PRAGMA ETIMOS srl
Via dei Bersaglieri 5 - 04011 APRILIA (LT)
Partita IVA / Codice Fiscale: 02838170591

Organizational Model

INDEX

1. *Introduction and background* 2
2. *Definitions* 2
3. *Goal* 3
4. *Scope of application* 3
5. *Data Controllers* 3
6. *Privacy Representative / DPO* 3
7. *Data Processors* 3
8. *Organization and Responsibilities* 3
9. *Treatment Analysis Form* 4
10. *Register of Processing Activities* 4
11. *Risk and impact assessment in data processing* 4
12. *Cyber Security Measures* 4
13. *Procedure for managing requests from Data Subjects* 5
14. *Notification procedure in the event of a data breach.* 5
15. *Code of Conduct* 5

1. Introduction and background

The European legislator has decided to renew the existing legislation on the processing of personal data (Directive 95/46/EC), which is now more than twenty years old, to adapt it to the current technological and social context that is strongly "data-centric": it has thus issued EU Reg. 679/2016 of the European Parliament and of the European Council on the protection of natural persons with regard to the processing of personal data, as well as the free movement of such data.

The GDPR is directly applicable in all EU member states as of 25 May 2018, having been adopted with the formula of the European Regulation; The GDPR pursues the aim of harmonizing the regulations of the member states on the processing of personal data, adapting it to the digital context and introducing what can rightly be defined as the strictest data protection legislation in the world, also capable of extra-territorial effects.

With the GDPR, the protection of personal data becomes a fundamental right of the individual, which is intended to be guaranteed by obliging those who carry out processing to comply with the principles of Privacy "by design" and "by default".

In line with the above principles, the GDPR emphasizes the characteristics of transparency and accountability required for the processing carried out on personal data, providing for the need to demonstrate compliance with the regulatory provisions of the processing carried out.

Therefore, the GDPR imposes new obligations on companies, government bodies, organizations and non-profit associations that offer goods and services to European citizens or that, in any case, in the exercise of their activity collect and process data referable to natural persons.

In light of the above and taking advantage of the harmonization achieved at European level, **PRAGMA ETIMOS srl** has decided to adopt this Personal Data Processing Organizational Model, in order to ensure compliance with the provisions of the GDPR and give full effect to the principles of privacy by design and by default.

2. Definitions

In this Personal Data Processing Organizational Model, the terms listed here have the following meanings:

Supervisory Authority	Public authorities in charge of overseeing the application of the GDPR; the list of competent authorities by country is attached here.
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); in particular with reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to your physical, physiological, genetic, mental, economic, cultural or social identity.
Health-related data	Personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information about the state of his or her health (see recital 35)
Recital 35	Personal data relating to health should include all data concerning the health status of the data subject that reveal information related to the past, present or future physical or mental health of the data subject. This includes information about the natural person collected in the course of his/her registration for the purpose of receiving or providing healthcare services as referred to in Directive 2011/24/EU of the European Parliament and of the Council; a number, symbol or specific element attributed to a natural person to uniquely identify that natural person for health purposes; information resulting from examinations and controls carried out on a body part or organic substance, including genetic data and biological samples; and any information concerning, for example, a disease, disability, risk of disease, medical history, clinical treatments, or the physiological or biomedical status of the data subject, regardless of the source, such as, for example, a doctor or other healthcare professional, a hospital, a medical device or an in vitro diagnostic test.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council.
MOTDP	This Organizational Model for the Processing of Personal Data.
Data Processor	The natural or legal person, public authority, agency or other body that processes or under whose responsibility and control personal data is processed on behalf of the Data Controller.
Titular	Legal representative of the Company who determines the purposes and means of the processing of personal data;
Treatment	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring,

storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion or destruction.

3. Goal

The adoption of this Personal Data Processing Organizational Model is aimed at ensuring compliance with all legal obligations imposed on the Data Controller of **PRAGMA ETIMOS srl** and in particular:

1. Defines an organizational model aimed at an effective and uniform management of Processing within the company;
2. Ensures that data subjects (employees, customers, suppliers, consultants and third parties) are entitled to the lawfulness of their Data Processing, as well as the possibility of exercising the rights guaranteed to them by the GDPR;
3. Ensures that Data protection is guaranteed right from the design of the flows describing the Processing and that Data protection measures are applied by default;
4. It establishes a procedure for the analysis of processing operations, providing the Data Controllers and data processors identified with the tools and criteria for the establishment of the Processing Register;
5. Identify the IT security measures implemented in **PRAGMA ETIMOS srl** to ensure the security of the Data.

4. Scope of application

This MOTDP is binding for **PRAGMA ETIMOS srl** through its Data Controller, who undertakes to adopt it, also pursuant to Article 47 of the GDPR, by signing the letters of adhesion referred to in form 000.
The Processing obligations assumed by the Data Controller pursuant to this MOTDP are also binding towards the data subjects or any internal and external data processors.

5. Data Controllers

The DATA CONTROLLER determines the purposes of the data processing of **PRAGMA ETIMOS srl** committing to carry out processing in accordance with this MOTDP and in a lawful, correct and transparent manner towards the data subjects. The Data Controller guarantees to the data subjects that:

- The Processing carried out complies with the stated purposes;
- The stated purposes are limited to what is necessary for the exercise of the Data Controller's activity;
- Only the data necessary for the stated purposes is used;
- The storage of the data is limited in time to a period congruous with the stated purposes;
- Systems are in place to ensure data retention,
- For each Processing, the criterion of legitimacy of the Processing is verified;
- At least once a year, a verification of the level of compliance with the regulations and a revision of the Processing Analysis Forms are promoted and improvement plans are defined in the management of the Treatments;
- The information provided to data subjects complies with those indicated in the Guidelines for the management of Processing and therefore mentions the existence of this MOTDP and its main contents, as well as provides the information necessary to activate the procedure described in Article 14 below.

