To:
European Data Protection Board (EDPB)
Postal address: Rue Wiertz 60, B-1047 Brussels
Office address: Rue Montoyer 30, B-1000 Brussels

Subject: Comments on the targeted update made on Guidelines 09/2022 on personal data breach notification under GDPR concerning paragraph 73

Dear Sir or Madam,

We, Telekom Austria AG would like to hereby express our appreciation to your work and the proposed changes to the Guidelines 09/2022 on personal data breach notification under GDPR. We understand that the EDPB as an independent European body, constantly contributes to the consistent application of data protection rules throughout the European Union and it has been our great pleasure to review the proposed changes to the Guidelines 09/2022 on personal data breach notification under GDPR and to provide our feedback.

It is our sincere hope that you will review and take into account our comments given below. We remain available for further clarification or discussion in regards to the feedback given.

On behalf of Telekom Austria AG,

Leschanz Judith, Data Protection Officer
M: +43 664 66 27986
T: +43 50 664 27986
E-mail: Judith.Leschanz@a1.at

Juris Doctor, Daniel Sanchez Cordero Canela
M: +43 664 66 34314
T: +43 50 664 34314
F: +43 50 664 9 34314
E-mail: daniel.sanchez@A1.group

Comment no. 1 – The proposed change introduces different application of the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR") for non-EU versus EU establishments,

i. **without any added value for the protection of personal data of the data subjects; and**
ii. **contrary to the spirit of GDPR and especially Article 3 (2) of the GDPR, as GDPR clearly:**
    a. **intends to be applicable with the same effect for non-EU establishments when they process personal data of EU data subjects as EU establishments; and**
    b. **has no intention of treating differently EU vs non-EU establishments.**

With great appreciation for the proposed changes, our opinion is that the proposed change provides different treatment of non-EU establishments compared to EU establishments, by adding more obligations for non-EU establishments, but also for supervisory authorities and by excluding the application of the one-stop-shop system for non-EU establishments. However, the proposed changes does not show or guarantee real benefit or improved position for the data subjects/supervisory authority.

It can also be interpreted that this scenario is not in accordance with the spirit of the GDPR, namely Article 56 and 60 in relation to Article 3(2) and it interferes with the goal that the GDPR wishes to achieve. If we take into account that GDPR is applicable also to non-EU establishments via the territorial application of Article 3(2) of the GDPR, and then we add to this the fact that Article 56 and 60 introduce the: (i) lead supervisory authority as competent to act for the cross-border processing activities; and (ii) cooperation of the lead supervisory authority with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus; then we can conclude that the proposed change will introduce situation where more supervisory authorities in European Union will lead procedure for the same data breach, with a possibility of different outcome in the countries, which is not the idea behind the Chapter 7 of the GDPR.

When the Guidelines for identifying a controller or processor's lead supervision authority (adopted on 13 December 2016, last revised on 5 April 2017) describes the manner of determination of the lead authority based on the main establishment, it is clear that "***The essence of the lead authority principle in the GDPR is that the supervision of cross-border processing should be led by only one supervisory authority in the EU***. In cases where decisions relating to different cross-border processing activities are taken within the EU central administration, ***there will be a single lead supervisory authority for the various data processing activities carried out by the multinational company."*** This would clearly mean that idea behind GDPR is to have unified approach towards data breach notification (concerning the same data breach) in the European Union therefore; the proposed change for non-EU establishments is not easy to be understood or justified.

In addition to this, having in mind the capacities of non-EU establishments and their struggle to align with GDPR and the obligations arising thereof, it brings another question. Namely, what will this mean for non-EU establishments in practice, viewed from a practical and formal point of view? This would impose many obligations within the short deadline of 72 hours, i.e. to investigate the facts behind the data breach, to prepare and to submit the notification to more than one

supervisory authority in the European Union. Given that this is hard to be fulfilled by non-EU establishments, it is our fear that this will lead to non-compliance with the GDPR due to mere impossibility to do so, lack of practice in determination and preparation of notifications for data breach, therefore it would only take non-EU establishments far from GDPR application, rather than bringing them closer and assuring personal data protection of EU data subjects.

Comment no. 2 - The proposed change introduces insecurity in the overall obligation for appointing representative under Article 27 of GDPR

The proposed sentence in paragraph 73 of the Guidelines 09/2022 on personal data breach notification under GDPR: "*This notification shall be done in compliance with the mandate given by the controller to its representative and under the responsibility of the controller*" introduce insecurity in the overall obligation for appointing representative under Article 27 of GDPR.

If we take into account that Article 27 (3) and (4) of the GDPR regulate that:

> "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.
>
> The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation."

It is clear that the GDPR has the intention to facilitate its application for non-EU establishments by allowing them to have one representative that will be mandated to address supervisory authorities and data subjects on all issues related to processing, for the purposes of ensuring compliance with this Regulation. Therefore, the previous solution in the Guidelines on Personal Data Breach Notification under Regulation 2016/679, adopted on 3 October 2017 (last revised 6 February 2018) makes more sense in the overall application of GDPR and it is aligned with the intention of the GDPR in this regard.

The proposed changes introduces insecurities in terms of opening many questions, including but not limited to:

- is it now an obligation to have more than one representative in the EU, in order for the representative to be able to submit the notification before the different authorities within the short deadline for data breach notification, or
- should the one appointed representative in the one EU country be expected to communicate with different supervisory authorities in different countries and to submit data breach notifications in such countries, especially if larger number of authorities are concerned?

In this view, it seems that this obligation is in direct contradiction with the clear focus and direction of Article 27 of the GDPR.

As a conclusion, we propose not proceeding forward with the proposed changes concerning paragraph 73 of the Guidelines 09/2022 on personal data breach notification under GDPR.