GDPR MANUAL
adopted pursuant to Art. 24 of Regulation (EU) 2016/679

Contents

1 - PURPOSE OF THE GDPR MANUAL

GR Elettronica S.r.l. (hereinafter the "Company"), in order to prove that its processing of personal data is compliant with Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter "GDPR"), has drawn up this document, i.e. the "GDPR Manual".

This document has been approved and updated by the top management and by the staff of the Company, with the help and support of the Data Protection Officer (DPO).

This Manual supersedes the Security Policy Document (Documento programmatico sulla sicurezza, DPS), which the Company kept updating until 2017; and it shall be the management and operating tool used to plan and monitor the adoption of appropriate technical and organisational measures pursuant to Articles 24 and 32 of the GDPR.

The GDPR Manual is therefore a valuable tool to:

- Define the tasks, instructions and responsibilities of the persons who - in various capacities - are tasked with personal data processing and with adopting security and protection technical and organisational measures;
- Describe corporate policies as well as any actions taken and requirements met in order to ensure an appropriate security level;
- Identify policies and measures allowing emergency management and ensuring business continuity and tool/data recovery;
- Specify actions allowing the control of the security system.

This Manual is comprised of paragraphs and Attachments:

- The paragraphs describe the actions to be taken and the general rules to be followed (as a consequence, they are available to everyone);

- The Attachments include the operating instructions and describe the technical and organisational measures taken by the Company (as a consequence, they are usually not publicly available, because they are documents of a confidential nature referring to critical processes).

2 – RESPONSIBLE ENTITIES - WHO

2.1. Data controller and data processor

The General Data Protection Regulation (GDPR), consistently with the Italian privacy code, identifies two special entities having specific responsibilities as concerns personal data processing, i.e.:

a) The **data controller**: GR Elettronica s.r.l. (hereinafter the "Company"), an entity considered as a whole and in the person of its provisional administrator;
b) The **data processor** (art. 28 GDPR): the natural or legal person providing sufficient guarantees in respect of the adoption of any appropriate technical and organisation measures needed in order for data processing to meet the requirements of the GDPR and to comply with the data subject's rights.

The data processors can be identified both inside the business organisation, i.e. the Company's employees, and outside, i.e. any figures who provide services or carry out an activity on behalf of the Company pursuant to a contract or deed and who are charged with data processing operations in the name and interest of the Company.

To this end, the Company draws up and updates a list of all the external collaborators, consultants and suppliers charged with activities and tasks entailing the need to access corporate electronic tools and consequently personal data for which the designation of a data processor needs to be made formal.

A list of the entities to be designated as data processors is available in Attachment **AL01**.

External entities can be charged with both operating tasks related to data processing operations and management functions of tools with privileged access profiles for which system administration functions are assigned.

Each entity listed in Attachment AL01 is therefore assigned the position of data processor by means of a special appointment letter (**AL02.01** and **AL02.02**) pursuant to art. 28 of the GDPR, based on whether the entity is an employee of the Company or an external entity.
The data processors are charged with the tasks and functions therein specified, included the tasks and functions related to system administration, if applicable.

2.2. Persons authorised to process personal data (i.e. persons tasked with data processing)

The data controller or data processor processes data through the appointment and help of natural persons, i.e. persons authorised to process personal data pursuant to art. 29 GDPR who, consistently with the privacy code, can still be called persons tasked with data processing.
According to the definition included in the GDPR, they are "anyone acting under the authority of the data controller or data processor, as duly instructed in writing".
Persons authorised to process personal data can be both inside and outside the business organisation, either self-employed or working inside an organisation.
Any person authorised to process personal data (i.e. persons tasked with data processing) is designated by the data processor through a special letter, whose general format is attached (**AL03**).

2.3. Personal Data Protection Officer (DPO)

The adoption of the GDPR has added to the entities mentioned in the two previous paragraphs the Personal Data Protection Officer (DPO), who is compulsory whenever data processing is carried out by a public authority and in the circumstances provided for in art. 37 of Regulation (EU) 2016/679.
The Company, although not required by law to do so, has decided to appoint a DPO in order to rely on a figure charged with consultancy and support tasks to the benefit of the data controller and data processors as well as GDPR-compliance monitoring tasks.
To this end a *data protection* expert was designated with the tasks listed in the appointment letter (**AL04**).

