GDPR in Context: Privacy Impact Assessments

Background

The General Data Protection Regulation (the "**GDPR**") will come into effect on 25 May 2018. The GDPR will be directly effective in each EU member state, with the aim that the same rules will be applied uniformly within the EU. This marks a shift in the approach to data protection at a European level, which until 25 May 2018 will rely on national implementing legislation in each EU member state.[1]

The period between now and 25 May 2018 is therefore the de facto transition period, during which organisations will need to assess their current approach to data protection, to undertake a gap analysis between that current approach and the requirements under the GDPR, and to implement any changes and improvements which are required to achieve demonstrable compliance with those GDPR requirements.

Overview

Privacy impact assessments ("**PIAs**") are not a new concept. However, the GDPR represents the first time that PIAs have been expressly mandated, in certain circumstances, under data protection legislation.

Undertaking a PIA essentially means applying a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative privacy impacts.

Mandatory PIAs

Under the GDPR, data controllers are required to undertake pre-processing assessments of the impact of their envisaged processing operations on the protection of personal data in circumstances where the processing is likely to result in a "*high risk*" to the rights and freedoms of individuals. The GDPR points to various factors which may be indicative of high risk, such as use of new technologies, new kinds of processing, or if there has not been a previous impact assessment or there has been a significant lapse of time since an initial assessment. In particular, however, PIAs will be required in the case of:

- systematic and extensive evaluations based on automated processing, including profiling;
- large scale processing of special categories of data or information relating to criminal convictions and activities; and / or
- systematic monitoring of public areas on a large scale.

In assessing the risk associated with the particular processing activities, a controller will need to look at the particular likelihood and severity of the risk, taking into account the nature, scope, context and purposes of the processing and the likely sources of risk. In undertaking a PIA, particular focus should be placed on measures, safeguards and mechanisms for mitigating risk, ensuring the protection of personal data and demonstrating compliance with the GDPR.

A single PIA may be undertaken for similar processing operations eg, where public bodies or industry plan to introduce a common application or platform.

[1]There will be national implementing legislation with regard to certain elements, in particular the sanctions regime. However, the general principles which govern the processing of personal data by both controllers and processors will apply automatically from 25 May 2018.

Privacy Impact Assessments

Supervisory authority consultations

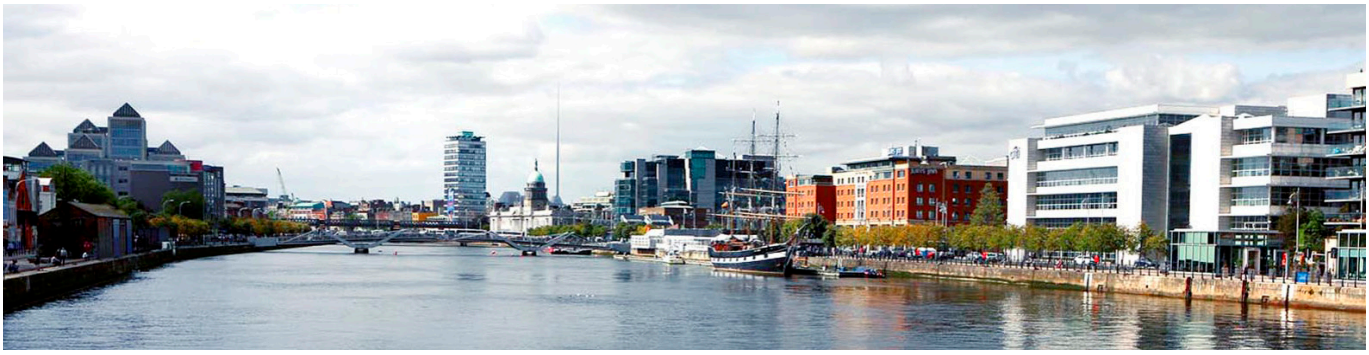
Where the PIA indicates that processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, there is a requirement to engage in a pre-processing consultation with the relevant supervisory authority.

The supervisory authorities are given a number of powers with respect to PIAs, including the ability to publish lists of circumstances in which PIAs will be required, with specific reference to social protection and public health, or if processing is likely to prevent individuals availing of a service or contract. Any such lists need to be notified to the European Data Protection Board.

The GDPR sets out timeframes for the consultations with the supervisory authorities, allowing the supervisory authority eight weeks for its initial review and the provision of written advice where it is of the opinion that the intended processing would infringe the GDPR, in particular where the controller has insufficiently identified or mitigated the risks. The supervisory authority can also apply a six week extension to take into account the complexity of the intended processing, in an appropriate circumstance.

Where consulting with the supervisory authority, a controller is required to include, within the PIA documentation provided to the supervisory authority, a description of the respective responsibilities of controllers or joint controllers and processers (including in particular for processing within a group of undertakings), the purpose and means of the intended processing, and any safeguards proposed to protect individual rights. The outcome of the PIA also needs to be communicated, and the supervisory authority retains the right to request additional information.

