawful if it is necessary to: (i) 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, (ii) compliance with a legal obligation to which the controller is subject, (iii) protect the vital interests of the data subject or of another natural person, (iv) the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, (v) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data).

Rights of Data Subjects

With the exception of the new rights introduced (e.g. right to portability, etc.), the GDPR confirms the rights of the Data Subjects already provided for by the previous legislation, such as: right of access, right of rectification and right of opposition (ref. par. 3.4.2.4).

Authorized Persons

Authorized Persons is no longer expressly envisaged in the GDPR, however the Data Protection Authority has specified[6] that this is compatible with the role of the person authorised to perform processing

3.3 New provisions

In addition to the substantial reversal of perspective referred to in the Introduction, the GDPR has also introduced some new features:

- ***Data Protection Officer (DPO)*** (Articles 37-39) - The DPO is one of the main innovations of the GDPR and constitutes one of the key elements of governance of the Personal Data Protection Model (as defined). Its designation aims to facilitate implementation of the GDPR by the Data Controller or Processor and is mandatory in some cases (ref. paragraphs 2.3 and 3.4.1.5);
- **Record of processing activities** (Art. 30) - The GDPR has introduced the obligation to set up and update a Record of processing activities, by the Data Controller in reference to the Processing activities carried out under its responsibility, and by the Data Processor for the processing activities carried out on behalf of each Data Controller, unless derogations for specific situations are met (ref. paragraph 3.4.2.8);
- ***Data Protection by Design*** (Art. 25, par. 1) - The GDPR has established that, prior to the start of new Processing or modification of existing Processing, the Controller implements measures that satisfy the personal data protection principles (ref. par. 3.4.2.5);
- ***Data Protection by Default*** (Art. 25, par. 2) - The GDPR has established that the Data Controller must implement adequate technical and organisational measures to ensure that, by default, only the Personal Data specifically required for the Processing are actually processed (ref. paragraph 3.4.2.5);
- ***Data Protection Impact Assessment*** **(DPIA)** (Art. 35) - The GDPR requires that, if Processing presents a high risk to the rights and freedoms of Data Subjects, before starting the Processing, the Data Controller must carry out a preliminary assessment of the impact on personal Data Protection (ref. paragraph 3.4.2.6);
- **Notification of a personal *Data Breach*** (Articles 33 and 34) - The GDPR has introduced the obligation to notify the supervisory authorities, without undue delay (and, where possible, within 72 hours), of any personal data breaches, while also communicating them without undue delay to the Data Subjects whenever a high risk to their rights and freedoms (ref. paragraph 3.4.2.10);
- **New rights of** Data Subjects (Articles 17, 18, 20 and 22) - The GDPR has strengthened the right to erasure ("right to be forgotten") and introduced the right to limitation of the Processing, the right to data portability, as well as the right not to be subjected to a decision based solely on automated Processing, including Profiling (ref. paragraph 3.4.2.4);
- **Data Processor** (Art. 28) - Compared to previous regulations, the GDPR has identified specific obligations and responsibilities also attributable directly to Data Processors. For example, they may receive requests from the Data Protection Authority, must implement technical and organisational measures to ensure a level of security appropriate to the risk, are directly liable subject to administrative sanctions and are liable for damage caused by the Processing not only

[6] n the "Guide to application of the European Regulation on the protection of personal data" published on the Data Protection Authority website, it states that although it does not expressly envisage the role of "processor representative" for the Processing (pursuant to art. 30 of the Privacy Code, repealed by the amendments introduced by Legislative Decree no. 101 of 10 August 2018), the GDPR does not rule out its presence as it refers to "persons who, under the direct authority of the data controller or processor, are authorised to process personal data

if they have failed to comply with Data Controller instructions, but also if they have failed to meet obligations specifically required of them by the GDPR. The Data Processor may also use sub-processors with the written consent of the Data Controller, imposing on the sub-processor, by contract or other legal document, the same obligations to which the Data Processor is subject (ref. paragraph 3.4. 2.7);

- **Security of Processing** (Art. 32) - Compared to the previous regulations, the GDPR has confirmed the relevance of data security obligations, no longer considering "minimum" security measures, but now requiring that the Data Controller and Data Processor adopt technical and organisational measures appropriate to the risk involved. To assess the adequacy of the measures, the Data Controller and the Data Processor must therefore analyse the risks[7] deriving from the type of Processing they intend to carry out, also in light of the classification of the Personal Data and possible consequences for the rights and freedom of the Data Subjects (ref. par. 3.4.2.9);
- **Certification** (Articles 42 and 43) - The GDPR has introduced the right to request recognition of GDPR compliance through certification mechanisms or data protection stamps and markings;
- **Extent of sanctions** (Art. 83) - The GDPR has significantly increased the maximum amount of sanctions, envisaging the option for the Data Protection Authority to impose administrative fines of up to €10,000,000 or, for companies, if higher, up to 2% of the annual global turnover, or up to €20,000,000 or, for companies, if higher, up to 4% of the annual global turnover, depending on the provisions violated.

[7] Risk to the rights and freedoms of the Data Subject, deriving from the destruction, loss, modification, unauthorised disclosure or accidental or unlawful access to Personal Data transmitted, stored or otherwise processed.

3.4 Model for the protection of Personal Data

In the aforementioned regulatory context that requires the Data Controller to plan, implement and demonstrate that it has adopted adequate technical and organizational measures, the Group has defined the Model for the protection of Personal Data.

In particular, the Model adopted by the Group consists of (i) an organizational model, (ii) an operational model and (iii) an architectural model.

Components	Areas covered
Organisational model	– **organization and roles** , i.e. the set of structures, bodies and roles involved in the direction and governance, execution and control of the Model for the Protection of Personal Data; – **people, culture and skills** , i.e. the set of internal and external resources involved in the Model for the Protection of Personal Data.
Operative model	– **processes and rules** , i.e. the set of internal company and Group-level provisions that guarantee compliance with the *Privacy Legislation* ; – **documentation** , i.e. the set of documents to be followed or adopted as part of processes and rules linked, directly or indirectly, to the protection of Personal Data.
Architectural model	– **Personal Data** , i.e. the set of Personal Data processed as part of company processes, both *staff* and *business-related*, on which decisions related to the Model for the Protection of Personal Data are based; – **technology and tools** , i.e. the set of application services that process Personal Data and the security, logical and physical measures adopted by the Group, broken down into prevention measures and protection measures.

