BOFFETTI
ALWAYS POWER AHEAD

Company policy for the protection of personal data, in order to protect the fundamental rights and freedoms of individuals according to EU Regulation 2016/679 - GDPR

1. PURPOSE

The purpose of this document is to describe the general principles of security and obligations of confidentiality of the information and personal data defined by the Data Controller, or by the Manager that Boffetti S.p.A. guarantees and ensures to all parties involved in data processing, in order to develop an efficient and safe management system of procedures and processes for the security of personal data in compliance with the fundamental rights and freedoms of individuals, in compliance with the European Regulation 2016/679, from now on GDPR.

2. DESCRIPTION

Goals pursued

Boffetti S.p.A. intends to pursue the security objectives of information, personal data, the technological, physical, logical and organizational structure and their management. This means achieving and maintaining a secure information management system through compliance with the principles set out in articles 5 and 6 of the GDPR;

- ✓ Lawfulness, correctness, transparency;
- ✓ Guarantee with respect to the management and collection of data for the sole contractual purposes, determined, explicit and legitimate, and subsequently processed in a way that is not incompatible with these purposes. These guarantees are applied and verified also in cascade with respect to any subcontractors;
- ✓ Adequate, relevant and limited to what is necessary with respect to the purposes for which they are processed (principle of "data minimization");
- ✓ Accurate and, if necessary, updated; all reasonable measures must be taken to promptly delete or correct inaccurate data with respect to the purposes for which they are processed ("accuracy");
- ✓ Kept in a form that allows the identification of data subjects for a period of time not exceeding the achievement of the purposes for which they are processed;
- ✓ Processed in such a way as to ensure adequate security of personal data, including protection, through appropriate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage "principle of integrity and confidentiality";
- ✓ Ensure that personal data are accessible only to duly authorized subjects and / or categories of the same;
- ✓ Safeguard the consistency of the information from unauthorized changes;
- ✓ Ensure that authorized users have access to information and associated architectural elements with reference to the roles and duties covered;
- ✓ Ensure that data management always takes place through safe and tested processes and tools;
- ✓ Ensure the reliability of the channels of origin of the information;
- ✓ Guarantee the protection and control of personal data.

Training

Considering that the GDPR in article 29 provides that all persons, employees, appointees, under the authority of the owner or manager must be duly instructed and therefore trained on the tasks, responsibilities and for carrying out data processing operations, as well as undertake to confidentiality, Boffetti SpA has drawn up an inter-company training plan based on the provision of services, internal roles and tasks, the activity carried out, the specific data processing and related risks.

The training is designed and implemented for the tasks and roles covered by employees and has the following characteristics:

- ➢ Specific - corresponding to the type of job / role performed;
- ➢ Appropriate - in relation to the type of data processing carried out;
- ➢ Permanent - it must provide for a time schedule and periodic updating, in particular for any new hires;
- ➢ Documented - its development and subsequent updates must result from registers, certificates or other forms that give evidence of it;

- Effective - the general and specific understanding and implementation of company procedures must be periodically verified

Towards our suppliers:

These principles and guarantees are verified at the time of choosing each of our suppliers. The implementation status of these guarantees is also systematically monitored.

3. APPLICATION

The policy for the protection of personal data applies to all internal staff and third parties who collaborate in the management of information as well as to all processes and resources involved in the design, implementation, start-up and continuous provision of services.

4. INFORMATION SECURITY POLICY

Fulfilments and procedures applied to client companies:

