Personal data breach notifications under the GDPR - proposal for a new notification procedure

Graça Pacheco Costa

October 2018

Disclaimer: This paper reflects the personal view of the author and not the institutional position of the European Data Protection Supervisor for which she works.

Abstract

Data breaches are security incidents which impact the fundamental right to data protection (see Article 8 paragraph 1 of the Charter of Fundamental Rights of the European Union and Article 16 paragraph 1 of the Treaty on the Functioning of the European Union) that require a comprehensive approach.

The European legislator has recognised these concerns in the new legislative framework on personal data protection, highlighting transparency and accountability. In this respect, one of the main innovations of the General Data Protection Regulation (GDPR – Regulation (EU) 2016/679) is the obligation for data controllers to notify the data breaches to the supervisory authorities - and in some cases, involved data subjects.

The GDPR provides guidelines regarding the deadline of these notifications, the competent supervisory authority, cases where it is also necessary to notify the data subjects, the consequences of non-notification, etc. (see Articles 33 and 34 of the GDPR). However, it does not cover the internal and external process necessary for the detection, reporting and mitigation of adverse effects, so that the notification of a personal data breach is made to the supervisory authority within 72 hours after the controller having become aware of it.

Therefore, this paper presents a case study where a personal data breach notification process was tested in a Portuguese company, in order to stream line communication among the different actors in a data processing ecosystem and comply with the requirements of the GDPR.

Keywords: personal data breach notification; GDPR; data protection.

Table of contents

Introduction

Who has never feared a personal data breach? Mankind has witnessed continuous technological revolutions, especially regarding Information and Communication Technologies (ICTs), which influence the way society interacts and which need new forms of practical and legal protection.

In fact, the current risks to privacy differ greatly from those who justified the emergence of the right to data protection. One of the factors that greatly contributed to this difference results from the emergence of a new stage of action for the public and private domains: the cyberspace. In this new space we see a multiplicity of new social, economic, political, etc. interrelationship, but also new challenges, risks and threats. However, it should be emphasized that the values, rules and principles of law prevailing in the physical world have their full application in the virtual world. Thus, fundamental rights such as the right to data protection, security and education are not incompatible with cyberspace and are even reinforced by the wider scope of its application in this new arena. The same applies to big data, large scale data processing[1], etc.

Nonetheless, the increasing interaction of the various actors in cyberspace and the increasing threats that overshadow this new era require a conscious and proactive attitude in the name of maintaining online and offline environment safe and protecting the people's personal data. According to the Eurobarometer on cyber-security[2], European citizens using the Internet reveal that personal data breaches are their main concern when conducting online transactions. There is also an increase in this concern among European citizens in 2017 (45% of respondents), compared to the Eurobarometers of 2014 (43% of respondents) and 2013 (37% of respondents).

Most of the incidents that impact confidentiality, availability and integrity of personal data result from human error, technical failures, computer attacks, malware and cyber-espionage. Error is part of the human condition and we cannot claim to live in a utopian world, without flaws, without 'Achilles' heels', even if we wish for it. For this reason and to better reinforce human fundamental rights it is necessary to acknowledge the possible risks and prepare ourselves for them. While we recognize that the scale and impact of personal data breaches are naturally amplified by the use of ICTs, we caution that these violations may also occur for data processed in a non-digital format.

The notion of data protection stems from the right to privacy and is not intended to protect the data per se, but the people to whom they refer to[3]. Therefore, the right to respect for private and family life is enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8) and Charter of Fundamental Rights of The European Union (Article 7). Additionally, the right to the protection of personal data is enshrined in the Charter of Fundamental Rights of The European Union (Article 8). Nonetheless, like many other fundamental rights, the right to data protection is instrumental in preserving and promoting other rights and freedoms. For this reason, the right to data protection is umbilically related to the protection of freedom, non-discrimination, freedom of expression, equality, image and identity, among other fundamental rights.

With a view to closing the gap in guarantees for personal data protection between the different legal systems of the European Union (EU), the European legislator decided to adopt a general regulation - the General Data Protection Regulation (GDPR) in 2016[4] - to standardize the level of protection of citizens in these matters. Among the new features of this regulation are the mandatory notification of personal data breaches by all data

[1] '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 means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (see Article 4(2) of the GDPR).

