General Data Protection Regulation

Impact assessment

"We demand rigidly defined areas of doubt and uncertainty!"

Douglas Adams

Article 33 of the GDPR imposes an obligation to conduct impact assessments:

"Where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and the purposes of the processing, is likely to result in a high risk for the rights and freedoms of individuals, the controller shall, prior to the processing, carry out an assessment of the impact... on the protection of personal data"

Specified risks

Article 33(2) of the GDPR sets out a list of processing operations that would constitute specific risks for this purpose, which includes: profiling; analysis of sensitive data relating to sex life, health, race and ethnic origin; and, large-scale CCTV monitoring of public places.

The national Data Protection Authority ("DPA") is also able to establish and make public a list of the processing operations that it considers likely to present specific risks to the rights and freedoms of data subjects, and for which they also require an impact assessment be undertaken.

Nature of the assessment

As a minimum, the assessment must contain:

- a systematic description of the envisaged processing operations;
- the purposes of the processing;
- the legitimate interest pursued by the controller (if applicable);
- an assessment of the risks to the rights and freedoms of the data subjects;
- the measures envisaged to address the risks; and,
- safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance.

The data subjects

The assessment must itself take into account the rights and legitimate interests of data subjects and other persons concerned. The controller should also seek the views of data subjects or their representatives on the intended processing, where appropriate.

Provision upon request

A data controller or processor that has received a request from a DPA for a copy of the impact assessment should provide the documentation, along with any other information that the DPA believes will allow it to carry out a proper assessment of compliance.

Prior authorisation and prior consultation

Prior consultation with the DPA by a data controller or processor may be necessary when the processing is of a specified risk or if the impact assessment indicates a high degree of risk.

A data controller or processor that wishes to undertake an international transfer of personal data without the safeguards of a legally binding instrument or of contractual clauses authorised by the DPA, would also be an example of a situation in which prior authorisation from the DPA must be obtained.

Prohibition on processing

A further example of the GDPR seeking to strengthen the position of the DPA as champion of the data is that the DPA is given the final word and, upon consideration of an impact assessment, can simply prohibit the processing in question or can suggest remedies to ensure compliance. The GDPR even allows for the DPA to prohibit processing on the basis of an insufficient assessment that does not properly identify the risks or how those risks can be minimised.

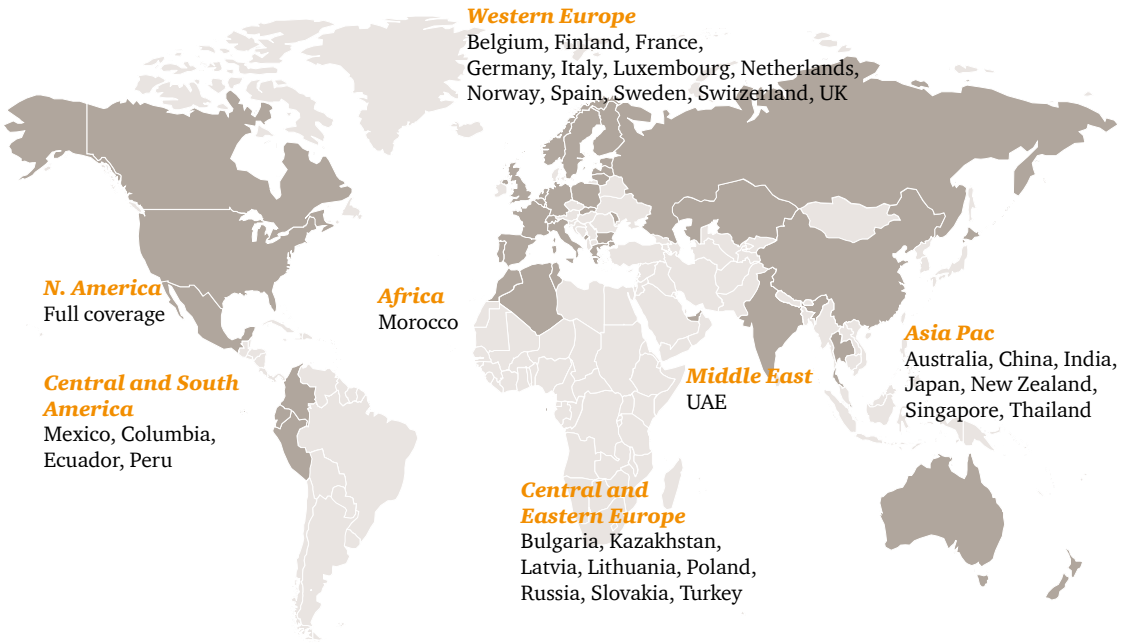
Data protection framework

The European Parliament has described impact assessments under the GDPR as being "the essential core of any sustainable data protection framework". It noted that such an assessment, if carried out in a full and thorough manner, would "fundamentally limit" data breaches and intrusions of privacy.

pwc

PricewaterhouseCoopers Legal LLP (London)

PwC's global privacy practice



PwC Luxembourg Contacts

Vincent Villers
Partner
2367
vincent.villers@lu.pwc.com

Frédéric Vonner
Partner
4173
frederic.vonner@lu.pwc.com

Sami El Euch
Director
2685
sami.eleuch@lu.pwc.com

Cédric Nédélec
Data Protection Officer
2186
cedric.nedelec@lu.pwc.com