Ovum
TMT intelligence | informa

Making Sense of Compliance: Data Protection in the EU and Beyond

Best practices for compliance and corporate governance

Publication Date: June 18, 2018

Rik Turner

Ovum view

Summary

The European Union's (EU) General Data Protection Regulation (GDPR), a set of requirements imposed on organizations to guarantee the privacy of information on EU citizens that is in their possession, came into force across all 28 member countries on May 25, 2018. The GDPR covers all organizations, regardless of whether they have operations within the EU, requiring various organizational changes, such as the appointment of a data protection officer (DPO), and imposing potentially hefty fines for data breaches. It seeks to embed the concept of "data protection by design" into organizational management and operations for organizations that acquire personal data. In this white paper, Ovum looks at the impact of the new regulation on all firms operating in the EU, and how technology can help these firms comply with the regulation.

What is the GDPR?

The GDPR is a Europe-wide regulatory framework for the protection of citizen data across the EU. It was passed by the European Parliament on April 14, 2016, and was formally adopted by the EU on May 4, 2016. It represents the culmination of four years of intensive activity on the part of all three of the EU's governing bodies (Council, Commission, and Parliament) and came into force on May 25, 2018, giving organizations that operate within Europe (including companies and their supply chains) less than two years to prepare their data processing infrastructure for compliance.

The GDPR is designed to serve as an update, by way of complete replacement, of the EU's previous regulatory provisions for data protection, namely the Data Protection Directive of 1995, known as Directive 95/46/EC.

There was a growing consensus, prior to the publication of the first draft proposal for the GDPR in December 2011, that the Directive was falling short in its objective of protecting citizen data, primarily due to developments in technology. The Directive was issued prior to the advent of smartphones, cloud, big data, and social media, a few tech trends that have radically changed the way individuals interact with technology and, just as profoundly, the way companies do business. Add to this socio-economic changes such as globalization, business process outsourcing, and remote working, which have exploded over the last two decades, and the new challenges to data protection and the need to bring regulation up to date became even clearer.

This need was perceived to be so pressing that the EU decided not to issue a Directive but rather a Regulation. A Directive would require transposition into the national law of each member state and bring with it inevitable time lags and the potential for differences between countries. By contrast, a Regulation is a supra-national piece of legislation that comes into force simultaneously across all EU members, without the need for further legislative action by their respective parliaments.

In addition to its greater immediacy, this approach is designed to harmonize legislation across the EU by leaving no room for different interpretation by the various parliaments. To this end, a company operating in more than one member state will be able to select which national regulator (i.e. a data protection authority, or DPA) it wants to interact with for GDPR purposes; that regulator then becomes its "one-stop shop" for EU-wide compliance adjudication (although the debate continues as to how the one-stop-shop principles will operate in practice).

Beyond the GDPR and the EU

The GDPR's extraterritoriality already widens the universe of companies that need to be concerned about compliance with this particular piece of legislation, but the potential impact of the EU's regulatory effort goes even further.

There is clearly increased regulatory interest in protecting personal data, fueled in part by the headlines about allegations of state-sponsored mass surveillance and major data breaches in various countries. In this context, the EU's endeavors can be seen as the advance guard of further data protection regulation.

The rest of the world is watching the GDPR to see how successful it is in regulating data protection within the EU, and many lawmakers and regulators around the globe will be readying themselves to emulate some of its provisions.

What are the GDPR's key features?

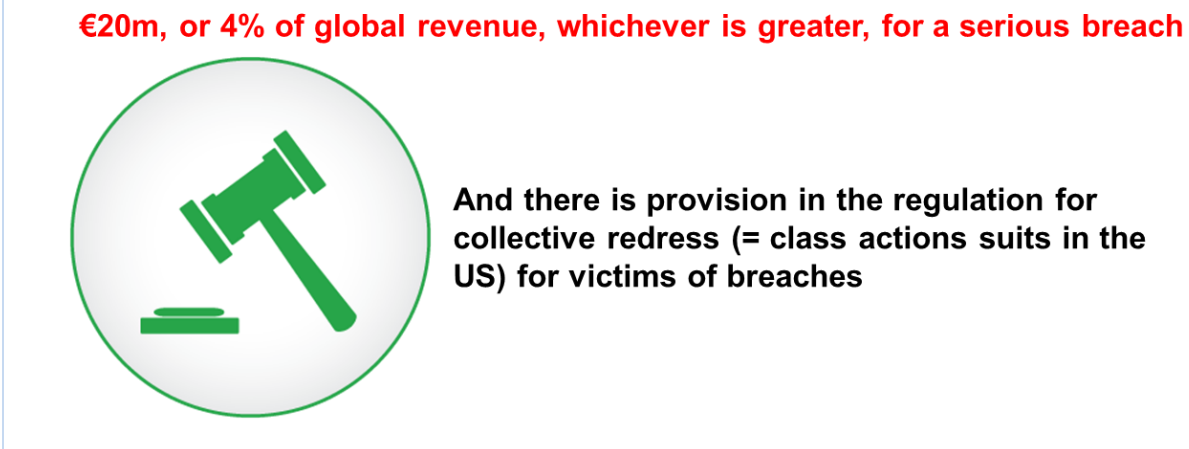
Potential fines become materially significant