[2] See Eurobarometer Europeans' attitudes towards cyber security, September 2017, p. 6 e 7, disponível em: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2171.

[3] It should be noted that personal data protection and information security are not the same. In fact, data protection is a fundamental right that includes information security, but is not limited to ensuring the confidentiality, availability and integrity of the information.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR).The GDPR has entered fully into force in 25 May 2018.

controllers[5] to the competent supervisory authorities[6][7] and the persons to whom there is a high risk of their rights and freedoms being affected. These notifications to the supervisory authorities aim to allow them to point to the controllers the necessary measures and precautions to be taken by and by the potentially affected data subjects. Therefore, this results in a greater accountability of the data controllers, but also the greater enforcement of the data subjects whose personal data were involved in a data breach.

The challenge is that the notification of personal data breach to the supervisory authority must be done not later than 72 hours after the controller has become aware of it[8]. After a personal data breach, time runs against the persons potentially affected and every minute counts towards an adequate and timely reaction.

In view of the above, this paper proposes the implementation of a personal data breach notifications procedure to facilitate the timely notification of personal data breaches to the supervisory authority and affected data subjects in accordance with Articles 33 and 34 of the GDPR. Therefore, to promote compliance with these legal provisions, we will explain this procedure – which was tested in a Portuguese company – and point out a set of good practices thereto related.

At this regard, it should be emphasized that where processors are involved in the processing of personal data, it is also necessary to involve them in the information chain and that they themselves have an obligation to communicate all information to the controller (see Article 33(2) of the GDPR).

Finally, it is worthy of mentioning that this paper is based on the Masters' thesis on personal data breach notification of the author, in which more detailed information on this matter is provided.

I. Personal data breach

Personal data breaches can have various levels of complexity and impact, and therefore have multiple perspectives. According to Article 4(1) of the GDPR 'personal data' means any information relating to an identified or identifiable natural person ('data subject'). The same Article defines as an identifiable natural person anyone who can be directly or indirectly identified, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

Taking into account the current reality of ICT and going one step further, the GDPR presents several new features and, to a certain extent, changes the paradigm of personal data protection. Among the innovations incorporated in this regulation, we find the extension of its territorial scope in comparison with the previous data protection legal framework. This extension means that the GDPR applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the Union, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- the monitoring of their behaviour as far as their behaviour takes place within the Union; or
- the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

[5] 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (see Article 4(7) of the GDPR).

[6] 'Supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR (see Article 4(21) of the GDPR).

[7] There are some exceptions to this rule, namely if the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons (see Article 33(1) of the GDPR).

[8] There are some exceptions to this rule, namely to provide the information in phases if it is not possible to provide all information at the same time (see Article 33(4) of the GDPR).

In comparison with the previous legal framework, besides the extension of the territorial scope, the GDPR highlights the controller's accountability and risk assessment. Though, in the absence of specific support in the GDPR for risk assessment, we need to rely on other complementary instruments. Among these, we highlight ISO 31000: 2009 – Risk management: principles and guidelines is an instrument of the International Organization for Standardization for risk management – although it does not focus especially on the protection of personal data – aiming to standardize the terminology and concepts, as well as to establish the principles and guidelines for the implementation of a process of analysis, evaluation and risk management, in order to improve the performance of organizations in this area

The ISO 31000: 2009 is structured in 4 stages, known as the PDCA cycle (Plan, Do, Check and Act). In this way, the risk management framework (plan) must first be drawn up. Next, the implementation phase (do) is highlighted. The third phase concerns monitoring and analysis (check), ending the fourth and final phase with continuous process improvement (act). In this way, organizations not only have a general perspective on the risks that can affect them, but also manage risk management to respond to changes that arise after their initial implementation. Risk assessment is important both to set the adequate technical and organizational security measures regarding a data processing and the response to a data breach.

Recital 75 of the GDPR materializes the risk for data subjects through several examples, such as 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. Data breaches may also involve other consequences for the controller (such as reputational damages, fines, etc.) and for society (as mistrust in the public data controllers, erasure of the medical-patient relationship with consequences for public health, etc.). All of them need to be addressed.

