02.03.2021

AMICE Response to EDPB consultation on draft guidelines on examples regarding data breach notifications

I. PRELIMINARY REMARKS

AMICE greatly appreciates the efforts made by the EDPB with the publication of *practice-oriented*, *case-based* guidance (i.e. the Guidelines 01/2021 on Examples regarding Data Breach Notification, adopted on 14 January 2021) to help data controllers in deciding how to handle data breaches and what factors to consider during a risk assessment.

As clarified by the EDPB, the document is intended to complement the Guidelines on Personal data breach notification under Regulation 2016/679 (WP 250) - which already provide a general guidance on data breach notification – in order to reflect the common experiences of the supervisory authorities (SAs) of the EEA since the GDPR became applicable and thus to address practical issues in more details.

With this in mind, taking into account the increasing relevance of personal data breaches in today's world, AMICE welcomes the opportunity to provide feedback on the draft guidelines before their final adoption by the EDPB. We believe this would provide specific insights into some of the cases mentioned in the draft Guidelines and it would make it possible to enhance the effective implementation of the Guidelines.

In brief:

- The Guidelines 01/2021, by providing recommendations on the actions necessary based on the identified risks (No risk - internal register; Risk - notify SA; High Risk - communicate to data subjects), **do not appear to be fully in line with ex Article 29 Working Party (WP) Guidelines WP 250** (which remain valid and which they aim to complement, as well as with the risk-based approach embedded in the GDPR), particularly about the elements and the circumstances to be considered when assessing the risk for the data subjects and the timeliness of data breach notifications;
- Should the EDPB decide to confirm its approach on personal data breach notifications, **by considering that notifying supervisory authorities is necessary for certain types of data breaches that do not have any substantial negative effect on data subjects and even that notifying high risk cases within the 72 hours' time-limit is unsatisfactory**, such an approach will have adverse effects not only for the data controllers that have to comply with extended notification obligations (due to a significant increase of administrative burdens) but also for the supervisory authorities, which are already resources-constrained (due to over-reporting).

II. THE RISK-BASED APPROACH IN THE GDPR - INTERPRETATION AND IMPLICATIONS

The GDPR embraces a risk-based approach to data protection that encourages data controllers to engage in risk analysis and to adopt risk-measured responses corresponding to the level of risk of their data processing activities (high-risk, risk, low risk).

However, the GDPR does not define the term "risk". Where the concept of risk appears in the GDPR, it is defined by reference to the "likelihood and severity" of a negative impact on data subject rights and freedoms and it is to be determined by reference to "the nature, scope, context and purposes of the processing" (Recitals 75 and 76 of the GDPR).

As regards to personal data breach notification, the GDPR sets out basic requirements for notification but leaves room for manoeuvre, with data controllers required to assess risks and make decisions themselves on whether notification is required, and if so, to whom (supervisory authority/data subjects).

This means that, although the GDPR introduces the obligation to notify a breach – as clarified by the Guidelines WP 250 – it is not a requirement to do so in all circumstances:

- Notification to the competent supervisory authority is required unless a breach is unlikely to result in a **risk** to the rights and freedoms of individuals;
- Communication of a breach to the individual is only triggered where it is likely to result in a **high risk** to their rights and freedoms.

Immediately upon becoming aware of a breach, it is then vitally important that the controller should not only seek to contain the incident but it should also assess the risk that could result from it. "*There are two important reasons for this: firstly, knowing the likelihood and the potential severity of the impact on the individual will help the controller to take effective steps to contain and address the breach; secondly, it will help it to determine whether notification is required to the supervisory authority and, if necessary, to the individuals concerned*" (page 23 of the Guidelines WP 250).

In this context, when looking at the factors to assess "risk" and "high risk", the Guidelines WP 250 refer to Recitals 75 and 76 of the GDPR already mentioned above that "*suggest that generally when assessing risk, consideration should be given to both the likelihood and severity of the risk to the rights and freedoms of data subjects. It states further that risk should be evaluated on the basis of an objective assessment*" (page 23 of the Guidelines WP 250).

