

PrivacyRules Global Alliance

Feedback to Guidelines 9/2022 on personal data breach notification under GDPR

 SHAKESPEARE
MARTINEAU

IWATA GODO
Established 1902

TIMELEX

PEARL COHEN

 D'LIGHT
D'LIGHT Law Group

Matouk
Bassiouny
& Hennawy

Tanner
DeWitt
solicitors


RP Legal & Tax

 Frost
Brown Todd LLC
ATTORNEYS

Background

About PrivacyRules

PrivacyRules was formed in 2017 by a group of legal and tech experts across Europe and America (<https://www.privacyrules.com/>) to address the growing demand for data protection and cybersecurity services. Launched in 2018, PrivacyRules is the world's only leading professional alliance of data privacy experts from the legal, tech and crisis communication disciplines. We formed this alliance to provide integrated and effective assistance and services to multinational companies and institutions.

In our early age of only four years we have grown dramatically, now with members in more than 60 jurisdictions worldwide and a number of tech, cybersecurity and crisis communication companies within the alliance or cooperating with us. With our members we offer unique services combining legal, technical and public relations advice to avail multinational clients of implementable and holistic data privacy solutions nationally and in all continents.

In addition to organising webinars, podcasts, in person conferences and e-conferences, PrivacyRules disseminates independent information on data privacy matters via all its platforms. In this way, our alliance contributes to the global awareness about privacy and is an active contributor to the international dialogue on data protection and cybersecurity. PrivacyRules regularly meets institutional interlocutors, at national and international level.

To find out more about us, please visit our [website](#) or follow us on [LinkedIn](#).

About this document

PrivacyRules recognises the fundamental role of the European Data Protection Board (hereinafter as EDPB) for the consistent application of data protection rules throughout the European Union (hereinafter as EU), for the cooperation between the EU's Data Protection Authorities, and for its relevance at international level since the EU data privacy interpretation and application has impact at global level.

Further to the EDPB European Data Protection Board Guidelines 9/2022 on personal data breach notification under GDPR (hereafter "the Guidelines"), our members are therefore pleased to provide the below feedback structured on the following high-level issues:

1. Brief description of the high-level issue of the Guidelines or Use Cases being commented on
2. Comment/feedback to the high-level issue
3. Proposed mitigation/solution/change to the issue

We are therefore pleased to submit this feedback with the aim of bringing to the EDPB's attention, for its consideration, not only observations on the Recommendations from EU legal practitioners, but also the ones issued by data privacy legal and technical experts from outside the EU.

This brief introduction of the given feedback has been developed by Geert Somers, Chair of the PrivacyRules European Committee and Partner at [Timelex](#), a niche law firm matching law and innovation.

Executive Summary

The concerns from the members of PrivacyRules relate to the fact that the draft Guidelines 9/2022 foresee that the mere presence of a representative does not trigger the one-stop-shop system, as such deviating from the previous guidelines WP250rev.01 on data breaches adopted by the Working Party. As a result, controllers without any establishment in the EU would now have to notify the breach to the local supervisory authorities in every Member State they are active in and where data subjects are affected, through their EU representative. The main concerns of PrivacyRules members can be summarised as follows:

1. The Draft Guidelines 9/2022 create an unnecessary administrative burden on non-EU establishments:

The general opinion is that the draft Guidelines 9/2022 create an unnecessary administrative burden on non-EU establishments, because:

- Non-EU established controllers will potentially be required to notify up to 40 data protection authorities, across 27 EU Member States, after identifying the affected data subjects and in which countries the data subjects reside;
- As there is no standardized breach form, the notification procedure will require the completion of multiple notification forms, mechanisms and languages unique to each authority;
- The notification procedure will have to be completed within the timeframe of 72 hours. Some members have the opinion that the obligation to notify within 72 hours is unfeasible.

As a result, some members fear that the draft Guidelines 9/2022 may:

- Discourage non-EU undertakings, especially small and medium-sized enterprises from doing business in the EU, as it causes a significant difference between EU establishments and non-EU establishments, even when they have appointed an EU representative;
- Create an opposite effect where, instead of greater cooperation, non-EU companies are disincentivized to report breaches due to it being excessively time consuming to report in every relevant EU Member State.

