MyData-TRUST S.A.
Boulevard Initials 7, Bte 3
7000 Mons (BELGIUM)
www.mydata-trust.com

28/11/2022

Comments on Guidelines 9/2022 on data breach notification under GDPR adopted on 10 October 2022.

Comments from:

MyData-TRUST

When DATA PROTECTION Meets Life Sciences

MyData-TRUST provides DATA PROTECTION services in the LIFE SCIENCE sector (such as privacy risk assessments, external DPO as a service, etc.). Active since 2017, it is registered under Belgian Laws. Its Multi-Disciplinary Team relies on Data Privacy Lawyers, IT Security Specialists and Clinical Experts. Our clients include among others Pharmaceutical, Biotech and Medical Device companies, Contract Research Organizations (CROs), Healthcare providers and associations.

Key messages

MyData-TRUST (hereinafter referred as "**MD-T**" or "**we**") welcomes the targeted update made in the recent Guidelines 9/2022 on data breach notification under GDPR ("Guidelines"), especially the clarification on the notification requirements concerning the personal data breaches at non-EU establishments.

However, the change operated into the paragraph 73 would, in our opinion, lead to an **over-bureaucratic, unfair, and disharmonized framework** with valuable resources driven **towards the paperwork and away from the protection** of data subject.

MD-T would like to emphasize the following aspect described in more detail below:

- We cannot deny the fact that the cooperation and mutual assistance mechanism foreseen by GDPR Art 60-62 cannot be applied in case of a controller or processor based outside of EU and not having an establishment in the EU. However, the cooperation mechanism aims to support handling of claims related to the cross-border activities and covers requests to carry out prior authorisations and consultations, inspections, and investigations.

  Reporting of data breaches does not always lead to an inspection or investigation and does not always result from an incompliance with regulation.

  The reporting of data breaches (Art. 33 of GDPR) points to the supervisory authority and does not refer at all to the cooperation mechanism. Despite this fact, the data breach reporting has been streamlined by the prior guidance[1] through the voluntary cooperation mechanism (since that was not in the scope of Art 60-62 of GDPR). Thus, this voluntary cooperation can in our view continue to be used without any contradiction with Art 60-62 of GDPR.

- The non-applicability of this voluntary cooperation mechanism to data controllers or processors not established in the EU could have a significant impact on the rights and freedoms of data subjects within the EU, and to the right of protection of personal data. Further, it could bring extra complexity for organizations regarding their notification's obligations.

Specific comments

Under the rules applicable to the GDPR and the newly issued EDPB Guidelines 9/2022, the data subject's right to the protection of personal data appears to be better protected in the context of a cross-border breach involving a controller established within the EU than in the context of a personal data breach at non-EU establishments. Indeed, cross-border breaches have more harmonized mechanisms to deal with the personal data breach in a fast and efficient manner and to reduce its adverse effects in a harmonious and coordinated way.

[1] European Data Protection Board, *Guidelines 01/2021 on Examples regarding Data Breach Notification*, adopted on 19 January 2021.

However, to better illustrate our statement, we will take the example of two personal data breaches:

1. The personal data breach occurs in an organisation established in the EU (Use case n°1) and;
2. The personal data breach occurs in an organisation established outside of the EU (Use case n°2).

In both situations, the breaches will affect EU data subjects.

Use case n°1: breach occurring in an EU-based organisation (cross-border breach)

In this first use case, the mechanisms put in place for the data breach seem harmonized with the possibility of notifying the breach to the lead supervisory authority which will investigate the breach. For instance, deciding on the risk of this breach to the rights and freedoms of the data subjects, the obligation to communicate this violation to the data subjects when the organisation had not yet chosen to communicate it. Notifying a single authority makes it feasible to respect the maximum amount of time allowed to notify a severe personal data breach, which is a maximum of 72 hours.

The mechanism of voluntary cooperation allows for a more adequate final decision by the lead supervisory authority. So, all other data subjects concerned by this personal data breach will receive the same decision and instructions from the lead supervisory authority and their right to protection of their personal data will be protected in the same way.

Use Case n°2: breach occurring in a non-EU-based organisation

In this second case, data subjects concerned may find their rights less guaranteed due to the obligation to notify the breach to each supervisory authorities of the Member State where the data subjects were affected by the breach.

The impacts on the right to the protection of personal data could be as follows:

- If several Data Protection Authorities ("DPAs") are involved, a risk of fragmentation could occur due to a lack of harmonization.

  The main factors creating this risk of fragmentation are:

  - **Different identification of reportable cases.** We can state that most DPAs have their own lists of reportable cases that differ from one another. There is

no such thing as a non-exhaustive list containing the main risks of a data breach that imply a notification to the DPA. Each organisation and each DPA of each Member State will interpret the risk assessment on its own way with its standard, most notable, Ireland and Italy have stricter criteria for reportable data breaches.

- **Non-applicability of the cooperation mechanism.** Because they are not under the definition of "cross-border processing" (Art 4, §23 of the GDPR), the mechanisms of cooperation, that apply "*to foster a uniform application of the data protection rules through a consistent interpretation and to ensure effective supervision and enforcement within the Union*"[2], would not be applicable.
- **Level of activity of the each DPA**. If many EU countries are concerned by the data breach, several DPAs could be competent. Some DPAs might have difficulties in processing the notification, taking for example of the limitation in technical and organizational resources). Most EU authorities say that they don't have enough resources to deal with data breaches and report that their staff are insufficient. They would like to do more audits and be focused on mitigation of the data breaches. In the cases of data breach reporting, forms need to be filled out, so the most time-consuming aspect is filling out the report forms with insufficient time for actual addressing of the data breach, thus creating a discrepancy between the workload and the task capacity.
- **The 72 hours breach notification deadline.** There is also a risk of not responding to the 72 hours breach notification deadline since each DPA determines on its own way how breaches should be notified. If all 27 Member States are affected by the same data breach and each Member State has a different data breach notification form, it becomes impossible for organisations to comply with the 72-hour deadline. If the 72 hours period is exceeded and the breach is not notified, this could incur further risks for the protection of the data subject's personal data.

[2] European Data Protection Board, *Guidelines 02/2022 on the application of art 60 GDPR, adopted* on 14 March 2022, p. 8.

An example we could offer for better illustrating this situation is the case of small companies with limited number of employees (less than 10 people) running clinical trials in 10 countries. Even if they have all information needed for data reporting, the completion of the data breach form for each country can add up to more than 72h. In this case, employees will have to spent 2 full days just fill in the forms and are unable to keep the deadline for breach reporting and mitigation.

- **Joint-controllership situation.** If one of the Controller is based outside the EU and the other Controller is based within the EU, then this voluntary cooperation should apply if one of the controllers is based in the EU.

MD-T deems that, when GDPR applies, no matter where an organisation is based, data breaches involving EU data subjects should be solved by using the same (or at least, a harmonized) mechanisms. The same data subjects should not be impacted in their rights depending on the establishment of the organisation.

In regard to the voluntary cooperation mechanism, the GDPR does not explicitly mention its scope. There is no sufficiently clear and coordinated procedure for non-EU organisations that encounter data breaches when processing the data of EU data subjects. We would like to mention that this is also the case for the notification of data protection officers. Each data protection authority has established or is establishing its national procedure. Taking this into consideration, the applicability of the voluntary cooperation mechanism in the event of a data breach at non-EU establishments will not go against the principles set forth in the GDPR.

Considering the lack of framework for this voluntary cooperation in the event of a data breach, we offer several recommendations for breaches at non-EU establishments:

- Implement a formal cooperation to have a better instruction and decision from the lead supervisory authority;
- Implement a lead supervisor mechanism to have more harmonized instructions and decisions;
- Implement a standard notification form available in several languages and available to access;
- Create a non-exhaustive list of the main data breach risks that trigger the need for notification to the DPA;
- Create a secure platform to notify data breaches more quickly and to centralize data breaches that have occurred to have specific cases on the types of breaches to be notified. This platform should be accessible to DPAs and open to notifications from DPO/DPR;
- Introduce a legal obligation for DPAs to provide feedback concerning the data breach notification and;
- Electronical portal to minimize and harmonize the bureaucratic procedure.

Conclusion

MD-T calls on the EDPB to urgently provide clarifications and harmonization to the issues and mechanisms in the context of data breach notification. The GDPR claiming to have an extraterritorial application should provide an equivalent protection of personal data to data subjects no matter where the organisation is located.

These clarifications and mechanisms would benefit all data subjects, organisations and DPAs alike.

MD-T is committed to share its expertise in the field and we remain at your disposal should you require further information or clarifications.