

N° rev	Date	Description	Ref. Parag.
0	12/10/2021	First emission	
1	15/12/2023	General review	
2	03/03/2025	Adequacy to the NIS 2 Directive	13

PRIVACY ORGANIZATIONAL MODEL

GLENAIR ITALIA S.P.A.

EU Regulation 2016/679

Legislative Decree no. 196/2003, updated to 101/2018



*- PROCEDURES and BEST PRACTICES -
for the correct treatment of personal data*

1 Introduction

The Organizational Model collects technical and organizational measures that Glenair Italia implements to ensure – and prove - the compliance with EU Regulation 2016/679 and Italian legislation on personal data treatment of physical individuals, which the Company performs, whether directly or through third subjects, who carry out the treatment on their own.

EU Regulation 2016/679 of the 27th of April 2016, “GDPR”, becomes definitively operating and applicable from the 25th of May 2018 in all Countries members of the European Union and pursues the purpose of enforcement of personal data protection of physical individuals, both within and out of European borders, therefore irrespective of the principle of territoriality, harmonizing the privacy rules of all Member States.

The adoption of adequate technical and organizational measures is imposed by the Holder by art. 24 and following of the GDPR, pursuant to which internal politics and measures to implement to satisfy the principles of the data protection from the phases of designing and data protection by default, shall consider, in concrete, the nature, the application field, the context and purposes of the treatment as well as the risks of harming rights and freedoms of the subjects involved.

To comply with such requirement, Glenair Italia wanted to elaborate this Organizational Model, which has the preventive execution of an aware and critical activity of internal audit, which has allowed the verification of each single company unit and aims at a licit and transparent management of the personal data treated.

This Organizational Model is reviewed and updated by the Privacy Referent and approved by the Holder.

2 Objectives

The objective of this Privacy Organizational Model is to ensure and prove that the treatment of personal data by Glenair Italia happens lawfully, correctly, and transparently according to juridical parameters identified by GDPR, and reachable through the realization of an internal and structured management.

Glenair Italia promotes by its collaborators a culture of privacy and protection and security of personal data, establishing those behavioral principles suitable to ensure transparency, security, and

correctness of the performed treatments, by increasing its reliability towards customers, strategic partners, employees and interested subjects.

This Organizational Model is composed of 14 Sections aimed at supplying a panoramic on the entire system of technical and organizational measures which, based on the concrete systematic and operating needs of Glenair Italia, are considered adequate, including principles, organizational rules, and control instruments to ensure the lawful, correct, and transparent treatment of personal data.

This Organizational Model aims at enforcing the ethics of work which characterizes the staff working with Glenair Italia.

For Glenair Italia, the competition factor is being able to aspire to correct management of personal data during the performance of its tasks.

Glenair Italia M.O.P. wants to avoid the possible imposition of pecuniary administrative sanctions as per art. 83 GDPR as well as those of a penal nature according to the national legislation by trying, with its adoption, to demonstrate the concrete, efficient and effective implementation of technical and organizational measures suitable for the data protection of each data treated directly or by third subjects which perform this task on the behalf of the Company.

3 Principles for the correct treatment of personal data

GDPR is composed of three inspiring principles which sustain the entire legislation and whose respect is protected by a sanctioning system towards Holders and responsible for the treatment.

Among the fundamental principles, we can find:

1. **accountability**, namely the liability principle: the Regulation doesn't carry out a punctual typification of technical and organizational measures, by expressing only in terms of its risk adequacy, considering the state of the art and the implementation costs, as well as the nature, the object, the context, and purposes of the treatment, and the risk of various probability and seriousness for rights and freedom of physical subjects (art. 32 GDPR). It is a relevant innovation, since the task of an autonomous decision on modalities, warranties, and limits of the personal data treatment, in compliance with the legislation and some criteria indicated in the Regulation is assigned to Holders. This imposes an integrated, concrete, and risk-based approach, which interests all company BU, and which shall give place to proactive behaviors.

2. **privacy by design**, which imposes the adoption of protection measures from the treatment design.
3. **privacy by default**, which prescribes the use, limited to predefined settings, only of necessary data to reply to specific purposes of the data management.

Glennair Italia wanted to update the above-indicated principles with operating news such as:

- a) the establishment of a **Register of treatment activities** (art.30 of GDPR and 171), which represents the starting point for the preparation of the entire documentation system, that will collect evidence, controls and processes that allow to meet the accountability of the privacy system.
- b) the **process for data breach management**, (art. 33 and 34 GDPR), i.e., the analysis of possible reporting of a data breach, which requires an aware analysis and knowledge of the information handled, but most of all organizational and technological investments in monitoring, security and subdivision methods of the damage that may derive.

