GLOBAL CORPORATE POLICY

PERSONAL DATA PROTECTION POLICY

Effective date	22 October 2024
Approved use	Approved for external dissemination

Content

1. Purpose

This Policy (the "**Policy**") sets out the rules and principles to follow in relation to the protection of the Personal Data (as defined below) of Almirall's stakeholders, within the scope of the activities carried out by the different departments and functional areas of Almirall, with the aim of ensuring compliance with the applicable laws on Personal Data protection.

2. Scope (Applicability)

This Corporate Policy applies to Almirall S.A. and the legal entities in Almirall group (altogether "**Almirall**" or the "**Company**"), and it is binding on all employees.

In the event an external third party is engaged by Almirall they should abide by this Policy to the extent they process Personal Data on behalf of Almirall.

3. Policy elements

Definitions

- Data Subject means an identified or identifiable natural person, owner of his/her own Personal Data.

- Controller means the natural or legal person, public authority, agency or other body which, alone (Independent Controller) or jointly with others (Joint Controller), determines the purpose and means of the Processing of Personal Data.

- Personal Data means information relating to natural persons: (i) who can be identified or who are identifiable, directly from the information in question; or (ii) who can be indirectly identified from that information in combination with other factors specific to the Data Subject.

- Personal Data Breaches mean any security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. Personal Data Breaches can include access by an unauthorised third party; deliberate or accidental action (or inaction) by a Controller or Processor; sending Personal Data to an incorrect recipient; computing devices containing Personal Data being lost or stolen; alteration of Personal Data without permission; and loss of availability of Personal Data.

- Processing Activity means any operation or set of operations performed on personal data or on sets of personal data including but not limited to collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, combination, restriction, erasure or destruction.

- Processor means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of a Controller.

Principles of Personal Data Protection

All Almirall employees must observe the following general principles when processing Personal Data:

(i) Lawfulness, fairness and transparency: Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject, ensuring that the Data Subject is duly informed.

(ii) Purpose limitation: Personal Data must be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with the purposes notified to the Data Subject.

(iii) Data minimization: Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

(iv) Accuracy: Personal Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

(v) Storage limitation: Personal Data must be kept in a way that permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for among others, scientific or historical research or statistical purposes to the extent the appropriate technical and organisational measures are implemented.

(vi) Integrity and confidentiality: Personal Data must be 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.

(vii) Accountability: Almirall must have in place the necessary procedures and tools to document and be able to demonstrate compliance with the above principles.

Almirall Privacy Program

Almirall is committed to upholding a comprehensive Privacy Program that adheres to the applicable laws on Personal Data protection.

The foundational pillars of Almirall Privacy Program shall encompass the following items:

- Governance of Personal Data, adopting the necessary Procedures and Protocols for the processing of Personal Data in compliance with the applicable laws and principles set out in this document, including the necessary collaboration with Data Protection Authorities.

- Data Mapping of Personal Data, maintaining a Record of Processing Activities (RoPA) with specific information of the departments involved in the Processing Activities carried out in Almirall.

- Risk management of the processing operations of Personal Data at Almirall, carrying out the necessary evaluations (Privacy by Design) and adoption of technical and organizational measures to ensure a level of security appropriate to the risk and maintained during its entire lifecycle.

- Information to Data Subjects, by means of privacy notices informing Almirall's stakeholders in a clear and plain manner about the processing operations of their Personal Data carried out by Almirall.

- Relations with third parties engaged by Almirall for any processing of Personal Data (e.g. Processors, Joint Controllers or Independent Controllers). This entails the adoption of appropriate safeguards when Personal Data is internationally transferred to third countries.

- Respect to Data Subject´s Personal Data rights, honouring privacy requests submitted by Data Subjects in accordance with the terms established in the applicable laws on Personal Data protection.

- Offering of training and awareness programs, to increase the knowledge, skills and attitudes of Almirall employees, with the aim of improving the processing of information containing Personal Data.

- Prompt response to Personal Data Breaches, analysing the impact and adopting without undue delays the necessary measures to mitigate any Personal Data Breaches, reporting to the relevant Supervisory Authority in accordance with the applicable laws.

- Monitoring compliance, to ensure that consistency and effectiveness of all the elements encompassing the Privacy Program.

Almirall Privacy Program is dedicated to safeguarding the privacy rights of all stakeholders, fostering trust with Almirall's customers and partners, and upholding Almirall's reputation as a responsible and ethical organization. To achieve these objectives, Almirall commits to allocating appropriate resources for the program's maintenance and monitoring.

Almirall Data Protection Network

All Almirall employees are obligated to adhere to the applicable laws concerning Personal Data protection and the principles outlined in this Policy. Notwithstanding this obligation, a dedicated Data Protection Network has been established to uphold, promote, and strengthen a robust culture of Data Privacy at Almirall. The Almirall Data Protection Network shall comprise the following functions:

- Data Protection Officer (DPO), who assumes the functions vested by law, including acting as a liaison with Data Protection Authorities.

- Almirall Privacy Office, composed by members of the General Counsel Area, responsible for setting the strategy and definition of the governance of Almirall Privacy Program, including but not limited to tracking developments in key jurisdictions and developing strategies to enable Almirall to meet the applicable requirements. This includes the coordination with Almirall Information Security department for finding synergies and development areas to ensure Personal Data is processed with integrity and confidentiality.

- Privacy Country Responsible: appointed for the Almirall legal entities in each country, the Privacy Country Responsible shall oversee and locally supervise the proper implementation of the various element's pillars of the Almirall Privacy Program. Additionally, the Privacy Country Responsible shall coordinate and provide support to Data Managers in the execution of their privacy-related duties.

- Data Managers: appointed from various business areas and departments in relation to the Processing Activities listed in Almirall's Record of Processing Activities (RoPA), Data Managers shall ensure the promotion and maintenance of a culture of privacy within Almirall. They shall also provide support in maintaining the different pillars of the Almirall Privacy Program.

The Almirall Data Protection Network shall promote Personal Data protection as a fundamental obligation of Almirall, fostering a culture of privacy where data protection is integral to Almirall's business activities, in line with ethical principles adopted by Almirall in the Code of Ethics.

4. Governance

Corporate Policy Sponsor: General Counsel		
Corporate Policy Owner: Global Data Protection Officer		
Overview of changes	Version	Effective Date
New Policy	1.0	22 October 2024

All employees are required to report any suspected violation of this Policy in accordance with Almirall Code of Ethics and other internal guidelines. Suspected violations can be reported to your direct manager, People & Culture, your local Compliance or Legal representative or through the SpeakUp! channel.