In light of the uniform level of Data protection, the transmission of Data between Data Controllers is permitted provided that: (i) the transmission is necessary for the purposes for which the data is Processed; (ii) the transmission was included among the processing operations listed in the information released at the time of collection of the Data; or that the transmission is necessary for the provision of a service from one company to another.

6. Privacy Representative / DPO

Not named.

7. Data Processors

There are no specific data processors

8. Organization and Responsibilities

In virtù della struttura organizzativa di **PRAGMA ETIMOS srl** viene di seguito indicata la mappatura dei processi in cui Titolare e Responsabili, nonché il DPO condividono responsabilità sui singoli Trattamenti:

Type of Treatment	Data Controller	Data Processor	Data Protection Officer
Common and sensitive employee data	√	√	
Common and sensitive patient data	√	√	
Video surveillance management and treatment (where implemented)	√	√	
Common Customer and Supplier Data	√	√	
Data profiling from marketing activities	√	√	
Profiling of data from commercial activities	√	√	
Processing and management of computer data	√		
Coordination of data analysis activities Treatments	√		
Verification of compliance with data processing	√	√	
Maintaining the Breach Log	√	√	
Monitor that personal data breaches are documented, notified and communicated;			
Privacy System Maintenance Audit	√		
Attribution and supervision of roles and responsibilities	√		
Inform and advise the Data Controller on the obligations arising from the legislation and keep the documentation provided for by it;			

9. Treatment Analysis Form

Compliance with the provisions of the GDPR assumes as an essential prerequisite the mapping of the processing processed.
In order to ensure completeness of the mapped information and uniformity of analysis, the Data Controllers and Data Processors will track the Processing carried out through the use of the Processing Analysis Form template.
The Processing Analysis Form will be filled in for each area of competence into which the Data Controller's business organization is divided, with an indication of each Processing carried out within this area.
Each form must indicate, at a minimum, the category of data subject, the time of data collection, the conditions of lawfulness of the Processing, the purposes of the Processing, the indication of the persons authorized to Process, the list of security measures used for each Processing and the risk assessment.

10. Register of Processing Activities

Pursuant to Article 30 of the GDPR, PRAGMA ETIMOS srl adopts a Register of Processing Activities.
In accordance with the approach given by this MOTDP, the Register of Processing Activities of each company is composed of the sum of the Analysis Forms of Processing carried out at each Data Controller, referred to in the previous point. The Data Controller is responsible for maintaining the Register of Processing Activities.

11. Risk and impact assessment in data processing

Each analysis sheet of the processing carried out must include an assessment of the potential risks in the event of a personal data breach. The risk and impact assessment for each treatment is reported in the treatment analysis sheet.

12. Cyber Security Measures

Acknowledging the importance of the planning and implementation of IT security measures for compliance with the principles of "privacy by design" and "by default", PRAGMA ETIMOS srl, in the person of its Data Controller, has adopted the following IT security policies and measures:

- Electronic archiving of data on client PCs in the Data Controller's office
- Correct management of access to electronic documents by staff
- Correct management of data back-ups managed at IT level
- Adequate Firewall and Antivirus systems in order to ward off malicious codes

In order to protect data and information, the Data Controller has adopted a specific "IT Privacy Policy" in which the specific security and protection measures are described and detailed.

13. Procedure for managing requests from Data Subjects

The Data Controller is the single interface for the collection of requests made by the various data subjects.
The dedicated mailbox will be indicated in all the information issued by the Data Controller, it will be the tool to communicate the willingness of the data subjects to exercise the rights guaranteed to them by the GDPR.
The Data Controller or Privacy Referent/DPO is responsible for examining the requests received, involving the Data Processors involved in the request, giving feedback to the data subject as to whether the request has been taken in charge, and providing for requesting the necessary actions to process the request and finally giving feedback to the data subject as to the actions taken.

14. Notification procedure in the event of a data breach

Anyone within PRAGMA ETIMOS srl who has reason to believe that there has been a breach of the Personal Data processed, is obliged to immediately inform the Data Controller, the Privacy Representative/D.P.O. and, where present, the Data Processor; Specific training on this point will be provided to all those authorized to the processing.
Upon receipt of the report, the Data Controller, the Privacy Representative/D.P.O. and, where present, the Data Processor, must notify the competent supervisory authority by filling in Annex 7, without undue delay and, where possible, within 72 hours from the time of the assessment.

- The notification to the Supervisory Authority must contain:
- A description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned as well as the categories and approximate number of records of the personal data concerned;
- Provision of the name and contact details of the data protection officer or other point of contact from which more information can be obtained;
    (a) describe the likely consequences of the personal data breach;
    (b) describe the measures taken or proposed to be taken by the controller to remedy the personal data breach and also, where appropriate, to mitigate its possible adverse effects.

If it is not possible to provide the information at the same time as the notification, a reservation for subsequent integration must be formulated.
The Data Controller keeps a record of the violations that have occurred as explained in form 005.

15. Code of Conduct

The Code of Conduct has also been designed and conceived specifically for PRAGMA ETIMOS srl, specifically designed and developed pursuant to art. 40 of European Regulation 679:2016.

Il Titolare

Lo Presti Gaetano

(Revised 05/06/2023)