Comments on EDPB draft "Guidelines 01/2021 on Examples regarding Data Breach Notification"

Introduction – high variation in current rates of breach notifications in EU Member States

CEDPO was represented at the Article 29 Working Party "Fablab" in Brussels on April 5th & 6th, 2017 by the author of this commentary, Fintan Swanton. The April 5th session on personal data breaches was co-chaired by Gwendal Le Grand (CNIL - FR) and Wilbert Tomesen (AP - NL).

Mr Tomesen noted that under pre-GDPR national data protection law, it had become from 2016 a legal obligation in the Netherlands to make breach notifications to the AP. He went on to say that the AP had estimated they would receive ca. 60,000 reports in the first year, but in fact they only received 7,000. However, in 2020, the AP did receive 66,257 breach notifications[1] under GDPR Article 33. In the longer term, therefore, the AP's estimate of the frequency of notifiable personal data breaches in its jurisdiction was quite accurate.

At the Fablab, Mr Le Grand mentioned that breaches then only needed to be reported in France by telecoms and internet service providers, under the terms of the "ePrivacy" directive, and at that time only "a couple" of such reports were received by the CNIL each year. By contrast, for example, Ireland's Data Protection Commissioner stated in her 2016 annual report[2] that she had received 142 breach reports that year from the Irish telecoms sector.

This high variation in personal data breach notifications in EU Member States remains the case. Breach notifications in 2020 at several higher population EU countries were as follows:

- Netherlands: 66,257 (388 per 100,000 of country population)
- Germany: 77,747 (93 per 100,000 of country population)
- France: 5,389 (8 per 100,000 of country population)
- Italy: 3,460 (6 per 100,000 of country population)

So, *pro rata*, the breach notification rates in France and Italy are respectively just 2.1% and 1.5% of the rate in the Netherlands.

---

[1] "GDPR fines and data breach reports increased in 2020", KINAST Attorneys at Law (Germany)
[2] "Annual Report, 2016", Data Protection Commission (Ireland)

One of CEDPO's member associations, the German Association for Data Protection and Data Security, initiated a survey in February 2021 among its members to evaluate examples of personal data breaches and the members' reaction to the respective incident. Several conclusions can be drawn from the survey:

i. Categories of breaches.

Typical categories of personal data breaches were: **personal data sent by mistake**, **access rights outside need-to-know**, **deletion of data**, **misconfigurations of IT systems, theft (hardware or paper files), loss of hardware of paper files, cyberattack**s.

The sending of personal data by mistake has been, *by far*, the incident reported by most of the member associations.

ii. Risk assessments.

Risk assessments varied concerning identical data breaches. Especially with regard to sending personal data via email using the CC instead of BCC functionality, controllers came to different conclusions regarding a notification obligation.
Besides, in many of the notified data breaches, an access to personal data could not be clarified by the controller. Interpretations between controllers varied, to which extent access to personal data needs to be proofed in order to be subject of Art. 33 or Art. 34 GDPR notification obligations. In some cases, where access could not be clarified, the criteria of a possible interest of the affected personal data to a third party was used in order to assess the likelihood of risks to the rights and freedoms of data subjects.

iii. Notice periods.

Complex examples of a possible personal data breach partially led to a delayed notification of the supervisory authority. The DPO, playing a pivotal role in assessing risks to data subjects in many companies, had to rely on information from other departments which could not be given in due time. Controllers refrained to notify until their own internal assessment of risks was complete. In other cases, a delay resulted from uncooperative data processors which delayed data breach notifications to controllers.

Observations on EDPB Guidelines case studies

Scope of breach risk assessment and worst case impact

The GDPR criteria for breach notifications to supervisory authorities and data subjects are based on risks "to the rights and freedoms of natural persons". This is broader than as described in paragraph 6, page 5 of the Guidelines, which states that "one of the most important obligations of the data controller is to evaluate … risks to the rights and freedoms of the data subjects".

The GDPR requires breach notifications to be made "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons." It does not limit this risk assessment to data subjects of the affected data.

The worst-case example of this is the ransomware attack on a Düsseldorf hospital in September 2020, which resulted in the death of a patient. It is unclear from news reports whether the deceased patient's personal data had been affected (if she had not been previously admitted to the hospital, it might not yet have had any personal data relating to her). But it could not have had a worse impact on her and her family[3].

The Guidelines should more accurately describe the scope of breach risk assessments, and provide clearer examples of the worst case impacts of breaches on natural persons, including but not limited to data subjects of affected data.

Human error breaches

Paragraph 8, page 6 of the Guidelines states that "Before a controller can fully assess the risk arising from a breach caused by some form of attack, the root cause of the issue should be identified …" It should be noted that, of course, while many breaches are caused by malicious attacks, such as the ransomware attack mentioned above, the large majority of data breaches are caused by unmalicious human error or system error.

Controller risk likelihood assessment

Paragraph 10, page 6 of the Guidelines states that "If a controller self-assesses the risk to be unlikely, but it turns out that the risk materializes, the relevant SA can use its corrective powers and may resolve to sanctions."

The fact that a risk the controller assessed to be unlikely does actually occur is not in itself proof that the assessment was incorrect. "Unlikely" does not mean "impossible". The SA should assess whether the controller, in light of the information available at the time it became aware of the breach, made a reasonable risk assessment.

