Comments on WP29 guidelines on personal data breach notification

28 November 2017

Comments on the Introduction

On page 5, the guidelines refer to Opinion 03/2014, stating that:

"In its Opinion 03/2014 on personal data breach notification, WP29 provided guidance to controllers in order to help them decide whether to notify data subjects in case of a breach. The opinion considered the obligations of providers of electronic communications regarding Directive 2002/58/EC and provided examples from multiple sectors, in the context of the then draft GDPR, and presented good practices for all controllers."

Opinion 03/2014 therefore considered both the ePrivacy Directive and the then draft GDPR.

We would like to understand the status of Opinion 03/2014.

To the extent that it relates to the ePrivacy Directive, will it remain valid?

To the extent that it relates to the GDPR, will it be replaced, in whole or in part, by the current guidelines?

Comments on Section I

On page 6, the guidelines state that "not all security incidents are necessarily personal data breaches".

We think this is a helpful clarification, and that the examples in Annex B provide further useful guidance.

The guidelines also state on page 6 and page 7 that:

"Whereas determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious. A breach will always be regarded as an availability breach where there has been a permanent loss of, or destruction of, personal data. The question may be asked whether a temporary loss of availability should be considered as a breach and, if so, one which needs to be notified".

The guidelines go on to state on page 7 that:

"…an incident resulting in personal data being made unavailable for a period of time is a security breach (and should be documented), yet depending on the circumstances, it may or may not require notification to the supervisory authority and communication to affected individuals."

The guidelines therefore appear to be saying that a loss of availability (whether permanent or temporary) is a data breach. If that interpretation of the guidelines is correct then the key question is whether or not the breach meets the risk thresholds set out in Articles 33 and 34 regarding notification to the supervisory authority and communication to the data subjects. We would like to ask for clarification that this is the correct interpretation of the guidelines.

We agree with the analysis in the three examples on page 7.

The paragraph above the ransomware example states that

"Furthermore, it should be noted that although a loss of availability of a controller's systems might be only temporary and may not have an impact on individuals, the fact that there has been a network intrusion could still be considered a confidentiality breach and notification might be required. Therefore, it is important for the controller to consider all the possible consequences of a breach."

Association for Financial Markets in Europe
London Office: 39th Floor, 25 Canada Square, London E14 5LQ, United Kingdom T: +44 (0)20 3828 2700
Brussels Office: Rue de la Loi 82, 1040 Brussels, Belgium T: +32 (0)2 788 3971
Frankfurt Office: Skyper Villa, Taunusanlage 1, 60329 Frankfurt am Main, Germany T: +49 (0)69 5050 60590
www.afme.eu

We think that the purpose of this paragraph is clear, but we think that the drafting could be clarified by rewording as follows:

"Furthermore, it should be noted that *even if* a loss of availability of a controller's systems *is* only temporary and the loss of availability *does not* itself result in a risk to the rights and freedoms of individuals, the controller would also need to consider whether there has been a confidentiality breach, and if so, whether that would need to be notified. The following example illustrates this point."

The guidelines state on page 8 that

"…the supervisory authority will also have the possibility to issue sanctions for failure to notify or communicate the breach (Articles 33 and 34) on the one hand, and absence of (adequate) security measures (Article 32) on the other hand, as they are two separate infringements."

We would like to understand how this guidance relates to the provisions of Article 83(3), which states that

"If a controller or processor intentionally or negligently, for the same or linked processing obligations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement."

Clarification would be helpful on whether, or when, an infringement of Articles 32, 33 or 34 would be considered to be "for the same or linked processing operations" for the purposes of Article 83(3), such that the total amount of the administrative fine would not exceed the amount specified for the gravest infringement.

Comments on section II

The guidelines state on page 9 that:

"WP29 considers that a controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. This will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. 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."

We agree with this interpretation.

We think that the examples provided are helpful, though in example 4 we believe that firms would not necessarily rely solely on a communication from a cybercriminal.