See the following paragraphs for a detailed description of each element of the Model for the Protection of Personal Data.

3.4.1 Organizational model for the protection of Personal Data

In order to achieve effective monitoring of the protection of Personal Data, the Parent Company and the Companies in scope need to adopt a clear and consistent governance process

The Group has defined roles and responsibilities, both at Parent Company and subsidiary level which guarantee guidance, governance, execution and control of the Model for the protection of Personal Data.

Area	Objective	Structures, committees and roles
Guidance and government	Ensure definition of the Model for the Protection of Personal Data, promoting its communication and correct implementation in compliance with Privacy Regulations.	– Board of Directors
Execution	Ensure implementation of the Model for the Protection of Personal Data defined, not only in compliance with the provisions of Privacy Regulations, but also with internal Group provisions.	– *Privacy* Officer – Top Management – *Process Owner* – *Privacy* Contacts – *Privacy* function – Arca Vita Purchasing Quality, Security and DPO Support Function for the latter and its Italian subsidiaries – Data processors – Authorized persons – *Teams* entrusted with specific roles in company procedures (e.g. *Task Force Data Breach*) – Area *Information* – Real Estate Management
Control	Identify, assess, manage and monitor compliance risks relating to Privacy Regulations and self-regulation rules.	– DPO[8] – Compliance function and Anti-Money Laundering – Risk Area – Audit function

The tasks and responsibilities of the Model for the protection of Personal Data are defined below .

[8] The DPO also carries out informative and consultative functions (ref. par. 3.4.1.5).

3.4.1.1 Board of Directors

The Board of Directors of each Company within the scope is ultimate responsible for the internal control and management system that handles *privacy risk* and ensures its constant completeness, operational efficiency and effectiveness, also for outsourced activities.

The Board of Directors of the Parent Company appoints a single Group DPO for Unipol and for the other Companies in scope, providing him/her with the resources necessary to carry out the tasks assigned (ref. par. 3.4.1.5), according to a *risk-based* approach .

For these purposes, as part of its strategic and organizational tasks, the Board of Directors of the Parent Company:

- approves this Policy and its subsequent amendments, following assessment by the Group Risk Committee;
- approves the organizational structure and the assignment of tasks and responsibilities for managing privacy risk;
- verifies that Top Management correctly implements the internal control and privacy risk management system in accordance with the directives issued and assesses its operational efficiency and adequacy;
- appoints the Privacy Officer ;
- receives an annual report from the DPO containing: (i) an assessment of the adequacy and effectiveness of controls implemented by the company to manage *privacy risk* , on activities performed, checks carried out, results that emerged and critical issues identified , providing an account of the implementation status of the related improvement actions, if implemented and (ii) a plan of activities which, according to a risk-based approach, indicates the verification actions considered most urgent with regard to *privacy risk* [9];
- ensures that the DPO is promptly and adequately involved in all matters relating to the protection of Personal Data;
- guarantees the resources necessary for the DPO to carry out his duties and access the Personal Data and Data Processes, and to update its specialist knowledge;
- ensures that any additional tasks and functions carried out by the DPO do not give rise to a conflict of interest.

The Boards of Directors of the other Companies in scope, within their own companies and for aspects applying to them, perform the same tasks as the Board of Directors of the Parent Company.

3.4.1.2 Top Management

Top Management implements, maintains and monitors the privacy risk internal control and management system based on indications of the Privacy Officer.

[9] The DPO's Report prepared for the Board of Directors of the Parent Company describes the activities carried out by the DPO, according to a *risk-based approach,* with reference both to Unipol and to the other Companies in scope. In addition, details of the alignment activities with the Group Companies with registered offices in Ireland are also provided.

3.4.1.3 Control and Risk Committee

The Control and Risk Committee of the Parent Company [10]and UnipolSai provide support functions to their respective Boards of Directors in identifying and managing the main corporate risks and in checking to ensure that they are correctly identified, appropriately measured, managed and monitored, and their compatibility with business management that constantly strives to achieve the planned strategic objectives.

In particular, both the Control and Risk Committees review and make proposals regarding this Policy and subsequent amendments. Additionally, they receive from the Group DPO the annual report as described in point 3.4.1.1, and they review it in advance of the Board of Directors.

3.4.1.4 Group Risk Committee

The Group Risk Committee, as part of its consultative function in support del General Director of the Parent Company, examines the proposals regarding the Policy and subsequent amendments.

3.4.1.5 *Data Protection Officer* (DPO)

The DPO is appointed based on his specialized knowledge of the regulations and practices regarding the protection of Personal Data, his professional expertise, ability to carry out the aforementioned tasks, as well as his autonomous and independent position; the DPO is allowed to perform other duties and functions provided that no conflicts of interest arise as a result.

The main duties of the DPO consist in informing and providing advice to the Data Controller, Processors and Authorized persons, as well as to supervising compliance with the *Privacy Regulations* and Group internal provisions on the protection of Personal Data, including the assignment of responsibilities, raising awareness and training of personnel involved in the Processing and related control activities.

As part of his control tasks, the DPO :

- Monitors and provides consultancy regarding applicable privacy regulations to the Process Owners and their respective Privacy Contacts, activating where necessary in accordance with the Group's regulatory monitoring and compliance adjustment process.
- identifies, also making use of the collaboration of the Compliance Function and Anti-Money Laundering, the Processes most exposed to the privacy risk;
- submits an annual report to the Board of Directors once a year containing: (i) an assessment of the adequacy and effectiveness of the controls implemented by the company to manage privacy risk, on the activities performed, checks carried out, results obtained and critical issues identified, providing an account of the implementation status of the related improvement actions, if implemented, and (ii) a plan of activities which, according to a risk-based approach, indicates the verification actions considered most urgent with regard to privacy risk. The action planning takes into account gaps identified in previous checks and any new risks;
- evaluates the internal control and risk management system in the *privacy area* also making use of the collaboration of the Compliance Function and Anti-Money Laundering, the Audit Function and the Risk Area;

[10] Pursuant to IVASS Regulation no. 38 of 3 July 2018, the Control and Risk Committee of the Parent Company also operates on behalf of the Group Companies with "strengthened" (excluding UnipolSai) and "ordinary" corporate governance.

- monitors the implementation of any adjustments defined, in accordance with company procedures in force (ref. paragraphs 3.4.2.5 and 3.4.2.6), regarding new Data Processing or the amendment of existing Data Processing;
- monitors the keeping of the Record of processing activities (ref. paragraph 3.4.2.8).