3 – LIST OF DATA PROCESSING TYPES - WHAT

The Regulation (EU) 2016/679 (GDPR) regulates the processing of personal data.

In particular:

- **Processing** means "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, erasure or destruction";
- **Personal data** means "**any information relating to an identified or identifiable natural person ("data subject")**; 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 on-line identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

An analysis of the definitions shows that the GDPR only and exclusively applies to the processing of personal data relating to natural persons, while the scope of application of the Regulation excludes any information on legal persons.

Personal data falls within two main categories:

1) S**pecial data:** any data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic data, biometric data, data concerning health or sex life or sexual orientation";

2) **Common data:** any information relating to natural persons identified or otherwise identifiable which is not likely to reveal states, facts and qualities under art. 9 of the GDPR whose processing is prohibited, unless the lawfulness and legitimacy presumptions under par. 2 of the article therein considered are applicable.

The Company, in order to properly handle data processing operations and prove that such processing is carried out in compliance with Regulation (EU) 2016/679, draws up and updates a list of electronic tools and computer systems that are used to process personal data or are considered critical for corporate processes in order to map the tools requiring protection.

The same Attachment also includes, together with the said tools and systems, a list of personal data processing types making up the basis for analysing and assessing the risks, for granting assignments and for making authorisations and instructions formal.

The list of tools and systems as well as of any data processing within the Company is included in Attachment (**AL05**).

4 – INSTRUCTIONS ON PERSONAL DATA PROCESSING AND PERSONAL DATA PROTECTION - HOW

4.1. Principles and purposes of security; definition of personal data processing modalities

In drawing up and updating this Manual, the Company has set the following security purposes:

1. To prove that appropriate technical and organisational measures were taken pursuant to art. 24 of the GDPR;
2. To ensure compliance with the privacy-by-design principle pursuant to art. 25 par. 1 of the GDPR;
3. To implement appropriate technical and organisational measures in order to ensure that, by default, only the personal data needed for each specific purpose (privacy by default) is processed pursuant to art. 25 par. 2 of the GDPR;
4. To reduce to acceptable and manageable levels any major security risks which might affect the Company's information system;
5. To keep the system as usable as possible, consistently with the security constraints provided for in the GDPR and any instructions by the National Supervisory Authority.

The definition of the tasks and instructions for the persons tasked with data processing is included in the relevant Attachment (**AL06**) and it also takes into account the Company's organization chart and organizational/operating manuals, to which reference is made in a dynamic and functional way and which are an integral and essential part of this Manual.

4.2. Data controller’s activities and actions ensuring compliance of data processing with the GDPR

The Company, in its capacity as data controller, determines the purposes and modalities of data processing.

Therefore, in order to ensure the compliance of data processing with the GDPR, the Company shall:

a) Appoint suppliers and entities outside the business organisation (listed in **AL01**) as external data processors by means of the model deed of appointment included in Attachment (**AL02**);

b) Designate as persons authorised to process personal data (i.e. persons tasked with data processing) the natural persons charged with data processing operations by means of the relevant letter (**AL03**);

c) Email (either to the individual address given by the Company or to the address specified upon signing the collaboration contract) to each person (either an employee or structured collaborator) written instructions for data processing (included in Attachment **AL06**);

d) Supervise compliance with the Company's instructions on security measures by the persons tasked with data processing and the entities appointed as external data processors, by taking any corrective and supplementary measures needed;

e) Collaborate with any entities charged with managing and administering the systems on defining the authorisation profile to be associated to the authentication credentials assigned to each person tasked with data processing. "Authorization profile" means "the set of information uniquely associated with a person that makes it possible to identify which data the said person can access and the data processing operations allowed to the said person". The authorization system is made up of the set of tools and procedures that enable access to the data and data processing modalities according to the applicant's authorization profile;

f) Demand that the authorization profile associated with each person tasked with data processing be disabled or changed, should the natural person cease to work within their structure of competence or if, for whatever reason, their professional profile was changed;

g) Supervise the activities carried out by the persons tasked with data processing by ensuring compliance with the Company’s operating procedures and instructions, including security measures.

The Company, as regards the management and maintenance of electronic tools, uses both internal staff and external entities appointed as system administrators in compliance with the Data Protection Authority's directions in the general provision of 27th November 2008, as amended and supplemented by the resolution of 25th June 2009.

