veriff

.

# Comment on the EDPB's Guidelines 9/2022 on Personal Data Breach Notification under the GDPR

PREPARED BY

Veriff's DPO Office

legal@veriff.com

PREPARED DATE

Nov 25, 2022

# About Veriff

1. Veriff is the industry leader in online identity verification, helping businesses achieve greater levels of trust and making the internet a better place for everyone. Our intelligent decision engine analyzes thousands of technological and behavioral variables linked to government IDs from over 190 countries. Founded in 2015, Veriff serves a global portfolio of organizations across the fintech, crypto, and mobility sectors. With offices in the United States, United Kingdom, Spain and Estonia, and 550 people from 60 different nationalities, every day we're dedicated to helping businesses and individuals build a more secure online world.

# Summary

2. Veriff does not support the amendment in paragraph 73 of the Guidelines 9/2022 on Personal Data Breach Notification under GDPR. Veriff is of the opinion that the amendment does not improve the protection of data subjects' rights. On the contrary, the amendment:
    i. increases costs for data controllers, demotivating companies from appointing a representative and reducing the number of foreign companies interested in directing business to member states with smaller markets;
    ii. creates extra administrative burden to supervisory authorities, making supervisory authority's response times longer; and
    iii. creates inequality between data subjects from different member states as member states have different practices around breach management.

# Background

3. On May 25, 2018, EDPB endorsed WP29 Guidelines on Data Breach Notification, which stated that when a controller is not established in the European Union and the controller experiences a data breach, then the controller is recommended to notify

the supervisory authority of a country where controller's representative is established. On October 18, 2022, EDPB published a renewed Guidelines 9/2022 on Personal Data Breach Notification under GDPR which drops a single contact point to notify a data breach and suggests that controllers established outside of the European Union should notify every member state where data subjects affected by the breach reside.

# Analysis

4. Firstly, the proposed amendment will bring additional costs to companies established outside of the European Union. Compliance with GDPR requires labor, and monetary and technological resources. Companies established outside of the European Union must commit resources to familiarize themselves with the data protection rules applicable in the European Union, establish organizational and technical solutions to fulfill obligations arising from the GDPR and contract a representative to guarantee protection of data subjects' rights and cooperation with the supervisory authority.

5. Each member state has their own supervisory authority, their own breach notification form and notification process specifics. Most member states have their own unique national language. Currently, companies need to know one singular breach notification form and a representative has to speak the language of that one specific country, regardless of the number of member states the company directs its business to. The proposed amendment requires that companies established outside of the European Union directing business to all countries where GDPR applies must now be prepared to notify 30 different supervisory authorities using 30 different notification forms in 26 different languages, all within 72 hours.

6. To be able to submit the notification in time, companies will need to allocate additional resources to contract outside counsels to familiarize themselves with notification specifics of different countries and required content of notification forms of all countries where GDPR applies. In case of a union-wide breach, companies will need to carry additional costs to translate relevant information and any following

communication with the supervisory authorities to 26 different languages and a representative must keep track of potentially 30 parallel proceedings. This requires excessively more country specific knowledge, language skills and working hours from a representative than notification obligation to one supervisory authority and brings enormous costs to maintain a representative's team. Therefore, the amendment significantly increases the costs of companies established outside of the European Union.

7. The increased costs will have two main consequences.

    I. Some companies may no longer appoint a representative. It is difficult for the European Union to enforce any of its policies and fines outside of the European Union. For this reason, the institution of a representative was created. Companies' motivation to appoint a representative is related to benefits it brings and the costs related to it. There are limited benefits to appointing a representative. With the amendment, the costs of maintaining a representative will increase significantly, making the appointment of a representative costly. With considerable costs related to maintaining a representative's team and little to lose from not appointing a representative, companies will have less motivation to appoint one. This will leave data subjects' rights unprotected and GDPR unenforceable upon these companies.

    II. Also the number of foreign companies interested in directing their business to member states with smaller markets may decrease. If a company is committed to compliance and present in all 30 countries where GDPR applies, it now has to appoint a representative who is capable of submitting the breach notification and communicating with a supervisory authority in 30 countries. This cannot be achieved by appointing one person. It is more likely achievable by contracting an international team of representatives. Considering the increase of the competences that are now required from the representative, it will cost significantly more to maintain the representative's team than before. The seven smallest countries by population make up around 1% of the overall

market of the countries where GDPR applies, while the seven biggest countries make up around 73% of the market. The 1% of the market just will not be worth the costs it takes for small- and medium-sized companies established outside of the European Union to maintain representative team's competence in the smallest countries.

8. Secondly, the proposed amendment will increase the workload of supervisory authorities, which will slow down their daily operations. In EDPB's report, 87% of supervisory authorities stated that they do not have enough human resources to carry out their activities.[1] Currently, in case a company established outside of the European Union suffers a breach, only one supervisory authority works with the notification. Parallel breach notifications to several supervisory authorities mean more work to all supervisory authorities and this will manifest itself in longer response times due to lack of human resources. This hinders their ability to guarantee the efficient protection of data subjects and will slow down cooperation between companies and supervisory authorities that is aimed at guaranteeing a good level of protection to data subjects' rights.

9. Veriff predicts that the increased workload of supervisory authorities will increase the number of supervisory authorities requiring a fee for their services. ICO has applied a fee for registering a company as a data controller. In the referred EDPB report, 77% of supervisory authorities stated that they do not have sufficient budget to carry out their activities.[2] As a solution to this problem, it is likely that more supervisory authorities will impose fees for their services. If additional fees are implemented, it will also increase the costs of companies established in the European Union.

10. Thirdly, the proposed amendment will contradict the aim of harmonized protection of fundamental rights within the European Union. The aim of the GDPR is to provide the

[1] EDPB Overview on resources made available by Member States to the Data Protection Supervisory Authorities. Available online: https://edpb.europa.eu/system/files/2022-09/edpb_overviewresourcesmade_availablebymemberstatestosas2022_en.pdf.
[2] See reference 1.

same standard of protection to data subjects regardless of their nationality and place of residence. For this reason, a regulation was adopted as opposed to an amended data protection directive. Currently, in case of a data breach with data subjects impacted in different member states, the case will be processed by a single supervisory authority guaranteeing the same outcome to all data subjects. With the proposed amendment, if the controller is not established in the European Union, there will be parallel proceedings. In parallel proceedings supervisory authorities may evaluate the risk to data subjects differently, yet outcome to data subjects should not depend on which member state they reside in. The contradictory decisions will create inequality between data subjects undermining the very aim of the GDPR.

11. The protection of data subjects' rights will further be undermined by the additional time it takes to get notification submitted in several member states. A controller is obliged to notify a breach without undue delay. As explained before, the proposed amendment requires companies to submit the notification to up to 30 different supervisory authorities in 30 different forms and 26 languages compared to the current one form, one supervisory authority and one language. It takes time to fill all the forms, translate necessary parts and submit them. Thus, the proposed amendment will slow down the notification process and be the source of delay, creating even more obstacles to efficiently protect data subjects' rights.

# Final notes

12. Veriff is grateful for the opportunity to provide comments and practical feedback on the EDPB's Guidelines on Personal Data Breach Notification under the GDPR. If you would like to discuss more on the provided comments or require additional information, feel free to contact Veriff's DPO Office via legal@veriff.com.