2. The Draft Guidelines 9/2022 cause legal uncertainty:

The general opinion is that the draft Guidelines create legal uncertainty about:

- The criteria to be met by non-EU controllers and processors to benefit from the one-stop-shop system;
- The interpretation of Recital 10 of the GDPR.

PrivacyRules members' comments on the EDPB Guidelines 09/2022

- EDPB Guidelines 9/2022 on personal data breach notification under GDPR

Member	Description of the high-level issue of the Guidelines or Use Cases being commented on	Comment/Feedback to the high-level issue	Proposed mitigation/solution/change to the issue
TIMELEX Timelex (BELGIUM)	Draft Guidelines 9/2022 aim to clarify the territorial scope of data breach obligations under the GDPR, i.e. in case of a breach at a controller or processor established outside the EU. According to the draft Guidelines 9/2022, when a non-EU controller or processor has a designated representative in the EU, its mere presence does not trigger the one-stop-shop system so that the breach will need to be notified to every single authority for which affected data subjects reside in their Member State. According to the draft Guidelines, this notification shall be done in compliance with the mandate given by the controller to its representative and under the responsibility of the controller.	It is stated in the draft Guidelines 9/2022 that the mere presence of a representative does not trigger the one-stop-shop system, as such deviating from the previous guidelines on data breaches adopted by the Working Party. Controllers without any establishment in the EU would now have to notify the breach to the local supervisory authorities in every Member State they are active in and where data subjects are affected, through their EU representative. In other words, the controller or processor established outside the EU can no longer make the notification just to the supervisory authority in the Member State where its EU representative is established. This situation creates: • Uncertainty about the criteria to be met by non-EU controllers and processors to benefit from the one-stop-shop system, • A significant difference between EU establishments and non-EU establishments, even when they have appointed an EU representative, and • An administrative burden on non-EU establishments.	There may be multiple ways to mitigate the negative consequences of the new regime on non-EU establishments. The first proposed solution is to revert Guidelines 9/2022 to the previous version (WP250rev.01) and to amend accordingly the WP29 Guidelines for identifying a controller or processor's lead supervisory authority (WP 244 rev.01) in order to achieve coherence between the two Guidelines. The second proposed solution is to mitigate the negative consequences of the new regime, especially regarding the administrative burden of notifying multiple national authorities. For example, a special simplified notification procedure for non-EU establishments can be developed. This way, these establishments can inform multiple national authorities of the data breach through a single notification process and deal with local supervisory authorities more easily. This would not only be in the interest of these controllers/processors, but also in the interest of national authorities (in terms of workload) and data subjects (to achieve a quick and efficient reaction in case of data breach).