The PIA report must contain at least a systematic description of the envisaged processing operations and of the purposes of the processing. Where the processing is legitimised on the basis of a legitimate interest pursued by the controller, this must be specified in the PIA. In addition the controller must have undertaken a necessity and proportionality assessment in relation to the purpose, and a risk assessment identifying those risks to individual rights and freedoms, as well as measures to address the risks. Those measures will include appropriate safeguards, security measures and other mechanisms to ensure protection, and measures to demonstrate compliance.



Other consultations

Where an organisation has appointed a data protection officer (“**DPO**”), the DPO will have an advisory role in relation to the PIA, and must be consulted as part of the PIA process.

In addition, where appropriate and without prejudice to any commercial or public interests and / or the security of the processing operations, controllers are also expected to seek the views of data subjects and their representatives.

Guidance

The Article 29 Working Party (“**WP29**”) has published a consultation on draft guidelines (the “**Guidelines**”) on PIAs and in relation to determining whether processing is “*likely to result in a high risk*”.

In the Guidelines, the WP29 has noted that PIAs can be an important tool for accountability, which in light of the accountability and transparency obligations generally under the GDPR, including the need for demonstrable compliance by controllers and processors, may be a relevant consideration in deciding to undertake a PIA even if one is not mandatory under the GDPR. The WP29 has also recommended that if there is a doubt as to whether a PIA should be undertaken, then a controller should carry out a PIA.

In relation to pre-GDPR processing activities, the WP29 has strongly recommended that a PIA should be undertaken where the processing meets the GDPR criteria. Similarly, if there is a significant change to the processing operations after the GDPR comes into effect, or a new technology is introduced, different purposes arise or if there are changes in the risks presented by the processing operations, controllers will also need to consider whether the requirement for a PIA is then triggered.

From the WP29’s perspective, the focus should be very much on the rights of the data subject, rather than the rights or obligations of the controller. Furthermore, in light of the transparency theme running through the GDPR, the WP29 recommends that serious consideration should be given by a controller to publication of the PIA or a relevant part of the PIA, albeit that the WP29 accepts that there may be commercial or security sensitivities which would restrict publication to some degree.

Matheson

Privacy Impact Assessments

High risk

The Guidelines specify a number of criteria which should be considered when assessing whether there is a high risk associated with processing operations, and indicate that the more criteria are met, the higher the likelihood that the processing operation will require a PIA. Meeting fewer than two of the suggested criteria (ie, only one) means that a PIA may not be required, but the WP29 has pointed out that this is not a strict rule and that, depending on any particular circumstances of the processing and taking into account its nature, scope, context and purposes, and the likely sources of risk, a PIA may nonetheless be required.

The criteria identified by the WP29 as indicia of high risk include:

- evaluation or scoring, including profiling and predicting;
- automated decision making with legal or similar effect;
- systematic monitoring including of public accessible areas, in particular where there may be a lack of awareness of the monitoring;
- processing of sensitive data, which in this context includes not only data defined as “special category” data under the GDPR, but data which may be generally considered as increasing possible risks individuals eg, financial data that may be used for payment fraud;
- large scale processing, which should be considered by reference to factors such as the number of data subjects (whether the specific number or the proportion of a relevant population), the volume and range of the data, the duration or the permanence of the data and the geographical extent of the processing;
- data set matching or combinations;
- processing of information in relation to vulnerable data subjects where there is an imbalance of power between the controller and the individual eg, children, employees or vulnerable segments of the population such as asylum seekers;
- innovative use of technological organisational solutions such as biometrics or the internet of things;
- cross border transfers taking into account the country of destination, the possibility of further transfers and the likelihood of transfers based on derogations rather than exemptions; and
- prevention of exercise of rights or the use of a service or contract eg, credit reference screening (which would also come under the evaluation or scoring category) resulting in an individual being denied a loan.

As with all the published methodologies, the WP29 guidelines emphasis that PIAs are a tool for managing risk, and involve an ongoing process.

Privacy Impact Assessments

Next steps

The significant strengthening of data protection rules which is inherent in the GDPR, and in particular the sanctions under the GDPR, emphasise the need to ensure that each organisation has full insight into the data flows concerning customer data and other personal data which it controls, and that it puts appropriate notifications, processing agreements, transfer arrangements and security arrangements in place.

Organisations will need to consider whether any of their current or proposed processing is likely to give rise to "high risk" to data subjects, taking into account the various criteria outlined above. Where such a high risk is likely to result, then a privacy impact assessment will need to be undertaken, with potential that an organisation will also need to consult with the relevant supervisory authority in advance of commencing the processing operations. However, in light of the accountability principle which underpins the GDPR, and in particular the focus on demonstrative compliance by controllers and processors with their GDPR obligations, it may be of benefit to controller to have a PIA process in place for any significant project or service which it proposes to implement and which has privacy impacts.

Contacts

Anne-Marie Bohan
PARTNER
D +353 1 232 2212
E anne-marie.bohan@matheson.com

Deirdre Kilroy
PARTNER
D +353 1 232 2231
E deirdre.kilroy@matheson.com

Chris Bollard
PARTNER
D +353 1 232 2273
E chris.bollard@matheson.com

Carina Lawlor
PARTNER
D +353 1 232 2260
E carina.lawlor@matheson.com

Christine Woods
ASSOCIATE
D +353 1 232 2147
E christine.woods@matheson.com

12.10.17