It derives that the risk analysis is contextual. Accordingly, the Guidelines WP 250 clarify that "*when assessing the risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring.*" To this end, the ex Article 29 WP provided for a valuable and detailed analysis of the criteria to be considered in the risk assessment:

- The type of the breach;
- The nature, sensitivity, and volume of personal data (the type and sensitivity of personal data that has been compromised by the breach represent a key factor; usually, the more sensitive the data, the higher the risk of harm will be to the people affected, although consideration should also be given to other personal data that may already be available about the data subject);
- Ease of identification of individuals;
- Severity of consequences for individuals;
- Special characteristics of the individuals and of the data controller;
- The number of affected individuals.

In light of the above, when assessing the risk that is likely to result from a breach, the controller should consider a combination of the severity of the potential impact on the rights and freedoms of individuals, having regard to the substantial negative effect of the breach on data subjects, and the likelihood of these occurring (as reaffirmed in Guidelines 01/2021). Clearly, where the consequences of a breach (i.e. the effects on data subjects) are more severe, the risk is higher and similarly, where the likelihood of these occurring is greater, the risk is also heightened (Guidelines WP 250, page 26).

This is a conclusion that in our opinion has not been entirely taken into account by the EDPB in the analysis and formulation of the cases described in the proposed Guidelines 01/2021. As a result, **the EDPB has indicated as necessary the notification to the supervisory authorities of data breaches with little or no substantial negative effects on data subjects. This creates a significant risk of over-reporting and will prevent data controllers in making effective use of the Guidelines**.

III. CASE NO. 16 – SNAIL MAIL MISTAKE

In particular, **we would like to refer to Case No. 16 (Snail mail mistake) which concerns the insurance business**. More precisely, the personal data breach at issue is originated by the dispatch of two letters, containing adjusted car insurance policies' offers addressed to two different policyholders, to one policyholder because the letters were inserted into one envelope due to a mechanical error of the automated enveloping machines.

Looking at the criteria identified by the ex Article 29 WP in the Guidelines WP 250, it is our opinion that in this case the EDPB has carried out a **risk assessment** that appears **too standardized and concise with the absence of a complete analysis of the factors that trigger a notification**.

As regards to the nature and sensitivity of the data involved, the EDPB specifies that the incorrectly delivered letter contains the name, address, date of birth, license plate number and the classification of the insurance rate of the current and the next year, without including health data according to Article 9 of GDPR, payment data (bank details), economic and financial data.

When looking at the ease of identification of individuals, the EDPB states that the effects on the affected person are to be regarded as **medium**, since the information disclosed to the unauthorized recipient are not publicly available, such as the date of birth, vehicle registration numbers and the insurance rate.

The EDPB affirms then that while many recipients will probably dispose of the wrongly received letter in the garbage, in individual cases it cannot be completely ruled out that the letter will be posted in social networks or that the policyholder will be contacted. Hence, when examining the severity of the consequences for the individuals, the EDPB concludes that the **probability of misuse of this data is assessed to be between low and medium.**

This is a conclusion, which the EDPB seems to adopt *a priori*, without taking into account that the analysis of such circumstances causing more severe effects on individuals has to be **contextualized and carried out on a case-by-case basis.** As indicated in the Guidelines WP 250 (page 24), the controller should assess the specific circumstances of the breach, the data affected, and the potential level of impact on individuals, as well as how likely this risk will materialise (and should not only refer to individual cases). For example, while it may be understandable that the risk of misuse might be higher – and consequently, the consequences for the individuals – if one of the policyholders is a well-known or a famous person, this is not always true in all circumstances.

There are no specific observations relating to the special characteristics of the data subject or the data controller, as well as to the number of affected individuals (which is one in this case).

In light of the above assessment, the EDPB concludes that the personal data breach at issue has to be notified to the supervisory authority, a conclusion that in our opinion, raises serious concerns.

Firstly, it is not entirely clear why the EDPB has adopted a different (stricter) approach compared to the one illustrated under Case no. 15, which instead concerns personal data sent by snail mail mistake that even includes sensitive data on food preferences of two individuals. In this context, the EDPB considers that the risks deriving from the nature, the sensitivity, the volume and the context of the personal data are low (as in the Case no. 16). The EDPB concludes that even if the information that someone is lactose intolerant is health data, the risk that this data will be used in a detrimental way should be considered relatively low. Conversely, in Case no. 16, the EDPB considers the possibility that a letter – with no sensitive data – received by mistake is posted on social networks more likely to occur, with no sound evidence to support this statement.