In addition, the DPO :

- cooperates with the Data Protection Authority and acts as a contact point for matters related to the Processing of Personal Data, and when necessary, where appropriate, is consulted on any other matter;
- acts as a point of contact for Data Subjects for all matters relating to the Processing of their Personal Data and the exercise of their rights;
- provides opinions and carries out other activities under its responsibility, based on company procedures in force, as part of the processes to definine the storage terms of of Personal Data (ref. par. 3.4.2.3), assessment and notification of a *Data Breach* (ref. par. 3.4.2.10) and the performance of a DPIA (ref. par. 3.4.2.6).

3.4.1.6 Privacy Function (and Arca Vita's Purchasing Quality, Security and DPO Support Function for the latter and its Italian subsidiaries)

Functions that support, to the extent of their competence, the DPO in performing the assigned tasks and also provide support in defining and implementing any necessary actions/measures.

3.4.1.7 *Privacy* Officer

The Privacy Officer :

- implements the guidelines specified by the Board of Directors, overseeing the planning, implementation and management of the internal privacy control and risk management system, and constantly verifying its adequacy and effectiveness;
- ensures alignment of the system to changes in operating conditions and to legal and regulatory measures;
- designates the Privacy Contact Person, who cannot be the same as the Privacy Officer himself;
- ensures that the Board of Directors is regularly informed on the effectiveness and adequacy of the internal privacy control and risk management system and in any event promptly whenever any significant critical issues are detected;
- promptly notifies any Personal Data Breach to the Data Protection Authority and, if necessary, communication to the Data Subjects, after obtaining the opinion of the Group DPO (ref. paragraph 3.4.2.10)

3.4.1.8 *Process Owner*

The Process Owner coordinates the Personal Data Processing operations carried out within the context of their assigned role and oversees privacy risk in the area under its responsibility, also with the support of the Privacy Contact.

The Process Owner:

- identifies the methods to be adopted in its area of responsibility so that the Processing of Personal Data takes place in full compliance with the provisions of Privacy Regulations and the Group's internal provisions, with particular reference to the principles of lawfulness, fairness and transparency, data minimisation, accuracy, limitation on storage, integrity and confidentiality;

- identifies the methods to be adopted so that the Personal Data collection takes place with prior communication to the Data Subject of the information required by the GDPR and the acquisition, where necessary, of the Data Subject's consent (ref. par. 3.4.2.2);

- organises and devises suitable measures, as part of their assigned company Areas/Departments/Functions, to guarantee the effective exercise of rights by the Data Subjects (ref. paragraph 3.4.2.4), and collaborates with the DPO, in compliance with company procedures, to provide prompt responses to related requests;

- guarantees the adoption of suitable technical and organisational measures to guarantee a level of security proportionate to the risk, taking into account the state of the art and costs of implementation, as well as the nature, subject, context and purposes of the Processing, and any risks to the rights and freedoms of the Data Subjects;

- with support from the competent company Areas/Departments/Functions, coordinates the process of starting new Data Processing or modifying existing Processing (ref. paragraphs 3.4.2.5 and 3.4.2.6);

- adopts suitable measures to ensure that the communication and dissemination of Personal Data take place in compliance with Privacy Regulations;

- adopts the necessary and appropriate measures to enable compliance with the Privacy Regulations when Processing Special Categories of Personal Data and data relating to criminal convictions and offences;

- adopts the necessary and appropriate measures to allow the use of foreign Data Processors and the transfer of Personal Data abroad, in compliance with conditions envisaged in the GDPR.

Furthermore, ,the *Process Owner* :

- identifies the scope of Data Processing permitted to the Authorized persons, as well as the databases and archives to which they have access, verifying the prerequisites and limitations on an annual basis;
- oversees and monitors compliance with the security measures in force by the Authorized persons operating under their responsibility, as defined in the various Group provisions;
- within the limits of assigned powers, manages relations with third-party suppliers that involve the Processing of Personal Data falling under its responsibility, supervising their work, also in accordance with provisions of the outsourcing and supplier selection policy (“Outsourcing Policy”);
- requests an opinion from the Group DPO if it intends to deviate from the retention periods defined in the specific Directive Internal to the Group (DIG), or initiate new Personal Data Processing operations or Data Processing that it does not consider included in the aforementioned DIG;
- promptly informs the Group DPO in the event of requests for information or documents, assessments and inspections by the Data Protection Authority, other judicial authorities or police authorities, collaborating in the preparation of documents, communications or filings on the

matter.

3.4.1.9 *Privacy* Contact

The Privacy Contact plays a fundamental role in supporting the Process Owner and the Group DPO in the operational activities required to implement the Model for the Protection of Personal Data, as well as in assessing and managing privacy risk to the extent of their responsibilities. He/she is designated on the basis of professional expertise, ability to carry out duties independently while also maintaining close contact with the Group DPO. The Privacy Contact should gain further specialist knowledge of the regulations and practices related to the protection of Personal Data through special training sessions.

The *Privacy Contact* :

- is involved whenever decisions have to be made that potentially have an impact on privacy issues falling under his/her Areas/Departments/Functions or Company ;
- guarantees continuous coordination with the Group DPO, for the purpose of proper control supervision in his/her business Areas/Departments/Functions or Company;
- may request advice from the DPO if they become aware of privacy issues in his/her business Areas/Departments/Functions or Company;
- contributes to raising awareness on the protection of Personal Data in the business Areas/Departments/Functions or Company for which they are responsible.

Furthermore, the *Privacy Contact* :

- with advice from the DPO, manages and responds to requests from Data Subjects to exercise their rights (ref. paragraph 3.4.2.4) in relation to the collection of data, documents and support formats, as well as other operations that may be necessary to provide feedback to the Data Subjects by the deadlines envisaged in the GDPR;
- upon instructions from the Process Owner, updates and maintains the Record of processing activities for Processing performed in his/her Areas/Departments/Functions or Company (ref. paragraph 3.4.2.8), also in reference to the IT services used;
- on instructions from the Process Owner, enters the new retention periods in the Record of processing activities after receiving the related opinion from the DPO;
- provides support to the Process Owner in the assessments required in the event of starting new Processing or when introducing changes to existing Processing (ref. paragraphs 3.4.2.5 and 3.4.2.6);
- participates in the team set up to assess the risk to the rights and freedoms of Data Subjects as part of the Data Breach procedure (ref. paragraph 3.4.2.10).

