Spolek pro ochranu osobních údajů

Comments on the EDPB's draft "Guidelines 9/2022 on personal data breach notification under GDPR"

We welcome the opportunity to present our comments to the recently published EDPB draft of amendment to Guidelines 09/2022 on data breach notification (Guidelines).

General comments

We appreciate the effort of the EDPB to provide opinions and recommendations on the GDPR. We also are aware that the current Guidelines are based on the original WP29 document WP250 rev. 01.

Nevertheless, we note that in our view, even if the EDPB is only amending the original WP29 Guidelines (adopted by the EDPB when the GDPR entered into force), it would be appropriate to carry out a full consultation in the sense of Article 70(4) GDPR on their entire content. The following considerations lead us to this conclusion in particular:

1. There is a difference between the legal position of the WP29 under Article 29 of Directive 95/46/EC and the EDPB, which is a formalised EU body. The position and influence of the EDPB and the Guidelines adopted by it is both de facto and legally (see e.g. Article 65 GDPR) much stronger than it was for the WP29
2. Although a public consultation was carried out by the WP29 when WP250 was adopted, no such consultation was carried out by the EDPB when it was adopted by EDPB
3. The original WP250 was adopted before the GDPR came into force
4. It has been more than 5 years since the adoption of the original WP250 and it would be appropriate for such important documents to seek public opinion on their current impact, taking into account the experience of more than 4 years of application of GDPR.

Specific comments

Point 73 was added to the Guidelines:

However, the mere presence of a representative in a Member State does not trigger the one-stopshop system[36]. For this reason, the breach will need to be notified to every single authority for which affected data subjects reside in their Member State. This notification shall be done in compliance with the mandate given by the controller to its representative and under the responsibility of the controller.

Unfortunately, we believe that the formulation of this point is somewhat simplified and does not sufficiently take into account the practical problems associated with notifying a data breach to multiple supervisory authorities. It should be assumed that there will be cases where notification under paragraph 73 should be made to most or even all national supervisory

Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562

authorities. The solution proposed by the EDPB overlooks a number of practical problems that may arise in individual situations.

It should be stressed that the notification of the data breach to supervisory authorities is not done as an end in itself. It is intended to ensure a high level of protection of data subject's rights and to allow, inter alia, the supervisory authorities to help the controller by providing advice to solve the problem. From this point of view, requiring the controller to notify data breaches to all supervisory authorities, even those with minimal data subjects under their jurisdiction, may even be counterproductive, as it may burden the controller's resources which could otherwise be directed more towards resolving the situation. In addition, there is a risk that, as part of the supervisory authority's consultation activities following the notification of data breaches, the controller will be contacted by multiple supervisory authorities with requests and recommendations that may not be fully compatible. This may then lead to overwhelming the controller or even to the controller not taking certain actions for fear of sanctions from some supervisory authorities.

Further, the risk associated with dealing with non-EU controller, where the actual possibility to sanction them could be in some situations low, cannot be overlooked. The imposition of overly extensive obligations may lead to such controllers preferring not to carry out data breach notifications at all or to adopt a „cherry picking" method, whereby they notify data breaches e.g. only to authorities that usually remain inactive (in a situation where it will be very difficult in practice to determine whether only data subjects from that country have been affected).

We therefore believe that a pragmatic approach based on procedural economy considerations should be adopted, helping the controller to focus on implementing effective measures rather than on formal notification to all concerned authorities in the cases where the real relevance of such a notification for the protection of data subjects' rights will be minimal.

From this point of view, we would like to propose to consider, for example, the following modifications:

1. Recommend that the controller indicate in the notification to which supervisory authorities the controller plans to notify the data breach and which supervisory authorities should be considered as the most significantly affected.
2. Emphasise that compliance with the 72-hour notification period is particularly important for those supervisory authorities where the largest number of data subjects (either in absolute numbers or, where appropriate, as a percentage of the population of the Member State concerned) are affected. Here, it should be taken into account that determining from which Member States the data subjects concerned come may be quite complicated, and may significantly burden the controller's resources which could be used more efficiently to address the substance of the data breach itself.
3. Allow the controller (or tolerate such a step) to make notifications to supervisory authorities that are unlikely to have serious effects in their Member State, in the English language first and possibly only subsequently in the language of the Member State concerned. In our experience, the language barrier of notifying a data breach in another language or even finding out how the notification is to be made can put a significantly burden the resources of smaller controllers in particular.
4. In our view, Articles 60 et seq. of the GDPR allow for the establishment of relatively close cooperation between supervisory authorities even in the case of data breach notifications by non-EU-based controllers. If the EDPB were to indicate in the Guidelines how such cooperation would take place or recommend steps to support it, this would allow affected

Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562

controllers to better and more quickly notify data breaches to those authorities for whom the notification will actually be relevant.

We are grateful for the opportunity to provide our comments on the draft Guidelines. However, we believe there is considerable room for review of the suggested approach towards the fines setting process for the benefit of the data subjects and motivation of responsible behaviour of the organisations.

Prague, 29.11.2022

JUDr. Vladan Rámiš, Ph.D., Chairman of the Committee
Alice Selby, LLM, Ph.D., CIPP/E, CIPM, Member of the Committee
JUDr. Ing. Jindřich Kalíšek
Spolek pro ochranu osobních údajů

Spolek pro ochranu osobních údajů / Data Protection Association
with its registered seat Hellichova 458/1, Malá Strana, 118 00 Praha 1 / Prague 1,
registration with public register: Municipal Court in Prague, file No. L 61299
Business ID No.: 03493679, e-mail: spolek@ochranaudaju.cz, tel.: 296210562