II. Personal data breach notification

Articles 33 and 34 of the GDPR define one of the main novelties of this legal instrument: the obligation of the controllers to notify a personal data breach to the competent supervisory authority and, in certain cases, the affected data subjects.

In that regard, it should also be noted that this duty to notify data breaches to the competent authorities is not entirely original. In fact, Directive 2009/136/EC and Regulation (EU) 611/2013 on privacy and electronic communications had already enshrined this obligation to providers of publicly available electronic communications' services. However, the RGPD's innovation is to extend the obligation to all controllers, independently of the sector in which they operate.

1. How to identify the competent supervisory authority?

In accordance with Article 51(1) of the GDPR, each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation.

Hence, in order to identify the competent supervisory authority, we need to assess if the personal data breach occurred in one single Member State or in several. If the personal data breach only occurred in one Member State, then the competent supervisory authority is the one on the territory of this Member State (cf Article 55 et seq. of the GDPR). Regarding transborder personal data breaches, depending on the circumstances of the personal data breach, the identification of the competent lead supervisory authority[9] may be a complex task. In that case, several scenarios may be envisaged:

- the supervisory authority of the main establishment or of the single establishment of the controller or processor (see Article 56(1) of the GDPR);

[9] Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60 of the GDPR (see Article 56(1) of the GDPR).

- if the subject matter relates only to an establishment in the Member State or substantially affects data subjects only in its Member State (see Article 56(2) of the GDPR), then the lead supervisory authority is the one of that Member State.

The relevance of this issue lies in the fact that the lead supervisory authority is the sole interlocutor of the controller or the processor in cross-border processing (see Article 56(6) of the GDPR).

2. What measures need to be taken when dealing with a personal data breach?

The European Data Protection Board (EDPB) is an independent European body whose mission is to contribute to the application of data protection rules in a harmonized manner within the European Union and to promote cooperation between the various data protection authorities in the 28 EU Member States. This body has been established by the GDPR and is composed of representatives of the national data protection supervisory authorities and the European Data Protection Supervisor (EDPS)[10].

Within the framework of its mission, EDPB highlighted some practical measures for data controllers and processors, regarding the notification of personal data breaches:

- Information concerning all security-related events should be directed towards a responsible person or persons with the task of addressing incidents, establishing the existence of a breach and assessing risk;
- Risk to individuals as a result of a breach should then be assessed (likelihood of no risk, risk or high risk), with relevant sections of the organisation being informed;
- Notification to the supervisory authority, and potentially communication of the breach to the affected individuals should be made, if required;
- At the same time, the controller should act to contain and recover the breach;
- Documentation of the breach should take place as it develops.

3. What information must be provided in a personal data breach notification?

Figure 1 – Comparative table between the personal data breach notification to the supervisory authority and the data subjects, in accordance with Articles 33 and 34 of the GDPR.

	Notification to the supervisory authority	Notification to the data subjects
LEGAL BASIS	Article 33 of the GDPR	Article 34 of the GDPR
TO WHOM	Competent supervisory authority according to Article 55 of the GDPR	Natural persons to whom the data breach is likely to result in a high risk to their rights and freedoms
DEADLINE	Not later than 72 hours after the controller has become aware of the data breach	Without undue delay
BY WHOM	The controller	
CONTENT	• Nature of the personal data breach, • Name and contact details of the data protection officer (or other contact point), • Likely consequences, • Measures taken or proposed to be taken.	

[10] In fact, the Directive 95/46 / EC, which was repealed by the GDPR, already provided in its Article 29 a group with an advisory and independent nature regarding the protection of persons with regard to the processing of personal data. This group became literally the Article 29 Working Group. With the RGPD, this working group has gained a new designation – EDPB –, a new statute, enlarged powers and mission.

III. Best practices and a communication/notification procedure for personal data breach

A. Best practices

In the light of the previous chapters, data controllers as well as processor should promote a culture of prevention, but also of reporting personal data breaches with a view to mitigating their adverse effects for both the data subjects and their own organizations. Below we list a set of good practices that facilitate the controllers' obligation to notify personal data breaches to the supervisory authority and affected data subjects. However, these best practices are not limited to the mere notification, as this implies a risk assessment, a description of the data and categories of affected data subjects, as well as the prior knowledge of some concepts (adoption of adequate security measures, data protection by design and by default, etc.). For this reason, in a holistic perspective, we will try to present good practices with a direct impact on the notification of personal data breaches, both to the supervisory authorities and to the affected data subjects.

