ISSN 2704-8012

European Journal of Privacy Law & Technologies

2019/2

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2019/2

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

Published Online by G. Giappichelli in Dicember 2019
www.ejplt.tatodpr.eu

DATA BREACH DISCLOSURE DUTIES

Mario Renna

Abstract

The Regulation (EU) 2016/679, on the protection of natural persons with regard to the processing of personal data, punctually regulates the data breach phenomenon. In the case of a personal data breach, the role of the controller becomes central, because he shall notify the personal data breach to the supervisory authority and communicate the personal data breach to the data subject.

Data breach regulations allow us to appreciate the principle of accountability, the centrality of the risk-based approach in data processing and the need to ensure effective protection of the rights and freedoms of data subjects.

Key-words: data breach; transparency; supervisory authority.

1. Introduction

The new rules established by the European Regulation 679/2016 (GDPR), regarding the communication obligations following a data breach, constitute an important index to grasp: *i*) the value of the effectiveness of the rights of the data subject and *ii*) the principle of accountability.

The dialogue between the data controller and the supervisory authority, as well as between the controller and the data subject, is not the most advanced expression of a dynamic approach to data security, but they are fundamental tools to ensure a continuous monitoring of the status of personal data.

2. Notification of personal data breach to the supervisory authority

The Art. 33 GDPR represents a fundamental change of pace, aimed at enshrining the security of the processing of personal data as a paramount principle and guiding value of the activity of the controller and of the data processor [see also Art. 5, par. 1, lett. *f*), GDPR] [1]. The security of processing aims to protect, on the one hand, the data subject from any risk of damage to fundamental rights and freedoms and, on the other hand, conforms the processing activity at every stage (Art. 32 GDPR) [2].

The obligation of the controller to notify personal data breach to the supervisory authority materializes the more general 'principle of accountability' [3]; in fact, the controller is obliged to notify, unless it is shown that any risk to the rights and freedoms of natural persons is unlikely. It is, therefore, a flexible duty, based on the procedural nature of risk management and modulated in relation to the nature and gravity of the personal data breach, as well as, specifically, the types of risk for the data subject [4]. According to the European Regulation, data breach means a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (Art. 4, no. 12, GDPR). Therefore, in the event of a breach, notification to the supervisory authority is mandatory for the

[1] See G Finocchiaro, 'Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali', in Ead. (ed.), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101* (Zanichelli, 2019), 12-13, 17; V Cuffaro, 'Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia: elementi per un bilancio ventennale', in Id., R. D'Orazio and V. Ricciuto (eds), *I dati personali nel diritto europeo* (Giappichelli, 2019), 19.

[2] S. Sica, 'Verso l'unificazione del diritto europeo alla tutela dei dati personali?' in Id., V. D'Antonio and G.M. Riccio (eds), *La nuova disciplina europea della* privacy (Wolters Kluwer-CEDAM, 2016), 8. See, also, F. Bravo, 'L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi', in V. Cuffaro, R. D'Orazio and V. Ricciuto (eds), *I dati personali nel diritto europeo*, (n 1) 804; A. Mollo, 'Gli obblighi previsti in funzione di protezione dei dati personali', in N. Zorzi Galgano (ed.), *Persona e mercato dei dati. Riflessioni sul GDPR* (Wolters Kluwer-CEDAM, 2019), 256.

[3] A. Mantelero, 'Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva', in G. Finocchiaro (ed.), *Il nuovo Regolamento europeo sulla* privacy *e sulla protezione dei dati personali* (Zanichelli, 2017), 321.; S. Vigliar, 'Data breach e sicurezza informatica', in S. Sica, V. D'Antonio and Riccio (eds), *La nuova disciplina europea della* privacy, (n 2) 245, 254. Cfr., anche, F. Bravo, *Il 'diritto' a trattare dati personali nello svolgimento dell'attività economica* (Wolters Kluwer-CEDAM, 2018), 107; D. Farace, 'Il titolare e il responsabile del trattamento', in V. Cuffaro, R. D'Orazio and V. Ricciuto (eds), *I dati personali nel diritto europeo*, (n 1) 746.

[4] F. Pizzetti, Privacy *e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, I (Giappichelli, 2016), 291, footnote 54.

controller within 72 hours from the time of knowledge, unless there are risks to the rights and freedoms of natural persons. The first paragraph of Art. 33 GDPR shows several critical elements [5].

First of all, it may be observed that the timeliness of the notification is closed within 72 hours of the knowledge. In order to comply with the regulatory obligation, the controller should have a technical structure that allows: i) a constant flow of information; ii) the assessment of the nature of the risks. Only through a specific monitoring and reaction procedure is it possible to regularly fulfill the prescribed duty [6]. The duty of adequate security measures to address and limit the risks of personal data breach requires an effective coordination of logistical plans, a context in which the role played by the controller is also inserted. The processor shall inform the controller without undue delay after becoming aware of a personal data breach (Art. 33, par. 2, GDPR): in the silence of the provision, the terms of execution of this duty can be established conventionally [Art. 28, par. 3, lett. *c*), GDPR).

