UNIVERSITÀ DEGLI STUDI DI MILANO

Public consultation reference:

Guidelines 9/2022 on personal data breach notification under GDPR

Table of Contents

1 Background

The EU Regulation n. 679/2016 (**GDPR)** introduced the specific requirement for a personal data breach to be notified to the competent national Supervisory Authority (article 33) and, in certain cases, to communicate the breach to the Data Subjects whose personal data have been affected by the violation (article 34).

The European Data Protection Board welcomes comments on the ***Guidelines 09/2022 on personal data breach notification under GDPR*** (**[1]**):

"The targeted update and this public consultation concern paragraph 73 of the Guidelines (marked in yellow in the document). Such comments should be sent ***29th November 2022 at the latest*** *using the provided form.*
Please note that, by submitting your comments, you acknowledge that your comments might be published on the EDPB website. The EDPB Secretariat staff screens all replies provided before publication (only for the purpose of blocking unauthorised submissions, such as spam), after which the replies are made available to the public directly on the EDPB public consultations' page. Unauthorised submissions are immediately deleted. The attached files are not altered in any way by the ***EDPB.*** *Please, note that regardless the option chosen, your contribution may be subject to a request for access to documents under Regulation 1049/2001 on public access to European Parliament, Council and Commission documents. In this case the request will be assessed against the conditions set out in the Regulation and in accordance with applicable data protection rules."* All legal details can be found in our *Specific Privacy Statement (SPS).*

[1] See https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-92022-personal-data-breach_en

2 About the Information Society Law Center (ISLC)

ISLC – Information Society Law Center at the Department "Cesare Beccaria" of the University of Milan is a multidisciplinary research center, founded in 2017 inside the "Cesare Beccaria" Department of Legal Sciences, devoted to the study of the so called "Digital Transformation Law" and the legal, technological, political and social aspects of the Information Society.

The aim of the Center is to conduct research on issues related to the relationship between law and the digital society, with particular attention to those changes – present and future – that will deeply affect our society.

3 About the project

The ISLC called for an internal consultation in order to provide the Commission with valuable input given the importance of the topic addressed in the Guidelines currently in public consultation.

Below are shown the fellows and affiliates from various public and private organizations around the world who contributed to this paper.

- Jose Belo
- Filippo Bianchini
- Pietro Boccaccini
- Chiara Bocchi
- Simone Bonavita (Executive Director of ISLC)
- Alessandro Cortina (PM)
- Massimo Farina
- Flavia Giglio
- Eyup Kun
- Nasiruddin Nezaami
- Livinius Nweke
- Claudia Ogriseg
- Matteo Sironi
- Denizta Toptchiyska

Special thanks are also due to Marco Alagna (external) and Emanuele Brambilla (external) for their collaboration on the project.

4 Comments

4.1 Bureaucratic issues

First of all, from a conceptual point of view, the change proposed in Paragraph 73 clashes with the need to streamline bureaucracy, which has been one of the guiding threads of the reform brought about by the GDPR.

Furthermore, from a substantive point of view, if the Data Controller shall "*where feasible, not later than 72 hours after having become aware of it*" notify the personal data breach to each of the 27 supervisory authorities, could be reasonable to create an EDPB Data Breach Notification Template in order to standardize and simplify the notification procedure to a non-EU Data Controller.

In conclusion, by following the new mechanism proposed by EDPB, there could be a risk that the Data Controllers not established in the European Union may tend to neglect the appointment of representatives as per Article 27 GDPR due to the possible excessive bureaucratic workload to comply with. In a cost-benefit analysis, a non-EU Data Controller EU may be more inclined to run the risk of an (only possible, and in any case appealable) administrative sanction for failure to appoint them rather than having to spend resources on each data breach notification, thus *de facto* weakening the protection mechanism.

It is our opinion that returning to the previous wording of paragraph 73 is desirable in order to avoid the problems mentioned above.

4.2 Organizational issues

The new paragraph 73 may make it quite difficult to meet the 72-hour deadline for the notification to a Supervision Authority (SA). In cases where a non-EU Data Controller has to notify a number of SAs, he has to deal with several practical problems by way of example and not limited to:

i. which Data Subjects were affected by the breach;

ii. their residency;

iii. how to notify each SA (as each SA may have specific procedures to be followed);

iv. which attorney to hire, as it is unlikely that the sole EU representative has sufficient expertise to manage all applicable notification procedures.

Additional organizational problems may arise as it should be clarified whether, in the case under paragraph 73, the notification is due to all SAs or only where the number of Data Subjects affected implies a greater severity of the breach. One of the factors to consider to assess the severity of the breach is, indeed, the number of Data Subjects/records of personal data affected, and such number may be lower in certain jurisdictions.