1. Adoption of a data protection policy

A data protection policy provides standards, methods, procedures and instructions – at strategic, tactical and operational levels – with the aim of ensuring the maintenance and systematization / standardization of security, as well as compliance with the legislation. This policy should address not only the organizational aspects of the organization, but also human and technological conditions.

2. Implementation of an incident response plan

Personal data breaches, as we have already mentioned in this paper, require a holistic strategy, including several phases: prevention, rapid detention, mandatory notifications by the applicable legislation, impact mitigation and learning to optimize the security measures applied to the processing of personal data and to prevent the same incidents to happen again.

3. Implementation of technical and organizational security measures

The adoption of appropriate technical and organizational security measures to ensure and prove the compliance of the personal data processing is an obligation of the controller, in accordance with Article 24 (1) of the GDPR. These measures can reduce the risk of personal data breaches, but also facilitate the rapid detection of data breaches. In accordance with the principle of accountability, the controller must determine the appropriate technical and organizational measures and implement them (see Articles 5 (2) and 24 (1) of the GDPR). To that end, impact assessments on data protection (see Article 35 of the GDPR), prior consultation of data protection authorities (see Article 36 of the GDPR) and the designation of a DPO (see Article 37 et seq. of the GDPR) are very relevant.

4. Certification and codes of conduct

The adoption of codes of conduct or certification mechanisms that contribute to the correct application of the GDPR is provided for in articles 40 and 41 of this same regulation. Codes of conduct and certification ensure that certain minimum requirements are implemented, whether in software, hardware, organizational structure, etc., regardless of the action or inaction of users / personal data subjects. In this way, the minimum level of data protection is elevated to a higher standard, leveraging this fundamental right to a level of protection that offers more guarantees than the minimum legal requirements.

5. Two-stage risk assessment

The DPO of the controller should perform an initial assessment of the personal data breach within 24 hours after having become aware of it, as well as a more detailed assessment approximately 48 hours after the initial assessment. This two-stage assessment allows an analysis of its severity and impact.

6. Investigating and documenting

In accordance to Article 33(5) of the GDPR, the controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with the GDPR.

7. Human and material resources

Personal data breaches may be detected by automated alerts, previously installed on computer systems, and / or by employees of the organization. In any case, controllers must employ human and technological resources to respond to possible data breaches and then notify the supervisory authorities and data holders where applicable.

8. Designation of a Data Protection Officer (DPO)

The controller and the processor shall designate a data protection officer in any case where:

a. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
b. the core activities of the controller or the processor consist of processing operations which, by their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
c. the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

Although the RGDP does not require the appointment of a DPO in other cases, it seems advisable to do so. The DPO is in the best position to contribute to the architecture of the data protection policy, advice the controller, centralise the information and communication with the different actors in cases of personal data breaches, etc. Therefore, the DPO should be given the necessary human and financial resources, as well as transparent access to the personal data processing, to carry out their tasks.

9. Training on personal data breach detection and reaction

Training in the field of ICT, but also on data protection issues, is essential for all persons involved in the processing of personal data. Thanks to training people can be made aware of the risks and procedures to be followed in the event of a breach of personal data. Therefore, the continuous training of employees, with a level of depth differentiated by professional categories or other criteria, taking into account their real needs and the risks to which they are subject, will enable their responsiveness and continuous update.

B. Proposal of a personal data breach communication/notification procedure

The GDPR does not indicate a specific communication/notification's scheme for the collection of the mandatory information required in the notification to the supervisory authority and of the affected data subjects. We, therefore, present a proposal for a procedure for personal data breach notification that is efficient[11], allows the deadlines established in that regulation to be met and can be used by controllers to facilitate compliance with the provisions of the GDPR[12].

As depicted in Figure 2 below, internal communications within the controller should precede external communications and both must take place prior to notifications to the supervisory authority and data subjects under the GDPR.