3.4.1.10 Authorized persons

The Authorized persons process personal data in their respective organisational areas, operating under the management and control of the Process Owner and in compliance with instructions received from the latter, in compliance with the Privacy Regulations and the Model for the Protection of Personal Data. They consult the designated Privacy Contact, when necessary.

Authorized persons are required to:

- perform processing operations lawfully and fairly only on Personal Data, also belonging to Special

Categories of data if essential, required for the activities entrusted to them and for related purposes, within the scope of duties assigned under their existing employment relationship, using the tools indicated or made available by the company to this end;

- ensure the confidentiality of the Personal Data of which they become aware or use for the aforementioned activities, refraining from communicating them to external parties other than those indicated by the company;
- process Personal Data so that, in compliance with company practices, they are accurate, complete, updated if required, relevant, necessary and not excessive for the purpose for which they are processed, in accordance with instructions received;
- ensure that Personal Data are stored in such a way as to allow identification for the time necessary for the purpose for which they were collected;
- arrange erasure of the data in the cases envisaged by the internal provisions in force;
- store and control Personal Data by adopting the envisaged security measures to avoid their destruction, loss, modification, unauthorised disclosure or accidental or unlawful access to the Personal Data transmitted, stored or otherwise processed;
- return to the Company all data involved in or acquired in the course of its activity, in the event of termination of the employment relationship, refraining from storing, duplicating, communicating or disseminating such data.

3.4.1.11 Data Processors

The Companies in scope only use Data Processors who offer adequate guarantees regarding the implementation of appropriate technical and organisational measures for the Data Processing carried out on their behalf, are able to meet the requirements of the GDPR and guarantee protection of the rights of Data Subjects.

The Processing carried out by the Data Processor is governed by specific contracts that bind the Processor to the Controller and define, inter alia, the duration of the Data Processing, the nature and purpose of the Processing, the type of personal data and the categories of Data Subjects, obligations and rights of the Data Processor and Data Controller (ref. paragraph 3.4.2.7).

3.4.1.12 Compliance function and Anti-Money Laundering

The Compliance Function and Anti-Money Laundering:

- annually presents to the Board of Directors a program of activities which, as deemed appropriate by the DPO and agreed upon with them, outlines the interventions to be undertaken concerning privacy risks.
- on the basis of the plan referred to in the previous point, evaluates the internal control system in the *privacy field* according to the process and methodologies described in the Function Policy Compliance and Anti-Money Laundering;
- informs the DPO about the results emerging from the activities and checks carried out on the privacy control *system* ;
- collaborates with the DPO on the Report submitted annually by the latter to the Board of Directors , with particular reference to the potential audits carried out and mutually agreed.

In Addition, the Compliance Function and Anti-Money Laundering participates in the *teams* set up to assess the risk to the rights and freedoms of Data Subjects as part of the Data Breach procedure (ref. paragraph 3.4.2.10).

3.4.1.13 ICT Area

The ICT:

- with reference to newly developed or re-engineered ICT services, it analyses the security risk to Personal Data in order to identify the security measures to be implemented and assesses their effectiveness;
- carries out a review of the effectiveness of the security measures in place, at least annually;
- carries out the relevant activities, based on the company procedures in force, as part of the processes of defining the terms of retention of Personal Data (ref. par. 3.4.2.3) and evaluation and notification of a *Data Breach* (ref. par. 3.4.2.10);
- provides support to the *Process Owner* and participates in the team established for the risk assessment for the rights and freedoms of the interested parties as part of the DPIA procedure (ref. par. 3.4.2.6);
- supports the DPO , in particular through the head of the IT security function, on IT issues, for example regarding security measures.

3.4.1.14 Real Estate Management

The Real Estate Management :

- carries out the assessment and analysis of the physical security risk of Personal Data, in order to identify the security measures to be implemented (e.g. regarding video surveillance), evaluating their effectiveness;
- carries out the relevant activities, based on the company procedures in force, as part of the evaluation and notification process of a *Data Breach* (ref. par. 3.4.2.10);
- provides support to the *Process Owner* and participates in the *team* set up to assess the risk to the rights and freedoms of the interested parties as part of the DPIA procedure (ref. par. 3.4.2.6);
- supports the DPO on issues relating to the physical security of Personal Data.

3.4.1.15 Risk Management Area

The Risk Management Area:

- submits an annual plan to the Board of Directors of activities that it intends to carry out as part of the operational risk management system, including privacy risk ; the plan of activities takes into account the Data Processing operations most exposed to privacy risk as identified by the DPO;

- on the basis of the plan referred to in the previous point, identifies and assesses operational risk according to the provisions of the Operational Risk Management Policy in force within the Group;

- with reference to privacy risk, informs the DPO of the results of activities carried out on the risk management system.

In addition, the Risk Management Area participates in the teams set up to assess the risk to the rights and freedoms of Data Subjects as part of the DPIA (ref. paragraph 3.4.2.6) and Data Breach procedures (ref. paragraph 3.4.2.10).

3.4.1.16 Audit Function

The Audit Function the task of evaluating and monitoring the effectiveness, efficiency and adequacy of the internal control system and of the additional corporate governance components, in relation to the nature of the activities conducted and the level of risks assumed, ensuring its alignment with the guidelines set by the Board, as well as addressing any adaptation needs through support and consultancy activities for other Areas/Departments/Functions within the company.

3.4.2 Operational model for the protection of Personal Data

Group -level provisions that guarantee compliance with the requirements of the *Privacy Regulation* , formalizing them within three categories of documents.

Category	Short description	Document type
High-level guidelines	The Group policies/guidelines provide guidelines to companies and corporate structures for managing *privacy risk* and define high-level processes for all or part of the companies in scope.	– *Policy* – *Directives* – *Intenal Group Directive*
Discipline processes	Definition of processes and procedures of the individual Companies in scope in implementation of policies/guidelines.	– Internal Company Directive
Operational rules	Definition of the detailed rules for the operations of one or more corporate structures of the Company within the scope, or of the distribution network, in line with process regulations	– Process Operating Rules – *Circulars/Provisions for the network* – *Forms*

3.4.2.1 *Accountability*

Pursuant a strong bureaucratic simplification promoted by the European Regulator (such as the elimination of the Authority's authorisation processes), the Data Controller is responsible for guaranteeing compliance with the principles established by the new regulations and keeping a continuous formal record of compliance, providing evidence of the reasons that led to the adoption of certain decisions and documenting the decisions made.

