VDA Position Paper on the EDPB Template for Notifications of Personal Data Breaches under Article 33 GDPR

Classification and assessment of the template from the perspective of the automotive industry

The German Association of the Automotive Industry (VDA) welcomes the initiative of the European Data Protection Board (EDPB) to achieve greater harmonisation of notification procedures within the European Union through a common European template for notifications of personal data breaches under Article 33 GDPR. A uniform notification format can help reduce existing differences between national procedures and facilitate the handling of cross-border personal data breaches for both companies and supervisory authorities.

It is particularly positive that the template distinguishes between initial notifications, follow-up notifications and the withdrawal of a notification, thereby taking account of the fact that, in the case of personal data breaches, the overall picture often only becomes complete in the course of further investigation.

At the same time, there are doubts as to whether the template fully achieves its objective of a simplified and practicable implementation of Article 33 GDPR. In particular, the distinction between initial and follow-up notifications, the scope of the mandatory information and the intended level of detail of technical information raise questions regarding compatibility with the structure of Article 33 GDPR and practical feasibility.

From the VDA's perspective, the template should therefore, in particular:

- safeguard the character of the notification under Article 33 GDPR as initial information to the supervisory authority;
- reflect the statutory minimum requirements of Article 33(3) GDPR without suggesting that additional mandatory information requirements are being established;
- restrict technical details to what is necessary for the data protection assessment;
- provide practical tool functionalities, in particular the possibility to save a notification as a draft before submission.

Key comments on the template and need for adjustment from the perspective of the automotive industry

1. Unclear distinction between initial notification and comprehensive incident documentation – clarify the function of the Article 33 GDPR notification as initial information

The VDA welcomes the fact that the template expressly distinguishes between initial notifications, including incomplete initial notifications, and follow-up notifications. This acknowledges that controllers regularly do not yet have all information on an incident at the time of the initial notification. Nevertheless, the template remains unclear as regards the distinction between incomplete initial notifications and subsequent supplements. The template already contains numerous mandatory items of information on risks, effects, affected data, countermeasures and information to data subjects, which can usually only be reliably assessed in the course of more in-depth technical analyses or forensic investigations.

This creates the risk that the notification under Article 33 GDPR will in practice develop from early information to the supervisory authority into largely complete incident documentation.

Article 33(4) GDPR expressly recognises that certain information may not yet be available at the time of the initial notification and may therefore be provided subsequently. This statutory separation between initial notification and later completion should also be reflected in the specific design of the template. The template should therefore clearly distinguish between mandatory information required for an initial notification under Article 33(3) GDPR and optional or supplementary information that may be provided at a later stage under Article 33(4) GDPR or only where available. Otherwise, there is a risk that the 72-hour deadline will be practically undermined because companies would have to gather information before submitting the initial notification that is typically only reliably available in the course of further incident clarification.

The practical relevance of this differentiation is particularly evident in complex cyber incidents. For example, following an attack on a vehicle platform or a customer portal, it may initially only be established that a security incident has occurred, while the scope, cause and possible effects on data subjects are still the subject of ongoing forensic investigations. In such cases, it must remain possible to submit an initial notification on the basis of the respective information available, without requiring a completed incident analysis or complete internal coordination with IT, Legal, Data Protection, Information Security, specialist departments and, where applicable, service providers.

Moreover, the higher the level of detail required for the initial notification, the greater the likelihood that information will have to be supplemented or corrected as new findings emerge. This ties up additional resources on the part of companies and may at the same time increase the administrative workload for the supervisory authorities, without necessarily improving the quality of the initial information.

From the VDA's perspective, there is in particular the following need for clarification and adjustment:

- clarification that the initial notification under Article 33 GDPR serves to inform the supervisory authority at an early stage on the basis of the available state of knowledge;
- clearer distinction between initial notification and follow-up notification in line with the principle of phased provision of information laid down in Article 33(4) GDPR;
- express marking of information that is mandatory in the context of the initial notification as opposed to information that may only be provided in a follow-up notification or only where available.

2. Expansion of the notification requirements beyond the statutory minimum information – limit mandatory information to the core elements of Article 33(3) GDPR

The VDA supports the EDPB's objective of recording personal data breaches throughout Europe according to criteria that are as uniform as possible. At the same time, the template contains various mandatory items of information that go beyond the content of a notification specified in Article 33(3) GDPR.

Against this background, the template should avoid creating the impression that additional notification requirements are effectively being established. This applies in particular to detailed information on affected systems and infrastructures, information on technical and organisational measures, in-depth descriptions of the risk assessment, information on the methodology of the risk analysis and further information on communication to data subjects and possible annexes.

In particular, requirements for a detailed description of the risk assessment, the methods applied and the factors taken into account should only be mandatory to the extent that they are essential for an initial assessment of the personal data breach by the authority. More extensive documentation may be useful in individual cases, but should not be made a precondition for a timely initial notification.

This could become a problem in particular for companies operating internationally with complex organisational and IT structures if coordination between the various specialist departments and service providers were required before notification. An increased need for coordination would mean that companies have to use additional resources to compile additional notification information while incident clarification is ongoing. The resulting coordination obligations would run counter to the objective of early notification under Article 33 GDPR.

A expansion of the notification requirements beyond the minimum requirements of Article 33 GDPR is also in tension with current European efforts to simplify regulatory requirements and reduce bureaucratic burdens for companies. The intended harmonisation of notification procedures should therefore not be associated with an expansion of information, evidence and documentation obligations, but should contribute to an actual simplification of notification practice. A common European notification template should standardise existing notification procedures, but should not create additional requirements that go beyond the statutory minimum. Otherwise, harmonisation would lead to a uniform, but not to a simpler, notification procedure.

From the VDA's perspective, there is in particular the following need for clarification and adjustment:

- limitation of the mandatory information to the notification content provided for in Article 33(3) GDPR;
- clear marking of information going beyond this as voluntary additional information;
- avoidance of a factual expansion of the statutory notification requirements through the template.

3. Limit security-relevant technical details to what is necessary for the data protection assessment

The template provides in several areas for detailed information on affected systems, software components, infrastructures and implemented safeguards. However, a request for this detailed information is not required in every case for the assessment of the requirements of Article 33 GDPR, because for the data protection assessment of an incident only the affected personal data, the possible effects on data subjects and the countermeasures taken are usually relevant. The specific technical design of internal systems is often of only secondary importance.

At the same time, the template partly requests information that goes beyond the description of the personal data breach itself and may allow conclusions to be drawn about a company's technical security architecture.

In the case of cyber attacks in particular, technical details may themselves be security-relevant. Companies in the automotive industry process data in a large number of highly networked development, production and vehicle platforms. Information on specific system architectures, security mechanisms used or internal infrastructure components may therefore affect additional protection interests.

From the VDA's perspective, there is in particular the following need for clarification and adjustment:

- limitation of technical details to the information necessary for the assessment under Article 33 GDPR;
- appropriate consideration of the confidentiality of security-relevant information;
- avoidance of unnecessary disclosure of internal system and security architectures.

4. Ensure the practical usability of the notification form

In addition to the substantive scope of the information requested, the practical design of the notification tool is also of considerable importance for a timely and quality-assured notification under Article 33 GDPR. From the VDA's perspective, the tool should make it possible to save a partially completed notification as a draft before submission.

In the case of complex personal data breaches in particular, the content of a notification must regularly be coordinated internally, missing information must be added step by step and various stakeholders such as Data Protection, Legal, IT Security, specialist departments and, where applicable, external service providers must be involved. A draft function would enable companies to prepare the notification in a structured manner without losing the work status or having to submit a notification prematurely that has not yet been coordinated. In addition, individual input fields should be designed in such a way that they comply with the principle of data minimisation and do not request personal data that is not necessary for the notification. This applies in particular to any identification numbers of the notifying person, unless such information is strictly necessary for the notification.

In addition, the template should allow multiple selections when categorising personal data breaches, in particular where an incident cannot clearly be assigned to a single category. In practice, personal data breaches often affect several protection objectives at the same time, such as confidentiality, integrity and availability. Limiting the choice to a single option may therefore lead to an abbreviated or inaccurate description of the incident.

From the VDA's perspective, there is in particular the following need for clarification and adjustment:

- improvement of user-friendliness by including a function for saving and later editing drafts;
- possibility of gradually adding information that is still missing before submission;
- clarification that no identification numbers of the notifying person are requested unless they are strictly necessary for the notification;
- possibility of multiple selections when categorising personal data breaches, where several protection objectives or categories are affected.

Conclusion

From the perspective of the automotive industry, the further consultation procedure should in particular be used to more clearly define the function of the notification under Article 33 GDPR as early initial information to the authority, to align the mandatory information more closely with the minimum requirements of Article 33 GDPR and to design the handling of technical details in a practicable manner. Corresponding clarifications would help to increase the legal certainty and practicability of the template without impairing the harmonisation purpose of the template.

Contact

Jürgen Mindel

Managing Director
juergen.mindel@vda.de

Dr. Ricarda Leffler

Head of Department & In-House Counsel
ricarda.leffler@vda.de

Susanne Jonetzko

In-House Counsel, Legal and Compliance, DPO
susanne.jonetzko@vda.de