After implementing the best practices above mentioned, once a possible personal data breach is detected, that suspicion should immediately be communicated to the DPO of the controller. Then, the DPO of the controller should perform an initial assessment of the personal data breach in cooperation with the ICT manager, within 24 hours after having become aware of it. This assessment should also provide concrete solutions to mitigate the impact of the breach. Meanwhile, if necessary the DPO should communicate that suspicion to the controller's legal and ICT departments. Once the DPO confirms the personal data breach, that information should immediately be communicated to the controller's highest management level and from that moment it starts the 72 hours deadline to notify the supervisory authority. Joint controllers and their representatives, as well as

[11] This proposal was tested in a Portuguese company. We have concluded that it not only promotes compliance with the provisions of the GDPR, but also facilitates the chain of communication between the various actors in data processing, promoting the right to data protection.

[12] Disclaimer: this proposal does not include notifications of breaches of personal data with a specific structure, such as the notification obligation imposed by Article 4 of Directive 2002/58 / EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

processors and their representatives[13], should also be notified of the personal data breach, in order to take the necessary security measures to mitigate the negative consequences of the breach.

Afterwards, approximately 48 hours after the initial assessment, a more detailed assessment should be made by the DPO with the necessary support of ICT and legal experts. This two-stage assessment allows an analysis of the personal data breach severity and impact, as well as the effectiveness of the reactive measures adopted after the controller becomes aware of the breach. Both analyses should focus on the GDPR criteria, i.e. nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned, the likely consequences of the data breach, measures taken or proposed to be taken by the controller to address the personal data breach, the degree of impact to the data subjects affected, etc. The difference between the two assessments of data breach stems from the time space between the two. Consequently, as more information will be gathered thanks to more time spent researching and collecting information, the degree of detail of each of the evaluations will be different and the controller can infer the effectiveness of their decisions and remedial action taken.

By the end of the detailed analysis, the DPO is in a position to assess if the data breach is likely to result in a risk to the rights and freedoms of natural persons and, in that case, the controller must notify the competent supervisory authority.

Since the DPO acts as the contact point for the supervisory authority on issues relating to processing (see Article 39(1) e) of the GDPR), it is advisable that this actor makes the notification of the personal data breach to the supervisory authority on behalf of the controller. Even in the situations when the personal data breach is unlikely to pose a risk to the rights and freedoms of natural persons – and, therefore, it is not required the notification to the supervisory authority – the DPO should keep a record of the information related to that breach, including the initial and detailed analysis and other relevant elements.

In the scenario where the personal data breach must be notified to the supervisory authority, the DPO should follow the format required by that authority. In case of the Portuguese Data Protection Authority (*Comissão Nacional de Proteção de Dados*), the data breach should be notified through a specific form available on its website (www.cnpd.pt) with specific fields in accordance to the requirements stated in the GDPR. In any event, the supervisory authority may require further information regarding a data breach and the DPO should be able to address those requests.

