Dear EDPB,

We wish to address part of the additional wording added in the new paragraph 73 of the proposed amendments to Guidelines 9/2022 on personal data breach notification under GDPR (the "Guidelines").

The wording of the relevant paragraph (the "Paragraph") is set out below:

- 73. However, the mere presence of a representative in a Member State does not trigger the one-stop shop system. 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. *(emphasis added)*

As a provider of the Article 27 Representative service, we are confused and concerned by the proposed addition of the underlined part of the Paragraph. Nowhere in GDPR, nor in any subsequent guidelines which we are aware of, is there a suggestion that the Representative is required to be involved in the notification of a data breach to an EU data protection authority – in fact, we believe the previous guidance of the EDPB makes such a declaration incompatible with the Representative's role.

Our reading of the GDPR – in line with the final words of the Paragraph – is that this duty sits with the data controller. Such duties are often performed within the remit of their Data Protection Officer ("DPO"), whose closeness to the data controller and familiarity with their data processing activities would enable them to do so in a reliable and effective manner, but the role of Representative under Article 27 is necessarily one which is at a distance from their data controller client – the Representative will always be in the EU; their client always outside it. This distance makes it harder for the Representative to provide an effective notification to the authorities, and certainly precludes their responding to any query subsequently raised by that authority (other than to acknowledge it and pass it to their client to provide a formal response – likely from their DPO).

The EDPB has fortunately already address the extent of the role of the Representative in your previous guidelines 03/2018, which make it clear that the Representative should not also provide the services of the DPO to the same client. With that being the case, the wording in the Paragraph appears to contradict those earlier guidelines, as it would cause the Representative to stray into an area which only the DPO is sufficiently qualified to deliver (or – where no DPO is required by GDPR - such other person at the data controller as is sufficiently knowledgeable about their data processing activities to do so).

The Article 27 Representative is not a role which is anticipated to have a detailed knowledge of the activities of its clients – although they will have the benefit of the maintained copy of their clients' Article 30 record of processing activities, they are unlikely to be able to provide significant updates to it without those updates being provided in detail by their clients. The role of the Representative is that of a European outpost of their clients, to which those in the EU may raise their concerns, and which will act as the mouthpiece of their clients within the Union – they reiterate the statements of their clients, they do not form those statements themselves. As a result, placing them as the party which is expected to make the notifications for non-EU data controllers (or even implying that should be the case) adds a significant risk of there being an inadequate or incomplete breach notification, which places the rights and freedoms of affected data subjects at further risk than has already arisen under the breach which gave rise to the notification.

It is also worth noting that, strictly interpreted, GDPR does not require the Representative to be established in all of the EU Member States where such a notification may be required; as noted in the Paragraph: "*the breach will need to be notified to every single authority for which affected data subjects reside in their Member State*". This further increases the risk of an inadequate or incomplete notification being made – for example, a Representative based in Estonia may not be familiar with the specific notification requirements of the data protection authority in Romania. Although the guidelines 03/2018 clarify the basic wording of GDPR Article 27(3) by stating that "the representative must remain easily accessible for data subjects in Member States where it is not established", which we have interpreted to mean that the Representative should be established – if not in all of the Member States where the data subject is based – at least in an adjacent Member State or one which is not overly distant from those Member States in which the data subjects are based, this is not an interpretation widely accepted by all providers of the Representative service, many of which operate from a single location in the EU in line with a strict interpretation of GDPR Article 27(3) ("The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.", *emphasis added*), there not being completely-clear guidance that this would fail to meet the EDPB's expectations regarding establishment of the Representative.

That isn't to say it should be impossible for a Representative to be involved in the notification process, where they are able to do so (a) without intruding on the domain of the DPO, and (b) competently in all the relevant jurisdictions where that notification is required, but we strongly believe – based on the wording of GDPR and the currently-issued guidelines of the EDPB – that this should not be an obligation placed or implied upon the Representative, except where specifically agreed with their data controller client.

Accordingly, we propose an adjustment to the Paragraph, so that it would read:

- 73. However, the mere presence of a representative in a Member State does not trigger the one-stop shop system. 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 the responsibility of the controller.

We would be happy to enter into further discussion on this point, if it would assist the feedback process.

Kind regards,

DataRep

(Data Protection Representative Limited (trading as DataRep), an Irish company incorporated under number 616588)