European Data Protection Board (EDPB) Draft Data Breach Guidelines

Date : January 29, 2021

What's this all about?

The European Data Protection Board (EDPB) has released for public consultation new draft guidelines on examples regarding data breach notification under EU GDPR. This article is a very brief overview of the draft guidelines.

Reporting to regulators – a reminder

Under the EU General Data Protection Regulation (EU GDPR), controllers are required to report personal data breaches to the relevant (EU) data protection supervisory authority and potentially also to inform impacted individuals about the data breach. In addition, processors have obligations to inform the controllers on whose behalf they process personal data of personal data breaches.

Regulatory guidance

Previously, the predecessor to the EDPB, the Article 29 Working Party, produced general guidance on data breach notification in October 2017. The new EDPB guidelines look to add to this, with practice-oriented, case-based guidance that aims to help data controllers as to how to handle data breaches and the factors to consider during risk assessment. In particular, the guidelines include:

- A list of categories of data breaches most commonly seen by the regulators, such as ransomware and data exfiltration attacks, internal human risk sources, and lost or stolen devices and paper documents, mailing errors and social engineering;
- Advice on how risks should be identified and assessed, highlighting the factors to be given particular consideration, e.g. prior measures, risk assessment, mitigations and obligations;
- Examples of the most common good or bad practices gleaned from the collective experience of the regulators; and,
- Examples of cases where the controller should notify the regulator and/or notify affected data subjects.

One specific example given was of a ransomware attack on data that was securely encrypted with state of the art encryption and was not exfiltrated for which a back-up existed. The EDPB's guidance in that particular fact-specific scenario was that there was no obligation to notify the data protection supervisory authority or affected individuals, but that the data breach should still be documented.

Interested parties have until 2 March 2021 to submit comments using the EDPB website form found (here: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/reply-form?node=1179).

This guidance may also prove useful to UK businesses, which (for the time being at least) are subject to the same underlying rules regarding data breach notification.

Takeaways

Business should consider doing the following:

- Use strong organisational and technical security measures to keep personal data safe;
- Have a clear data breach response plan that you are ready to set in motion as quickly as you can, and fire drill it;
- Know when you are required to notify regulators and affected individuals if there is a data breach involving personal data, and do so within the prescribed timeframes;
- Maintain data breach logs of all personal data breaches;
- Be prepared to update and remediate your organisational and technical security measures and procedures

based on your experience of dealing with personal data breaches;
- Submit comments on the proposal by 2 March 2021 should you wish; and,
- Keep an eye out for the final guidance from the EDBP.

The EBPB's guidance can be found here: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach_en

We report on data protection issues here: https://www.corderycompliance.com/category/data-protection-privacy/

We report about compliance issues here: https://www.corderycompliance.com/news/.

For more information please contact Jonathan Armstrong or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com