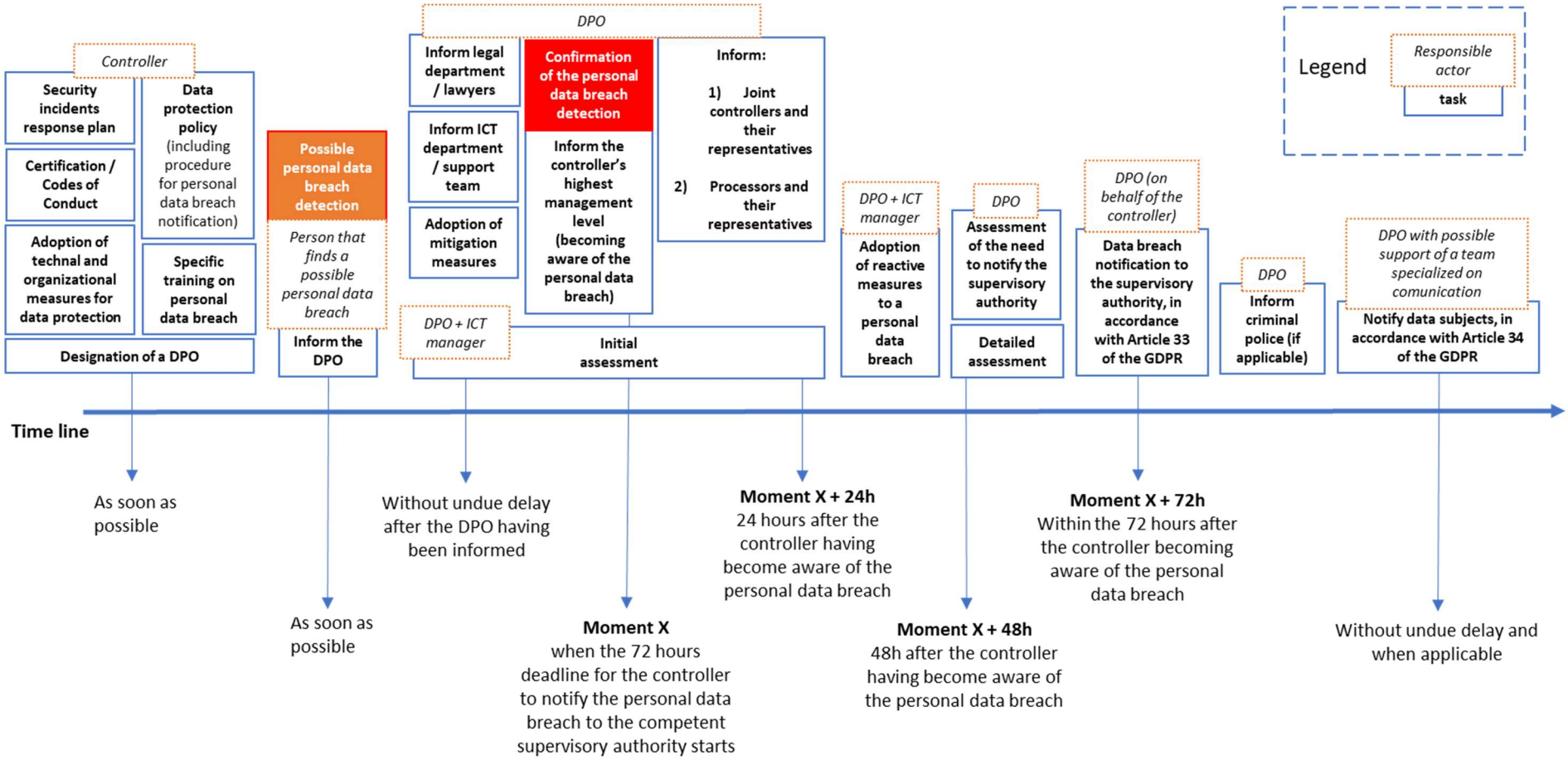
The notification to the affected data subjects should be done after the notification to the competent supervisory authority. Despite Article 34(1) of the GDPR states that the notification to the data subjects should be done without undue delay, Recital 86 of the same regulation lays down that such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. Therefore, the notification of the data subjects should only take place after the notification of the supervisory authority and, if necessary, the law-enforcement authorities. In fact, Recital 88 of the GDPR provides that the rules and procedures concerning the format and procedures applicable to the notification of personal data breaches should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach. In this scenario, the controller may be requested by the law enforcement authorities to delay the notification of the data breach to the concerned data subjects.

In the light of the above, we have drafted a flowchart (see Figure 2 below to better visualize the relevant deadlines, actors and communication steps of this procedure proposal, so that the controller complies with the GDPR's requirements on personal data breach notification (see Article 33 and 34 of the GDPR).

We have demonstrated the effectiveness of this proposal in a Portuguese company by assessing the level of knowledge of employees before and after a specific training on the response to personal data breaches, the adoption of this procedure and its test in a real-time fictitious data breach. The feedback from the DPO of the company regarding this procedure was very positive, especially because of the awareness raising to all staff through training, the commitment of the high management board and the reassurance in knowing exactly what steps to follow next.

[13] Representatives of controllers or processors not established in the Union (see Article 27 of the GDPR).

Figure 2: Personal data breach notification procedure proposal – including minimum previous measures that allow the quick identification of a breach – which triggers the communication chain between the several actors and the respective deadlines[14].



[14] The internal and external communications scheme described below assumes that the person who detects the breach of personal data is part of the internal structure of the controller. However, it can be adapted to reported to the decision-making bodies of the controller. Basically, as soon as the chain of information reaches the EPD of the controller, the chain of communications provided for above applies to the breaches of personal data detected by a person within the structure of the controller.

