Comments on Guidelines 9/2022 on personal data breach notification under GDPR

Mauricio Tavares <evilgenius@privacytestdriver.com>
Privacy Test Driver

Page 20 paragraph 28:
(Typo) Replace “10,000,000 EUR or up to 2 % if the total worldwide” with “10,000,000 EUR or up to 2 % of the total worldwide”

Page 11, Paragraph 33 AND page 12 paragraph 35
(Question) When reporting the personal data breach incident, should the controller provide documentation/evidence of when it became aware or does a line in the incident report station “we became aware on Tuesday 27th after realizing the computer one of our employees contacted us stating was slow and unresponsive was actually being used to exfiltrate data” suffices? “Aware” is a bit vague.

page 12 paragraph 35
(Question) What is a ‘”short” period of investigation’? 1 day? 1 week? 1 month? After all, once investigation is made, the impact analysis takes place so controller can verify whether this was a personal data breach and proceed accordingly. If I were to use American law parlance, there is a “reasonable person” principle[1], which talks about how a reasonable person would react.

page 13 paragraph 41
(Note) Timely here does remind me of the “reasonable person principle” mentioned above. The reason I mention it again is that we need to define what “appropriate” is here. No controller has the budget to “secure all things” so there will always be a risk. While come companies are guilty of blatant of negligence, technical and organisational measures evolve with time. And some may have been prohibitively expensive for the controller to implement, so it made a privacy risk analysis. How would this analysis count during a privacy data breach? Once again “reasonable” is a bit vague. A Less Vague definition would imply “if you follow NIST SP 800-53 framework (using it because you mentioned it earlier) you have shown reasonable data protection. Now, if an attacker still manages to break into your servers, we are not going to fine you.”

page 14 paragraph 45
(Note) I believe that puts undue stress onto the controller as the processor may only report the personal data breach after a few weeks of finding it. The “without undue relay” needs to be quantified.

1 https://www.cambridge.org/core/books/abs/tort-law/reasonable-person/19FA345C7D50A61EBAB5289568A89ECB