The GDPR is designed not only to update the data protection legislation in the EU but also to give it sharper teeth. To this end, the fines for data breaches are far more draconian than those under the previous regulatory regime. The GDPR defines "personal data" as any information relating to an identified or identifiable natural person ("data subject").

Whereas the 1995 Directive was silent on the specifics of what constituted a data breach, the GDPR defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

For a serious breach, the legislation empowers a DPA to impose a fine of €20m or 4% of global revenue, whichever is greater. For example, if Amazon Web Services or Google were fined, the penalty would run into billions of dollars. While there may be room for negotiation as to what constitutes "serious," it is clear that the theft of data containing millions of credit card numbers or medical records would definitely fall into this category.

Figure 1: Serious fines



Source: Ovum

Breach notification is required within 72 hours

In the event of a personal data breach, notice must be given to the relevant DPA as soon as the controller becomes aware that a personal data breach has occurred, without undue delay and, where feasible, not later than 72 hours after having become aware of it.

If notification is not made within 72 hours, the controller must provide a "reasoned justification" for the delay. In the event of a data processor being breached, it has a responsibility to notify the data controller, which in turn is under the obligation to inform the DPA.

It is noteworthy that the present UK data protection authority, the ICO, imposed a penalty notice on telecoms operator TalkTalk in October 2016 for £400,000 for a breach of the UK Data Protection Act. This was due to TalkTalk's failure to adequately protect its customers' personal data from unauthorized access and deal with the security breach notification in a timely manner. Not only is this the highest fine to be imposed under the UK legislation to date, but it also represents a shift toward DPAs taking data breaches more seriously as the GDPR intends.

In the US in 2008, 134 million credit card details were exposed in a breach at Heartland Payment Systems, although it was not discovered until nearly a year later. As a consequence of Heartland being out of compliance with the PCI DSS standard for payment card processing, the company was prevented from processing payments until May 2009 and had to pay an estimated $145m in compensation, demonstrating the significant costs and reputational damage of such breaches, even without the additional penalties that the EU would have imposed had the GDPR been in force at the time.

Meanwhile, if the controller deems that a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, it must also inform the data subject(s) whose data has been breached, and this must be done "without undue delay."

There is an exception to the requirement for breach notification, which is when the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

There will clearly be much negotiation between DPAs and data controllers as to the interpretation of this clause, and Ovum's advice is not to rely on being able to invoke it in the event of a breach.

The scope of legislation expands in terms of function…

The GDPR expands significantly the types of companies that have to comply with the legislation in comparison with the 1995 Directive. In addition to what it calls "data controllers" (i.e. companies that collect personal data from EU citizens for commercial purposes, such as retailers, banks, and insurance companies), the advent of the world of cloud services means that the new legislation also covers so-called "data processors."

This refers to companies that have no commercial interest in the data per se, but who provide the computer or storage infrastructure whereby data controllers can manipulate it. In other words, the GDPR extends to cloud service providers (CSPs), who are thus subject to the same data protection requirements and potential penalties for breaches.

