PROCEDURE FOR MANAGING VIOLATIONS OF PERSONAL DATA

in application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data

RPS S.p.A. ***Riello Power Solutions***
37045 Legnago (VR) - ITALY - Viale Europa 7 - T +39 0442 635811 - F +39 0442 629098
www.riello-ups.com - riello@riello-ups.com
CAPITALE SOCIALE € 1.230.278 i.v. - R.E.A. VR n° 252286 - Registro Imprese / C.F. / P.IVA 02647040233

INDEX

RPS S.p.A. ***Riello Power Solutions***
37045 Legnago (VR) - ITALY - Viale Europa 7 - T +39 0442 635811 - F +39 0442 629098
www.riello-ups.com - riello@riello-ups.com
CAPITALE SOCIALE € 1.230.278 i.v. - R.E.A. VR n° 252286 - Registro Imprese / C.F. / P.IVA 02647040233

1. INTRODUCTION

RPS S.p.A. (hereinafter, also, "**Owner**" or "**Company**") is required, pursuant to

(i) of the General Data Protection Regulation - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data (hereinafter "**GDPR**") and

(ii) of Legislative Decree no. 196/2003 containing the "Code regarding the protection of personal data" integrated with the changes introduced by Legislative Decree no. 101/2018 (hereinafter the "**Code**"), hereinafter, jointly, "**Regulations on the protection of personal data**",

to keep the personal data processed in the context of their activities safe and to act without undue delay in the event of a data breach (including any notifications to the competent Guarantor Authority and any communications to interested parties).

It is of fundamental importance to prepare actions to be implemented in the event of alleged, potential or actual violations of personal data, this is in order to avoid risks for the rights and freedoms of the data subjects, as well as economic damage to the Company and to be able to detect in the times and in the manner provided for by the GDPR, the Guarantor Authority and/or the interested parties.

2. PURPOSE

The purpose of this procedure is to define the flow of activities for the management of violations of personal data processed by the Data Controller.

3. RECIPIENTS

This procedure is aimed at all subjects who for any reason process personal data within the competence of the Data Controller such as:

- employees, as well as those who in any capacity - and therefore regardless of the type of relationship - have access to personal data processed during their employment on behalf of the Data Controller (hereinafter "**Internal recipients**");
- any subject (natural person or legal person) other than Internal recipients who, by virtue of the contractual relationship in place with the Data Controller, has access to the aforementioned data and acts as Data Processor pursuant to art. 28 of the GDPR or autonomous Data Controller (hereinafter "**External recipients**"),

Both Internal recipients and External recipients are hereinafter generically referred to as "Recipients".

All Recipients must be duly informed of the existence of this procedure, by means of methods and means to ensure their understanding.

4. DEFINITIONS

- *personal data,* any information concerning an identified or identifiable person; the person is considered identifiable if they can be identified, directly or indirectly, with particular reference to an identifier such as the name, an identification number, location data, an online identifier or one or more characteristic elements of their physical identity, physiological, genetic, psychological, economic, cultural or social (hereinafter "**Personal Data**");
- *treatment*, any operation or set of operations, carried out with or without the aid of automated processes and applied to personal data or sets of personal data, such as the collection, registration, organization, structuring, storage, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, comparison or interconnection, limitation, cancellation or destruction (hereinafter "**Treatment**");

RPS S.p.A. ***Riello Power Solutions***
37045 Legnago (VR) - ITALY - Viale Europa 7 - T +39 0442 635811 - F +39 0442 629098
www.riello-ups.com - riello@riello-ups.com
CAPITALE SOCIALE € 1.230.278 i.v. - R.E.A. VR n° 252286 - Registro Imprese / C.F. / P.IVA 02647040233