It would also be useful to clarify whether paragraph 73 must be interpreted as meaning that the notification must be sent to all the authorities of Member States where merely affected Data Subjects reside, or only to the authorities of Member States where Data Subjects whose rights and freedoms are at risk in the meaning of art. 33 GDPR. The specification is very important, as the consistency mechanism provided under art. 60 GDPR is not applicable to cases referred to by paragraph 73. Therefore, it is crucial to understand which authorities should be involved in the process triggered by the breach notification.

A narrower interpretation of paragraph 73 would suggest that the notification has to be directed only to supervisory authorities in the Member States of Data Subjects whose rights and freedoms are put at risk according to the risk assessment imposed by art. 33 GDPR. However, the current formulation of paragraph 73 opens to another possible interpretation. The breach may affect the concerned Data Subjects differently, without putting at risk the rights and freedoms of all of those individuals whose data were impacted by the breach. However, the fact that only a part of these individuals is at risk suffices to trigger the notification under art. 33 GDPR. At the same time, even if the rights and freedoms of some of the concerned individuals are not at risk that does not mean that they are not generally "affected" by the breach, as the expression may indicate an effect caused by the breach not necessarily resulting in a threat to rights and freedoms. Paragraph 73 may thus be read as triggering a notification not only to the authorities of the Member States where individuals at risk reside, but to all the authorities of Member States where individuals that are merely affected by the breach reside. The issue may arise when a certain data breach does not affect all the involved Data Subjects to the same extent. For example, when a disclosure of certain personal data affects more natural persons, the volume and nature of the disclosed personal data may differ for each individual, thus influencing the evaluation of individual risks.

4.3 The problem of the identification and residence of the Data Subjects

Depending on the interpretation chosen, paragraph 73 should also include some additional guidance for the controllers with regard to how to meet this obligation. Paragraph 69 provides guidelines about the case where cross-border breaches inside the EU occur, and the controllers need to identify the lead supervisory authority to which address the notification pursuant to the one-stop-shop system. Paragraph 69 states that "when drafting its breach response plan, a controller must make an assessment as to which supervisory authority is the lead supervisory authority that it will need to notify". Similarly, if paragraph 73 imposes a notification to the authorities of all the Member States where impacted Data Subjects reside, it should also include indications concerning the necessary information to include in the breach response plan (in this case, the Member State where the Data Subjects reside, so that the controllers pursuant to art. 3.2 GDPR may identify the relative authorities). Nevertheless, the guidelines should also address the potential issue deriving from the controllers not being in possession of the information about where the Data Subjects reside. First of all, both art. 33 GDPR and the guidelines do not require the controllers to necessarily have comprehensive information about the Data Subjects and data concerned by the breach, in order to issue the notification. In fact, art. 33.3(a) clearly provide the possibility for an approximation in giving such information to the supervisory authority, and the guidelines. The provision also offers the possibility to provide the information in phases, where necessary (art. 33.4 GDPR). Moreover, as established by art. 11.1 GDPR, the controller must not acquire additional information in order to identify a Data Subject for the only purpose of complying with the Regulation. The provision sets out a restrictive approach applicable to the mentioned scenario, for which the controllers should not collect information about the country where Data Subjects reside for the only purpose of the notification under paragraph 73. A corollary of this consideration is that the guidelines should provide an alternative solution, when the controller has doubts about how many and which authorities need to be notified pursuant to art. 33 GDPR, or how to identify them in the absence of certain Data Subjects' information. In a way similar to paragraph 69, paragraph 73 should indicate the authority that the controller must notify, at the minimum, in these cases.

In another way, summarizing the above, is important to note that the residency of the Data Subjects may be non-necessary data to be collected and processed for most processing activities: but paragraph 73 may

make it necessary to collect the residency of all Data Subjects, in order for the Data Controller to be able to notify all SAs of the country of residence of the Data Subjects affected by a breach. Collecting this data may increase risks for Data Subjects, particularly in light of the fact that such data will be collected by a non-EU Data Controller.