A further issue arises in the case of cross-border infringements, that is to say concerning the interested parties belonging to different Member States. In this case, through a coordination of Articles 55 and 56 GDPR, it can be argued that, where notification to the public authority is mandatory, communication by the data controller must take place with supervisory authority leader, as the supervisory authority of the main or of the single establishment of the data controller.

With regard to infringements occurring in establishments outside the European Union, pursuant to Art. 3, par. 2, and Art. 27 GDPR, it can be noted that the notification must be sent to the national supervisory authority of the Member State in which the representative of the controller is established in the European Union. The transnational dimension of the personal data breach therefore requires an exclusive and timely exchange of views, in order not to exacerbate the formal obligations of the controller and to ensure that the competent authority takes measures to immediately protect the data subject.

Having said this, it is necessary to consider as the first paragraph of Art. 33 GDPR links the notification obligation to the ascertainment of an etiological connection between data breach and risks for the rights and freedoms of natural persons, assigned to the evaluation of the data controller. With respect to an underestimation of events, then denied by the production of damages, and, therefore, before the risk of liability for damages (Art. 82, par. 1, GDPR) and administrative pecuniary sanctions for non-fulfillment of the obligation to notify [Art. 83, par. 4, lett. *a*), GDPR], it is reasonable to assume that the data controller

[5] P. Voigt and A von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide* (Springer, 2017), 65.

[6] Bravo (n 3) 110; Mantelero, (n 3) 323.

adopts a so-called 'low-threshold notification behavior' [7].

Regarding the substantive profiles of the notification, it should be noted that it is necessary for the controller to communicate at least: the nature of the data, the categories and the approximate number of data subjects, as well as the categories and approximate number of records and contact details of the data protection officer or other contact point to obtain information. Furthermore, is required: a description of the likely consequences of the personal data - thus emphasizing the centrality of the 'risk based approach' - and the measures taken or proposed to be taken to remedy, including, where appropriate, measures to mitigate the possible adverse effects. In addition to the possibility for the controller to provide additional information to the minimum required by the standard, it is possible to proceed through a notification in phases: more precisely 'where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay'. In the event that the controller does not have all the elements normally required for notification, he can carry out the obligation of information in a graduated manner: in this way, the controller fulfils its obligation, justifying the reasons for a non-exhaustive notification, and has an immediate contact with the supervisory authority.Finally, the responsibility of the data controller is linked to the record of any data breach, as well as of the consequences and countermeasures taken for this purpose. This information support must allow enable the control authority to verify compliance with the regulatory provisions.

3. Communication of data breach to the data subject

Following the occurrence of data breach phenomena, the obligation to inform the data subject is left to the assessment of the level of risk carried out by the data controller, possibly assisted, in relation to their mutual skills, by the processor and the data protection officer [8]. In order to prevent arbitrary assessments, *Recital* 76 GDPR indicates that the risk assessment should refer to a concrete and prudent analysis and, at the same time, should be based on objective criteria [9].

---

[7] Voigt and von dem Bussche (n 5) 68.

[8] N Brutti, 'Le figure soggettive delineate dal GDPR: la novità del Data Protection Officer', in E. Tosi (ed.), Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice* Privacy (Giuffrè, 2019), 144.

[9] *Recital* no. 76 'the likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk'.

Risk assessment is a fundamental step to demonstrate the adequacy of organizational arrangements in terms of security processing. Unlike a probabilistic assessment (*ex ante*), which is the one conducted in the data protection impact assessment, Art. 34 GDPR invites you to estimate the risk through a precautionary assessment and subsequent to the infringement [10].

The communication to the data subject complements the duty to react and reduce the harmful consequences: this communication must allow the data subject to be aware of the risks and to be able to react promptly and effectively [11]. Furthermore, the GDPR conditions the mandatory nature of notification to the ascertainment of an etiological link between data breach and high risks for the rights and freedoms of natural persons: also in this case, in order to avoid administrative and tortious liability, it is easy to foresee that the data controller adopts the low-threshold notification behavior.

The communication obligation is elastic: it is not required if the controller has implemented adequate technical and organizational protection measures and these measures have been applied to the personal data affected by data breach (in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as encryption).

At the same time, the communication must not work where the controller has immediately implemented measures to prevent the occurrence of a high risk to the rights and freedoms of data subject. In such cases, the communication does not uarantee an effective protection of the person concerned and would involve a mere bureaucratic burden. Furthermore, communication will not be required if it would involve a disproportionate effort. In this case, a public communication or a similar measure is carried out according to which the person concerned is informed equally effectively. The exemption circumstances, in order not to frustrate the effectiveness of the rights of the data subject, must be interpreted in a restrictive and objective manner, taking as a parameter of the non-execution the concrete presence of unforeseeable circumstances, such as to alter the normal course of 'processing'.

With regard to the substantive profiles, it should be noted that the controller is required to: *i*) provide details of the data protection officer or other contact point where more information can be obtained; *ii*) describe the probable consequences of the personal data breach and the measures taken or to be taken to remedy and, furthermore, to mitigate the possible adverse effects [12].