 RP Legal & Tax RP Legal & Tax (ITALY)	The update to Guidelines 9/2022 aims to introduce more onerous personal data breach notification obligations on data controllers who are not established in the EU, but who are still subject to the GDPR according to art 3.2 GDPR. These controllers - who do not benefit from the one-stop-shop system provided for EU companies- shall be required to notify "every single authority for which affected data subjects reside in their Member State."	First of all, to be able to identify all the competent supervisory Authorities, the controller should be aware of who are the data subjects affected by the data breach and, even more difficult, to identify in which countries these data subject reside. Secondly, as of today there is not a standardized breach notification form to be used by the controller across all EU member States; on the contrary, each authority has its own reporting form and most of the forms have different formal and linguistic requirements. Taking in consideration these two aspects, it is clear that such update to the guidelines 9/2022 would lead to a slowdown in the data breach notification process and, thus, it is hard to imagine how a non-EU company could actually be able to complete different notification forms within only 72 hours. All this would undermine the timeliness of the notification procedure or, even worse, disincentivize the non-EU controllers to proceed with such notification, given the excessive onerousness of the procedure.	The new paragraph 73 of the Guidelines 9/2022 should be deleted and the current solution should remain in force. With the current solution remaining implemented, in fact, both the identification of the competent authority to which notifying the data breach and the data breach notification process itself would be easier and faster to manage, so that it would be more likely that non-EU-based controllers would notify within the time limits provided by the GDPR.
 Shakespeare Martineau (UK)	The original Guidelines on Personal Data Breach Notification were prepared by the Article 29 Working Party. The EDPB adopted these when it was established in 2018 and soon revised them, introducing the requirement that processors notify controllers of breaches without undue delay instead of deeming the controller to be aware of the breach as soon as the processor discovered it (which was unrealistic and impractical), and also introducing the sensible requirement that non-EU controllers only need notify breaches in the EU member state where their EU representative was situated. The recent EDPB proposal seeks to reverse this pragmatic solution, so the new Guidelines will say: "However, the mere presence of a representative in a Member State does not trigger the one-stop-shop system.	The proposed change will be impractical and burdensome. There is no one standardised form used by the various supervisory authorities so companies will need to find, complete and translate numerous differing forms, leading to potential inconsistencies in the various reports, which will be unhelpful when the breach is analysed by the authorities. Resources will be diverted to completing the differing complex forms at a time when the focus of the business and its relevant personnel should be on investigating and stemming or rectifying the causes of the breach and mitigating the effects on data subjects. In practice, in the case of a breach affecting multiple jurisdictions, it will not be possible to complete the multiple submissions within the required 72 hour period. Companies will take time to carry out the often difficult task of establishing where affected data subjects reside and then wait until all forms have been completed consistently, based on the latest knowledge of the facts, and then translated, before submitting the forms, so in practice all the submissions will be delayed potentially beyond the 72 hour deadline.	The Guidelines should remain unchanged. This will not remove the existing need to notify both the ICO under the UK GDPR as well as the relevant EU supervisory authority, but this is far more workable than potentially having to notify multiple EU supervisory authorities. The change seems to be being proposed for pedantic reasons related to whether the appointment of a representative triggers the one-stop shop arrangement, and overlooks the fact that there is no evidence that the existing guidelines have led to breaches being under- or inadequately reported in practice.

 Shakespeare Martineau (UK)	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."	An unintended consequence of the proposal will be that companies will be tempted not to report breaches which should have been because of the bureaucratic, resource intensive and burdensome effort involved. They will be more inclined to convince themselves that the breach is low risk and does not require reporting. Furthermore, non-EU companies which would have dutifully appointed a GDPR representative because of the one stop shop advantages of breach reporting may, if this advantage is removed, be inclined to conclude that it is better to run the risk of breaching the Article 27 requirements rather than going to the trouble and expense of appointing a representative and perhaps making it easier for data subjects to complain and for a supervisory authority to take action against them.	
 Frost Brown Todd (USA)	The key change in the updated version consists in paragraph 73 and regards "breaches at non-EU establishments". Contrary to the provision for companies established in the EU, non-EU established companies shall notify the supervisory authorities in each and every EU member state where data subjects are impacted.	The new guidelines will place a substantial burden on U.S. companies without an EU establishment to comply with the guidelines, given the short notice deadlines. The burden will fall heavily on small-medium size U.S. companies with EU customers without a sophisticated understanding of the GDPR.	U.S. companies that collect personal information are required to provide notices to all states in which there is an individual who was or may have been a subject of a data breach. Therefore, data mapping of the customer's location (i.e., the state) is part of the data breach compliance process. U.S. companies without subsidiaries established in the EU should extend their data mapping process to identify where their EU customers are located. U.S. companies who are controllers should also review their data processing agreements to ensure that the processor will notify the data breach with ample time for the controller company to report the data breach to the proper data protection authorities.

