July 2017

GDPR: The Data Protection Impact Assessment

Introduction

The General Data Protection Regulation (EU 2016/679) ("**GDPR**") aims to ensure that organisations which process personal data embed data privacy into their business model. To this end, it introduces a requirement that a data protection impact assessment ("**DPIA**") be completed by organisations before they embark on any new business initiative which involves the high-risk processing of personal data. While certain organisations engaged in high-risk processing may already carry out such impact assessments as a matter of good practice, the GDPR now imposes this as a statutory obligation.

What is a DPIA?

The DPIA is a tool which requires organisations involved in certain types of high risk processing to:

(i) analyse each of the steps involved in the proposed processing activity and identify the purpose of such proposed processing;

(ii) assess the necessity and proportionality of that processing; and

(iii) identify and manage the potential risks to the privacy of data subjects which arise from that activity.

For further information on any of the issues discussed in this article please contact:

Breeda Cunningham
DD: + 353 (0)1 673 1846
breeda.cunningham@dilloneustace.ie

Rose McKillen
DD: + 353 1 673 1809
rose.mckillen@dilloneustace.ie

Its purpose is to ensure that all relevant privacy and data protection issues are identified by an organisation before work on a project or initiative actually commences. A single DPIA may address a set of similar processing operations that present similar high risks.

In what circumstances is a DPIA necessary?

In general, a DPIA is required under the GDPR when the processing of personal data is "*likely to result in a high risk to the rights and freedoms of natural persons*". It is particularly relevant where the proposed processing involves a new technology.

The GDPR has identified three types of processing operations for which a DPIA is required which include:

(i) a systematic and extensive evaluation of personal aspects relating to data subjects which is based on automated processing, including profiling and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(ii) processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences; or

(iii) systematic monitoring of a publicly accessible area on a large scale.

However, it should be noted that the above is a non-exhaustive list and that a DPIA will also be required in other cases where the processing of personal data involves a "*high risk to the rights and freedoms*" of the data subject. The Article 29 Data Protection Working Party has prepared guidelines (the "**Guidelines**")[1] which provide criteria that should be considered in determining whether a processing activity is such that warrants a DPIA being completed.

The GDPR also provides that individual Member States must identify "high risk" processing operations in respect of which a DPIA must be completed. Member States may also set down that certain kinds of processing of personal data will not require a DPIA to be carried out.

Failure to carry out a DPIA where it is required under the GDPR, carrying out a DPIA in an incorrect way or failing to consult the competent supervisory authority may result in an administrative fine being imposed.

In what circumstances is a DPIA advisable?

Organisations may choose to implement a DPIA on a voluntary basis before commencing a new project which will involve the processing of personal data in order to (i) ensure that the

[1] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 adopted on 4 April 2017. It must be noted that these Guidelines were subject to consultation which closed in May 2017 and may be subject to change.

organisation complies with its obligations under the GDPR and (ii) if necessary, demonstrate to the Data Protection Commission at a future date that it identified all relevant risks associated with the processing of the personal data and took appropriate steps to resolve or mitigate those risks before the processing activity began.

In cases where it is not clear whether or not a DPIA is required, the Guidelines recommend that a DPIA is carried out. If an organisation determines that a DPIA is not required on the basis that the processing is not "likely to result in a high risk", it should document the reasons for this determination.

What role will the Data Protection Commission play?

If, after a DPIA has been completed, certain risks to the privacy of individual data cannot be fully mitigated by reasonable means, an organisation will be required to consult with the Data Protection Commission before work on the relevant project or initiative begins.

What's next?

The obligation to prepare a DPIA will apply to any new processing operations which meet the criteria outlined above and which are initiated after the GDPR becomes effective on 25 May next. If there is a change of the risk posed by an existing processing operation after 25 May, it should be assessed to ensure that it is carried out in line with the DPIA.

The Guidelines also strongly recommend that organisations carry out a DPIA for processing activities which are already under way before next May where such processing involves a "high risk" to the rights and freedoms of data subjects. Organisations will therefore need to consider whether any existing and new processing activities undertaken by them are such that a DPIA should be implemented in order to ensure compliance with the GDPR.

DILLON EUSTACE

Dublin
33 Sir John Rogerson's Quay, Dublin 2, Ireland. Tel: +353 1 667 0022 Fax: +353 1 667 0042.

Cayman Islands
Landmark Square, West Bay Road, PO Box 775, Grand Cayman KY1-9006, Cayman Islands. Tel: +1 345 949 0022 Fax: +1 345 945 0042.

New York
245 Park Avenue, 39th Floor, New York, NY 10167, U.S.A. Tel: +1 212 792 4166 Fax: +1 212 792 4167.

Tokyo
12th Floor, Yurakucho Itocia Building, 2-7-1 Yurakucho, Chiyoda-ku, Tokyo 100-0006, Japan. Tel: +813 6860 4885 Fax: +813 6860 4501.