Submission to the EDPB's consultation on incident reporting template

Broadcom would like to thank the EDPB for the opportunity to comment on this important initiative. Broadcom believes that incident reporting is a crucial accountability step often under difficult circumstances when an incident either accidental or unlawful impacts the ability of controllers and processors to protect personal data. Addressing the incident reporting requirements using a single reporting template is a key simplification step. It reduces the burden of different incident reporting requirements imposed by EU law and ensures consistency with reporting obligations under GDPR across different supervisory authorities.

Broadcom strongly supports this EDPB initiative and encourages its continued development. Drawing from practical testing by our privacy team, we submit the following observations and recommendations for the EDPB's consideration to further refine the template.

Early reporting vs detailed reporting

An important point to consider when reflecting on incident reporting is that often GDPR mandated notification timelines of 72 hours result in a notification having to be made before the investigation has yielded meaningful information relating to the nature, cause and impact of the incident. Consequently organizations often adopt an approach of submitting a "preliminary" notification which is then supplemented by a "followed up" notification as investigations mature and more evidence is uncovered. The template does not seem to fully take the aforementioned approach into account. Therefore, we recommend that the template be streamlined taking the practical aspects of notification into consideration; thereby resulting in a template that distinguishes between "preliminary", "follow up" and "full" notification as permitted by the GDPR. As a result, the level of detail and some of the individual questions may require further calibration to reflect the different stages.

Standardisation

Broadcom strongly recommends that the EDPB template in its final format becomes the standard template for all GDPR incident reporting across all supervisory authorities. There is no benefit in maintaining local/national reporting templates as it leads to confusion and uncertainty as to how a submissions need to be made. There should be a single template that can be applied to all incidents (not just cross-border) and all jurisdictions and supervisory authorities. This creates simplification and economies of scale. It enables organizations to have a single workflow to populate the template and prioritize their investigatory steps accordingly. The existence of additional national templates nullifies the economies of scale and benefits of the single mechanism without any tangible added value.

Number of records impacted in an incident

Broadcom believes that the template requirement to disclose “number of records” impacted in an incident is adding an unnecessary level of complexity in the incident reporting process. The number of records is less important in the risk assessment in comparison to the total number of impacted individuals as well as the nature and sensitivity of impacted personal data. The “number of records” is often a metric that is not clear during the investigation. In addition, it can often be the case that the number of records is not reflective of the true incident risk as the number of records may contain duplicative personal data information. Therefore, we would strongly recommend that the template emphasizes number of impacted individuals and nature/sensitivity of personal data as key elements of risk assessment and leave the number of records as an additional relevant but optional metric.

Risk assessment methodology

The template requires to disclose the risk assessment methodology. We suggest deleting this question as unnecessary or at least making it optional. At this point, whereas there are several well-established risk assessment methodologies in the industry to assess risk and impact from a cybersecurity incident, there is no broadly accepted methodology for the privacy impact of a cybersecurity incident. Organizations may use a combination of methodologies as the investigation unfolds or may have developed their own methodology tailored to their operations. Disclosing the methodology may risk disclosing attorney-client privileged advice. Making the question optional allows companies with such concerns to skip the question, while responses may still be collected from organizations wishing to disclose the methodology applied. In this context we would like to highlight the methodology developed by ENISA together with other supervisory authorities based on the ePrivacy provisions. That methodology continues to be used as one of the indicators to determine the severity and impact of an incident. We would recommend that the EDPB works together with ENISA to update the methodology, fully align it to the GDPR requirements and make it available in the context of EU regulatory simplification as one of the tools that could be used in assessing an incident. .

Contact points

The template assumes that for a single incident there may be multiple contact points such as a DPO or a legal representative. The template goes on to assume that there may be another third person who reported the incident to the supervisory authority. Whereas all these are possibilities, in practice the step of reporting is often managed by one individual that has overall responsibility for privacy or compliance within an organization and at whose direction the report is submitted. Therefore, it would be advisable that the template allows for one individual representing the organization thus eliminating the existence of other “possible” contact points.

Other observations

The template seems to have questions that are either duplicative with certain other questions or create confusion due to the possible overlap. It is recommended that these sections are simplified and streamlined. In particular:

- The template assumes that the controller is established in the EU but then goes on to ask the same questions about non-established controllers. This should be marked as optional because it may not be applicable
- The template is asking for detailed insight on the incident and continues further with a field asking for further detailed description - This is potentially duplicative. As mentioned earlier during early reporting often organizations do not have full visibility of the incident. Insights can be shared but with a degree of uncertainty while detailed reporting may be problematic. Therefore, the template on this topic comes across as inherently contradictory. While we understand the need to cater for different scenarios perhaps a better approach would be to make clear from the beginning whether a notification is “initial” or “follow-up” which would then enable more detailed description. In any case the requirement for detailed description should appear in only one field
- Line 57b covers the possibility that measures are potentially subverted, which is further followed up in line 76 but without any reference to 57b
- Line 63 requires description of systems, software and infrastructure that is involved in the data breach. Realistically that may not be visible within the first 72 hours of incident notification therefore this question may not be suitable in cases of initial notification.