MPR PARTNERS
MARAVELA, POPESCU & ASOCIAȚII

WE TRANSLATE LEGAL
TO BUSINESS

DATA BREACH NOTIFICATION UNDER E-PRIVACY DIRECTIVE AND GENERAL DATA PROTECTION REGULATION

Abstract: Data breach notifications were firstly introduced in 2009 by means of amendments to the E-Privacy Directive, where such data breaches occurred in connection with the provision of publicly available electronic communications service. Further on, GDPR extended data breach notification obligation to all industries. The initial scope was to have a single notification regime, as E-Privacy Directive was intended to be replaced by E-Privacy Regulation, when GDPR became applicable. Since E-Privacy Regulation has a long way until entering into force, an electronic communications provider has difficulties in navigating through two regulatory regimes when it comes to data breach notifications.

1. General remarks

The obligation to notify personal data breaches to the relevant national authority and, in some cases, to the individuals affected, has become mandatory for the first time under the amended Directive 2002/58/EC122[1] (hereinafter referred to as the "**E-Privacy Directive**"). This followed the broader review of the regulatory framework for electronic communications in 2009, which had affected five different EU directives.

As the E-Privacy Directive applies only to providers of publicly available electronic communications services (the "**Telecom Providers**") and since the risks associated with breaches of personal data held by other entities may be at least comparable, the Regulation (EU) 2016/679 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 (the "**GDPR**") included the obligation to notify personal data breaches regardless of the sector.

The GDPR extended the breach notification requirement to all entities that process personal data, irrespective of the sectors where such entities operate. The initiative was

more than welcomed, as it is in accordance with the "right to know" of the individuals affected and is a key element of transparency and accountability.

For the purpose of this article, it is particularly important to mention that in the proposed E-Privacy Regulation the obligation to notify data breaches was placed only under the GDPR[2], thus the Telecom Providers would cease to be subject of the obligation to notify privacy incidents under two different legal frameworks.

Although the intentions of the EU legislator were to offer more legal certainty, the fact that the entry into force of the E-Privacy Regulation continues to be delayed creates a dire need to some clarifications regarding the overlap between the obligation arising from the E-Privacy Directive and the one arising from GDPR.

2. Interplay between GDPR and E-Privacy Directive

Privacy and data protection are core values of the European Union[3], thus the EU legislator needs to make continuous efforts in order to set down specific and efficient rules to protect personal data and to ensure the confidentiality and security of electronic communications, backed by strong enforcement.

The data protection legal framework is two-fold: GDPR aims to protect the data subjects' rights in connection with the processing of personal data, while E-Privacy Directive concerns the protection and confidentiality of personal data in electronic communications.

However, this is not what the EU legislator envisioned when it took the decision to reform the data protection package, as the prediction was to also repeal E-Privacy Directive and to create an E-Privacy Regulation, in order to ensure consistency with the GDPR and legal certainty for users and businesses alike by avoiding divergent interpretation in the Member States[4]. As the latter revision has not been completed in due time and the Council of the European Union's viewpoint is still pending, the GDPR came into force, leaving several loopholes to be filled.

GDPR became applicable in May 2018, while the E-Privacy Directive revision is still pending, so the Telecom providers continue to be subject to a double notification regime. Thus, several queries arise: when a Telecom Provider is tackling a personal data breach under which legislative act's criteria will it assess the same, what term should be observed for submitting the same, which supervisory authority should receive the notification?

Building on the experience on breach notification that has been gained by those national data protection authorities already implementing personal data breach notification requirements[5], GDPR defines a personal data breach as **"***a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*[6]. Meanwhile, in E-Privacy, due to the fact that the obligation to notify personal data breaches was intended to be industry

specific, the definition added that such personal data breaches need to be "*in connection with the provision of a publicly available electronic communications service in the Community*".

Keeping in mind that these definitions overlap, it may be said that when a telecom provider discovers a personal data breach and it can be ascertained that the same is in connection with the electronic communications provision, the obligation to notify arises only under the E-Privacy Directive, while when facing any other personal data breach, the obligation arises only under the GDPR.

However, as long as the breach is related to personal data, another interpretation could be that even if the breach is in connection with the electronic communications provision, the obligation to notify arises under both legislative acts. This interpretation seems to be supported also by the European Data Protection Board (the "**EDPB**").

Last year, the EDPB has issued guidelines on the interplay between the E-Privacy Directive and GDPR. The paper provides the interpretation of Article 95 from GDPR, stating that the electronic communications providers "*who have notified a personal data breach in compliance with the applicable national E-Privacy legislation are not required to separately notify data protection authorities of the same breach pursuant to article 33 of the GDPR*".

It can be understood from the above text that the EDPB approach is that a personal data breach should be notified under both legislative acts, regardless of the fact that the E-Privacy Directive particularises the personal data breaches to those who are in connection with the electronic communication services. In our view, the obligation should arise only under E-Privacy Directive, as a *lex specialis.* But EDPB decided to give a solution to a non-issue, complicating the situation of Telecom Providers, while leaving other hypotheses out of the regulatory framework. The Telecom Providers are thus lacking clarity regarding the data breach notifications.

In practice, the main issue the Telecom Providers are facing concerns the criteria applicable for notifying a data breach. The delay in adopting a new E-Privacy Regulation that will ensure a single regime for the notification of personal data breaches, under GDPR, puts a lot of pressure on Telecom Providers in deciding what regime (due to the interpretation provided by EDPB) and, most importantly, what criteria to apply when deciding to notify a data breach.

When creating the data breach regime under E-Privacy Directive, the EU legislator defined the core elements of the notification system and left the definition of details on circumstances (including criteria to assess the likelihood of adverse effects), procedures and formats to be set by the Commission by ways of implementing measures, in order to ensure consistency across sectors[7].