The Group therefore defined a set of technical and organisational measures to guarantee, and suitably demonstrate, that the Data Processing is carried out in compliance with Privacy Regulations; these include: i) the definition of the organisational model, with assignment of roles and responsibilities, formal drafting of appointments, definition of processes, procedures and traceable controls; ii) the preparation and provision of training and information sessions on the protection of Personal Data for employees and persons in specific roles; iii) the creation of operational support tools.

3.4.2.2 Privacy Policy and consents

The Data Controller provides the Data Subject with specific information, to ensure correct and transparent Data Processing, which varies depending on the collection method of the Personal Data (from the Data Subject or through alternative channels, e.g. public sources).

If the Data Processing is based on consent, the Data Controller must be able to demonstrate that the Data Subject has given valid consent (ref. paragraph 3.2) to the Processing of their Personal Data. The Data Controller may not process Special Categories of Personal Data and/or data related to criminal convictions and offences for the pursuit of its own legitimate interest, but exclusively in the presence of conditions

envisaged in the GDPR (in addition to explicit consent from the Data Subject, e.g. when Data Processing is necessary to protect a vital interest of the Data Subject or other natural person, etc.)

In order to adapt to the above forecasts, the Group defines:

- disclosure and consent templates in line with GDPR requirements;

- a repository (“Privacy Lab”), on the company intranet, in which the various templates in force and the official privacy documentation of the Group are gathered;

- an operating process that governs the updating/management of the disclosure and consent templates, as well as operating rules to ensure the correct collection, registration and storage of consents and withdrawals, identifying roles and responsibilities entrusted to corporate Bodies/Areas/Directorates/Functions of the Parent Company and the Companies in scope.

3.4.2.3 Personal data retention periods

As part of the information to be provided to the Data Subject, the Data Controller defines the retention period for the Personal Data processed, i.e. the criteria used to determine this period, after which the Personal Data are anonymised/erased.

The Group therefore defines:

- the retention periods envisaged in the Privacy Regulations and other regulations applicable to the business sectors of the Companies in scope;
- an operating process that governs the activities that determine, validate and control new retention periods (in derogation of or not specifically attributable to those identified in the previous point), identifying roles and responsibilities entrusted to corporate Bodies/Areas/Directorates/Functions of the Parent Company and the Companies in scope; the process also envisages assessment of the IT impacts resulting from implementation of the new retention periods by the competent structures.

3.4.2.4 Rights of the Data Subject

The Data Subject is entitled to exercise the following rights:

- **Right of access** : he right to obtain from the Controller confirmation as to whether or not Personal Data concerning him or her are being processed, and, where that is the case, access to the Personal Data and to a specific set of information (e.g. purpose of the Data Processing, categories of Personal Data);
- **Right of rectification**: the right to obtain from the controller the rectification of inaccurate personal data concerning him or her; taking into account the purposes of the Processing, the Data Subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement
- Right to withdraw consent: the right to withdraw consent at any time and with the same ease with which it was granted, without prejudice to the lawfulness of the Data Processing based on consent given before withdrawal;
- Right to erasure ("right to be forgotten") : the right to obtain from the Data Controller the erasure of Personal Data concerning him or her without undue delay, which corresponds to the Data

Controller's obligation to erase such data without undue delay if certain conditions are met[11];

- **Right to limit the Processing** : right to obtain from the Data Controller, when certain conditions are met [12], that the use of your data and, therefore, the Processing, is limited to what is necessary for conservation purposes;
- **Right to data portability** : if the data are processed by automated means, the Data Subject may request [13]the Data Controller to (i) receive " *in a structured, commonly used, machine-readable and interoperable format* " a subset of Personal Data which concern it and to keep it for further use for personal purposes on personal media or in a private *cloud ;* or (ii) transfer them to another Owner " *without impediments* " and where this is technically feasible;
- **Right to object** : this is the right of the Data Subject to object at any time, for reasons connected with his/her particular situation, to the Processing of his/her Personal Data carried out in the public interest or for a legitimate interest of the Data Controller, including Profiling or for direct marketing purposes
- **The right not to be subject to a decision based solely on automated Data Processing**, including Profiling, that produces legal effects concerning the Data Subject or that significantly affects the Data Subject personally, unless certain exception conditions are met.

The Data Controller, through the Privacy Contact and with the advice from the DPO, provides feedback to the Data Subjects in response to requests to exercise the aforementioned rights without undue delay and, in any case, at the latest within one month of receipt of the request [14].

In order to adapt to the above provisions, the Group defines:

- an operating process governing management of the rights of Data Subjects, identifying roles and responsibilities entrusted to corporate Bodies/Areas/Directorates/Functions of the Parent Company and of the Companies in scope;

- dedicated channels to convey and collect requests from Data Subjects, such as the institutional websites of the Parent Company and Subsidiaries (ad hoc form);

- a repository in which to track requests from Data Subjects managed by the Group, including supporting documentation.

[11] For example, the Personal Data are no longer necessary for the purposes for which they were collected or otherwise processed; the Data Subject withdraws the consent on which the Processing is based and there is no other legitimate reason for processing the data; the Data Subject objects to the Processing of Personal Data and there is no legitimate overriding reason to proceed with the Processing; etc. (see art. 17)

[12] The Data Subject may exercise this right against the Data Controller when at least one of the following conditions is met: (i) the Processing is unlawful (but the Data Subject does not want his/her data erased); (ii) the Data Subject has previously exercised the right to rectify his/her data (for the period necessary to verify its accuracy); (iii) the Data Subject has objected to Processing (for the time necessary to verify whether the legitimate reasons of the Data Controller do not prevail over those of the Data Subject); (iv) the Data Subject needs to protect his/her rights in legal proceedings (and therefore wants to prevent erasure of the data by the Data Controller)

[13] The Data Subject may exercise this right if he/she personally provided the Personal Data and the Processing is carried out by automated means and on the basis of consent or a contract to which he/she is party

[14] This deadline may be extended by two months if necessary, taking into account the complexity and number of requests. The Data Controller informs the Data Subject of this extension, and of the reasons for the delay, within one month of receiving the request.

3.4.2.5 *Data Protection by Design and Data Protection by Default*

The Data Controller, when planning Data Processing by design, implements adequate technical and organizational measures[15] to effectively implement the principles of protection of Personal Data (ref. par. 3.2), and integrate the necessary guarantees into the Processing in order to meet regulatory requirements and protect the rights of the Data Subject, taking into account the state of the art and costs of implementation, as well as the nature, scope, context and purposes of the Data Processing, as well as the varying probabilities and seriousness of risks inherent in the Processing on the rights and freedoms of the Data Subjects.