- *data controller*, the person, public Authority, service or other body which, individually or together with others, determines the purposes and means of the treatment of personal data; when the purposes and means of such treatment are determined by the law of the European Union or of the Member States, the data controller or the specific criteria applicable to his designation may be established by the law of the Union or of the Member States (hereinafter "**Data Controller**");
- *data processor*, the person, public Authority, service or other body that processes personal data on behalf of the data controller (hereinafter "**Manager**");
- *interested*, any identified or identifiable natural person (hereinafter "**Interested**");
- *data protection officer*, is a technical consultant designated by the data controller, whose skills are governed by the GDPR (hereinafter "**DPO**" or "**RPD**");
- *team privacy*, is a group of people appointed by the Data Controller with the function of:
  (i) carrying out, also with the help of external consultants appointed by the Company, all the related and necessary activities for compliance with the legislation on the protection of personal data;
  (ii) managing the Privacy Organizational Model adopted by the Data Controller;
  (iii) liaising with the DPO
  (hereinafter "**Team privacy**");
- *supervisory authority*, the independent public authority established by a Member State pursuant to Article 51 of the GDPR (for Italy this authority is identified with the "Guarantor for the protection of personal data") (hereinafter the "**Authority**");
- *breach of personal data*, the breach of security that accidentally or unlawfully involves the destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed (hereinafter "**Violation**" or "**Data Breach**").

Violations can occur for various reasons which may include but are not limited to:

- disclosure of confidential data to unauthorized persons;
- loss or theft of data or tools in which the data is stored;
- loss or theft of paper documents;
- corporate infidelity (for example: a data breach caused by an internal person having authorization to access the data produces a copy distributed in a public environment);
- unauthorized access (for example: a data breach caused by unauthorized access to systems computer with subsequent disclosure of the information acquired);
- cases of computer piracy;
- databases altered or destroyed without authorization issued by the relative “owner”;
- viruses or other attacks on the computer system or company network;
- violation of physical security measures (for example: forcing doors or windows of rooms security or archives, containing confidential information);
- loss of laptops, devices or company IT equipment;
- sending e-mails containing personal and/or particular data to an erroneous recipient.

5. MANAGEMENT OF VIOLATION COMMUNICATION

Violations are managed by the Data Controller with the help of the Team Privacy and with the supervision of the DPO.
Specifically, the Team Privacy and the DPO have the task of assisting the Data Controller in resolving issues relating to a suspicious, presumed or actual Data Breach event, expressing themselves in relation to the following aspects (exemplary and not exhaustive) where applicable:

1. determine whether or not the breach in question should be considered a breach;
2. assign a severity level to the Violation;

RPS S.p.A. ***Riello Power Solutions***
37045 Legnago (VR) - ITALY - Viale Europa 7 - T +39 0442 635811 - F +39 0442 629098
www.riello-ups.com - riello@riello-ups.com
CAPITALE SOCIALE € 1.230.278 i.v. - R.E.A. VR n° 252286 - Registro Imprese / C.F. / P.IVA 02647040233

3. ensure that a correct and impartial investigation is initiated, conducted, documented and concluded;
4. identify the requirements for resolving the Violation and monitor the solution;
5. coordinate with the Authority;
6. coordinate internal and external communications;
7. ensure that involved parties are adequately informed.

If deemed appropriate and necessary, following the outcome of the first analyzes conducted on the potential degree of severity and specificity of the Violation, the Data Controller, having also consulted the Team Privacy and the DPO, may also involve additional experts in the management activities of the Data Breach. external (by way of example, an IT security expert or an external communication agency to assist the Data Controller in case of need for communication to third parties).

In the event of a suspected, presumed or actual breach, it is extremely important to ensure that the same is dealt with immediately and correctly in order to minimize the impact of the breach and prevent its possible repetition.

In the event that one of the Recipients becomes aware of a suspected, presumed or actual Violation, he must immediately notify as follows:

(i) if they are an Internal recipient, to his area/function manager who will deal with the support of the recipients themselves, to inform the Data Controller by completing **Annex A** - "Data Breach communication form" to be delivered by hand or sent by e-mail to privacy@riello-ups.com;

(ii) if it is an External recipient, inform the Data Controller without undue delay by completing **Annex A** - "Data Breach external communication form" to be sent by e-mail to privacy@riello-ups.com

6. VIOLATION MANAGEMENT PROCESS

To manage a personal data breach it is necessary to follow the following steps:
Step 1: Identification and preliminary investigation
Step 2: Containment, data recovery and risk assessment
Step 3: Eventual notification to the Authority
Step 4: Possible communication to the involved parties
Step 5: Documentation of the breach

Step 1: Identification and preliminary investigation

Annex A, duly completed, will allow the Data Controller, with the help of the Team Privacy and with the support of the DPO, to conduct an initial assessment regarding the communication received, in order to establish whether a hypothesis of Data Breach and whether a more in-depth investigation of the incident is necessary, proceeding in this case with Step 2.
In the event of a breach of data contained in an IT system, the Data Controller must also involve the IT Manager or their delegate in the event of absence in the entire procedure indicated in this document.

