General Data Protection Regulation

Data protection by design and by default

"Design is a funny word. Some people think design is how it looks. But of course, if you dig deeper, it's really how it works."

Steve Jobs

The principle of data protection by design and by default is set out at Article 23 of the GDPR:

"Having regard to the state of the art and the cost of implementation... the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective way and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This applies to the amount of data collected, the extent of their processing, the period of storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible to an indefinite number of individuals."

Need for change

The EU Data Protection Directive did not explicitly include privacy by design. However, given that the right to privacy is a fundamental element of the European Convention on Human Rights, it was clear that those designing technology ought to consider privacy as part of their product design, in the same way that they would take measures to not discriminate on the basis of race or gender as part of that process. The formalisation of that position is therefore included in the GDPR.

The principle

The principle of privacy by design and by default is consistent with, and an extension of, the requirement for data minimisation under Article 5 of the GDPR; namely that systems and technology should be designed in such a way so as to ensure that: (i) data processing is limited to what is necessary for the purpose for which the data was collected; and, (ii) only those within an organisation who need to access the personal data can do so.

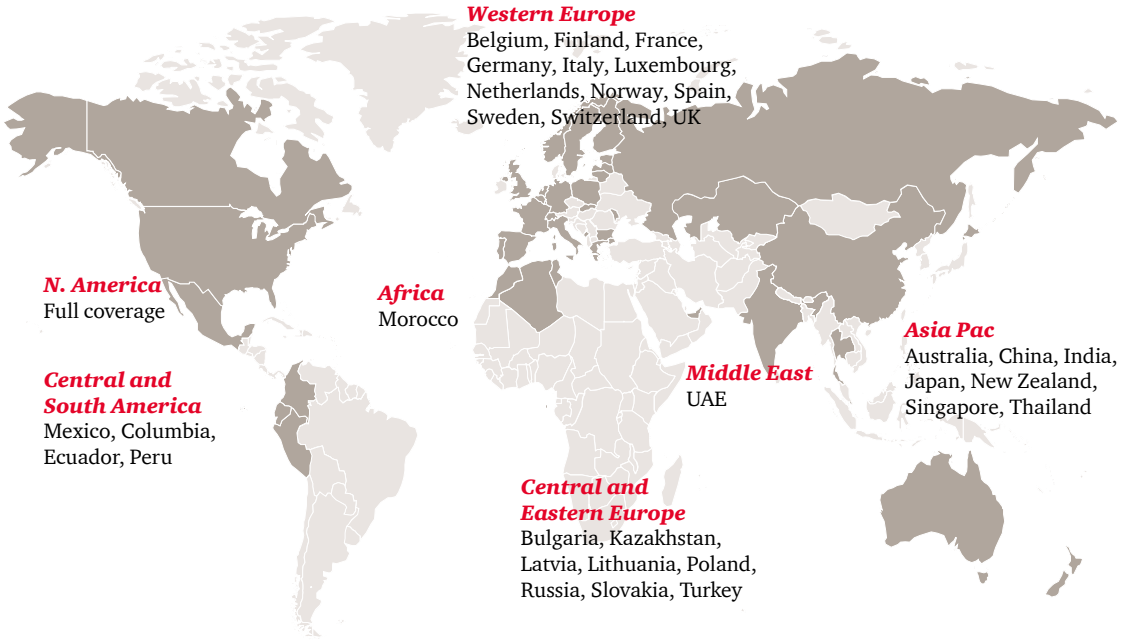
Certification

The GDPR provides for a voluntary certification by which entities can demonstrate compliance with the principles of design and default by way of data protection seals and marks. Given that the privacy rights that the GDPR promotes are likely to change the expectations of citizens, when considering future products, such a proposal provides for a commercial advantage to those that choose to obtain these seals and marks, rather than just a regulatory obligation - again furthering the principle that the subjects are champions of the data.

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

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