In addition, the Data Controller ensures that, by default, only the Personal Data necessary for each specific Data Processing purpose are processed. This obligation applies to the quantity of Personal Data collected, the scope of Processing, the retention period and accessibility.

In order to comply with the above provisions, the Group defines:

- an operatingl process that governs activities to guarantee *Privacy by Design* and *Privacy by Default,* identifying roles and responsibilities entrusted to Bodies/Areas/Directorates/Functions of the Parent Company and the companies in scope;
- a working method and operating tools to assess the privacy impact, at the start of any Project or Evolutionary Change[16].

3.4.2.6 *Data Protection Impact Assessment* (DPIA)

Within the context of Data Protection by Design as described above, the Data Controller, also in consultation with the DPO, before starting the Processing, when the Processing could present "a high risk to the rights and freedoms of natural persons[17]" considering the nature, subject, context and purposes of the Processing, carries out an assessment of its impact on data protection - especially when the use of new technologies is envisaged.

The DPIA is not mandatory for each Processing operation and it is sufficient to perform one overall impact assessment to examine a set of similar Data Processing operations that present equally high risks (for example, Processing operations similar in terms of: nature, scope, context, purpose, risks).

The Data Controller is also required to consult the Data Protection Authority before starting with the Processing, if the DPIA indicates that the Processing would present a high risk despite the related risk mitigation measures identified.

In order to comply with the above provisions, the Group defines:

- an operational process, governing the preparation and execution of a DPIA, the related reporting and any prior consultation with the Data Protection Authority, identifying roles and responsibilities entrusted to the corporate Bodies/Areas/Directorates/Functions of the Parent Company and the Companies in scope;

---

[15] E.g. pseudonymisation, which consists in the Processing of Personal Data in such a way that it can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is stored separately and subject to technical and organisational measures intended to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

[16] For the definitions of Project and Evolutionary Change), see DIG/UGH/232 of 25 June 2018 adopted in compliance with the Privacy Regulations.

.

17 Processing is considered to be high risk if it: (i) leads to systematic and global assessment of personal aspects of natural persons, based on automated Data Processing, including Profiling, and on which decisions are based that have a legal effect or similar significant impact on such natural persons; (ii) involve, on a large scale, Special Categories of Personal Data or related to criminal convictions and offences; (iii) refer to the large-scale systematic surveillance of an area accessible to the public.

- a methodology to support the assessment of the need to carry out a DPIA and for execution of the DPIA if necessary.

3.4.2.7 Suppliers and contracts

For Personal Data protection purposes, the GDPR regulates the possibility that certain Processing operations are carried out by Data Processors, respectively specifying the roles and responsibilities of the Data Controller and the Data Processor.

In order to comply with the above provisions, the Group:

- prepares contractual or other legal document templates, including specific clauses (e.g. transfer of data outside the EU, sub-processors, etc.) and annexes, which allow adequate protection of the Companies in scope against their respective Data Processors;
- defines an operating process that governs the selection and management of suppliers, as well as the signing and filing of related contracts, identifying roles and responsibilities entrusted to corporate Bodies/Areas/Directorates/Functions of the Parent Company and the Companies in scope;
- implements a platform for the digital management of contracts or other legal documents and related filing, which also acts as a database for the personal data of suppliers of the Companies in scope, with specific indication of those processing Personal Data on behalf of these Companies as Data Processors.

3.4.2.8 Record of processing activities

The Record of processing activities makes it possible to keep track of all Personal Data Processing operations carried out by each Company within the scope, also as Data Processor.

The content as envisaged in the GDPR varies depending on whether it is the Register of the Data Controller or Data Processor.

The Data Controller Record of processing activities contains: (i) the name and contact details of the Controller, the joint controller where applicable, the EU representative of the Controller and of the DPO; (ii) the purposes of Processing; (iii) a description of the categories of Data Subjects and Personal Data; (iv) the categories of recipients to whom the Personal Data have been or will be disclosed, including recipients in Third Countries or international organisations; (v) where applicable, transfers of Personal Data to a Third Country or to an international organisation, including identification of the Third Country or the international organisation; (vi) where possible, the deadlines set for erasure of the various data categories; (vii) where possible, a general description of the technical and organisational security measures.

In addition to details referred to in points (v) and (vii), the Data Processor Record of processing activities contains: (i) the name and contact details of the Data Processor(s), of each Data Controller on behalf of which the Data Processor operates, the EU representative of the Data Controller or Data Processor and, where applicable, of the DPO; (ii) the categories of Processing carried out on behalf of each Data Controller.

The GDPR exempts companies with less than 250 employees from the obligation to keep a Record of processing activities, unless the Data Processing operations performed could present a risk to the rights and

freedoms of the Data Subject or consist of non-occasional Processing that includes particular Categories of Personal Data or Personal Data relating to criminal convictions and offences.

In order to comply to the above provisions, the Group:

- establishes , through a specific IT application[18], the Personal Record of processing activities, for each Company in scope with the aforementioned requirements in its capacity as Data Controller and Data Processor (as appropriate);
- defines an operating process that governs the updating, validation and keeping of the Record of processing activities, identifying the roles and responsibilities entrusted to the corporate bodies/functions of the Parent Company and the Companies in scope

3.4.2.9 Risks and safety measures

The Data Controller and the Processor, taking into account the state of the art and the costs of implementation, as well as the nature, object, context and purposes of the Processing, as well as the risk of varying probability and severity for the rights and freedoms of the Data Subject, are required to implement technical and organizational measures to guarantee a level of security appropriate to the risk. These measures include, for example:

- the ability to continuously ensure the confidentiality, integrity, availability and resilience of Processing systems and services;
- the ability to promptly restore availability and access to Personal Data in the event of a physical or technical incident;
- a process to regularly verify and evaluate the effectiveness of technical and organizational measures in order to guarantee Processing security;
- encryption of Personal Data and pseudonymisation.

In order to comply to the above provisions, the Group defines an operational process and the related methodology to be used in performing a risk analysis [19]and to identify appropriate measures in relation to address the risk in question, identifying roles and responsibilities.

The technical and organizational measures adopted for each Processing operation performed are briefly described in the appropriate field of the Record of processing activities and reported in detail in the documents governing the operating process.