 Matouk Bassiouny & Hennawy (EGYPT)	The key change in the updated version consists in paragraph 73 and regards "breaches at non-EU establishments". Contrary to the provision for companies established in the EU, non-EU established companies shall notify the supervisory authorities in each and every EU member state where data subjects are impacted.	From a policy perspective this would increase data protections for data subjects, as breaches would now be more widely reported, and this would theoretically increase data protection coordination between different European countries. However, this would be somewhat impractical especially for non-European countries, Egyptian law at the moment only requires for Egyptian companies to notify the authorities in Egypt of such data breaches. In dealing with European nations, Egyptian companies would find it time-consuming and impractical to issue notifications of data breaches to the data protection authorities of every EU member state where data subjects are impacted. This may create an opposite effect where, instead of greater cooperation, non-EU and non-European companies are disincentivized to report breaches due to it being excessively time consuming to report to every relevant EU member state.	Reporting breaches should be limited to the most relevant GDPR supervisory authorities. In cases where a data breach occurs in interactions between European and non-European countries, breach reports should be made to the authorities of the countries in which the relevant companies are headquartered. For example, should a data processing agreement be implemented between three companies, one located in Egypt and the other two located in France and Britain, breach reports should be made to the relevant data protection authorities in those three countries. This would maintain cooperation and coordination, but limit the scope of notification to be more practical.
PEARL COHEN Pearl Cohen (ISRAEL)	The 2018 version of the guidelines (WP250rev.01) stated that where a controller is not established in the EU, "WP29 recommends that notification should be made to the supervisory authority in the Member State where the controller's representative in the EU is established". The proposed update to the guidelines would change this radically, such that "the breach will need to be notified to every single authority for which affected data subjects reside in their Member State"	The duty to notify the competent data protection authority of a personal data breach arises from Article 33(1), which states that such notification shall be made "to the supervisory authority competent in accordance with Article 55". As explained in detail below, proper interpretation of this phrase warrants that it be construed beyond its plain literal meaning, such that controllers established outside the EU be required to notify a personal data breach to the supervisory authority in the territory where that controller's EU representative resides. The need for more than a literal interpretation of this phrase is exemplified by the scenario of a "cross-border processing" within the EU. Paragraph 69 of the EDPB's guidelines rightfully recognizes that in case of such EU cross-border processing, "the controller will need to notify the lead supervisory authority". The EDPB's guidelines recognize this practical approach even though the plain literal meaning of Article 33(1) refers to the supervisory authority competent in accordance with Article 55, which in turn states that "Each supervisory authority" is competent to act. Moreover, Article 56, which governs the concept of "lead supervisory authority" expressly states that it is "without prejudice to Article 55".	The text of the 2018 version of the guidelines (WP250rev.01) should remain unchanged regarding the notification of personal data breaches by a controller not established in the EU. Paragraph 73 in the proposed update to the guidelines should be rescinded.

PEARL COHEN

**Pearl Cohen
(ISRAEL)**

Indeed, even though a literal reading of Articles 33(1), 55(1) and 56 warrants that a personal data breach in case of a "cross-border processing" within the EU be notified to each supervisory authority where the impacted data subjects reside, the EDPB has rightfully construed this beyond the literal text, to accomplish the more sensible, workable and proper result that achieves the overarching purposes of the GDPR. And this is precisely what the EDPB properly did when it endorsed the 2018 version of these guidelines, which "recommends that notification should be made to the supervisory authority in the Member State where the controller's representative in the EU is established".

The existing recommendation to have a single-notification authority has been in place for nearly five years, and has proven to be proper, workable, and equitable. Introducing a radical amendment to this recommendation at this time, as the EDPB now proposes, warrants considerable outweighing reasoning, none of which was offered by the EDPB and none is likely to exist.

Finally, the proposed update to the guidelines implicates significantly adverse consequences, which themselves dissuade from adopting the EDPB's proposed update:

1. Non-EU established controllers will potentially be required to notify upwards of 40 data protection authorities, across 27 EU member states (taking into account Germany's 16 Länder-specific authorities), using multiple notification forms, mechanisms and languages unique to each authority, all within the timescale of 72 hours. By imposing this requirement, the EDPB is almost intentionally designing a mechanism that is virtually guaranteed to render all non-EU established controllers that suffer a notifiable personal data breach, infringers of the GDPR.
2. The resulting unworkable burden creates a chilling effect from doing business in the EU, distinctively against non-EU established controllers. It establishes a blatantly unlevel playing field for non-EU established controllers, compared to EU-established controllers.