In addition, while in the case of data concerning health it is usually assumed that the breach is likely to result in a high risk for the data subject, the EDPB clarifies 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. Contrary to some other food preferences, the EDPB specifies that lactose intolerance can normally not be linked to any religious or philosophical beliefs.

Finally, the EDPB deems the quantity of the breached data and the number of affected data subjects as very low (in Case no. 16 only one individual is involved compared to two participants in Case no. 15).

It follows that the EDPB does not deem necessary to notify the supervisory authority in Case no. 15, while reaching a different conclusion with respect to Case no. 16 with no clear and valid comprehensive explanation.

Moreover, given that, despite the organizational and technical measures adopted by the data controllers, it will probably never be possible to completely prevent a postal delivery error in a mass mailing using fully automated machines (as highlighted by the EDPB), **it is foreseeable that an increasing number of personal data breaches such as the one reported in Case no. 16 will have to be reported.**

This implies that significant resources will have to be dedicated to report very low risk personal data breaches, instead of having them focused on preventing and managing risk/high risk security incidents.

IV. NOTIFICATION TO THE SUPERVISORY AUTHORITY WITHOUT UNDUE DELAY

With respect to the guidance provided on the promptness of the notification obligation to the supervisory authority, we would like to take this opportunity to ask for a clarification.

When describing the mitigation and obligations under Case no. 01 (para. 24), the EDPB notes that **in high-risk cases, notifying a data breach within the 72-hour longstop provided by the GDPR may be unsatisfactory**; the key is to notify data breaches "without undue delay" and such high-risk cases may require earlier notification.

The EDPB however makes this statement in the context of the analysis of a breach that is considered **unlikely to result in a risk to the rights and freedoms of natural persons** - and that does not require communication to the data subjects, nor to the supervisory authority – **without providing concrete examples of a high-risk data breach**, which requires early notification.

It is important to recall what the GDPR and Guidelines WP 250 already have a coherent risk-based approach that does not match the examples given in the proposed Guidelines.

In the case of a personal data breach, the GDPR requires the data controller to notify the personal data breach to the supervisory authority competent in accordance with Article 55 without undue delay and, where feasible, not later than 72 hours after having become aware of it (Article 33, para 1, GDPR). The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject (Recital 87 of GDPR).

In light of the above, we would like to remind of the importance of the analysis of the circumstances of the specific breach (see Guidelines WP 250, page 11). In some cases, even when all appropriate technological protection and organisational measures have been implemented, it may take some time for the data controller to establish if personal data have been compromised and therefore to assess whether to notify or not. Thus, as already pointed out by the EDPB itself in more than one paragraphs of the Guidelines 01/2021, **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**, rather than *de facto* automatically require data controllers to notify the case.

V. CONCLUSIONS

We thank the EDPB for the opportunity to comment on the Guidelines 01/2021 and we call on the EDPB **to avoid imposing on data controllers the requirement to automatically notify the supervisory authorities of almost any type of personal data breaches, reaffirming instead the importance of a contextualized, case-by-case risk assessment**.

The ultimate objective of the Guidelines should be to provide both organisations and the resource-constrained supervisory authorities with a helpful and practical tool to prevent over-reporting of personal data breaches.

To this end, we feel that a possible reformulation of the Guidelines in line with the arguments described above would enhance the implementation of the notification obligation.

The insurance industry is keen to work with the EDPB to achieve a pragmatic and operationally effective outcome.

About AMICE (Association of Mutual and Cooperative Insurers in Europe)

AMICE is the voice of the mutual and cooperative insurance sector in Europe. The Brussels-based association advocates for appropriate and fair treatment of all mutual and cooperatives insurers in a European Single Market. It also encourages the creation and development of innovative solutions for the benefit of European citizens and society.

Mutual and cooperative insurance follows the principles of solidarity and sustainability and is characterised by customer-membership and a democratic governance. The mutual business model, with its focus on using surpluses for the benefit of its members, is the natural way to provide insurance.

Mutual and cooperative insurers have a market share of more than 30% of the European insurance sector, with more than €420 billion in premiums written and over 410 million policyholders across Europe.