We would suggest clarifying example 4 by rewording as follows:

"A cybercriminal contacts the controller and claims to have hacked its system, but offers no evidence either that they have encrypted the controller's data or that they have unlawfully obtained personal data. In that case, the controller would first need to investigate the situation to establish with a reasonable degree of certainty whether or not a breach has in fact occurred. During this period of investigation, the controller would not be regarded as being "aware". The controller would be "aware" as soon as reasonable certainty is established."

Article 33(2) states that:

"The processor shall notify the controller without undue delay after becoming aware of a personal data breach."

Article 33(1) states that:

"In the case of a personal data breach, the controller shall without undue delay and, where feasible, within 72 hours after having become aware of it, notify the personal data breach to the supervisory authorities…, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."

We think the sequencing set out in the GDPR, combined with the guidelines on page 9, is clear:

- The processor identifies a security incident and assesses whether there has been a personal data breach
- Where the processor's assessment is that there has been a personal data breach, the processor notifies the controller
- The controller (having been notified) should have a reasonable degree of certainty that there has in fact been a personal data breach
- The controller, at that time, becomes "aware" of the personal data breach
- The 72-hour timeframe starts running at that time
- The controller then assesses whether the breach is likely to result in a risk to the rights and freedoms of individuals

The guidelines however state on page 11 that:

"…the processor… must notify the controller without undue delay. The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as "aware" once the processor has become aware."

We do not think this sentence is consistent with the sequencing set out above or the language as stated within the GDPR. The GDPR attributes awareness to the controller; in a processor context, this would be based on the notification by the processor, unless the controller became aware of the breach independently.

We suggest that the sentence be clarified by rewording as follows:

"…the processor… must notify the controller without undue delay. The controller then establishes with a reasonable degree of certainty whether there has in fact been a personal data breach. At that time, the controller becomes "aware"."

We note that this is also consistent with example vii in Annex B, where it is stated that "Assuming the website hosting company [a data processor] has conducted its own investigation the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having "become aware" once they have been notified by the hosting company (the processor)."

We have two further comments on the section on processor obligations.

The guidelines state on page 11 that:

"The controller retains overall responsibility for the protection of personal data, but the processor has an important role to play to enable the controller to comply with its obligations."

We believe that this statement does not properly reflect the fact that under the GDPR both the controller and processor have obligations for the protection of personal data. While we agree that it is the controller that has the obligation to notify the supervisory authorities under Article 33(1), we do not think it is correct as a matter of law to say that the controller retains overall responsibility "for the protection of personal data".

We therefore suggest that the sentence be clarified by rewording as follows:

"The controller has the obligation to notify under Article 33(1), and the processor has an important role to play to enable the controller to comply with that obligation."

The guidelines on page 11 state that:

"Article 28(3)(f) states that the contract or other legal act shall stipulate that the processor "assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36…"

The guidelines go on to say that:

"As is explained above, controllers are required to specify how the requirements expressed in Article 33(2) should be met in their contract with their processor."

We do not think it is correct to say that "controllers are required to specify…". We think that Article 28(3)(f) is clear that "the contract …shall stipulate". The contract is negotiated between the controller and the processor. We therefore suggest clarifying, by rewording as follows:

"The contract between the controller and processor should specify how the requirements in Article 33(2) should be met."

The guidelines on page 12 state that:

"Where precise information is not available (e.g. exact number of data subjects affected) this should not be a barrier to timely breach notification. The GDPR allows approximations to be made in the number of individuals affected and the number of personal data records concerned."

We think this guidance could be especially relevant in the event of a system being hacked, where it may be difficult to identify the records that have been hacked, and therefore may be difficult even to make a reasonable approximation. We would suggest including a sentence as follows:

"In the event of a hack, it may be difficult to identify the records that have been hacked, and therefore may be difficult even to make a reasonable approximation within the stipulated timeframe for notification of the personal data breach."

The guidelines on page 14 state that:

"…a controller experiences multiple, similar confidentiality breaches over a short period of time, affecting large numbers of data subjects in the same way. A controller could become aware of a breach and, whilst beginning its investigation, and before notification, detect further similar breaches, which have different causes. … Strictly speaking, each individual breach is a reportable incident. However, to avoid being overly burdensome, the controller may be able to submit a "bundled" notification representing all these breaches, provided that they concern the same type of personal data breached in the same way, over a relatively short space of time."