This approach has been identified as being the best option since the use of implementing measures should have allowed more detailed, precise and flexible rules, rules that could be integrated in the Directive afterwards.

Unfortunately, the implementing measures have never been adopted. Both the entities subject to notification and the supervisory authorities, have been facing the need to assess if an incident is notifiable or not based on too vague defined criteria– i.e. the provider needs to inform the individuals about the breach "*when the personal data breach* ***is likely to adversely affect*** *the personal data or privacy of a subscriber or individual*" (our emphasis).

As opposed to the data breach notification regime under E-Privacy Directive, GDPR aimed to create a risk-based approach when assessing whether or not a breach should be notified, giving consideration to the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring. This approach was built on the fact that, based on the experience with the application of E-Privacy Directive, the EU legislator identified a notification fatigue phenomenon[8]: entities would notify the supervisory authorities any incident, regardless of its gravity, in order to avoid fines for not notifying when they should have.

Indeed, under Article 3 section 2 of the Regulation no. 611/2013, the criteria to be considered by Telecom Providers when assessing whether a personal data breach is "*likely to result in a risk*" are:

(i) the nature and content of the personal data concerned, in particular where the data concerns financial information, special categories of data referred to in Article 8(1) of Directive 95/46/EC, as well as location data, internet log files, web browsing histories, e-mail data, and itemised call lists;

(ii) the likely consequences of the personal data breach for the subscriber or individual concerned, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation;

(iii) the circumstances of the personal data breach, in particular where the data has been stolen or when the provider knows that the data are in the possession of an unauthorised third party.

Also, according to the guidelines issued by the Article 29 Working Party, the following criteria should be taken into account when assessing the risk that may be entailed by a breach:

(i) the type of breach;

(ii) the nature, sensitivity, and volume of personal data;

(iii) ease of identification of individuals;

(iv) severity of consequences for individuals;

(v) special characteristics of the individual;

(vi) the number of affected individuals.

Although such criteria might be considered enough to help the Telecom Providers in correctly identifying and notifying personal data breaches in connection with the provision of a publicly available electronic communications service, as mentioned above, in practice, a notification fatigue phenomenon appeared mainly because these criteria are too general and are not entirely useful to help when a decision has to be made if a certain data breach should be notified or not. Therefore, it is still challenging to evaluate when the breach "may result *in a high risk* to the rights and freedoms of the natural persons" (our emphasis), as the variety of breach that may occur is very high or when the notification is not needed as "*the high risk to the rights and freedoms of data subjects is* ***no longer likely to materialise***" (our emphasis).

As Telecom Providers need to rely on the Regulation no. 611/2013 criteria, because the E-Privacy Directive lacks any assessment criteria and the implementing measures proposals were never adopted, a possible approach is for Telecom Providers confronted with an incident to apply *mutatis mutandis* the criteria provisioned by the GDPR as well as by any future implementing measures.

By adopting this solution, Telecom Providers will benefit from all the lessons learnt in this period when the data breach notification under both E-Privacy Directive and GDPR was applicable. This approach will also help diminish the notification fatigue phenomenon that now threatens to encompass both types of data breach notification, since as per the statistics of a recent report[9] *over 160,000 data breach notifications have been reported across the 28 European Union Member States plus Norway, Iceland and Liechtenstein since the General Data Protection Regulation came into force on 25 May 2018.*

3. Steps to be considered

As long as both GDPR and E-Privacy Directive apply, a legislative intervention to regulate this transitory situation is needed. The over-notification phenomenon requires the legislator attention and responsibility.

As mentioned above, a solution may be providing for a unified set of criteria that Telecom Providers must consider when assessing the risks of a breach and, as the E-Privacy Regulation already stipulates, eliminating the obligation to notify the personal data breaches under the E-Privacy Directive.

Moreover, it is important that the individual's right to know does not become an unnecessary burden too and that only those impactful events that might trigger an action on his or her side be communicated.

The interests at stake must be balanced and analysed by the EU Legislator in order to provide the transparency and clarity required by the affected individuals, the criteria needed by companies in order to prioritise their resources and to ease the activity of the supervisory authorities.

*****

Cristina Crețu

Senior Privacy & Technology Consultant

cristina.cretu@mprpartners.com

Laura Dinu

Associate

laura.dinu@mprpartners.com

Citations

[1] Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications (Electronic Communications Data Protection Directive), last amended by the Directive 2009/136/EC.

[2] *Justification: The Commission Regulation (EU) 611/2013 setting out specific rules on data breach notifications should be repealed as its legal basis, Directive 2002/58/EC, will be repealed, and the GDPR will apply for breach notifications* from Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

[3] Article 7 of the Charter of Fundamental Rights of The European Union, Article 8 of the European Chart of Human Rights.

[4] Proposal for a Regulation of The European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

[5] More on this topic available in the Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments issued by Article 29 Working Party.

[6] Article 2 from E-Privacy Directive and Article 4 point 12 from GDPR.

[7] Article 4 section 5 from E-Privacy Directive.

[8] Commission Regulation (Eu) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications

[9] *It was estimated that currently 3,000 data breach notifications take place in the EU for the telecoms sector every year, calculated on the basis of 319 data protection breaches reported to the UK DPA in 2008/2009 and extrapolated for the EU28. The average cost for businesses for dealing with these notifications was assumed to be 400 EUR,* in the Commission Staff Working Paper on Impact Assessment on the General Data Protection Regulation proposal, 25.01.2012, SEC 2012(72), Annex 9 and p. 101.

[10] GDPR Data Breach Survey 2020, report issued by DLA Piper, available online at: https://www.dlapiper.com/en/us/insights/publications/2020/01/gdpr-data-breach-survey-2020/ (last accessed on February 3, 2020).