Step 2: Containment, data recovery and risk assessment

Once it has been established that a Data Breach has occurred, the Data Controller together with the Team Privacy and the DPO will have to establish:

- if there are actions that could limit the damage that the Violation could cause (ie physical repair of instrumentation; use of backup files to recover lost or damaged data; isolation/closure of a compromised sector of the network; change of access codes ... etc.);
- once these actions have been identified, who are the subjects who must act to contain the Violation;
- whether it is necessary to notify the Authority of the Violation (where it is likely that the violation

RPS S.p.A. ***Riello Power Solutions***
37045 Legnago (VR) - ITALY - Viale Europa 7 - T +39 0442 635811 - F +39 0442 629098
www.riello-ups.com - riello@riello-ups.com
CAPITALE SOCIALE € 1.230.278 i.v. - R.E.A. VR n° 252286 - Registro Imprese / C.F. / P.IVA 02647040233

presents a risk to the rights and freedoms of individuals);
- whether it is necessary to communicate the violation to the involved parties (where the violation presents a high risk for the rights and freedoms of individuals).

In order to identify the need for notification to the Authority and communication to the involved parties, the Data Controller, assisted by the Team Privacy and the DPO, will assess the seriousness of the Violation using a specific "Data Breach Risk Assessment Form" which must be examined together with Annex A, also taking into due consideration the principles and indications referred to in Articles 33 and 34 of the GDPR.

Step 3: Eventual notification to the Authority
Once the need to notify the Authority of the Violation suffered on the basis of the procedure referred to in Step 2 has been assessed, as required by the GDPR, the Data Controller must do so, without undue delay and, where possible, within 72 hours from the moment in which he became aware of.
If the notification to the Authority is not made within 72 hours, the communication must also be accompanied by the reasons for the delay.

The notification must at least:
a) describe the nature of the Violation including, where possible, the categories and approximate number of Data Subjects concerned as well as the categories and approximate number of personal data records in question;
b) communicate the name and contact details of the DPO or other contact point from which to obtain more information;
c) describe the likely consequences of the Violation;
d) describe the measures taken or proposed to be adopted by the Data Controller to remedy the breach and also, where appropriate, to mitigate any possible negative effects.

If and to the extent that it is not possible to provide the information at the same time, the information may be provided to the Authority in subsequent stages without further undue delay.

Step 4: Possible communication to the interested parties
Once the need to communicate the Violation to the Data Subjects has been assessed on the basis of the procedure referred to in Step 2, as required by the GDPR, the Data Controller must do so, without undue delay.
The communication to the interested parties must be written in clear and simple language and must contain:
a) the name and contact details of the DPO or other contact point from which to obtain more information;
b) a description of the likely consequences of the Violation;
c) the description of the measures taken or which the Owner proposes to adopt to remedy the Violation and, if necessary, to mitigate its possible negative effects.

As for the methods of communication, case by case, the Data Controller must always privilege the method of direct communication with the interested parties (such as e-mail, SMS or direct messages). The message must be communicated in a simple and transparent way, thus avoiding sending the information in the context of newsletters, which could be easily misunderstood by the interested parties. In the event that direct reporting requires an effort deemed disproportionate, then a public communication can be used, which must be equally effective in direct contact with the interested party.

Step 5: Documentation of the Violation
Regardless of the need to notify the Authority (step 3) and/or notify the Data Subjects (Step 4) of the Violation, whenever a potential Data Breach is communicated by the Recipients through attachment A, the

RPS S.p.A. ***Riello Power Solutions***
37045 Legnago (VR) - ITALY - Viale Europa 7 - T +39 0442 635811 - F +39 0442 629098
www.riello-ups.com - riello@riello-ups.com
CAPITALE SOCIALE € 1.230.278 i.v. - R.E.A. VR n° 252286 - Registro Imprese / C.F. / P.IVA 02647040233

Data Controller is required to document it.
This documentation activity will be implemented through the maintenance by the Owner, with the help of the Team Privacy, of a special "Register of breach of personal data".
The Personal Data Breach Register must be continuously updated and made available to the Authority if it requests access.

