Activities requiring Data Protection Impact Assessment under Luxembourg law

Insights - 22/03/2019

The Luxembourg National Data Protection Commission (*Commission nationale pour la protection des données*, CNPD) has published a list of processing operations which require a mandatory data protection impact assessment in accordance with article 35 of the General Data Protection Regulation (GDPR).

What is a data protection impact assessment (DPIA)?

A DPIA represents a meaningful analysis of the impact of data processing on the data subjects concerned (processing which is required to be respectful of the privacy of such data subjects, in consonance with the fundamental principles of the GDPR).

What does a list of processing operations contain?

The list put forward by the CNPD does not consist of a comprehensive list of processing operations outside of which a DPIA would not be necessary – it is limited to those operations for which a data controller will necessarily need to perform a DPIA. The requirement for a DPIA in relation to operations not featured on the list will have to be assessed in accordance with the criteria of article 35, GDPR and the Guidelines on Data Protection Impact Assessment (WP248), issued by the Article 29 Working Party.

Certain operations in respect of which a DPIA is mandatory:

- (subject to a limited exemption for health professionals providing certain services) involving the processing of genetic data (article 4 (13), GDPR);
- involving the processing of biometric data (article 4 (14), GDPR) for the purpose of identifying data subjects;
- involving the combination, matching or comparison of personal data collected from processing operations with different purposes (from the same or different controllers) – that

produce legal effects / have a significant impact on the data subject;

- that consist of or include regular and systematic control of the activities of employees – that produce legal effects / have a significant impact on employees;
- certain operations for historical research / scientific or statistical purposes; and
- that consist of the systematic tracking of the geographic location of data subjects.

Certain of these operations also need to fulfil the criteria laid down in the guidelines issued by the European Data Protection Board.

The CNPD has also emphasised the obligations on the controller to: (i) perform the DPIA prior to any such processing being undertaken, and (ii) consult with the CNPD prior to processing which could result in a high risk to data subjects (in the absence of measures taken by the controller to mitigate the risk).

Non-compliance

Under the GDPR, non-compliance with GDPR requirements could lead to fines imposed of up to 20million (EUR) or 4% of a group's worldwide turnover, whichever is greater. However for DPIAs this is in a lower category of up to 10million (EUR) or 2% of a group's worldwide turnover, whichever is greater. It is therefore important to comply with the requirements of the new legislation.

Actions we can help you with in the coming weeks:

1. help you to determine whether or not a DPIA should be undertaken;

2. assist you in a review of processing activities that you may currently be undertaking or are contemplating undertaking, and help verify whether any of those might qualify for a mandatory DPIA;

3. if areas of potential high risk are identified, recommend steps to mitigate that risk and consult with the CNPD.

Contact us

Our dedicated GDPR team would be happy to assist you on all aspects of DPIAs (including providing DPIA templates) and the GDPR in general, so please do speak to your usual contact at Ogier for assistance.

For additional information, please contact Ogier in Luxembourg.

About Ogier

Ogier is a professional services firm with the knowledge and expertise to handle the most demanding and complex transactions and provide expert, efficient and cost-effective services to all our clients. We regularly win awards for the quality of our client service, our work and our people.

Disclaimer

This client briefing has been prepared for clients and professional associates of Ogier. The information and expressions of opinion which it contains are not intended to be a comprehensive study or to provide legal advice and should not be treated as a substitute for specific advice concerning individual situations.

Regulatory information can be found under Legal Notice

Meet the Author

Anne-Gaëlle Delabye

Partner

Luxembourg Legal Services

E: anne-gaelle.delabye@ogier.com

T: +352 2712 2039

Key Contacts

Bertrand Géradin

Partner

Luxembourg Legal Services

E: bertrand.geradin@ogier.com

T: +352 2712 2029

Related Services

Corporate

GDPR

Legal