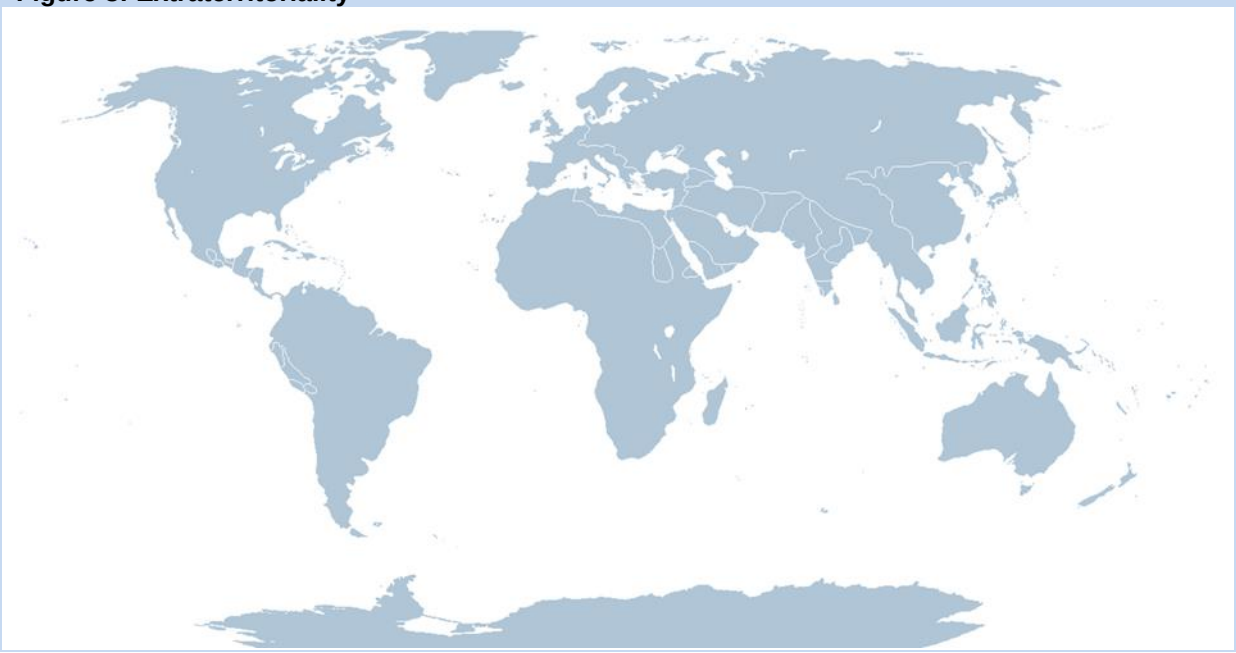
Figure 2: From data controllers to data processors

Source: Ovum

…and geography

The other major change in the GDPR is its "extraterritoriality," which means that it covers not only companies that are domiciled in the EU but also those that collect, process, and/or store EU citizens' personal data, whether they be data controllers or processors. In essence, this means the legislation is global in its jurisdiction and impact.

Figure 3: Extraterritoriality



Source: Ovum

Cross-border data transfers are strictly controlled

Another aspect of the geographical reach of the GDPR is in the area of cross-border data transfers. This refers to the situation in which a data controller or processor seeks to send EU citizens' personal data to a country or international organization outside the EU.

There are major implications here – for instance, when companies run data centers in multiple locations around the globe and routinely carry out data replication between them for disaster recovery/business continuity purposes. It is no coincidence that several major tech firms have in recent years announced investments to set up data centers in the EU, and the safest bet would be to carry out any replication of EU citizens' data between data centers within the EU, rather than involving any in other geographies.

The GDPR also stipulates that it is not lawful to transfer personal data out of the EU in response to a legal requirement from a third country. In other words, it is illegal for, say, a US company to send data on an EU citizen to servers in the US in response to an order from a court in its home country.

There are, of course, exemptions to these restrictions. A key one came in July last year, when the EU approved the so-called Privacy Shield agreement with the US, which is designed to supersede the Safe Harbor agreement. That agreement was ruled invalid by the European Court of Justice in 2015 after a private citizen in Austria sued Facebook in the wake of Edward Snowden's revelations of widespread and systematic surveillance of EU data subjects by US intelligence agencies. The Privacy Shield agreement is meant to address such concerns while enabling companies to make cross-border data transfers for legitimate corporate purposes.

Under the agreement, "the US has provided the EU with written assurance that the access of (US) public authorities for law enforcement and national security will be subject to clear limitations, safeguards, and oversight mechanisms and has ruled out indiscriminate mass surveillance of European citizens' data," according to a statement issued by the European Commission's Vice

President for the Digital Single Market, Andrus Ansip, and its Commissioner for Justice, Consumers and Gender Equality, Vera Jourova. A debate continues among the EU data protection authorities and law makers as to how robust the EU-US Privacy Shield agreement is in providing the necessary safeguards for EU personal data.

The concept of consent is now more restricted

The concept of data subjects' consent for the use of their data was already present in the 1995 Directive, but it has undergone considerable restriction within the GDPR.