7. LIABILITY

Compliance with this procedure is mandatory for all Recipients and failure to comply with the provisions of the same may result in disciplinary measures against non-compliant employees or the termination of existing contracts with non-compliant third parties, in accordance with the regulations in force.

8. PERIOD OF PRESERVATION OF THE RECORDS ON THE BASIS OF THIS DOCUMENT

Document	Legal basis of the treatment	Retention period
Data Breach internal and external communication modules	(Article 6, paragraph 1, letter c), GDPR) Treatment necessary to fulfill a legal obligation to which the Data Controller is subject (Article 6, paragraph 1, letter f), GDPR) Treatment necessary for the pursuit of the legitimate interest of the Data Controller connected to the management of its organization	Permanent
Documented decisions of the Data Controller regarding the Violation	(Article 6, paragraph 1, letter c), GDPR) Treatment necessary to fulfill a legal obligation to which the Data Controller is subject (Article 6, paragraph 1, letter f), GDPR) Treatment necessary for the pursuit of the legitimate interest of the Data Controller connected to the management of its organization	5 years
Notification of a Violation	(Article 6, paragraph 1, letter c), GDPR) Treatment necessary to fulfill a legal obligation to which the Data Controller is subject (Article 6, paragraph 1, letter f), GDPR) Treatment necessary for the pursuit of the legitimate interest of the Data Controller connected to the management of its organization	5 years
Personal data breach log	(Article 6, paragraph 1, letter c), GDPR) Treatment necessary to fulfill a legal obligation to which the Data Controller is subject (Article 6, paragraph 1, letter f), GDPR) Treatment necessary for the pursuit of the legitimate interest of the Data Controller connected to the management of its organization	Permanent

9. MANAGEMENT OF THIS DOCUMENT

The person in charge of this document is the Owner, who must check the document at least annually and, where necessary, make any changes/updates.

Attachment:

- "A - Data Breach internal communication module"

RPS S.p.A. ***Riello Power Solutions***
37045 Legnago (VR) - ITALY - Viale Europa 7 - T +39 0442 635811 - F +39 0442 629098
www.riello-ups.com - riello@riello-ups.com
CAPITALE SOCIALE € 1.230.278 i.v. - R.E.A. VR n° 252286 - Registro Imprese / C.F. / P.IVA 02647040233

Annex "A" - Data Breach communication form

If a suspected, presumed or actual breach of personal data is detected, it is necessary to immediately notify the Data Controller by completing the following form to be sent by e-mail to the following address: privacy@riello-ups.com

Data Breach Communication:

□ **INTERNAL RECIPIENT ***

Details of the person making the report:

Surname and name	
Assignment/Duties	
Contact details (e-mail address, telephone number)	

□ **EXTERNAL RECIPIENT ***

Data of the person making the report:

Company name	
Contact details of the DPO (where appointed)	
Surname and name of the reporting subject	
Contact details (e-mail address, telephone number)	

* indicate, alternatively, whether the person making the report is an internal Recipient or an external Recipient.

*****

DESCRIPTION OF THE EVENT

Date of discovery of the violation (date, time)	
Date and place of the violation (date, time, place)	
Description of what happened	

RPS S.p.A. ***Riello Power Solutions***
37045 Legnago (VR) - ITALY - Viale Europa 7 - T +39 0442 635811 - F +39 0442 629098
www.riello-ups.com - riello@riello-ups.com
CAPITALE SOCIALE € 1.230.278 i.v. - R.E.A. VR n° 252286 - Registro Imprese / C.F. / P.IVA 02647040233

Description of how it happened	
Categories and approximate number of data subjects involved in the violation	
Other relevant details (any actions taken at the time of discovery of the violation, etc.)	

By the Data Controller (or of the contact person appointed by it)		**DATE AND TIME OF RECEIPT OF THE FORM:**	
Reception mode:		Progressive reporting number (from Data Violation Register):	
Systems involved:			
Vulnerabilities detected:			

RPS S.p.A. ***Riello Power Solutions***
37045 Legnago (VR) - ITALY - Viale Europa 7 - T +39 0442 635811 - F +39 0442 629098
www.riello-ups.com - riello@riello-ups.com
CAPITALE SOCIALE € 1.230.278 i.v. - R.E.A. VR n° 252286 - Registro Imprese / C.F. / P.IVA 02647040233