- ✓ Verification of the data that will be processed with identification of the various types of data and categories to which they belong. Verification of the purpose of each treatment and of the legal basis on which each of them is based, also in order to provide adequate information to the interested parties, as required by art. 13 and 14 of the GDPR;
- ✓ The preparation of the information (or its updating) which must be provided to the interested parties in compliance with all the elements indicated in articles 13 and 14 of the GDPR. In particular, interested parties must be made aware of the rights that the Regulation recognizes them (right of access, right to be forgotten, right of rectification, right of limitation and opposition to processing, right to data portability); the information for the subjects interested in the data processing for which the customer is the data controller are provided by the customer if data collection is provided for in the software or services developed or configured;
- ✓ The preparation of the register of personal data processing activities, if it is necessary according to the provisions of art. 30 of the GDPR, i.e. in the event that the company or organization that processes the data has more than 250 employees. This register must also be drawn up in the event that the company or organization has fewer than 250 employees, but carries out a processing of data that presents a potential risk for the rights and freedoms of the data subjects; of particular categories of data referred to in Article 9, paragraph 1, or personal data relating to criminal convictions and offenses referred to in Article 10;
- ✓ The establishment of a procedure to be adopted in the event of any data breaches (so-called Data Breach referred to in articles 33 and 34 of the GDPR), for example upon the occurrence of a disclosure (intentional or not), destruction, loss, the modification or unauthorized access to the personal data being processed. The GDPR in fact provides for specific obligations in the event that a violation of this kind occurs, due to a cyber-attack, unauthorized access or an accident. In these cases, the GDPR requires, as required by art. 33, the Data Controller is obliged to notify the supervisory authority of the violation within 72 hours (or in any case without delay). In the event that the violation occurred leads to presume that there is also a high and current danger to the rights and freedoms of the data subjects, the latter must also be directly informed without delay of what happened;
- ✓ In art. 35 of the GDPR, the Data Controller (and with the possibility of consulting the Data Protection Officer if appointed) is obliged to carry out an impact assessment on data protection in the event that a type of processing, also in consideration of the nature, object, context and purposes of the processing itself, presents a high risk for the rights and freedoms of individuals. It should be noted that the GDPR does not establish a real obligation to carry out the impact assessment, but please note that the Regulation provides for a general obligation, for the Data Controller, to implement the appropriate measures in order to adequately manage the risks. for the rights and freedoms of the interested parties that may derive from the processing of their data. It will therefore be appropriate to carry out the impact assessment even when the Owner does not have a regulatory obligation to do so;
- ✓ Articles 37 - 38 and 39 introduce another fulfilment required of the Data Controller which consists in the designation of the Data Protection Officer also referred to as Data Protection Officer. This appointment, as required by art. 37 of the GDPR, is mandatory only in a number of cases, in particular, in the event that the data processing is carried out by a public authority or by a public body (with the exception of the judicial authorities when they exercise their functions); when the main activities carried out by the data controller or data processor consist of operations which, due to their nature, scope or purpose, require regular and systematic monitoring of data subjects on a large scale; and finally in the event that the main activities carried out consist in the large-scale processing of sensitive data or data relating to criminal convictions and crimes consisting in the unlawful processing of personal data. As also suggested by the Group of 29, the consultative and independent body, composed of a representative of the personal data protection authorities designated by each Member State that has prepared the Guidelines dictating

the appointment of the Personal Data Protection Officer, when the Regulation does not specifically require the appointment of a DPO, this figure may in any case be designated by the data controller or data processor on a voluntary basis.

Instructions for internal and / or external subjects who interface with our organization

Particular importance is attached to the procedures of the Management System for the Protection of Personal Data, indicated in the instructions and training that must be provided to the staff and to which there is an obligation to strictly follow.

There is also an obligation to inspect the names of the personnel authorized to process data relating to the assigned area, whether they are owners, managers or agents (as defined in the organization chart).

The staff is required to read it and to communicate any inaccuracies to its representatives. If the working tools allow the connection with other databases, the authorization will include the task of processing also the data of the connected databases, to the extent that this will be necessary for the efficient and correct performance of your duties and always in compliance the authorization profile and the possibilities and procedures indicated in the instructions received.

5. RESPONSIBILITY FOR INFORMATION SECURITY POLICY

The "data controller" and the "manager" are responsible for the secure information management system, in line with the evolution of the business and market context, evaluating any actions to be taken in the face of events such as:

- ✓ Significant business developments;
- ✓ New threats compared to those considered in the risk analysis activity;
- ✓ Significant security incidents;
- ✓ Evolution of the regulatory or legislative context regarding the secure processing of information;

Periodically or if necessary, a review must be carried out to verify the efficiency and effectiveness, as well as the adequacy of the technical / organizational measures applied, in compliance with and for the ultimate purpose of data protection, fundamental rights and freedoms of persons.

Calusco D'Adda, 02/03/2022

General Manager Boffetti S.p.A.

Riva Carolina

BOFFETTI
Amministratore Unico
Carolina Riva