---

[10] A. Mantelero, 'La gestione del rischio', in G. Finocchiaro (ed.), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, (n 1) 524.

[11] Voigt and von dem Bussche (n 5) 96-97.

[12] See, Pizzetti (n 4) 294.

4. Data breach between responsibility and transparency: WP29 Guidelines Personal data breach notification under Regulation 2016/679

The Guidelines on Personal data breach notification under Regulation 2016/679, as last revised and adopted on 6 February 2018 by the WP29, clarify the operation of the dialogue between the controller, the supervisory authority and the data subject. The Guidelines appear to be very useful in highlighting some points of non-immediate clarity. First of all, the moment of the actual knowledge of a data breach by the controller – starting from which the 72 hours for the notification begin – coincides with the moment in which there is a reasonable awareness of the verification of a security incident that compromise the personal data.

The time factor undergoes obviously variability according to the circumstances of the breach: however, 'the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required' [13].

The time factor is also related to the structural dimension of the security system. The Guidelines show that it is appropriate to have effective and efficient internal procedures, regulated by alert mechanisms and inspired by a fruitful cooperation between the controller, the processor and the data protection officer. The plurality of subjects involved in the processing confirms the need to activate synergistic procedures, functional to the preventive relief of data breach risks and to the adoption of reparatory and restorative measures following damage caused [14].

Therefore, notification to the supervisory authority becomes a dialogue between the controller and the public authority, but also a communication conditioned by the flow of data deriving from the collaboration between the controller, the processor and the data protection officer. Pursuant to Art. 33, par. 2, GDPR, the processor 'shall notify the controller without undue delay after becoming aware of a personal data breach', providing any information useful for the final decision of the controller to notify the data breach or less. Furthermore, the presence of the data protection officer is of fundamental importance if it is deemed to have the duty to inform and advise the controller or processor, and to cooperate with the supervisory authority and act as a contact point with the su-

[13] WP29 Guidelines Personal data breach notification under Regulation 2016/679, 11.

[14] Brutti, (n 8) 143; R Panetta, 'Privacy is not dead: it's hiring!', in Id. (ed.), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018* (Giuffrè, 2019), 18.

pervisory authority on any request relating to the data processing (Art. 39, par. 1, GDPR).

The notification obligations intends to guarantee an effective protection of the fundamental rights and freedoms of natural persons: safeguarding these rights and freedoms demonstrates the relational dimension of data processing, but it also constitutes a limit for notification. Indeed, the data controller, having ascertained the nature and the impact of the data breach, may refrain from informing the public authority when it is unlikely to harm the rights and freedoms of natural persons [15]. The risk assessment therefore becomes particularly relevant in order to guide the behavior of the controller [16].

With regard the data breach communication to the data subject (Art. 34 GDPR), the Guidelines reiterate the need to ensure effective protection of the rights and freedoms of the data subject, specifying the boundaries of the communication. First of all, note that the communication must take place without undue delay. The controller, as soon as possible, must inform the data subject, so that he can take the most appropriate measures to protect himself from further negative consequences of the breach. Communication must be effective and rendered in a understandable language; therefore, it cannot be transmitted through generic sources (press releases, company blogs), thus discounting an unjustifiable rate of abstractness, nor, even less, alongside other non-conferring news with the actual phenomena of data breach [17].

---

[15] See, e. g., A. Vivarelli, *Il consenso al trattamento dei dati personali nell'era digitale. Sfide tecnologiche e soluzioni giuridiche* (ESI, 2019), 187.

[16] *Recital* no. 75 'the risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects'.

[17] The Guidelines precise that 'examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media. A notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an individual. WP29 recommends that controllers should choose a means that maximiz-

As previously stated, the data breach notification (a) and the data breach communication (b) are functional to safeguarding the fundamental rights and freedoms of natural persons, therefore they are not absolute and are calibrated with respect to a risk (a) and the high level of risk (b).

In general, when assessing the risk to individuals due to a violation, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring. WP29 therefore recommends the assessment should take into account the following criteria: a) the type of breach; b) the nature, sensitivity, and volume of personal data; c) ease of identification of individuals; d) severity of consequences for individuals; e) special characteristics of the individual; f) special characteristics of the data controller; g) The number of affected individuals.

5. Concluding remarks

The security of the processing and the effectiveness of the protection of the data subject – guiding principles of the GDPR – find concretization in the duty imposed on the data controller following the data breach. Risk assessment translates the principle of accountability: only a correct risk assessment will allow the data controller to punctually comply with the GDPR discipline and not to be exposed to administrative or extra-contractual liabilities.

Risk assessment also evokes the need for a structured risk management system: it is therefore necessary to have several professional figures involved in data processing and to adopt adequate and effective prevention and reaction measures. The effectiveness of the protection of the rights and freedoms of the data subject is clearly stated in the disclosure duties: it is, therefore, necessary for the data subject to be informed of the extent and consequences of the data breach. Only through a continuous knowledge of the state of one's personal data are the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data really protected (Art. 1, par. 2, GDPR).

es the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean the controller employs several methods of communication, as opposed to using a single contact channel'.