General Data Protection Regulation

The legal issues in jargon-free English

Who the rules will apply to

The existing EU Data Protection Directive ("the Directive") only applies to organisations that have a presence or use equipment in the EU and are in charge of how information about people is used ("data controllers"). The General Data Protection Regulation (GDPR) is much wider in its scope and means that the new law applies directly to more organisations. Any organisations that are active in Europe will need to comply with the GDPR. This includes those organisations with no establishment in the EU but which are directing goods and services at people in the EU or are monitoring people there. For example, a US retailer that has no establishment in Europe but directs the marketing of products at customers based in the EU will need to comply with the GDPR.

Service providers do not have to comply with data protection laws when handling information about people on behalf of their clients (unless their clients include wording in their contracts to make them do so). The new law applies directly to those service providers that handle information about people based in the EU on behalf of other organisations.

Personal data

The definition of personal data under the data protection directive was very broad and included virtually any information that may have allowed identification of an individual. The GDPR aims to clarify the types of data under the definition, including elements such as location data and online identifiers. Additionally, the Regulation adds genetic data and biometric data to the catalogue of data attributes considered sensitive and requiring special measures and increased protection.

The Directive permitted use of personal data only in limited circumstances, of which one of the most often relied upon by organisations is an individual's consent. The GDPR makes consent much harder to obtain and prove, thereby forcing organisations to re-examine how they collect and use personal data.

Proving compliance

There are new compliance requirements imposed by the GDPR. Most organisations will need to be able to prove they are complying with the law by producing evidence to support how they are complying. This means having paperwork documenting what personal data is used by the organisation and how. Organisations now have to demonstrate to regulators how they comply and if they cannot, this will be a failure. Organisations have to perform and document privacy risk assessments and privacy audits as a matter of course where the activity poses a specific privacy risk. Again not doing this and not having evidence of doing this will be a failure. Examples of activities that would be deemed to pose a specific privacy risk are profiling, processing sensitive personal data, biometric data and CCTV monitoring on a large scale. The requirement to have paperwork in place is a big change for organisations as it could be a failure merely to not have the necessary evidence. Regulators will have the power to audit organisations to verify compliance with the law and their first question will no doubt be about the paperwork.

pwc

PricewaterhouseCoopers Legal LLP (London)

Getting it right from the start

Organisations will need to consider privacy at the outset and throughout the design of any new system, product, service or process. This is referred to as "privacy by design" in the GDPR and compels entities to ensure that personal data is used in a way that is in line with citizens' rights. In addition, organisations must only process the minimum amount of personal data necessary for a particular purpose and will be required to implement default settings that minimise data collection to only the personal data that is necessary for that purpose.

Handling failure

Entities will be required to report contraventions of the law to the regulators and to the people affected. Public disclosure of failure is likely to fuel regulatory sanctions and compensation claims, as well as causing damage to brand and reputation.

Organisations need to report incidents of this kind within 72 hours. They will need to provide information about : (i) the nature of the incidents; (ii) the categories and number of people affected and the categories and number of records concerned; (iii) details of the Data Protection Officer or contact point; (iv) likely consequences of the breach; (v) measures taken and that will be taken; and, (vi) steps to mitigate the impact of the incident.

People dedicated to compliance

Organisations are free to appoint a dedicated Data Protection Officer (DPO) in order to help with satisfying the onerous provisions of the GDPR - and may will need to in order to cope - however, organisations will be compelled to appoint a DPO if one of the following conditions applies:

- The organisation is a public authority.
- Part of the organisation's core activity requires regular monitoring of individuals.
- Part of the organisation's core activities require large-scale processing of sensitive personal data.

Regardless the DPO will be responsible for ensuring that an organisation gets data protection compliance right. In order to carry out this task to the highest standard, the DPO is required to carry out the role 'independently' and without any instructions regarding the exercise of his or her function.

The DPO's role includes, but is not limited to, informing and advising the organisation of its obligations under the GDPR, monitoring compliance with the GDPR and requirements relating to privacy by design, privacy impact assessments, data security and the rights of individuals. The DPO will also act as a contact point for the supervisory authority and will be required to co-operate at the authority's request.

Many organisations will find that the appointment of a dedicated DPO is a useful way to demonstrate their willingness to engage with the process and take privacy seriously, which is likely to present a commercial advantage in a world in which the expectation of citizens will evolve to come to expect the rights under the GDPR to be properly protected.

Being a supplier

An entity handling another organisation's information will now be directly liable under the GDPR for failure to meet certain obligations. The current Data Protection Directive only indirectly applies to organisations receiving instructions to process personal data, for example, through a contract. Even so, the only mandatory contractual obligations are to act on instruction of the organisation supplying the data and to implement appropriate security measures to safeguard the personal data. Under the GDPR, the obligations are more extensive and include:

- Paperwork – having paperwork in place to demonstrate compliance with obligations under the GDPR.
- Getting privacy right – implementing processes to ensure you get privacy right from the start which is likely to include risk assessments and designing technology in a way that is not privacy intrusive.
- Security – complying with the security requirements set out by the GDPR directly, instead of through contracts with data controllers.
- Data Protection Officers – the organisation may need to appoint a DPO with the prescribed skills and experience.
- If things go wrong – your organisation will be required to inform its controllers/ customers and provide prescribed information "immediately after the establishment" of a breach and certainly within 72 hours.