The designation of natural persons as system administrators takes place by means of the model appointment letter included in Attachment **AL06**, which shall be delivered in person or sent by certified email (PEC) to the person or consultant to be appointed as system administrator or to be designated as external data processor with system administration functions.

The latter shall officially designate the natural persons charged with system administration tasks, in the interest and on behalf of the Company, which is the relevant data controller.

4.3. – Lawful data processing and information obligations

Personal data shall be processed in a lawful, fair and transparent manner pursuant to art. 5 of the GDPR.

Besides that, data shall be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.

Therefore, the data subject or the person providing the data shall, upon collection of the data, be duly informed in the modalities provided for under articles 12 – 13 – 14 of the GDPR.

To this end the Company has drawn up forms including the different information notices to be used for the said obligation.

In addition to the information obligation and in order for the data processing to be lawful, the legitimacy rules set forth for the collection and processing of common data and special data under articles 6 and 9 of the GDPR, respectively, shall be followed.

As concerns the processing of the personal data of which the Company is the controller, it is usually not necessary to acquire the data subject's consent, as the processing purposes are related to the performance or provision of services under a contract to which the data subject is a party, i.e. in order to fulfil a legal obligation.

The forms to be used to fulfil the information obligation and to acquire the data subject's consent by the person tasked with data processing, if needed, are included in Attachment **AL07**.

5 – SECURITY OF PERSONAL DATA – WHY

5.1. – Risk assessment and analysis, security plan

Art. 32 of the GDPR provides that "taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of data processing as well as the risk of

varying likelihood and severity for the rights and freedoms of natural persons, the data controller and the data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk".

Security can be defined as "the set of measures suitable to ensure the availability, integrity and confidentiality of managed information" and consequently "the set of all measures suitable to protect the information system from any threats of attack".

The risks of data loss - including accidental loss -, unauthorized access and unlawful or unauthorized data processing may be due to (by way of example and not of limitation):

- Malfunctioning of hardware and software systems, software applications and services;
- People outside the organization (hackers, spies, terrorists, vandals etc.);
- Natural disasters (floods, fires, earthquakes, storms etc.);
- People within the organization;

and they can be identified as:

- Accidental,
- Intentional.

Making a computer system secure entails not only implementing a whole set of specific technological and organizational countermeasures able to override all possible attacks to the service system, but also placing each identified countermeasure within an organic security policy which takes into account the technical, logistical, organizational, administrative and legislative constraints imposed by the technical and organisational structure in which the Company operates and which justifies each countermeasure within an overall framework.

Therefore, the main objective of a security system is the protection of information.

To this end, the so-called **R.I.D. Warranty** ("**Riservatezza – Integrità – Disponibilità"**, i.e. Confidentiality, Integrity, Availability) is required for all corporate automated information systems, electronic tools, paper documents and archives.

For the sake of completeness, the definitions of each warranty are as follows:

- **Confidentiality:** only authorized users can access the information needed;
- **Integrity:** protection against deterioration or damage; protection of data accuracy and completeness;
- **Availability:** the information is made available when required and within a relevant context.

The assets to be protected certainly include:

- Digital data;
- Paper documents;
- Information flows

as well as material components such as:

- Servers;
- Computers;
- Networks;

but also:

- Staff:
- Buildings;
- Offices.

The approach to security shall be based on a logic of prevention - use of risk management methods and tools - rather than on a logic of emergency management or mere control/supervision.

In order to meet all requirements in terms of security and protection of tools and data, the system architecture is based on 3 essential elements:

- Company's security policies;
- Organizational and technological solutions;
- Individual attitudes.

An information security management system that is efficient and effective enables the organization to:

- Keep abreast of new threats and vulnerabilities and consider them in a systematic manner;
- Handle accidents and losses with a view to prevention and continuous improvement of the system;
- Get to know when security policies and procedures are not implemented soon enough to prevent potential damage;
- Implement major policies and procedures.

Technical and organisational measures shall be taken by using a **self-determination process**. Care shall therefore be taken to reduce any risks which may affect processed personal data within the Company and which concern the information system as a whole.