Conclusion

1. The right to respect for private and family life is enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8) and Charter of Fundamental Rights of The European Union (Article 7). The right to the protection of personal data is enshrined in the Charter of Fundamental Rights of The European Union (Article 8).

2. To that extent, the GDPR has changed the paradigm of personal data protection, by including among its novelties the obligation of all controllers to notify the personal data breaches they suffer to the supervisory authority and concerned data subjects (when it is likely to result in a high risk to their rights and freedoms), in accordance with Articles 33 and 34 of the GDPR.

3. In order to meet the deadlines, as well as to collect the necessary information for adequate notification of personal data breaches to the supervisory authority and data subjects under the GDPR, we believe that the controller should adopt not only the adequate security measures - both preventive and reactive, foreseeing the possibility of personal data breaches - as well as good practices.

4. Among these good practices we recommend the planning and adoption of a data protection policy, the implementation of a security incident response plan, the adoption of adequate technical and organizational security measures for each personal data processing, the adoption codes of conduct or certifications on data protection, biphasic assessment of the impact of personal data breaches, investigation and documentation of all procedures, investment on human and material resources for the detection and repair of personal data breaches, including the designation of an data protection officer (DPO) and the establishment of a personal data breach support team, the training / awareness-raising of all employees and the cooperation between supervisory authorities in transnational data breaches.

5. Additionally, we outline a proposal for a data breach notification procedure to respond to the requirements set at this regard in the GDPR. Although the GDPR does not expressly prescribe the adoption of an internal and external personal data breach procedure, we consider that it contributes to the controller's compliance with the requirements for notifications of personal data breaches listed in that regulation.

6. The inevitable primacy of the DPO in this proposed communications procedure and notifications of breaches of personal data demonstrates the relevance of this actor in the ecosystem of a personal data processing as a specialist in the subject, an informed assessor of the risks for data subjects and a privileged contact point with the various concerned players.

7. In our view, this proposal promotes the data subjects' fundamental rights, highlights the controller's compliance with the GDPR and enhances data protection in general. For that reason, we believe that this procedure can and should be replicated in other SMEs and organizations that are personal data controllers.

Bibliography

ANDRESS, Jason, The Basics of Information Security – Understanding the Fundamentals of InfoSec in Theory and Practice, 2.ª edição, Elsevier/Syngress, 2014.

BOYCE, Joseph, JENNINGS, Dan, Information Assurance – a practical guide: Managing Organizational IT securit risks, Butterworth Heinemann, 2002.

CANOTILHO, José Gomes, Direito Constitucional e Teoria da Constituição, 5.ª Edição, Almedina, 2002.

CASEY, Eoghan, Handbook of Digital Forensics and Investigation, Academic Press, 2010.

CASTELLS, Manuel, A Era da Informação: Economia, Sociedade e Cultura, Volume I, A sociedade em rede, Fundação Calouste Gulbenkian, 2011.

FARINHO, Domingos Soares, Intimidade da Vida Privada e Media no Ciberespaço, Almedina, 2006.

GOODMAN, B. and FLAXMAN, S., European Union regulations on algorithmic decision-making and a "right to explanation". 3rd ed., New York: University of Oxford, 2016, available in: https://arxiv.org/pdf/1606.08813.pdf.

GUTWIRTH, S. and de HERT, P., «Privacy, data protection and law enforcement. Opacity of the individual and transparency of power», in Privacy and the criminal law. Antwerp/ Oxford: Intersentia, 2006, pp.61-104.

LAMBERT, Paul, The Data Protection Officer – Profession, Rules and Role, CRC Press, 2016.

MALATRAS, Apostolos, et al., Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities, Computer Law & Security Review, volume 33, Issue 4, August 2017, p. 458-469.

TAVARES SILVA, Pedro, et. al., Segurança dos Sistemas de Informação, Edições Centro Atlantico, 2003.

VAN WEERT, Tom, K. MUNRO, Robert, Informatics and the Digital Society – Social, Ethical and Cognitive Issues, Springer, 2003.

VARGES GOMES, Mário, Código da Privacidade e da Protecção de Dados Pessoais na Lei e na Jurisprudência, Centroatlantico.pt, 2006.