Identified risks

Paragraph 25, page 9 of the Guidelines includes a table template headed "Actions necessary based on the identified risks". It indicates a breach notification is only unnecessary if a breach has caused "No risk". The criterion for not making a breach notification is not "no risk", but "unlikely risk". As the Guidance itself notes, e.g., it is at least theoretically possible that currently encrypted personal data may in future be possibly decrypted.

CASE No. 15: Personal data sent by mail by mistake

"A list of participants on a course in Legal English which takes place in a hotel for 5 days is by mistake sent to 15 former participants of the course instead of the hotel. The list contains names, e-mail addresses and food preferences of the 15 participants. Only two participants have filled in

[3] "German police probe 'negligent homicide' in hospital cyberattack", Deutsche Welle

their food preferences, stating that they are lactose intolerant. None of the participants have a protected identity. The controller discovers the mistake immediately after sending the list and informs the recipients of the mistake and asks them to delete the list."

The Guidelines assessment that "… in this particular case no risk can be identified that the breach will lead to physical, material or non-material damages of the data subject due to the unauthorised disclosure of lactose intolerance information" is not agreed with by CEDPO.

For example, it is entirely possible that one or more of the 15 former participants who received the email in error would decide in good faith to contact the affected data subjects to let them know of the breach. This in turn is quite likely to at least cause embarrassment and distress – i.e., non-material harm – to the data subjects. This non-material harm will be worsened if the data subjects first hear of the breach in this way, rather than by notification from the controller admitting the breach has occurred, and advising on how resulting risks are being contained.

This case is very similar to the next case (16 snail mail). In both cases wrong recipients receive an email or a mail by mistake and find out personal information about another person. The conclusions should therefore be identical unless the facts differ. Indeed, in this case, like in the snail mail case, there is a risk that an unintended recipient discloses the information publicly (e.g. on social networks). So, the critical difference between the two scenarios is that in case 15, the recipients have all been contacted and we assume that they gave assurances that they deleted the email. We suggest to present case 16 before case 15 and to better illustrate the differences between the two scenarios.

CASE No. 16: Snail mail mistake & CASE No. 17: Identity theft

"An insurance group offers car insurances. To do this, it sends out regularly adjusted contribution policies by snail mail. In addition to the name and address of the policyholder, the letter contains the vehicle registration number, the insurance rates of the current and next insurance year, the approximate annual mileage and the policyholder's date of birth. Health data according to Article 9 GDPR, payment data (bank details), economic and financial data are not included. Letters are packed by automated enveloping machines. Due to a mechanical error, two letters for different policyholders are inserted into one envelope and sent to one policyholder by letter post. The policyholder opens the letter at home and takes a look at his correctly delivered letter as well as at the incorrectly delivered letter from another policyholder." (Case 16)

"The contact centre of a telecommunication company receives a telephone call from someone that poses as a client. The supposed client demands the company to change the email address to which the billing information should be sent from there on. The worker of the contact centre validates the client's identity by asking for certain personal data, as defined by the procedures of the company. The caller correctly indicates the requested client's fiscal number and postal address (because he had access to these elements). After the validation, the operator makes the requested change and, from there on, the billing information is sent to the new email address. The procedure does not foresee any notification to the former email contact. The following month the legitimate client contacts the company, inquiring why he is not receiving billing to his email address, and

denies any call from him demanding the change of the email contact. Later, the company realizes that the information has been sent to an illegitimate user and reverts the change." (Case 17)

The Guidelines' assessments of Cases 16 & 17 are not entirely consistent. While it is true that the exposure of data in Case 16 was accidental and not malicious as in Case 17, it is still significant personal data that could possibly be abused for identity theft. And, as described above in comments on Case 15, the person who received the letter by mistake might also in good faith send it on directly to the affected data subject, potentially causing anxiety, especially if the person has not heard anything about the breach directly from the controller.

Conclusions

The current high variation in breach notifications indicates that controllers in some EU countries are not taking this obligation seriously, thereby risking seriously increased impact on affected natural persons. The EDPB needs to achieve a consistent adherence to breach notifications across all member states.

In particular, the Article 33 criterion for notifications to supervisory authorities – "notify the personal data breach …. unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons" – is intentionally a very low threshold.

And this highlights another common misinterpretation of the breach notification requirement. "A risk", as referred to in Art. 33.1, is the severity of a potential impact multiplied by the likelihood of the impact. But the notification requirement Is based solely on the likelihood of the risk, not its severity. If **any** negative impact on natural persons is possible from the breach, regardless of whether its severity is low, medium, or high, it must be reported to the SA unless the possibility of the impact occurring is "unlikely".

The main logic is that the SA will re-assess the risk and, if it has a different view on it to the controller's, it may recommend or order measures to contain the risk. This is also the rationale for the 72-hour deadline for notifications, so the SA's re-assessment can be done "in an appropriate and timely manner" (Recital 85). So, regardless of how low the controller considers the risk impact severity to be, it must still be reported to the SA unless **occurrence** of the impact is unlikely.

Also, an appropriate scale of breach notifications allows supervisory authorities to detect and respond to patterns of breaches which are occurring across groups of controllers.

However, to meet these supervisory authority functions, the Guidelines descriptions of the scope of the breach notification obligation and its examples of risk assessment could be improved.

In summary, the main rationale for making breach notifications is to assess & manage the resulting risks to natural persons. The current broad failure to meet GDPR notification obligations is exacerbating these risks.

Fintan Swanton,
LLM MSc CEng FICS MBCS.

02 March 2021