Public consultation on Guidelines 9/2022 on personal data breach notification under GDPR

Bruno RASLE's contribution– bruno_rasle@halte-au-spam.com – Tel. +33 6 1234 0884

In Chaville (France), 29th october 2022

---

1. **When does a controller become "aware"?**

The draft again addresses this important issue (p.11), but without giving a definitive answer to the question « *Whom - inside the controller - are we talking about? Is it the representative (the highest hierarchical level) or any member of the controller?* ».

This uncertainty leads to aberrant behaviour in some companies, where employees voluntarily delay informing senior management on the (erroneous) grounds that this avoids triggering the 72-hour rule!

The text passage « *It is important that when a breach is detected it is reported upwards to the appropriate level of management so it can be addressed and, if required, notified in accordance with Article 33 and, if necessary, Article 34* » suggests that, as soon as any employee of the organisation is aware of the breach, the 72 hours start. The project should clarify this to stop the deviant behaviour mentioned above.

It would also be useful to clarify that the 72 hours are natural ones, not working hours.

2. **Joint controllers**

In page 13, the draft would benefit from the suggestion to inform the other controller and his DPO of the breach.

3. **Processor obligations**

In point 44 (p.14, « Processor obligations »), it is understood that the controller is considered to be « aware of the breach » as soon as it is informed by its processor.

This rule is surprising because:

- It assumes that the processor has carried out a perfect investigation on which the controller has nothing to say

- Contrary to the situation in which the breach does not concern any processor, it does not allow the controller any time for investigation (although he has it in point 34 : « *…the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware"* »).

This is due to a major design error of the GDPR, which is to let a processor decide whether a security incident impacting personal data it processes on behalf of a controller is (or is not) a breach within the meaning of Article 4.12 of the GDPR.

This puts controllers in a state of total dependence: if their processor makes a mistake in classifying the incident (or deliberately disguises its nature as a breach), they are not informed and therefore cannot notify the breach to the supervisory authority, nor to the data subjects.

As the draft cannot rewrite the GDPR, is there not a way to encourage controllers and their processors to clearly address the issue of incident qualification when formulating the contract under Article 28 of the GDPR?

In point 45 (p.14), the last sentence is surprising! It gives the impression that the 72 hours (if possible) that the controller has to (possibly) notify the authority of the breach are linked to the time that the processor takes to notify the breach to his client.