The Company's system of personal data protection is based on the following general principles:

- All information (data, documents, archives, ...) shall be protected and made available;
- In order to ensure the confidentiality of contents and information, security must also cover electronic data communication networks;
- Security measures for the protection of any areas and premises housing paper files and servers deemed "sensitive" for corporate activities shall be provided for. The relevant technical features and protection measures against unauthorized access shall be monitored;
- All data processing operations carried out using tools connected to the electronic communications network shall be traceable, ensuring the non-repudiation of the operations carried out based on a system of digital authentication that makes it possible to check the identity of "who is doing what";
- Adequate technical and organisational security measures shall be provided for as concerns access to the premises housing any servers and electronic tools used, possibly locating and placing them either in one single location or in connected locations, in order to allow improved management of the tools as well as of active and passive security;
- Any extraordinary event or accident likely to affect data and system security shall be analysed and reported in written form;
- All projects for the development of new systems and/or services that have a transversal nature and may affect the Company's information system, shall be managed in compliance with the provisions of this Manual;
- Likewise, any changes made to organizational processes shall be documented either in this Manual or in the documents of the Company's quality system.

In particular, the risk analysis and assessment are carried out based on the attached table **AL08** by identifying the individual threats and vulnerabilities for which the extent of the risk was determined in terms of probability (P) and damage (D) according to the parameters (high - medium - low) associated with each threat.

Upon completion of the analysis and risk assessment and subject to art. 32 of the GDPR, the technical and organisational security measures listed and described in the security plan included in Attachment **AL09** are determined.

The security plan is comprised of three parts:

1) A description of the security measures taken upon completion of the analysis and risk assessment as shown in Attachment AL08;
2) An emergency plan on natural events (i.e. disasters) or intentional/negligent human actions that may disrupt work processes or information flow continuity, causing stoppages and non-conformities. The emergency plan is *5.2. Emergency management; restoration of data and tool availability*, adopted in order to ensure conformity with certification standards - see the Company's documentation in use;
3) An operating manual, which describes the technical and organisational security measures and gives advice on how to properly use the devices and carry out data processing operations.

5.2. Emergency management; restoration of data and tool availability

The Company, within the framework of the certification system of corporate processes, has drawn up a plan to analyse and assess activities and events liable to cause the disruption or stoppage of production processes (as referenced in Attachment **AL09**).

Such events affect corporate and production processes that make up the Company's core business and require thorough analysis and assessment.

From the point of view of data protection, "business continuity" means "the set of activities aimed to restore the state of the computer system or part of it, including the physical/organizational aspects and the people needed for its operation, in order to bring it back to its condition before the disaster".

In order to ensure the business continuity of the systems and consequently of personal data processing, and in order to cope with events likely to cause damage to the electronic tools and the destruction or loss of critical information, actions designed to cope with any emergency and production process disruption should be provided for.

Therefore, continuity solutions shall take into account the effect of an event and not its causes.

On the contrary, the prevention of such events is usually entrusted to methods of intervention (such as measures for the security and physical integrity of tools and data) that are not classified as "continuity solutions".

In order to ensure production continuity, the Company shall define, within the framework of the emergency plan (mentioned or referenced in Attachment **AL09**):

a) The procedures for business continuity management, including outsourced procedures. The plan shall take into account any potential criticalities related to human, structural and technological resources and shall comprise appropriate preventive measures. The Company shall test the functionality of its business continuity plan on a yearly basis;

b) The ***disaster recovery plan*** (which is part of the business continuity plan mentioned under a): it identifies the technical and organizational measures needed to ensure the operation of major IT procedures and data processing centres at sites that are alternative to production sites.

The Company's business continuity plan relates to critical activities and processes.

The continuity plan is drawn up and the business continuity measures are adopted in compliance with the following principles:

1) Analysis of the context and possible emergency situations following natural events or human behaviours/events causing the destruction or loss of data and tools or blocking the system, resulting in disrupted institutional and service activities;
2) Identification of the events likely to disrupt business continuity that should be taken into account;
3) Identification of scheduled and non-scheduled events that may result in disrupted business continuity;
4) Identification - for each critical service or process to be protected - of the set of technological, procedural, workspace and human resources needed to restore the provision of such service or process.
5) Identification of any measures needed to ensure its operational effectiveness. Consequently, procedures should be provided for to ensure business continuity, in particular data copying and recovery as well as parallel systems;
6) Planning of measures for personal data recovery following damage or destructive events;

7) Identification of the security measures to be taken to ensure business continuity and to restore data and systems within no more than seven days from the event;

8) Scheduling of the in-house controller's inspection of the proper operation of systems and organizational procedures for business continuity and data recovery, both by in-house staff and by external entities charged with adopting the procedures and implementing the systems.

