



Personal Data Protection Policy

Contents

1. INTRODUCTION..... 3

2. PURPOSE AND SCOPE 3

3. OPERATING PRINCIPLES AND COMMITMENTS 3

4. MONITORING MECHANISMS 5

5. DISCLOSURE AND DISSEMINATION 5

6. APPROVAL AND VALIDITY 5

1. INTRODUCTION

ENAIRe, a state-owned company of the [Ministry of Transport, Mobility and the Urban Agenda](#), is responsible for the planning, management, coordination, operation, maintenance and administration of air traffic, telecommunications and aeronautical information services, as well as of the communications infrastructure, facilities and networks of the air navigation system, with the aim of ensuring that the service is provided safely, efficiently, continuously and sustainably.

The protection of individuals in relation to the processing of personal data constitutes a fundamental right of citizens. The Charter of Fundamental Rights of the European Union and the Treaty on the Functioning of the European Union state that everyone has the right to the protection of their own personal data.

ENAIRe, in the exercise of the duties assigned to it by law, regularly processes personal data in accordance with the General Data Protection Regulation (EU Regulation 2016/679 - GDPR) and Organic Law 3/2018 of 5 December, on the Protection of Personal Data and the guarantee of digital rights (LOPDGDD).

2. PURPOSE AND SCOPE

The purpose of this Policy is to set out the guiding principles that ENAIRe uses when processing personal data and to guarantee the fundamental right to the protection of personal data. It equally seeks to safeguard the right of persons to honour and privacy when it comes to their personal data.

This Policy applies to ENAIRe and all employees, the members of ENAIRe's Management Committee and Governing Board, who are required to know, understand and comply with the provisions of this Policy.

Similarly, persons acting on behalf of and representing ENAIRe without being part of its organisation will undertake to act in accordance with this Policy when representing the Company or acting on its behalf in the performance of their duties.

3. OPERATING PRINCIPLES AND COMMITMENTS

This Policy relies on the following principles on the protection of personal data:

- **General principles**

- ⇒ ENAIRe will comply with the [personal data protection regulations and any other regulations that are determined in accordance with any binding rules or agreements](#) that may be adopted, and will ensure that the principles set out herein are considered in:

- The design and implementation of procedures that involve the processing of personal data.
- The services offered by ENAIRe.
- Any contracts and obligations that are entered into.
- The implementation of any systems and platforms that allow access, including by third parties, to the personal data of natural persons.

- **Protection principles relating to processing:**

- ⇒ [Principles of legitimacy, legality and fairness](#). The processing of personal data shall be fair and lawful, in accordance with data protection regulations. Personal data must be collected for one or more specific and legitimate purposes, in accordance with the applicable law. When this is necessary, the free, prior and informed consent of the data subjects will be obtained. ENAIRe shall not collect or process data of a special category, unless this is necessary in keeping with data protection laws. If it does so, it shall ensure that it abides by all the rules applicable to this type of processing.

- ⇒ **Minimisation principle.** Only that personal data that is strictly necessary to satisfy the purpose stated by ENAIRe in each case will be collected.
- ⇒ **Principle of accuracy.** The personal data will be accurate and up to date. If it is not, it must be corrected or deleted.
- ⇒ **Principle of limitation.** The processing of the personal data collected will be limited to complying with the stated purpose.
- ⇒ **Storage principle.** The personal data collected will be stored only for as long as strictly necessary to comply with the stated purpose, unless legal provisions allow for longer storage periods.
- ⇒ **Principles of integrity and confidentiality.** Technical or organisational measures will be implemented to ensure that the data is properly safeguarded against unauthorised access, loss, theft, damage or alteration. Likewise, the confidentiality and secrecy of the data will be guaranteed. Any disclosure to third parties outside the legally established cases is unacceptable.
- ⇒ **Principle of accountability.** Steps will be taken to ensure that evidence is available to prove regulatory compliance at all times.
- ⇒ **Principle of protection through design and by default.** Any data processing requires the protection of the personal data of people through design and by default. ENAIRe will guarantee, and be able to prove, that as part of each data processing step, the protection of the rights of individuals guides its actions from the outset. Similarly, ENAIRe must do the corresponding risk assessment that each processing activity has on the rights of people and, when necessary, carry out the corresponding prior impact assessment. ENAIRe will also appoint a Data Protection Officer, who will interface with the Spanish Data Protection Agency and make its Data Processing Activities Register public. Finally, ENAIRe will document and notify the relevant authorities, when necessary, of any incident that results in the destruction, loss or alteration of the personal data it processes, and of any unauthorised access to it, and it will take the necessary measures to resolve and reduce the negative effects of any such events.
- ⇒ **Principles of transparency and information.** The processing of personal data will be transparent in relation to the person concerned, who will be provided information on the processing of their data in a way that is understandable and accessible. ENAIRe will inform data subjects of the processing when the data is collected, unless this is not possible, in which case the data subject will be informed as soon as possible.
- ⇒ **Data Processors.** When ENAIRe outsources works and/or services that require contractors to process the personal data of ENAIRe employees, it will ensure that the security measures applied to the processing are equivalent to those implemented by ENAIRe. This requirement will also be guaranteed to be applied to subcontractors if they are used. Finally, ENAIRe guarantees that the legal clauses governing the processing of personal data by authorised third parties are incorporated into the relevant contractual conditions.
- ⇒ **International data transfers.** ENAIRe will generally not process data that involves transfers of personal data outside the European Economic Area (EEA). However, should this happen, the data subjects will be expressly notified of this circumstance and the necessary consent will be obtained.
- ⇒ **Rights of persons.** Data subjects have the right to access, rectification, deletion, objection, limitation and portability, as well as not to be subject to automated decisions that affect their interests, and to withdraw the consent given, if any. ENAIRe will allow and facilitate the exercise of these rights by data subjects with the entity itself and with the Spanish Data Protection Agency.

4. MONITORING MECHANISMS

The body responsible for supervising the operation of and compliance with this policy is the [regulatory compliance body](#).

5. DISCLOSURE AND DISSEMINATION

In compliance with the requirements of international transparency standards and practices, this Policy will be made available to all stakeholders on ENAIRE's [website](#) for their information and consultation.

Similarly, the Policy will be appropriately communicated and [disseminated](#) internally using existing tools, to aid everyone acting on behalf of ENAIRE to understand and apply it.

6. APPROVAL AND VALIDITY

Following its presentation to the Management Committee on 19 April 2023, this Policy was approved by ENAIRE's Governing Board at its meeting of 26 April 2023, coming into force on that date. It shall remain in force until amendments are made to the Policy, which will be properly communicated.

This Policy repeals and replaces the General Data Protection Policy (v.1.1) of 24 January 2023.

This Policy is subject to review and updating as needed to adapt it to any regulatory, social, economic or organisational changes.