Paragraph 73, therefore, could indirectly lead a Data Controller to always collect the residence of Data Subjects in order to always be able, in the event of a data breach, to correctly identify the relevant SAs to which to report. Such behaviour, however, would also entail possible conflicts with the data minimisation principle 5.1(c)

4.4 The lack of a consistency mechanism for cases falling under paragraph 73

Pursuant to art. 33 and 34 GDPR, the controller has to carry out an assessment about the risk or high risk for rights and freedoms of Data Subjects derived by a breach, and consequently decide whether it has a notification duty. In the case of art. 34 GDPR, the controller may justify its decision not to communicate the breach to individuals on three grounds for exception, in spite of the breach posing a high risk which would require the notification. However, the cooperation and consistency mechanism provided by the GDPR outlines a procedure for the lead authority to efficiently cooperate with other concerned authorities, once the former receives the notification. Therefore, the risk assessment of the controller may be subject by an evaluation of the authorities concerned and potential conflicts between the authorities involved may be solved through the dispute resolution mechanism of the EDPB (art. 65 GDPR). However, the cooperation and consistency mechanism established under the GDPR does not apply to controllers to which paragraph 73 of the guidelines refers, as they do not have an establishment in the EU (Guidelines 8/2022, paragraph 49). To limit the potential fragmentation and inconsistency deriving from the notification having to be addressed to numerous authorities (paragraph 73) and the lack of a clear coordination system between them, the guidelines should provide additional instructions/prescriptions for the controllers on how to interpret articles 33 and 34 GDPR, so that the methods and criteria of non-EU actors concerned by paragraph 73 may be harmonized. Concepts like those of "risk" and "high risk" should be clarified, also considering that risk categories like discrimination and damage to reputation (paragraph 102) may assume a different meaning and extent depending on the national context where the breach occurs. The exception to the notification to individuals based on the

disproportionate effort that the controller should perform could also be further investigated in relation to the situations to which paragraph 73 refers.

4.5 About the example section

This section is very important to ensure that Data Controllers and Data Processors are provided with practical guidance on how to concretely apply the GDPR, even more in case of a data breach when, within a tight deadline, many evaluations and fulfilments have to be complied with More examples will be welcomed, and such examples shall also include an explanation of how to proceed in the case under (new) paragraph 73. Indeed, the steps to be taken by the notifying entity shall be clarified as it is unlikely that the 72-hour deadline is met in case of notifications due in a number of EU countries: the Data Controller may not have a representative in all EU countries were the Data Subjects affected by the breach reside, and it shall be explained how the controller has to proceed from a practical point of view, especially in more complex cases (e.g. where the controller cannot determine the residence of the affected Data Subjects within the 72-hour deadline, or where the controller cannot hire a lawyer in all countries where the breach has to be notified within the 72-hour deadline).

4.6 Additional comments

- Article 33 establishes the conditions under which a Data Controller is obliged to notify a personal data breach to an SA. The notification obligation arises in case of a personal data breach unless it is unlikely to result in a risk to the rights and freedoms of natural persons. In par. 73 of the Guidelines the concept "affected Data Subjects" is used in order to direct the controllers to the national supervisory authorities that have to be notified. In parallel, the concept of "substantially affected Data Subjects" is used in GDPR in the context of defining the "supervisory authority concerned" (art. 4(22)) and it is further clarified in part 1.1.1. of WP29 Guidelines for identifying a controller or processor's lead supervisory authority. It is important to highlight the difference between the two standards "affected" and "substantially affected" Data Subjects in order to be clearer about the competent national authorities to receive notification for a personal data breach.

- Art. 27, par. 2 of GDPR provides some exceptions from the obligation of a Data Controller established outside the EU to appoint a representative in the EU. It should be reflected in the last sentence of par. 73 which at the moment refers only to the cases when there is an appointed representative in the EU.
- It should be clarified whether, in the case under paragraph 73, such documentation shall *(i)* be consistent with any guidelines issued by all SAs (or it is sufficient that it is consistent with the guidelines issued by the SA of the country of the EU representative) and whether the documentation shall *(ii)* be in the language of all the SAs involved (or only in the language of the SA of the country where the EU representative is established).
- Given the tight timeframe under Article 33 of the GDPR, it could be burdensome for the Data Controller and/or for its Representative to provide a Data Breach notification to several SAs. The EDPB, exercising its powers under Article 70.1(a) of the GDPR, might suggest that SAs consider the 72-hour deadline met if satisfied for at least one notification.
- As the European landscape for electronic signature technologies is not yet fully unified, a non-EU Data Controller may have to adopt multiple electronic signature tools to proceed with notifications to different SAs. Creating a single electronic signature technology valid within the EU could facilitate, from an organizational point of view, the notification procedures for a non-EU Data Controller.
- The flow chart section shall take into account also the case under new paragraph 73.

In conclusion, although outside the scope of this consultation, we point out that it would be appropriate to take into account that Paragraphs 135 mention NIS Directive. Since on November 10th the European Parliament has adopted NIS2 draft text, which imposes, inter alia, notification obligations in phases, including an initial notification within 24 hours of becoming aware of certain incidents or cyber threats (instead of simply "without undue delay" as in the NIS Directive) this section of the Guidelines should be amended in order to reflect NIS2 requirements.