Two different indicators shall be considered in order to define to what extent a critical system should be kept in operation:

1) **RTO** (**Recovery Time Objective** - maximum time of unavailability of the service), i.e. the time within which the service must be restored;

2) **RPO** (**Recovery Point Objective -** sustainable data loss), time between the occurrence of an emergency and the latest useful and recoverable data saving.

For example, the need for a service or process to be restarted within 48 hours from an emergency and the requirement not to lose more than 6 hours of data updating shall entail that the parameters are set as follows:

- RTO = 48 h;
- RPO = 6 h.

The study of the context is characterised by two different steps:

1) Risk analysis: determination of the risks to which a critical processing unit or provided service is subject; analysis of vulnerabilities; identification of possible safeguards;

2) Business impact analysis: its purpose is to identify the consequences of each critical event and to assess their impact on the organization's operation.

The plan for emergencies, business continuity and data recovery management (included in section 2 of Attachment **AL09**) shall take into account at least the following scenarios of crisis:

- Inaccessibility or destruction of structures housing operating units or equipment critical for each processing unit;

- Unavailability of staff essential to ensure the continuity or operation of critical tools;

- Disrupted operation of infrastructure (including power supply, electronic communications networks, blocked or damaged tools);
- Data corruption due to malicious attacks;
- Unavailability of systems and tools as a result of malicious attacks by third parties.

The business continuity and recovery plan shall state:

- The measures needed to reduce the impact of an emergency;
- Any resources alternative to unavailable resources;
- Any organizational measures controlling the system during an emergency;
- Any procedures for managing the return to normalcy.

In preparing the recovery plan (also called "disaster recovery plan"), the following operations shall be carried out:

1) Definition of roles and responsibilities;
2) Analysis of events that can lead to the destruction or corruption of data or electronic tools;
3) Description of actions to be taken in an emergency for system and data recovery.

In order to ensure business continuity and verify the system administrators' work and the compliance of security measures with the relevant regulations governing data protection, the Company shall appoint an entity to an independent impartial position (using attached form **AL10)** to whom surveillance and control functions shall be assigned, also in order to ensure that the security and protection measures comply with the GDPR pursuant to articles 24 and 32 of Regulation (EU) 2016/679.

List of Attachments to the GDPR Manual

Document	Description	Latest revision	Reason(s) for update	Recipients	Distribution methods
AL01	List of external collaborators, consultants and suppliers	25/05/2018	First version	Reserved document	Internal document
AL02.01	Designation letter of internal data processor	31/01/2019	First revision	Company's employees	Designation through delivery of paper material or email or publication on the web site's reserved area
AL02.02	Designation letter of external data processor	31/01/2019	First revision	Company's collaborators, consultants and suppliers	Designation through letter sent by certified email (PEC) to the address shown on portal www.inipec.gov.it
AL03	Designation letter of persons authorised to process personal data	31/01/2019	First revision	Employees, collaborators, temporary workers, consultants	Designation through delivery of paper material or email or publication on the web site's reserved area
AL04	Designation of personal data protection officer	25/05/2018	First version	Data Protection Officer (DPO)	Certified email (PEC) to the relevant entity
AL05	List of electronic tools and personal data processing types	25/05/2018	First version	Reserved document	Internal document
AL06	Instructions on data processing	31/01/2019	First revision	Data processors Persons authorised to process personal data	Certified email (PEC) or publication on reserved area or delivery by hand
AL07.01 _____ AL07.02 _____ AL07.03	Forms for consent and information notices	31/01/2019 _____ 25/05/2018 _____ 25/05/2018	First revision _____ First version _____ First version	Customers, suppliers, employees, collaborators, workers	Add information notice to delivery notes, invoices, emails Delivery to each employee or collaborator when they are employed or sign the contract Collection of consent, whenever needed, through signature of one copy of the information form
AL08	Risk assessment and analysis	25/05/2018	First version	Reserved document	Internal document
AL09	Security plan	31/01/2019	First revision	Reserved document	Internal document
AL10	Appointment of control and supervision operator	25/05/2018	First version	Control and supervision operator	Signature as acknowledgement of receipt and acceptance of one copy of the assignment letter upon appointment