B.T.V. S.p.A.
Sede Legale: Via Luca Della Robbia, 25 - 36100 VICENZA
Tel. 0444 394600 - Fax 0444 394678
C.F. - Reg. IMPR e P.IVA 03277970244
Cap. Soc. € 2.010.000,00 i.v. - R.E.A. VI - 312.681

PROCEDURE FOR PERSONAL DATA BREACH

pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council dated 27th of April 2016, concerning protection of natural persons with regard to the processing of personal data and free circulation of data

INDEX

1. PREFACES

B.T.V. S.P.A (HEREINAFTER, "OWNER" OR "COMPANY") IS REQUIRED, UNDER

(i) General Regulation on Data Protection - (EU) 2016/679 Regulation of the European Parliament and Council of 27th April 2016, concerning natural persons protection with regard to the processing of personal data and free circulation of the a.m. data (herinafter named "**GDPR"**) and
(ii) n. 196/2003 Legislative Decree including "Personal Data Code" and completed with modications of n. 101/2018 Legislative Decree (herinafter named **"Code"**),

hereinafter, together with "**Regulation of personal data**",
to preserve personal data safe within its activity and act without undue delay in case of breach of the same data (including any notifications to the Guarantor Authority in charge and any communications to the interested parties).
It is of paramount importance to establish any actions to be implemented in the event of alleged, potential or actual violations of personal data. It avoids any risk to the rights and freedom of the interested parties, as well as any economic damage to the Company. And it allows to intervene early, according to GDPR with regard to the Guarantor Authority and/or the interested parties.

2. PURPOSE

The purpose of this procedure is to define the flow of activities to manage personal data breaches which are handled by the Data Controller.

3. RECIPIENTS

This procedure is addressed to all subjects dealing with personal data which are in charge of the Data Controller, such as:

- Employees, as well as those people who for any reason - and regardless of their kind relationship with - have access to personal data processed during their employment relationship on behalf of the Data Controller (hereinafter "**Internal Recipients**");
- any subject (either natural or legal person) other than internal Recipients who, in reason of the relationship with the Data Controller, has access to the aforementioned data and works either as Data Processor pursuant to art. 28 of the GDPR or independent Data Controller (hereinafter "**External Recipients**") hereinafter generically referred to as "**Recipients"**.

All recipients must be duly informed of the existence of this procedure, through any method and means which simplify its understanding.

4. DEFINITIONS

- *personal data*, any information relating to an identified or identifiable natural person; an identifiable natural person is one person who can be identified, either directly or indirectly, with particular reference to an identifier such as a name, an identification number, any location data, an online identifier or one or more elements specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (hereinafter "**Personal Data**");
- *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 methods, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other way of making available, comparison or interconnection, limitation, erasure or destruction (hereinafter "**Processing**");
- *data controller*, the natural or legal person, public authority, agency or any other body which, alone or together with others, defines purposes and means of the processing of Personal Data; in case the purposes

and means of such processing are determined by Union right or Member State law, the data controller or the specific criteria applicable to its designation may be established by Union or Member State law (hereinafter "**Data Controller**");

- *data processor*, the natural or legal person, public authority, service or other body that processes personal data on behalf of the data controller (hereinafter "**Processor**");
- *data subject*, any identified or identifiable natural person (hereinafter "**Data Subject**");
- *data protection officer or data protection officer responsible*, is a technical consultant appointed by the data controller, whose skills are regulated by the GDPR (hereinafter "DPO" or "DPO");
- *privacy team*, is a group of people appointed by the Data Controller with the function of:
  (i) carrying out all the activities which are related and necessary for *compliance* according to the Legislation on the protection of personal data, also by means of external consultants appointed by the Company;
  (ii) to manage the Privacy Managing Model adopted by the Data Controller;
  (iii) to relate with DPO (hereinafter "**Team Privacy**")
- *Authority od control,* an independent public authority established by a Member State pursuant to Article 51 of GDPR (for Italy, this Authority is identified with the "Guarantor for the protection of personal data") (hereinafter "**Authority**");
- *Breach of personal data*, breach of security that involves accidentally or unlawfully destruction, loss, modification, unauthorized disclosure or access to personal data which have been spread, stored or processed (hereinafter "**Breach**" or "**Data Breach**").

Breaches might occurr for different reasons, including for example:

- disclosure of confidential data to unauthorized persons;
- loss or theft of data or instruments in which the data are stored;
- loss or theft of paper documents;
- company inaccuracy (for instance: data breach caused by an internal person who is authorized to access the data and discloses a copy of it in a public environment);
- abusive access (for example: data breach caused by unauthorized access to systems computer systems with subsequent disclosure of the information acquired);
- cases of computer piracy;
- modified databases or destroyed without authorization issued by the respective "owner";
- viruses or other attacks on computer systems or to the company network;
- violation of physical security measures (for example: forcing of doors or windows of security rooms or archives, containing confidential information);
- loss of laptops, devices or company computer equipment;
- sending e-mails containing personal data and/or details to the wrong recipient.

