WIRTSCHAFTSKAMMER ÖSTERREICH

Guidelines 01/2021 on Examples regarding Data Breach Notification

The Austrian Federal Economic Chamber provides the following comments:

The guidelines of the EDPB outline cases in which a data breach has to be reported. They provide practical examples what kind of preemptive measures have to be taken to ensure that data breaches do not occur. Furthermore, the EDPB provides examples what kind of measures have to be taken to make sure that data breaches are recognized and reported in time. These efforts are highly appreciated.

Nevertheless, it has to be noted that the cases outlined are quite clear and evident from our point of view. It would consequently be helpful, if the EDPB also provided exemplary "borderline cases" regarding the notification to the Supervisory Authority (SA) and affected data subjects, including the main aspects, that have to be considered. This would enhance legal certainty for data controllers and could moreover relieve SAs as only reportable data breaches would be reported.

The Federal Industry division names two open points:

- What still urgently needs to be added and remains a grey area is the question in which case a possible data breach leads to a violation of the rights and freedoms of natural persons. It would be very helpful if there were more examples from practice. For example, when is it crucial to report a data breach which has caused damage in the form of reputational harm? In which case must the data subject also be notified in the event of damage to reputation? Which situation is to be considered as reputational harm etc.
- On page 6 it is stated that the assessment, whether a breach is likely to result in a risk to the rights and freedoms of the data subject, should be made at the time the organization becomes aware of the breach. Controllers should not delay the notification by waiting for a detailed forensic examination and mitigation steps. However, in some cases it seems to be crucial to have a detailed forensic examination before the assessment can be finalized and the authority is informed.

Moreover, it would be appreciated, if EDPB could reevaluate the "Guidelines on Personal data breach notification under Regulation 2016/679 - WP250rev.01" and create a unified document structured in the same way as the new guidelines. This would provide a coherent guideline for data controllers and offer support for the assessment of data breaches.

Best regards

Dr. Rosemarie Schön
Director

Legal Policy Department
Austrian Federal Economic Chamber