		3.The notification of a personal data breach to a myriad of member states' data protection authorities sets a scene that marveously contravenes Recital 10 of the GDPR, which states that "Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union".	
 Tanner De Witt (HONG KONG)	Aligned with the comment expressed by the Israeli expert as per above.	Aligned with the comment expressed by the Israeli expert as per above.	Aligned with the comment expressed by the Israeli expert as per above.
 D'LIGHT Law Group (SOUTH KOREA)	Aligned with the comment expressed by the Israeli expert as per above.	Aligned with the comment expressed by the Israeli expert as per above.	Aligned with the comment expressed by the Israeli expert as per above.
 Iwata Godo (JAPAN)	The key change in the updated version consists in paragraph 73 and regards "breaches at non-EU establishments". Contrary to the provision for companies established in the EU, non-EU established companies shall notify the supervisory authorities in each and every EU member state where data subjects are impacted.	Although Japan has obtained adequacy decision from the EU, extra-territorial application of the GDPR would apply to non-EU establishment in Japan, if it processes EU personal data in conjunction with its provision of services or goods to the EU member state. In case of the extra-territorial application of the GDPR and where data breach would occur, such non-EU establishment (in Japan) must notify to DPA at each of the member state. This exercise can be done by the representative appointed, but very cumbersome (sometimes the data subject may move among the member state and sometimes hard to designate the data subject in a specific EU member state).	If the member state where EU representative is appointed would serve as lead supervisory authority for the purpose of notification to the DPA in the EU, this would reduce the time and cost for notification. It is unbalance that the establishment in the EU are able to use the lead supervisory authority system. As the non-EU establishment must appoint EU representative in one of the EU member state, to use such member state as lead supervisory authority would be a simple solution and would make rationale for the duty to appoint the EU representative (and not in every EU member states where data subjects are located.).

Contributing PrivacyRules members

BELGIUM: TIMELEX ATTORNEYS

GEERT SOMERS:
GEERT.SOMERS@TIMELEX.EU

TIMELEX

ITALY: RP LEGAL & TAX
ATTORNEYS

CHIARA AGOSTINI:
CHIARA.AGOSTINI@REPLEGAL.IT



UK: SHAKESPEARE MARTINEAU
LLP

KIM WALKER
KIM.WALKER@SHMA.CO.UK

SHAKESPEARE
MARTINEAU

USA: FROST BROWN TODD

YUGO NAGASHIMA
YNAGASHIMA@FBTLAW.COM

Frost
Brown Todd LLP

EGYPT: MATOUK BASSIOUNY
& HENNAWY

TAMER FAWKI
TAMER.FAWKI@MATOUKBASSIOUNY.COM

Matouk
Bassiouny
& Hennawy

Contributing PrivacyRules members

ISRAEL: PEARL COHEN
ATTORNEYS

DOTAN HAMMER
DHAMMER@PEARLCOHEN.COM

PEARL COHEN

HONG KONG: TANNER DE WITT

PÁDRAIG WALSH
PADRAIGWALSH@TANNERDEWITT.COM

Tanner 
De Witt
solicitors

SOUTH KOREA : D'LIGHT LAW
GROUP

KYOUNG MIN PYO
KMP@DLIGHTLAW.COM

D'LIGHT 
D'LIGHT Law Group

JAPAN: IWATA GODO

AKIRA MATSUDA
AMATSUDA@IWATAGODO.COM

IWATA GODO
Established 1902

On behalf of PrivacyRules, we would like to express appreciation for the EDPB's openness to receiving feedback about its Guidelines from data privacy practitioners. We stand ready to provide additional clarifications regarding our comments if needed.

PrivacyRules and its members contributing to this feedback authorise the publication of the present document and of the content of the feedback provided therein, in full or in part, wishing that the authorship of these comments will be credited.

Coordinated by
Alessandro Di Mattia

Legal & Executive Officer, PrivacyRules Ltd.

CONTACT US

PrivacyRules

American Headquarters:

PrivacyRules, Ltd.
151 West 4th Street
Suite 200
Cincinnati, OH 45202, USA

European Office:

Via dei Della Robbia 112,
50132, Firenze
Italy (IT)

Email

info@privacyrules.com

www.privacyrules.com

