European Data Protection Board

Reference: SH-342-2018

Angelene Falk
Australian Information Commissioner and Privacy Commissioner
By email only

Subject: Co-operation with the European Data Protection Board (D2018/010231)

Brussels, 23 January 2019

Dear Ms. Falk,

I would like to thank you again for your letter of 16 October 2018 and for your question related to the publication of the data breach notification. I would like to assure you that international collaboration is equally valued on my end. I especially welcome your interest to cooperate with the European Data Protection Board (EDPB).

As you know, the predecessor of the EDPB, the Article 29 Working Party, has adopted guidelines on the notification of personal data breaches. These guidelines were endorsed by the Board and they give a general overview on the interpretation of Article 33-34 of the EU General Data Protection Regulation (GDPR). We have enclosed them for your convenience, but you can find these and all other EDPB guidelines on our website, through the following link: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

For your information, the GDPR provides for a duty to communicate the breach to the individuals when the breach is likely to result in a high risk to their rights and freedoms. The Supervisory authorities may intervene to order this communication, where needed.

With regard to your question on transparency of data breach notifications received by supervisory authorities, the guidelines do not provide an answer, as the GDPR is silent on whether supervisory authorities can publish the notified data breaches. To be able to provide you with a detailed answer, I have gathered input from the members of the EDPB about their national practices.

Having summarised the replies, we have concluded that national data protection rules do not foresee any provisions in relation to the publication of notified data breaches. According to currently applicable national practises, supervisory authorities (SAs) can be divided in two groups:

1. SAs which do not make publicly available any information related to the notification of data breaches;
2. SAs which publish statistics or general information about data breaches that do not allow the controller to be identified.

The replies were similar in the fact that, as a general rule, the name of the controller was not published.

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

As regards the second group, the general information published may contain data, such as:

- date of the notification,
- date of the breach,
- nature of the breach,
- number of data subjects concerned,
- category of data concerned, and
- category of data subjects concerned.

The statistics are made publicly available on an annual basis or once per quarter. According to Article 59 of the GDPR, supervisory authorities shall draw up an annual report on its activities and this annual report may include a list of types of infringement notified. Some of the supervisory authorities make available to the public the statistics and general information on data breaches notified in the annual report.

Please let me add that different rules apply if a national supervisory authority launches an investigation on the bases of a data breach notification. In this case, some of the supervisory authorities are obliged by law to publish the result of the procedure including the name of the controller. Additionally, please note that my reply does not cover the issue of requests submitted in application of national access to information laws.

The practice currently followed in Australia and the EU is quite similar as data breaches have to be notified to the competent authority who may publish statistical reports without allowing the controller to be identified. One of the main purposes of the data breach notification to the individuals and the supervisory authorities is to limit the damage caused to individuals by the data breach. The legislator obliges the controller to do deep fact-finding and to take all the necessary steps to mitigate the damage within a short time limit and this, under the supervision of the authority. My anticipation is that the systematic publication of the name of the controller by the supervisory authorities might have as adverse effect that the controller would abstain from notifying the authority to preserve its reputation.

I hope that the information provided will help you and I am looking forward to our fruitful cooperation in the future.

Yours sincerely,

Andrea Jelinek

In copy: Sophie Higgins, Director, Regulation and Strategy Branch (Sophie.Higgins@oaic.gov.au)

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels