Ovum

TMT intelligence | informa

Ovum's Mini-Guide to GDPR

Alan Rodger,

Senior Analyst,

Infrastructure Solutions

Summary

Catalyst

The EU's General Data Protection Regulation (GDPR) will come into legislative force from May 25, 2018, affecting enterprises and service providers globally that are responsible for personal data on EU citizens. Because GDPR applies across boundaries of size, market activity, and geography, few organizations can afford to ignore its significant impact. Preparations require broad analysis of current operational activities and, commonly, significant investment in change. End users are increasingly aware of the value of their personal data, and expect enterprises to protect it rigorously – addressing GDPR is essential to protecting brand value, for organizations that could suffer from the negative impact of noncompliance to customer relationships, as well as due to the considerable financial penalties that can be imposed by regulators.

Ovum has a wealth of in-depth research into the regulation and its impact on enterprises, and service providers and their markets, and we can also help individual organizations by reviewing their GDPR-related plans. We provide this mini-guide in order to highlight a number of areas that organizations should consider in preparing for GDPR's impact.

Major areas of GDPR's impact

Each of these areas of impact could have significant budgetary, IT, HR, governance, and communications implications:

- **Awareness:** Decision-makers and key people in an organization must be aware that the law is changing and identify the areas that could cause compliance problems, and must plan an ongoing approach from a leadership level.
- **Information held:** Organizations should document what personal data they hold, where it comes from, and with whom it is shared. Information audits across the organization are likely to be necessary.
- **Communicating privacy information:** Current privacy notices should be reviewed and necessary changes planned. GDPR imposes new requirements such as explaining the legal basis for processing data, regulated data retention periods, and the right for individuals to complain to the Data Protection Authority (DPA). All information must be provided in concise, easy-to-understand language.
- **Individuals' rights:** Organizational procedures must incorporate all the new rights that individuals will have, including how personal data would be deleted, or provided electronically for transfer in a commonly used format under users' right to data portability.
- **Subject access requests:** GDPR imposes new timescales and requirements, and in most cases organizations will not be able to charge for access requests. It must be possible to demonstrate why unfounded or excessive requests are refused. Many organizations that do not already allow users to access information online may consider implementing systems that make it possible.
- **Consent:** Organizations should review how they seek, obtain, and record consent from users, at a more granular level and across a broader range of operational activities than previously. Consent must be sought to hold and process GDPR-regulated "legacy" data that is already

within the organization. Users must also be given the opportunity to withdraw their consent at any time.

- **Legal basis for processing personal data:** Organizations must record the legal basis for their processing of all types of personal data, for each different context in which the data is used.
- **Children:** GDPR mandates specific protection for children's personal data, particularly with regard to internet services such as social networks. Organizations must be able to verify an individual user's age and, if necessary, gather and record consent from parents or guardians. Organizations that offer services intended for children face significant implications and will have to ensure that children can understand privacy notices.
- **Data breaches:** Procedures must be in place to detect, report, and investigate data breaches, and GDPR imposes aggressive timescales in which to do so. Breaches causing the individual to be likely to suffer some damage will have to be reported to the DPA. Failure to report breaches could result in fines, on top of fines for the breach itself.
- **"Data protection by default and design":** GDPR upgrades this well-known "best practice" to a legal requirement – along with **data protection impact assessments (DPIAs)**. DPIAs will be mandated to assess the data-related impact of any change involving risk of impacting data privacy/protection. Data protection by default and design is a broad obligation that may span strategic and operations activities in many organizations.
- **Data protection officers:** Organizations are required to designate a data protection officer to take proper responsibility for data protection compliance, and to interface with the DPA.
- **International:** Organizations that operate internationally will have to determine which DPA they will refer to. In case of uncertainty over which supervisory authority is the lead, organizations should map out where they make their most significant decisions about data processing. This will help determine their main establishment and therefore their lead supervisory authority. Data location is also regulated by GDPR.

Penalties for noncompliance

One of the best-known elements relating to GDPR is the high level of potential penalties for compliance failures, as their scale could significantly impact the financial position of some organizations.

Fines up to €10m, or 2% of a company's worldwide annual turnover in the previous financial year (whichever is higher), could apply to each infringement of the obligations of:

- data controllers and processors
- certification bodies
- monitoring bodies in charge of supervising compliance with a code of conduct.

Fines up to €20m, or 4% of a company's worldwide annual turnover in the previous financial year (whichever is higher), could apply to each breach of:

- the basic principles for processing, including conditions for consent
- the data subject's rights
- the rules for transfers of personal data to a third country or an international organization
- any obligations included in national law

- noncompliance with an order of a DPA, or with a limitation on processing or transfer of data, or failure to grant access to the DPA.

Recommendations for enterprises

Ovum believes that enterprises are at risk of failing to fully assess the impact of GDPR on their capabilities, processes, and operations. The scope of assessment should be broad within organizations, encompassing legal expertise, privacy practitioners, IT leaders, business operations, and other sources of expertise, depending on specialisms and current practices. An assessment of the organization's legal position relating to the regulation should be foundational for further major areas of activity.

Many of the changes that will be necessary within organizations due to GDPR can be used to general advantage (e.g., improving customers' trust in the organization, understanding enterprise data more holistically, or targeting investment in security protection according to risk). However, there is an inherent imbalance between the scope of some of the activities that will be necessary and the deadline for legislative compliance, so gaining organizational commitment to strategic aims that could be associated with GDPR-related change may be challenging.

Recommendations for service providers

The scope of requirements arising from GDPR is extensive. Many service providers will be able to offer customers their assistance with some, rather than all, of this broad operational range. The ability to offer broader expertise to customers via partners that can fulfill requirements in different areas may provide further revenues and an enhanced customer perception of increased relationship value.

GDPR is the most recent of numerous compliance responsibilities to bring opportunities to software and service markets, due to affected organizations seeking to protect against the consequences of noncompliance. Badging offerings as "compliant" with any legislation is only one step toward aiding customer compliance, as it is customers' organizational processes that need to be compliant, beyond the IT systems and services that may power those processes. We do believe that customers perceive additional value to be available from services that provide automated, integrated compliance-monitoring features. Ovum strongly advises service providers to be accurate in marketing solutions that may address some of the requirements of GDPR, as this is the best approach for long-term credibility and reputational integrity.

Appendix

Further reading

The EU's General Data Protection Regulation, TE0007-001037 (August 2016)

EU's General Data Protection Regulation (GDPR) to have Greater Impacts on Enterprises, IT0018-001525 (April 2017)

Data Privacy Legislation Impact on Enterprises, IT0018-001493 (April 2016)

Author

Alan Rodger, Senior Analyst, Infrastructure Solutions

alan.rodger@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

CONTACT US

www.ovum.com
analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo