Response to the Public Consultation on the EDPB Template for Data Breach Notification

Introduction and general observations

Rakuten Group, Inc. welcomes and supports this project of a common, unified template to be implemented by all supervisory authorities in the EEA.

For global companies, this EDPB initiative enables a streamlined breach notification process for large-scale breaches by providing a standardized format that can be easily replicated when notifying multiple supervisory authorities.

To go even further, Rakuten would welcome the EDPB's advocacy for the establishment of a one-stop-shop mechanism for controllers not established in the EEA, through which a single submission would be distributed to all relevant supervisory authorities. While this could be proposed through the introduction of the single–entry-point in the Digital Omnibus proposal[1], it may take years to be adopted and implemented. To achieve this sooner, the EDPB's collective work outside of a lengthy legislation modification process might be suitable, and the publication of this template is a first step in this direction.

To further streamline the process, Rakuten would welcome clarification on the languages of submission. For a global company and in cross-border cases, an English-language submission significantly improves the operational burden of the process. While Rakuten understands the necessity of local-language communication, especially for data subjects, we welcome the proposal of an English-language template and would appreciate it if Data Protection Authorities could indicate whether the submission of English notifications is acceptable.

We would welcome a consistent approach across supervisory authorities on the acknowledgement of receipt. Some authorities provide a clear confirmation or reference number, while others do not, leaving controllers uncertain whether the notification was successfully submitted. A standard receipt should confirm the date and time of submission, the authority reference number, and, ideally, provide a downloadable copy or

[1] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)

summary of the submitted notification for accountability and audit-trail purposes.

Comments on the length of the template

Regarding the template itself, it appears too detailed and complex to complete, given the express GDPR requirements and the current notification forms made available by the supervisory authorities. For instance, the document outlining all the requirements for submitting a breach notification through the CNIL website is seven pages long, while the EDPB template is 30 pages long.

This relative length of the document can nonetheless be explained by the numerous precisions and explanations provided by the EDPB. For instance, Rakuten Group, Inc. welcomes the clarification regarding the "number of records", which was not defined in the GDPR although it is required in the notification and is a key factor when assessing the severity of the breach. Some items are also marked as non-mandatory, such as the economic sector in which the organization is active, which we assume would be used as a basis for statistical reports. The ability to include the internal reference number (item 7) also facilitates better cross-referencing between the notification and the internal data breach record.

However, even with these welcomed additions, the document contains more than 40 mandatory items, some of which with free-text answers, which makes it especially complex to file in light of the strict 72-hour deadline to submit a report. While it is possible to notify in a phased way and to start by submitting an incomplete notification, this increased complexity would probably lead to additional pressure for the person(s) in charge of filling such an intricate document.

Items not required by GDPR

We note that one reason for the length is that some parts of the template appear to exceed the explicit legal requirements for notifications, by making it mandatory to provide information that is more relevant to the notifying entity's internal purposes. Clear examples of this can be found in Section 3.5. "*Measures in place when the personal data breach occurred*" and 4.4. "*Measures taken (or proposed to be taken) to prevent similar personal data breach*", Item 51 "*Further description of the discovery of the personal data breach*" or Item 63 "*Description of the systems, software, services, and infrastructures involved in the personal data breach and where they are located*".

While this information is indeed useful for breach management, integrating it into the notification template theoretically would theoretically subject it to the 72-hour deadline. Such information would

still be relevant in case of important and high-risk breaches and could be requested during further investigations by supervisory authorities. It should, however, not be made mandatory for other, less serious breaches, as this would lead to additional pressure on notifying entities and even complexify the processing of notifications by supervisory authorities, by making all notifications overly detailed.

This could on the other hand be useful in case of an eventual future template for breach records. While this might already be planned, and in line with a previous paragraph, the notifying entity should be able to receive a copy of the notification containing all this information, to support organizations in their internal compliance.

Finally, under item 89 ("*Outcome of the risk assessment carried out by the controller*"), we believe that including "unlikely to result in a risk" as an option in the notification form may confuse the notifier, as such breaches are normally not notifiable. If retained, this option should be clearly framed as relevant only where a controller has already notified provisionally and later concludes that the breach was not notifiable. Otherwise, it may encourage unnecessary notifications instead of supporting controllers in properly documenting low/no-risk incidents internally.

Practical considerations

On a similar, more practical note, the marking of items as "mandatory" should be revised to ensure that not filling items that are not expressly required by GDPR would not prevent the submission of the notification. In any event, preliminary notifications should be submissible even when mandatory items are not filled in, given the very nature of such submissions.

Still on the concrete aspects of the template, it is unclear whether it would be possible to add multiple attachments belonging to the same category. For instance, one data breach could lead to different communications to data subjects, depending on how they were or are likely to be affected by the breach. This point should be further clarified to ensure that technical implementation of the template does not prevent notifying entities from submitting a complete and thorough notification.

Conclusion

In conclusion, Rakuten Group, Inc. supports this initiative from the EDPB, and wishes that the implementation of this template will facilitate the notification of data breaches across the EU, in line with the overarching objectives to reduce regulatory pressure on companies active in Europe.

About Rakuten Group, Inc.

Rakuten Group, Inc. (TSE: 4755) is a global technology leader in services that empower individuals, communities, businesses and society. Founded in Tokyo in 1997 as an online marketplace, Rakuten has expanded to offer services in e-commerce, fintech, digital content and communications to 2 billion members around the world. The Rakuten Group has around 30,000 employees, and operations in 30 countries and regions. For more information, visit https://global.rakuten.com/corp/.