Reff | Associates

Legal Weekly Alert

01 November 2017

In this issue:

On October 3 2017, Article 29 Working Party[1], in view of ensuring harmonized application of the Regulation regarding Protection of Personal Data starting by 25 May 2018, adopted the following guidelines:

- Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679
- Guidelines on personal data breach notification under Regulation 2016/679
- Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679

[1] European entity established under the basis of the present Directive regarding Data Protection, entity that is giving advices, issuing recommendations and opinions about protection of individuals in regard of processing personal data at EU level

On October 3 2017, Article 29 Working Party, in view of ensuring harmonized application of the Regulation regarding Protection of Personal Data starting by 25 May 2018, adopted the following guidelines:

- Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679
- Guidelines on personal data breach notification under Regulation 2016/679
- Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679

Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679

The document discusses the framework and the manner of applying administrative fines in accordance with the provisions of the European Regulation no. 2016/679, which is intended to help supervisory authorities to identify the most appropriate criteria to impose appropriate administrative fines and also to reach a decision on applying various other sanctioning measures (such as temporary or permanent limitation of processing).

Thus, if there is a breach of the Regulation, the competent supervisory authority should identify the most appropriate measures in relation to that situation, taking into account, inter alia, the following principles:

- Infringement of the Regulation should lead to the imposition of "equivalent sanctions".
- Like all corrective measures chosen by the supervisory authorities, administrative fines should be "effective, proportionate and dissuasive".
- The competent supervisory authority will make an assessment "in each individual case".
- A harmonized approach to administrative fines in the field of data protection requires active participation and information exchange among supervisory authorities.

The Guidelines establishes how general conditions should be interpreted in order to impose administrative fines under the Regulation and a number of different elements that should also be considered, taking into account the criteria set out in these conditions, as follows:

- the nature, gravity and duration of the infringement;
- the intentional or negligent character of the infringement;
- any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- the degree of responsibility of the controller or processor taking into account technical and organizational measures implemented by them pursuant to Articles 25 and 32;
- any relevant previous infringements by the controller or processor;
- the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
- the categories of the personal data affected by the infringement;
- the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
- where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
- adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42;

- any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

Guidelines on Personal data breach notification under Regulation 2016/679

The document tackles the mandatory requirements for the obligation of notification in case of data breach notification and also the steps that the controller or processor may adopt in order to comply with this obligation.

In order to clarify the obligation of notification laid down by the Regulation, a number of issues are being described, such as: understanding the concept of security of personal data processing and, respectively, its breach, various types of security breaches, possible consequences of such breaches, while providing a series of examples for a better understanding of the concepts.

At the same time, details about terms and conditions for notifying the supervisory authority are provided, as follows: the timing of the notification, the manner in which the information needs to be sent to the supervisory authority, the existence of a situation in which personal data breaches may affect persons in one or more states, as well as the necessary conditions to be met for the situation where the notification is not required.

In addition, different aspects and examples are mentioned in relation to cases where the personal data breach has to be communicated to the person whose data has been the subject of a potential security breach, setting out the necessary conditions that should be considered when making the notification, namely: the information to be transmitted, how to contact the individuals in question, and also, the conditions to be met if the notification is not necessary.

Also, the document provides information on how the risk assessment is important for the controller to take effective actions to manage the incident and to know whether authority notification is required. The risk assessment should take into account several factors such as: the type of infringement, its nature, its sensitivity, the amount of personal data involved, how easy it is to identify the individuals, the severity of the consequences for individuals or the number of persons affected.

Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679

The document presents specific provisions on the automatic decision making process, mentioning the essential condition, namely, that the automated process should be based on the fact that there must be no human intervention in the process. This Guide provides a description of notions like 'legal effects regarding the data subject' and 'similarly consequences that affect the subject to a similar significant extent', and by giving examples, there are being presented different situations of the effects on the individuals following an automatic process of decisions.

The document contains explanations on each of the exceptions provided by the Regulation in which automatic decisions could be taken without the person concerned having the right to choose not to be the subject of such a decision solely based on automatic processing:

- when is necessary for signing or performing of a contract between the data subject and a data controller;
- when authorized by Union or national law applicable to the controller and which also provides appropriate measures to protect the legitimate rights, freedoms and interests of the data subject;
- when it is based on the explicit consent of the person concerned;

At the same time, a description of the rights of individuals in relation to the automated decision-making process is provided within the Guidelines, namely:

- the controller is obliged to inform data subjects and to provide clarification on how the controllers must inform them about the way in which the decision-making process works;
- the right of access of the subjects to information regarding the existence of an automated decision-making process;
- the right not to be the subject of a decision based solely on an automated decision-making process;

In addition, general provisions on profile generation are mentioned, to which general principles of data protection are applied. Therefore, data controllers that do profiling and decision making process must comply with the general principles of the data processing activity set out in Article 5 ("*Principles relating to the processing of personal data*") of Regulation 2016/679, as well as the legal bases regarding processing provided by Article 6 ("*Legality of processing*") of the European Regulation.

Finally, the document contains brief recommendations to data controllers on different practices, recommendations established on the basis of the experience gained by Member States of the European Union in order to meet the provisions of the Regulation.

For further questions, please contact us.

Silvia Axinescu
Managing Associate Reff & Associates
+40 21 2075 428
maxinescu@reff-associates.ro

Reff | Associates