Citizens' rights

The GDPR contains a heavy emphasis on data subjects' rights. These include for a data subject to access their personal data, to amend it, and the right to erase personal data that is incorrect or no longer relevant. These new rights will essentially allow an individual to better monitor and amend their data, as well as delete data upon request. Another right is that a data subject can request the transfer of their personal data from one service provider to another service provider upon request, which is referred to as 'data portability.' These processes will all require sophisticated business infrastructures to handle and manage individuals' requests and processing. Other rights enjoyed by a data subject will include subject access without a fee, data rectification and a right to object to data processing.

What will happen if it goes wrong

A failure to comply with the Regulation could result in fines of up to 4% of the entity's annual worldwide turnover. Regulators will be empowered to carry out audits and inspections of entities. There is currently increased pressure by citizens for privacy and data protection and pressure groups will be given the right to engage in group litigation or class action suits to recover compensation for even the distress caused by a lack of compliance with the law. Public disclosure of a failure to comply with the GDPR will also result in a very real risk of potential damage to brand and reputation.

Making data impersonal

Both the Directive and the GDPR impose obligations regarding "personal data", which is defined as data relating to an identified or identifiable person. If personal data can be manipulated such that the individuals can no longer be identified from the data and it is irreversibly anonymised, then it will not be subject to the provisions of the GDPR.

Full anonymisation of data is very difficult to achieve in practice, but there is a useful half-way house between personal data and anonymous data, which is data that is pseudonymous. Data that falls into this category is subject to less rigorous restrictions than personal data and is also referred to as pseudonymised data or "shadow data", which is defined in the GDPR as: "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information".

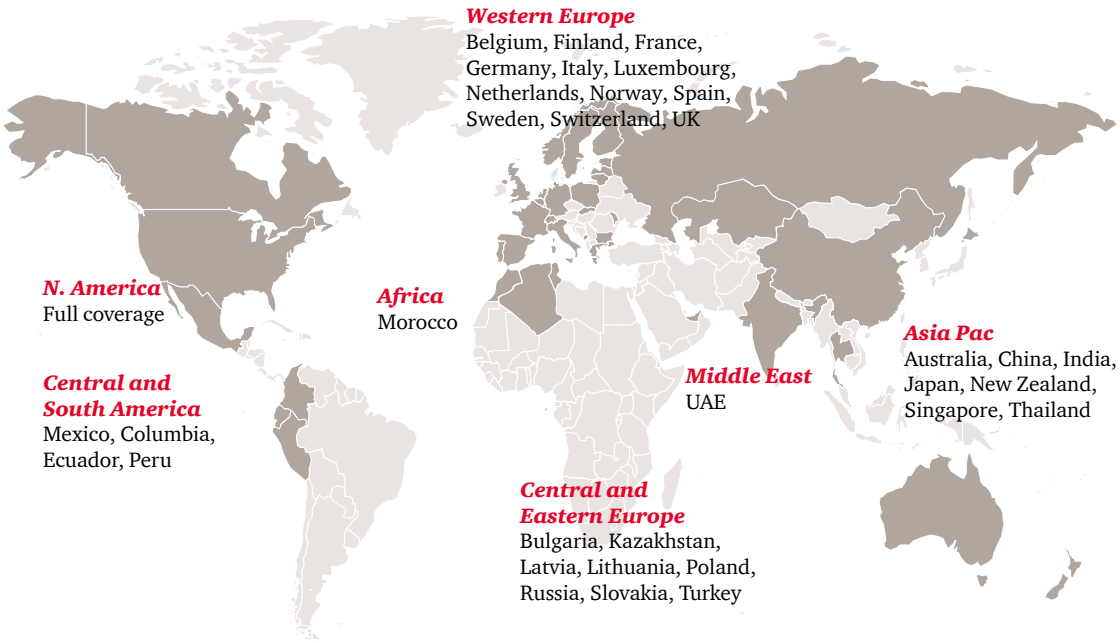
Sending information abroad

Organisations are still be able to send personal data outside of the EU where the European Commission has deemed that there is an adequate level of protection for the citizens' rights.

There are a number of grounds that entities can rely upon, such as contractual permissions and consents from individuals. Additionally, the European Commission has adopted Decisions approving other mechanisms for transfers of personal data, including "Model Contractual Clauses" and "Binding Corporate Rules". The Court of Justice of the European Union has recently ruled that another of the mechanisms flowing from a European Commission decision called "Safe Harbour" is invalid.

The Safe Harbour Decision has been one of the main legal mechanisms for the transfer of personal data from Europe to the United States for the past 15 years. Now that the Decision has been declared invalid, it cannot be used to render these transfers of personal data lawful. The other transfer mechanisms are now arguably also vulnerable to the same kind of challenge faced by the Safe Harbour Decision, although they currently remain perfectly valid. Most entities that are transferring personal data to the United States will be able to point to substantial protections in their organisations for data protection and privacy, such as governance frameworks, policy frameworks and privacy and security controls and measures. It would be sensible for entities to identify those protections, so that they have answers on hand if challenged. Businesses should also consider conducting reviews of their supply chains, to understand whether those whom they rely upon are themselves reliant on Safe Harbour. Putting in place mechanisms to monitor complaints and inquiries about data transfers should be considered as a top priority.

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