Whereas the Directive made it possible for controllers to rely on implicit and "opt-out" consent in some circumstances, the GDPR requires the data subject to signal agreement by "a statement or a clear affirmative action." The new legislation also introduces restrictions on the ability of children to consent to data processing without parental authorization.

The Regulation states that consent must be "freely given, specific, informed, and unambiguous," explaining that a clear signaling action could, for instance, be ticking a box on a website or choosing the technical settings for information society services. However, pre-ticked boxes, inactivity, or silence on the part of the data subject will be considered insufficient evidence of consent.

With the expansion of legislation to cover data processors as well as controllers, the Regulation also allows for the splitting of consent to process the data and consent for data to be used for marketing purposes. Data subjects can even give consent to specific parts of the process. Clearly, there are challenges here, in that the subject can remove or change consent at any time. This means we may see more companies asking if they have the customer's consent to record on each and every call, requiring their technical infrastructure to handle stopping that recording on an ad hoc basis.

It is important to understand that, under the GDPR, it is not always necessary for the data subject to give their explicit consent in order to justify data processing. If personal data needs to be gathered, stored, and processed for contractual reasons or to satisfy legal obligations placed on the organization (such as a separate law or regulation that demands that certain data is recorded), or if there are legitimate operational or business reasons why the organization needs to process certain data (such as employee data required to operate the business), then it can be recorded without the need to gain explicit consent first. These distinctions are important as they can help support and simplify the approach needed for certain business-critical processes and activities.

Restrictions on profiling

In addition to restrictions on the geographical movement of data, the GDPR imposes limits on data profiling, which it goes into some detail to define. The legislation states that data processing may be characterized as "profiling" when it involves

- the automated processing of personal data
- the use of that personal data to evaluate certain personal aspects relating to a natural person.

The key word here is "automated," in that the GDPR only considers profiling to be the result of automated analytics processes, leaving companies free to carry out manual (i.e. human) analysis. Examples of profiling include the analysis or prediction of aspects concerning the natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

This is clearly of great concern to major web properties such as Amazon and Google, which have built a huge business from running analytics on the data they amass. They use this data to analyze how users behave on their websites and generate insights for actions such as targeted marketing and price differentiation strategies.

There are also implications, for instance, for best action activities in contact center environments. If someone has opted out or complained, there may be a need to change the way that data is presented.

While profiling is not expressly prohibited altogether, the GDPR states that a data protection impact assessment should be made where personal data are processed for making decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data.

Furthermore, certain sections within the Regulation specify that the data subject has a right to be informed of the consequences of such activity. Indeed, they make it clear that the controller must disclose "the existence of automated decision-making, including profiling," along with "the significance and the envisaged consequences of such processing for the data subject."

Data subjects also have the right to object to "profiling to the extent it is related to direct marketing," thus halting profiling and avoiding the consequences of any profiling-based decision. In concrete terms, this would mean that someone could not suffer "automatic refusal of an online credit application or e-recruiting practices without any human intervention."

The Right to be Forgotten (RTBF) and the right to data portability

In order to expand individual control over the use of personal data, the GDPR also introduces two new rights for data subjects: the Right to be Forgotten (RTBF) and the right to data portability.

The Regulation formally creates the Right to be Forgotten (RTBF, also known as the Right to Erasure), following on the recognition of a similar right in a 2014 case brought before the European Court of Justice. This right allows individuals to request the deletion of personal data, and where a controller has publicized the data, it requires other controllers to also comply with the request.

This is a major operational issue, as it means that the controller will need to be able to locate every instance of that data within its own infrastructure (which may well be held in one or more public clouds). The controller will also need to be aware of every other controller that has a copy of it so as to notify them of the need to delete it.

The GDPR creates the right to data portability, which requires controllers to provide personal data to the data subject in a commonly used format, and to transfer that data to another controller if the data subject so requests.

Companies must appoint a data protection officer

Another key provision in the GDPR mandates that a data protection officer (DPO) should be appointed at any data controller and processor whose activities involve "regular and systematic monitoring of data subjects on a large scale," or if the entity conducts large-scale processing of "special categories of personal data" (such as data revealing racial or ethnic origin, political opinions, and religious or philosophical beliefs). The responsibilities of a DPO will be

- to inform and advise the controller or processor and its employees of their obligations to comply with the GDPR and other data protection laws

- to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, training data processing staff, and conducting internal audits
- to advise with regard to data protection impact assessments when required under Article 35
- to work and cooperate with the controller's or processor's designated supervisory authority, and serve as the contact point for the supervisory authority on issues relating to the processing of personal data
- to be available for inquiries from data subjects on issues relating to data protection practices, withdrawal of consent, the Right to be Forgotten, and related rights.