5. MANAGEMENT OF BREACH COMMUNICATIONS

Violations are managed by the Data Controller with the help of the Privacy Team and under the DPO supervision. In particular, the Privacy Team and the DPO have the task of supporting the Data Controller in resolving issues relating to a alleged, presumed or actual Data Breach event, with regard to the following aspects (exemplary and non-exhaustive) where applicable:

1. to establish whether or not the breach in question should be considered a Violation;
2. to assign a severity level to the Violation;
3. to ensure that a fair and impartial investigation is set off, conducted, documented and concluded;
4. to identify the requirements to solve the Breach and monitor the solution;
5. to co-operate with the Authority;
6. to organize either in or out communications;
7. to ensure that data subjects are adequately informed.

Following the first analysis on the potential degree of seriousness and peculiarity of the Breach, the Data Controller, together with the Privacy Team and the DPO, may also involve additional external experts in the Data Breach management activities if deemed necessary (for example, an IT security expert or an external Communication agency in order to support the Data Controller in case of need for communication to third parties).

In the event of a suspect, alleged or actual Breach, it is of utmost importance to ensure that the Breach is handled with immediately and correctly so as to reduce the impact of the Breach and avoid any possible occurrence.

In the event that one of the Recipients notices a suspect, alleged or actual Violation, he must immediately notify it as follows:

(i) if it is an internal Recipient, to its ept. Manager who will inform, with the support of the recipients th the Data Controller by filling in Annex **A** – "Data Breach Communication form" to be sent by email at privacy@battistolli.it and for information at dpo@battistolli.it.

(ii) if it is an external Recipient, the Data Controller must be informed without undue delay by filling in Annex **A** – "Data Breach external communication form" to be sent by email to the privacy@battistolli.it address and for information to dpo@battistolli.it address.

6. MANAGEMENT OF BREACH PROCESS

To manage a personal data breach the following steps must be observed:
Step 1: Identification and preliminary investigation
Step 2: Control, data recovery and risk assessment
Step 3: Possible notification to the Authority
Step 4: Possible communication to the interested parties
Step 5: Documentation of the Violation

Step 1: Identification and preliminary investigation
Annex A, duly filled in, will allow the Data Controller to carry out an initial assessment about the communication received, together with the help of the Privacy Team and with the support of the DPO. This is aimed at proving whether a Data Breach event has actually occurred or if a more in-depth investigation is required, proceeding in this case with step 2.
In the event of a breach of an IT system data, the Data Controller must also involve the IT Manager or a representative in case of absence, about the whole procedure of the present document.

Step 2: Control, data recovery and risk assessment
Once a Data Breach has occurred, the Data Controller together with the Privacy Team and the DPO must establish as follows:
• if there are any possible actions to reduce the damage caused by the Breach (i.e. tool physical fixing up; use of backup files to recover lost or damaged data; isolation/close of a damaged sector of the network; change of access codes... etc.);
• once the a.m. actions have been identified, who are the subjects who must act to limit the Violation;
• whether it is necessary to notify the Violation to the Authority (in the event that the violation is likely to entail a risk for the rights and freedoms of natural persons);
• whether it is necessary to communicate the violation to the data subjects (in the event that the violation has a high risk for the rights and freedoms of natural persons).

In order to identify the need for notification to the Authority and communication to the interested parties, the Data Controller, together with the Privacy Team and DPO, will assess the seriousness of the Violation by means of a special "Risk Assessment Form related to the Data Breach" which must be examined together with Annex A. Principles and hints as per Articles. 33 and 34 of the GDPR must also be taken into account.

Step 3: Possible notification to the Authority
Once the need to notify the Violation suffered by the Authority has been assessed - according to the procedure as per step 2, as required by the GDPR- the Data Controller must do so, without undue delay and if possible within 72 hours he was acquainted with it.
If the notification to the Authority is not made within 72 hours, the notification shall also be accompanied by an explanation about the reasons for such a delay.

The notification shall at least:
a) describe the nature of the Breach including, if possible, either categories and approximate number of Data Subjects or categories and approximate number of records of the personal data which are concerned;
b) communicate the name and contact details of the DPO or of any other contact point to get more information;
c) describe the consequences which may arise from the Violation;
d) describe the measures taken by the Data Controller to remedy the Breach and also to mitigate its possible negative effects.