3.4.2.10 Notification of a *Data Breach*

The Data Controller is required to notify the *Data Breach* to the Data Protection Authority, without unjustified delay and, where possible, within 72 hours of becoming aware of it. The obligation does not apply if the Data Controller is able to demonstrate that the Personal Data breach is unlikely to present a risk to the rights and freedoms of the Data Subject.

The Data Controller must also notify the Data Subject of the Personal Data breach without undue delay in case of high risk for the rights and freedoms of the Data Subject.

[18] The support tool for managing the Record of processing activities and the related updating process allows the tracking of all changes implemented

[19] Risk for the rights and freedoms of the interested party, deriving from the destruction, loss, modification, unauthorized disclosure or access, accidentally or illegally, to Personal Data transmitted, stored or otherwise processed.

In order to comply to the above provisions, the Group defines:

- an operational process of notification to the Data Protection Authority /communication to Data Subject of a *Data Breach* identifying roles and responsibilities entrusted to corporate Bodies/Areas/Directorates/Functions of the Parent Company and the Companies in scope ;
- a risk assessment methodology for the rights and freedoms of the interested party associated with the *data breach* being analyzed and the consequent obligations of notification to the Data Protection Authority /communication to Data Subject;
- a Register of Data Breaches, which includes supporting documentation.

3.4.2.11 Transfer of Personal Data to Third Countries or international organizations

The transfer of Personal Data to Third Countries[20] is prohibited, in principle, by the GDPR, unless the country in question guarantees an adequate level of protection of the Personal Data. The European Commission has the power to establish such adequacy through a specific decision. With regard to countries not included among those considered adequate, as an exception to the aforementioned ban, transfer to third countries may also be allowed on the basis of contractual means that offer adequate guarantees..

In order to comply with the above provisions, the Group defines an operational process to manage the transfer of Personal Data to Third Countries or international organisations, which involves verification:

- of the existence of an adequacy decision of the European Commission in favour of the Third Countries;
- the adoption, for Third Countries deemed inadequate by the European Commission, of appropriate guarantees for the transfers of Personal Data, including:
- of adhesion to the " *Data Privacy Framework* ", the US program which certifies the commitment of the organizations that join it to respect the European data protection principles and therefore allows the transfer of data between the European Union and the USA;
- the " *Binding Corporate Rules* " (binding corporate rules), as a contractual instrument approved by the competent Supervisory Authority designed to allow transfer between companies in the same business group;
- *Standard* Contractual Clauses ", pursuant to Article 46, second paragraph, letter c) of the GDPR and Commission Implementing Decision (EU) 2021/914 of 4 June 2021, through which the importer of Personal Data based in a Third Country contractually guarantees to the European exporter that it will carry out the Processing in compliance with European principles of data protection, also in the third country of destination. [21].

[20] This refers to countries outside the European Union or the European Economic Area.
[21] These clauses remain in force until they are revised or modified.

3.4.3 Architectural model for the protection of Personal Data

The Group adopts an architectural model for the protection of Personal Data which guarantees a level of security adequate to the risk of varying probability and severity for the rights and freedoms of the Data Subject.

3.4.3.1 Classification and retention of Personal Data

The GDPR requires that the Data Controller appropriately classify the categories of Personal Data processed, with particular reference to Special Categories of Personal Dada and data related to criminal convictions and offences. In fact, the Data Controller is allowed to process such data only in compliance with certain guarantee conditions and in the presence of strictly established legal bases.

Furthermore, the Data Controller is required to inform the Data Subject regarding:

- the retention period of the Personal Data or, if this is not possible, the criteria used to determine that period;

- the Personal Data on which the Data Subject may exercise the right to portability.

In order to comply with the above provisions, the Group defines:

- a classification of Personal Data - in line with standards defined in the Group Policy on Data Governance and in the Information Security Policy, for the protection of data from internal and external threats - aligned with the Personal Data categories indicated above, as well as identifying and keeping track of Personal Data subject to portability;

- the retention periods for Personal Data processed by the Group, in compliance with legal obligations (where present), or, if this is not possible, the criteria used to determine such periods (ref. paragraph 3.4.2.3).

3.4.3.2 IT Services

The Group has a list of IT services that process Personal Data for which the Companies in scope are the Data Controllers or Data Processors. Specifically, for each application service processing Personal Data, the Group has an integrated catalogue of the following information: processes and activities (Data Processing “containers”), purposes of the Data Processing, categories of data processed, categories of Data Subjects, internal contacts for the protection of Personal Data, categories of subjects performing processing under authorisation, external data processors, any data communications and transfers outside the EU.

The Group also has information on infrastructures (e.g. Buildings; Servers) where such data are housed, both proprietary owned by third parties. In particular, the Data Controller pays attention to any cases in which Personal Data are stored or processed outside EU borders, adopting the appropriate safeguards, depending on the country in question, to ensure an adequate level of protection of the Personal Data transferred.

See the map of Information Systems and Group Record of processing activities for more information on the Processing of Personal Data linked to the IT systems.

3.4.3.3 Security measures

Taking into account the state of the art and costs of implementation, as well as the nature, subject, context and purposes of data Processing, and likewise the risk of varying probability and seriousness to the rights and freedoms of the Data Subjects, the Data Controller and the Data Processor must implement adequate technical and organisational measures to ensure a level of security appropriate to the risk. In light of the indications emerging from the assessment of risks of varying probability and seriousness to the rights and freedoms of Data Subjects associated with the Data Processing operations recorded in the Register of each

Company within the scope, the Group defines a set of technical measures - logical and physical - that guarantee an adequate level of security (ref. paragraph 3.4.2.9)

POLICY REGARDING THE PROTECTION AND ENHANCEMENT OF PERSONAL DATA

COMMITMENTS MADE BY THE UNIPOL GROUP FOR THE PROTECTION AND ENHANCEMENT OF PERSONAL DATA

(“ *UNIPOL DATA VISION* ”)

[PAGE INTENTIONALLY LEFT BLANK]

Contents

1 Introduction

This document, which is an integral part of the Personal Data Protection and Enhancement Policy (the "Policy"), defines the commitments made by the Group for the protection and enhancement of Personal Data with respect to its customers and all stakeholders. The attention that Group dedicates to the protection and enhancement of personal data in running its business guarantees respect for the values of Unipol Group contained in the Charter of Values and the Code of Ethics, demonstrating its accountability in the decision-making process and the dialogue with its stakeholders

2 Scope of application

This attachment applies to the Parent Company and the Companies in scope.