A direct consequence of the general principles above defined on accountability, privacy by design and privacy by default, is that full compliance with GDPR imposes that the personal data treatment shall happen according to principles of legality, correctness, and transparency.

As in the previous legislation, the treatment is lawful when is justified on a juridical basis which, without prejudice to the information obligation in charge of the treatment Holder, can consist in what follows:

1. consent of the interested subject which shall be free, specific, informed and unequivocal, as the alleged or silent consensus are not allowed: in other terms, it shall be manifested by an "establishment or unequivocal positive action". Moreover, for "sensitive" data at art. 9 of GDPR, it must also be "explicit", not necessarily "documented in writing" nor to handle in "written format", although such modality is the most suitable to prove its performance, its unequivocal and explicit nature.
2. contractual obligations, namely the treatment is lawful when necessary for the execution of a contract in which the interested subject is partially involved or for the execution of precontractual measures adopted upon request.
3. law obligations that apply to the treatment holder, in which case the purpose is specified by law.
4. lively interests of the interested person or of third parties: namely if it is necessary for the safeguard of lively interests of the interested subject or another physical subject but can only be used as a legal basis if none of the other conditions of lawfulness can find concrete application.

5. prevailing legitimate interest of the holder or thirds, whose data are communicated, namely when the treatment is necessary for pursuing legitimate interests of the Holder of the treatment or of third parties, to the condition that interests or fundamental rights of the interested subject or thirds don't prevail, when these require the data protection, in case of a minor.

6. public interest or exercise of public powers, i.e., relevant to the performance of a task of public interest or linked to the exercise of public powers, for which the Holder is responsible (by State or Union law) and in such case, the purpose shall be specified for law.

Personal data treatment is **correct** when transparent against the interested subjects, namely when personal data is treated for clear, explicit, and lawful purposes, and without any impropriety or deceiving towards data subjects (being prohibited confusion or partial information).

Transparency isn't only a fundamental principle of the treatment, but also a real right of the interested subject: modalities for the collection of data and its use shall be transparent and correct.

Data subjects shall be informed about the purposes of the treatment, its modalities, and the address of the treatment Holder before the start of the treatment. Modalities shall be explained in a comprehensible manner, so that interested subjects can understand what will happen to their data.

The data subject shall rely on an effective procedure, which is easily accessible and allows access to the treated data in a reasonable time, so to be aware of the data detained by the Holder. In such sense, the Holder has a time limit (which can be prolonged in some circumstances) to manage and exercise the right proposed by an interested subject.

4 Definitions

Hereinafter are shown the main terminology necessary for a correct comprehension of the legislation on personal data treatment of natural persons.

1) **Personal data:** any information referring to an identified or identifiable physical person (**Interested**); a physical person is considered as identifiable when this can be identified, directly or indirectly, with reference to an identification as:

- Name or surname
- E-mail address
- Photo and voice
- Identification number (ID card, Fiscal Code, Passport, etc.)
- Data on the location
- Online identification

- One or more elements of the physical, physiological, genetic, psychic, economic, cultural, or social identity
- 2) **Particular data:** any information revealing:
- Racial or ethnic origin
 - Political opinions
 - Religious or philosophical beliefs
 - Trade union membership
 - Genetic data
 - Biometric data aimed at identifying uniquely a natural person
 - Data on health, sexual life, or sexual orientation of the subject
- 3) **Judicial data:** data related to penal sentences and crimes or linked to security measures (penal jurisdiction).
- 4) **Treatment:** any operation or set of operations, performed with or without automatized processes and applied to personal data, as:
- Collection
 - Registration
 - Organization
 - Structuration
 - Storing
 - Adaptation or modification
 - Extraction
 - Consultation
 - Use
 - Communication through transmission, diffusion, or any other form of provision
 - Comparison or cross-connection
 - Limitation
 - Cancellation or destruction
- 5) **Treatment Holder:** physical or juridical person, who decides purposes and modalities of the treatment.
- 6) **Responsible for the treatment:** physical or juridical person, public authority, service, or any other organism, which treats personal data on behalf of the Holder.