Whether it is not possible to provide the information at the same time, the information shall be provided to the Authority in subsequent stages without further undue delay.

Step 4: Possible communication to interested parties
Once the need to communicate the Breach to the Data Subjects has been, assessed according to the procedure described in step 2, as required by the GDPR, the Data Controller must do so, without undue delay.
The communication to interested parties must be written in a clear and simple language and must contain:
a) the name and contact details of the DPO or other contact point to get more information;
b) a description of the likely consequences of the Breach;
c) a description of the measures taken or proposed by the Data Controller to remedy the Breach and, where appropriate, to mitigate its possible negative effects.

As far as the methods of communication are concerned, on a case-by-case basis, the Data Controller must always prefer the method of direct communication with the interested parties (such as email, text messages or direct messages). The message must be communicated in a simple and transparent manner, thus avoiding sending the information by means of newsletters, which could be easily misunderstood by the interested parties. In the event that direct reporting requires an effort which is deemed excessive, a public communication may be used, which must be equally effective in direct contact with the data subject.

Step 5: Documentation of the Breach
Regardless of the need to notify the Authority (step 3) and/or the communication to the Data Subjects (step 4) of the Breach, whenever a potential Data Breach is communicated by the Recipients through Annex A, the Owner is required to provide documentary evidence of it.
This documentation activity will be carried out by the Data Controller, with the help of the Privacy Team, through the keeping of a special "Register of personal data breaches".
The Register of Personal Data Breaches should be continuously updated and made available to the Authority if required to.

7. EMPOWERMENT

Compliance with the a.m. procedure is mandatory for all Recipients and failure to comply with the provisions of the same may result in disciplinary measures against defaulting employees, that is to say the termination of existing contracts with defaulting third parties, according to the regulations in force.

8. RETENTION PERIOD OF RECORDS BASED ON THIS DOCUMENT

Documento	Base giuridica del trattamento	Periodo di conservazione
Data Breach internal and external communication forms	(Art. 6, paragraph 1, lett. c), GDPR) Processing which is necessary to fulfil a legal obligation to which the Data Controller is subject (Art. 6, paragraph 1, lett. c), GDPR) Processing which is necessary to obtain the legitimate interest of the Data Controller related to the management of its organization	Everlasting
Documented decisions of the Data Controller regarding the Breach	(Art. 6, paragraph 1, lett. c), GDPR) Processing which is necessary to fulfil a legal obligation to which the Data Controller is subject (Art. 6, paragraph 1, lett. c), GDPR) Processing which is necessary to obtain the legitimate interest of the Data Controller related to the management of its organization	5 years
Breach communication	(Art. 6, paragraph 1, lett. c), GDPR) Processing which is necessary to fulfil a legal obligation to which the Data Controller is subject (Art. 6, paragraph 1, lett. c), GDPR) Processing which is necessary to obtain the legitimate interest of the Data Controller related to the management of its organization	5 years
Register of personal data breaches	(Art. 6, paragraph 1, lett. c), GDPR) Processing which is necessary to fulfil a legal obligation to which the Data Controller is subject (Art. 6, paragraph 1, lett. c), GDPR) Processing which is necessary to obtain the legitimate interest of the Data Controller related to the management of its organization	Everlasting

MANAGEMENT OF THIS DOCUMENT

The Data Controller who is the person responsible for this document, must check the document at least once a year and, if necessary he must bring any changes/updates.

Annex:

- Data Breach internal communication form

Annex "A" - Data Breach Communication Form

If a suspected, alleged or actual personal data breach is detected, it is necessary to immediately notify the Data Controller by filling in the following form to be sent by e-mail to the following address: privacy@battistolli.it and for information at dpo@battistolli.it.

Data Breach Communication

Filling in date:	

□ **INTERNAL RECIPIENT ***

Information of the reporting person:

Surname and name	
Task	
Contact information (e-mail, phone number)	

□ **EXTERNAL RECIPIENT ***

Information of the reporting person:

Company/Company name	
DPO contact information (where appointed)	
Surname and name of the reporting person	
Contact information (e-mail, phone number)	

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

*****

EVENT DESCRIPTION

Date of discovery of the breach (date, time)	
Date and place of the breach (date, time, place)	
Description of what occurred	
Description of what occurred	
Categories and approximate number of subjects involved in the breach	
Volume (also approximate) of personal data subject to violation	
Other relevant details (any action taken when the breach was discovered, etc.)	

By the Data Controller (or the contact person appointed by him)	**DATE AND TIME OF FORM RECEIPT**	
Receipt mode	Progressive Reporting N° (from Data Breach Register):	
Systems involved:		
Vulnerabilities detected:		