With reference to the Group companies with registered office in a country not belonging to the European Union, without prejudice to the fact that they have their own policies on the protection of personal data consistent with the Policy, the commitments made by the Group to protect and enhance Personal Data will be shared as part of coordination efforts between Unipol Group DPO and the DPOs appointed at local level. This is so that the Group companies with registered office in a country not belonging to the European Union can evaluate the methods for incorporating the above-mentioned commitments within their respective policies.

3 Unipol Data Vision

Increasingly often, we speak of data relating to natural persons, and particularly those connected to their behaviours, choices, movements and preferences, as a point of departure for the creation and development of products, services and innovative solutions that respond to the actual preferences of end users. Therefore, great opportunities for social and economic development are linked to the availability of Personal Data and their use by those in possession of them.

To fully realise these opportunities, it is necessary to build a transparent and balanced relationship between the parties to whom the data refer and those who are using such data. It is specifically necessary for the Data Subjects to always be aware of the purposes for which their data have been collected and how they are processed and used, to always be certain that their data are adequately protected and to always be able to exercise the rights recognised to them by regulations on the protection of personal data. Thus, it is necessary that the value created through the analysis and processing of personal data be shared, that is, that the parties to whom the data refer can also benefit from it, directly or as part of the collectivity.

Within the Group, for example, the use of Personal Data by an insurance company is necessary to be able to play its social role, by underwriting risks as knowledgeably as possible, so it can define adequate tariffs capable of making claim management sustainable. The increasing quantity of data that companies can collect and analyse can boost the capacity of insurance companies to protect their customers from risks in an accessible manner.

In the Group, considering the different businesses run by the Companies in scope (for example, insurance, long-term rental, hospitality), a wide range of Personal Data are processed, which relate to various moments in the life of natural persons, their behaviours, their available resources, their health, habits and preferences. This aspect will have increasing impacts with the growing spread of new connected devices (such as black boxes in vehicles, online services in homes). Information collected by new connected devices are particularly valuable and must be processed carefully, not only to ensure the protection of the natural persons to whom such data refer, but also to share the value that can be generated from their management using advanced

methods, for example, with reference to the insurance business, by improving the prevention of risks linked to health/illness, safe driving, house burglary and leaving minors unattended in parked vehicles.

4 The five commitments undertaken by the Group for the protection and enhancement o personal Data

With a view to increasingly implementing the system for protecting and enhancing Personal Data that the Group has developed, while acting in a transparent manner with customers and with all stakeholders so as to strengthen their trust in the Group, five commitments have been identified which the Group has made and intends to move forward with in this area.

In particular:

- Respect : the Group undertakes to perform data collection, analysis and processing activities with full respect for the values guiding its actions, as expressed in its Charter of Values and Code of Ethics;
- Protection : the Group protects the Personal Data held: this represents the first pillar for guaranteeing the rights of customers and all stakeholders with which the Group enters into contact. In line with what is set forth in the Group Sustainability Policy, due to the increasing role played by information technology in business activities and processes, which concerns relations with stakeholders, particularly with regard to employees and customers, and the resulting exchange of data and information, Unipol Group is committed to paying constant attention to guaranteeing a responsible approach to data management. This approach is developed over time consistent with regulatory, cultural and technological changes and is oriented towards the adoption of advanced protection systems while promoting awareness amongst stakeholders concerning how and for what purposes their personal data are processed. The Group will continue to invest resources to keep update and strengthen the data security protection system;
    - Information : the Group companies transparently inform their customers about the use of the personal data collected, enabling them to understand the impacts of their decision to share data.
    - Understanding : the development of solutions based on Personal Data and their processing - such as Artificial Intelligence (AI) systems - aims to identify innovative approaches to improve products and processes. The Group undertakes, even when developing technological solutions, to always put human beings and their needs at the centre; their understanding is fundamental for those who develop these solutions, in order to create inclusive and non-discriminatory systems;
- Value creation : the Group believes that use of Personal Data represents a significant area for shared value creation. In particular, looking for example at the insurance sector, as the Group's predominant business, it is believed that the use of data can boost value for:
- customers, who thanks to the use of data can benefit from a better understanding on the part of the Group companies of their actual protection needs and solutions that provide targeted, concrete responses to those needs; through data, it is also possible to develop tools, services and processes intended to prevent and reduce risks;
    - the Group , due to the fact that the collection and use of data allow for increased knowledge of risks, which leads to more knowledgeable underwriting and thus greater overall sustainability; furthermore, through data, insurance companies are capable of developing more effective products and services to protect their customers and offer them greater opportunities;

- the community, due to the fact that the availability of data for the Group and the technological skills developed support the development of solutions that pool the contributions of multiple players, particularly through public-private partnerships[22] , to meet the needs of the community.

5 Personal data enhancement Work Group

Notwithstanding the provisions on the protection of personal data adopted by the Group in its Personal Data Protection and Enhancement Policy, as well as what is set forth in the Group Policy on Data Governance and the Information Security Policy, Unipol Group has defined its commitments on responsible data management in the Group Sustainability Policy, which defines the duties of the Board of Directors and the Board Committees regarding the identification, assessment and management of the main risks connected to topics with an environmental, social and governance impact, deemed "material" for the Group and its reference stakeholders (so called "ESG" factors and the relative risks).

In this context, and in line with the objective of enhancing Personal Data, a Work Group ("Data Ethics Work Group") has been established at Group level, which is responsible for: (i) understanding and evaluating the impact on stakeholders of the enhancement of Personal Data underlying projects launched or to be launched, or business activities, ensuring that the opportunities and impacts are proportionate with a view to respecting the values set forth in the Charter of Values and the Code of Ethics (ii) taking decisions consistent, on a case by case basis, with the company's vision and with the Group's values referred to above.

The Task Force meets at least once per year and consists of departments/functions of Unipol Group/UnipolSai that play a key role for the understanding and management of those impacts: Innovation Area, Beyond Insurance Area, Information Area, Marketing and Communication Area and the Sustainability Function. The Legal Department, the Compliance and Anti-Money Laundering Function, the Ethics Officer and the Group Data Protection Officer also play an advisory role on the Task Force. The Group Data Protection Officer is called upon to express an opinion on specific queries raised by the Task Force as well as regarding personal data protection matters, without prejudice to the activities he or she performs with reference to new processing or changes to existing processing, in line with the provisions of the Personal Data Protection and Enhancement Policy.

[22] For example, the public-private partnerships launched for the improvement of sustainable mobility in cities, for homecare and for the adoption of adequate tools to assess, prevent and manage risks linked to catastrophic events.