- 7) **Responsible for Data Protection/Data Protection Officer:** subject designated for the possessed professional qualities, in particular for the specific knowledge of legislation and praxis on data protection and ability to perform the following tasks:
- Inform and advise the Holder and the employees performing the treatment on obligations deriving from laws.
 - Oversee the compliance with the legislation on personal data protection.
 - Cooperate with control authorities.
 - Be a contact point for control authorities.
- 8) **Consensus of the interested subject:** any representation of the free, specific, informed, and unequivocal will of the data subject, with which the consent can be manifested, through declaration or unequivocal positive action, that personal data are subject to processing.
- 9) **Information:** document with which the following information is given to the data subject:
- Identity and contact data of the treatment Holder
 - Contact data of the person responsible for the data protection
 - Purposes of the treatment
 - Any addressee and the possible categories of addressee of personal data
 - Intention of the Holder to transfer personal data to a third country or an international organization
 - Time of storage of personal data
 - Rights of the interested subject (15-22 GDPR)
 - Right to propose any claim to a control authority (Guarantor for personal data protection)
 - Juridical basis of the treatment
 - Presence of an automatized decisional process, including profiling
- 10) **Violation of personal data, so-called Data Breach:** the security violation which accidentally or unlawfully leads to:
- Destruction
 - Loss
 - Modification
 - Unauthorized disclosure
 - Access to personal data transmitted, kept or treated
- 11) **Recipient:** natural or juridical subject, who receives communication of personal data.
- 12) **Archive:** any structured set of personal data accessible according to defined criteria.

8 Requests of the interested subject – exercise of a right

8.1.1 Introduction

The Holder of the treatment has appointed an internal Privacy Contact within the Company who has the function of giving feedback to communications with which the interested subjects exercise their rights.

Unless the Data Controller proves that the interested subject cannot be identified, the person appointed by the Holder shall give feedback without unjustified delay, communicating in a concise, transparent, and intelligible way and with clear and simple language. The maximum time for the feedback to a request by the subject of interest is of **one month** from the receipt. Such a term can be extended to two months, when necessary, considering the complexity and the possible number of obtained requests. The Holder of the treatment, or the appointed subject, informs the interested subject of the possible prorogation and the due causes of the delay within a month from the receipt of the request.

In case the request of the interested subject can't be fulfilled, the latter shall be informed with no delay, at least within a month from the receipt of the request, of the reasons of the non-compliance and the possibility to postpone the claim to the Privacy Guarantor or to propose a judicial remedy to competent Authorities.

Whenever the interested subject requests to exercise his rights, it shall always be ensured that he is the holder. Feedback communications to the requests of the interested subject are free. When the requests are manifestly unjustified or excessive, in particular in case of redundancy, the Holder can:

- Charge a reasonable fee by considering any administration cost sustained to give feedback to the interested subject.
- Refuse to meet the request. In this case, the Holder will have the duty to demonstrate the unjustified or excessive feature of the received request.

The Data Controller has adopted measures suitable for giving the interested subject all information that the latter could ask for, by creating an e-mail address dedicated to communications of the interested subjects.

9 Violation of Personal Data– Data Breach

9.1 Introduction

Glenair has identified in the IT Team and in the Privacy Contact (gdpr@glenair.it) the figures responsible for the management of Data Breach within the Company. As Data Breach or Violation of Personal Data, we mean a “security violation which leads – accidentally or unlawfully – to the destruction, the loss, the modification, the unauthorized disclosure or the access to personal data transmitted, stored or treated”.

A violation of personal data can compromise its **confidentiality**, the **integrity**, or the **availability**.

10 Guidelines in protection of the Company Know How

Glenair Italia, to protect the digital heritage represented by information and personal data, has provided to make its employees and collaborators sign precise confidentiality agreements.

11 Selection criteria for external managers of Glenair Italia

Glenair Italia, to ensure that its personal data is treated by applying appropriate measures by external suppliers and partners, has regulated the flow of such data by preparing a Data Processing Agreement for each company and transversal outsource. This Agreement disciplines and regulates, in compliance with the requirements imposed by art. 28 of GDPR, the partner’s responsibilities concerning the data processing performed on behalf of Glenair Italia as Holder of the Treatment.

The following procedure applies to new Outsourcers:

- 1- The treatment which shall be done in outsourcing, is preliminarily discussed with the IT Manager which will evaluate the potential risks of the processing and will notify the Holder in case of gaps with the requirements imposed by the legislation.
- 2- Once the partner has been chosen among those selected for the treatment activity in outsourcing, a copy of the contract is forwarded to the IT Manager.
- 3- The IT Manager prepares the DPA that will be attached to the draft of the contract.
- 4- Once the DPA is signed, a digital copy is stored in the dedicated folder in the Privacy Organizational Model folder.