We think this is a useful approach.

We would suggest adding a sentence as follows:

"In practice, the controller may initially not be sure whether the breaches concern the same type of data breached in the same way, but controllers should be able to submit a bundled notification if it appears reasonable to do so, while undertaking a detailed root cause analysis."

We think it would also be helpful to include an Example to illustrate the guidelines on bundled notification.

The guidelines on page 15 state that:

"…whenever a breach affects the personal data of individuals in more than one Member State and notification is required, the controller will need to notify the lead supervisory authority. … A controller may wish to proactively also report an incident to a supervisory authority which is not its lead authority, for example if the controller knows that individuals in other Member States are affected by the breach."

Our understanding is that reporting to a supervisory authority which is not the lead authority is entirely voluntary. The relevant part of the flowchart in Annex A states includes the following sentence

"If the breach affects individuals in more than one Member State, notify each competent supervisory authority accordingly."

We suggest that as the flowchart heading refers to "requirements" this sentence should be deleted.

Comments on Section III

Article 34(1) states that:

"When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."

Annex B provides a non-exhaustive list of examples.

Example ii states in the Notes/recommendations column that:

"If the risk is not high, we recommend that the controller to notify the data subject, depending on the circumstances of the case. For example, notification may not be required if there is a confidentiality breach for a newsletter related to a TV show, but notification may be required if this newsletter can lead to political point of view of the data subject being disclosed."

We think that the first sentence of Example ii is not consistent with Article 34(1), because it seems to suggest notifying the data subject "if the risk is not high".

We would suggest clarifying by deleting the first sentence.

The guidelines on page 18 state that:

"Article 34(3) states three conditions that, if met, do not require notification to individuals in the event of a breach."

We would suggest adding another box to the flowchart in Annex A to reflect this. The box should be added just above the box which states "Notify affected individuals…"

We would also suggest minor rewording to the guidelines to make clear that communication to the data subject shall not be required if *any* of the three conditions is met.

Comments on Section IV

The guidelines on page 20 state that:

"…when assessing the risk to individuals as a result of a breach, the controller will be considering the specific circumstances of the breach, including its severity and potential impact. WP29 therefore recommends the assessment should take into account the following criteria… Article 3.2 of Regulation 611/2013 provides guidance [on] the factors that should be taken into consideration in relation to notification of breaches in the electronic communication services sector, which may be useful on the context of notification under the GDPR."

For ease of reference, we think it would be useful to include the text of Article 3(2) of Regulation 611/2013, either in the footnote or in an Annex.

The guidelines on page 22 state that:

"[ENISA] has produced recommendations for a methodology of assessing the severity of a breach, which controllers and processors may find useful when designing their breach management response plan."

Page 1 of the ENISA recommendations states that:

"It is planned to further develop the methodology with the aim to generate a final practical tool for data breach severity assessment."

We would be interested to understand the current state of play with the ENISA work.

Comments on Section V

The guidelines on page 23 state that:

"…if the controller considers that any of the conditions in Article 34(3) are met, then it should be able to provide appropriate proof that this is the case."

We would suggest clarifying this by replacing "proof" with "evidence".

Comments on Section VI

The guidelines on page 24 state that:

"In addition to the notification and communication of breaches under the GDPR, controllers should also be aware of any requirement to notify a particular personal data breach under other associated legislation that may apply to them, which can vary between Member States, including the following:

…eIDAS Regulation

…NIS Directive

…Citizens' Rights Directive

…Breach Notification Regulation (pursuant to the ePrivacy Directive)

We note that banks may also be subject to notification obligations under Payments Services Directive 2.

We appreciate that the present guidelines are focused on the GDPR. We would however suggest that it could be useful in due course to undertake a review of the coherence of the multiple requirements.

Comments on the Annex

We have included comments above on the flowchart and on selected examples.

Contacts

Richard Middleton
Managing Director, Co-Head of Policy Division
AFME
T 020 3828 2709 | M 07 584 583 122
E richard.middleton@afme.eu

Walter McCahon
Policy analyst
UK Finance
T 020 3934 1131| M 07 725 683263
E walter.mccahon@ukfinance.org.uk