An early draft of the GDPR limited the requirement to appoint a DPO to companies with more than 250 employees, but the final version has no such restriction. Companies of any size have to appoint a DPO.

How technology can help with GDPR compliance

Once an organization has identified what information actually constitutes personal data, for how long that data has a legitimate use, how it can be secured, and how it can be provided to the citizen, the next question is how this process will be managed and the data identified.

The sponsor of this white paper, Verint Systems, offers its Customer Analytics and Compliance platform to address this data management challenge.

- The Regulation cites encryption as a key way to protect data. With data protected through encryption from the point of capture, it is secured whether at rest or in transit, right up to the point of recall.
- The system provides the ability to search and recall engagements wherever there is a personal identifier associated with the data. Historically, many such interactions are not marked with the customer's identity; therefore, the extensive integration capabilities of the platform, including the ability to capture identification data from the agent's screen, enable the organization to identify at a basic level whom the data is related to.
- Not all interaction data contains the same level or types of personal data. The ability to identify and categorize non-structured voice and text content into a form that allows appropriate handling is a key requirement. Through Customer and Desktop Analytics, the additional context required to manage the data appropriately, based on areas such as level of risk and legitimate use, is made available.
- The platform's archival and export capabilities further provide the ability to manage the retention of captured data based on its categorization. This enables an organization to keep the personal data only for the time it is required and minimizes exposure of redundant data. It also enables interactions to be exported for provision to the citizen, or to an alternate supplier, in standard formats.
- Automated Verification tests and verifies systems across multiple applications (e.g. ACD, IVR, recording, desktop applications, routers, firewalls) to ensure optimum operation and supports regulatory compliance. It actively checks systems for issues and proactively simulates user transactions to validate performance, providing enhanced control and awareness of system health, status, and performance to avoid issues with service availability, data integrity, and data breaches. For GDPR, this helps ensure optimum operation and support.

- Organizations that use Microsoft Skype for Business or Cisco Jabber as part of their customer and enterprise communications can also now benefit from Verint Recording to address their collaboration technology compliance needs. Interactions from across the enterprise – from contact centers to back-office operations, branches, and trading floors – and across a wide range of communication modes including newer collaboration capabilities, can all be captured using these capabilities. For GDPR, this means all interactions which involve protected data are properly archived or deleted.
- Although the product suite offers strong analytical and automation capabilities, these need not cause problems with the GDPR's prohibition on profiling (described earlier). Whether optimizing employee scheduling or automating quality monitoring, at each point recommendations can be delivered to a manager for selection and execution, thus ensuring that the regulation is complied with.

Customer analytics has traditionally been used to help organizations understand the voice of their customer for operational improvement programs, but with data privacy becoming a hot topic from both a legislation and a customer concern perspective, this analysis brings an additional level of understanding and management capabilities to an organization.

A word on Brexit – Beware the data residency issue!

On June 23, 2016, the UK voted to leave the EU, raising obvious questions regarding the future of the country's financial sector and whether or not it would need to comply with regulation emanating from Brussels. The leaving date currently stands at March 29, 2019.

While the full repercussions of Britain's exit from the EU will only become clear over the coming months and years, the country will of course seek a trade agreement with the EU that will enable it to sell into and buy from member states on favorable terms. Judging by the example of other non-member countries such as Norway and Switzerland, the likelihood is that the UK will not only have to continue to contribute to the EU's budget, but will also have to remain in lockstep with the EU on matters of regulation in order to benefit from any preferential treatment in trading with the bloc.

There is, of course, a potential impact of Brexit for companies headquartered outside the EU, namely an issue of data residency. If they have a data center in the UK, any personal data on EU citizens that is sent to that facility would fall into the category of a cross-border transfer; that is, the data would be leaving the territory of the EU.

Thus, even if a company's principal European data center is, say, in Germany, it would need to be aware that any replication of the EU citizens' personal data to the UK facility, for instance for purposes of business continuity, could be in violation of EU restrictions on where such data can be transmitted to and where it can reside.

Appendix

Author

Rik Turner, Principal Analyst, Infrastructure Solutions

rik.turner@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