GDPR, Brexit and the shifting landscape for EU data regulations

Reproduced by NTT Communications with kind permission from 451 Research

By Penny Jones @ 451 Research

The EU's General Data Protection Regulation (GDPR, or Regulation 2016/679) was published on May 4 in the Official Journal of the EU. This set the time frame for when the regulation would come into effect. Companies – be they service providers, enterprises or otherwise – must comply by May 25, 2018. This provides two years to ensure compliance, but there will be ongoing concerns over interpretation at global, EU and national levels.

Hefty fines following a points-based system will be handed down for noncompliance (e.g., for data loss, fines are set at a maximum of 4% of worldwide revenue, with a cutoff of €20m [$20.8m], and in some cases this will be 2% of annual revenue and €10m, depending on the gravity of the situation).

This means GDPR is a regulation that every company dealing with personally identifiable data of EU citizens – from payment card data to information processed in the cloud – will need to be paying close attention to.

We covered GDPR when it was a draft in December 2015

There have been some updates, which we will highlight in this report. We will rehash the leading requirements as they relate to the service-provider industry and look at some of the reactions so far, taking into account the UK's vote to leave the EU (Brexit) and why this doesn't exclude UK companies from compliance.

In this report, we will also look at national reactions (important because national Data Protection Authorities [DPAs] will police the regulation) and some of the requirements companies should start considering now, including the hiring of a data protection officer (DPO) to manage and provide guidance on compliance.

The 451 Take

A lot has changed regarding data regulations in Europe through 2016, and uncertainty still abounds as a result. That is no excuse, however, for companies holding off on developing processes for compliance.

It will be the onus of anyone dealing with data to ensure they have a documented way of proving to law enforcers that they have made suitable efforts to comply with GDPR (even if it is by their best interpretation) or face hefty fines.

Companies, governments and industry bodies are all looking to release guidelines that can help clear the murky waters, and companies and service providers should pay close attention to these.

Over time, we expect to see certification bodies such as the Payment Card Industry also look to reduce risks through new offers of accreditation. Companies and service providers need to remember that GDPR is wrapped in processes, and for now compliance will be valued in the ability to document and prove the efforts they have taken to become compliant. This will lead to discrepancy, for certain, but also leaves companies with the ability to mold practices in the way that enables them to best do business while protecting citizen data.

GDPR Rehash

The GDPR applies to organizations processing data inside the EU, and those outside that offer goods or services to EU citizens. It is broken down by 'controllers' – those that say how and why personal data is processed – and 'processors' – those that act on the controller's behalf, such as a cloud or other service provider.

Processors are required to maintain records of personal data and processing activities, and are legally liable if there is a breach

They have an obligation to maintain written records of processing activities carried out on behalf of the controller, designate a DPO (more on this later), appoint a representative in the EU when not operating in the region and establish processes for notifying the controller of a breach without undue delay.

They will need to carefully consider supply and other commercial agreements.

Controllers are required to ensure contracts with processors comply with the GDPR

They must maintain certain documentation, conduct a data-protection impact assessment for more risky processing, and implement data protection 'by design and default.'

The original GDPR draft required controllers to notify or seek approval from the DPA for a range of activities – this requirement has been removed, with data controllers now required to put in place effective procedures and mechanisms focusing on more high-risk operations (such as those involving new technologies), and to carry out protection impact assessments to ascertain the severity of a risk.

A DPA could require notification if the processing is seen to result in a high risk, and may provide written advice and use enforcement powers if necessary. (For this reason, it is essential to sign up for notifications and guidance.)

Providing services inside the EU from outside

For those providing services to citizens inside the EU (even if free) from outside, a representative in the EU could be required. 'Offering of services' can be evidenced by the offering of goods or services, and can be seen through use of local language or currency on sites where goods can be ordered, for example. It also applies where any form of activity can be seen as the monitoring of an individual's behavior.

The GDPR applies to 'personal data,' which can include a range of information; such as personal identifiers (e.g., IP addresses and HR data), customer lists and contact details, with both automated personal data and manual filing systems. It also imposes restrictions on the transfer of data outside of the EU.

Transfers can take place where the European Commission has identified a third country or territory as having adequate levels of protection, or where compliant with Chapter V of the GDPR.

In many cases, transfers will be done using legally binding agreements, binding corporate rules, template transfer clauses adopted by the Commission (or a supervisory authority approved by the Commission that provides standard data-protection clauses or approved code of conduct), or a certification mechanism provided for by the GDPR. Transfers largely require an individual's informed consent.

Additional Considerations

Other key considerations in the GDPR that controllers and processors must be aware of include: the right to data portability (which allows citizens to move data from one SP to another), the need to document operations (including categorization of the different types of data collected and time limits for erasing this), the right to be forgotten and the right to know when you are hacked (within 72 hours from the time a processor or controller becomes aware of a breach).

GDPR and Brexit

It would be easy for many companies to assume that - provided the UK hits the button on Article 50 and begins the process of exiting the EU - UK organizations won't need to comply with EU regulations like the GDPR. But the Secretary of State, Elizabeth Denham, has publicly highlighted that it will take two years to implement Brexit once Article 50 is triggered, meaning the UK will still have to comply with EU regulations.

The Information Commissioner’s Office

The Information Commissioner's Office (ICO) says that, for this reason, the UK will implement GDPR and then look post-Brexit at how it might be able to rework requirements, with the focus being on maintaining high levels of data protection.

The ICO will be prioritizing some areas of the GDPR and releasing a paper on this over the coming months; this will offer guidance on how UK companies can be compliant. It is not surprising. The UK had a considerable part to play in the forming of the GDPR, and government bodies including Tech UK have highlighted a need to provide adequate data-protection regulations to ensure the industry is viewed as a 'safe' destination for EU data.

It is expected that any regulations that are born post-Brexit will have a similar emphasis on protection, and could possibly benefit from improved back-office methods and reduced complexity. Either way, many believe that in today's data-driven world, protection at this level is simply good governance – 'privacy by design' should increasingly be a part of the service-provider and enterprise strategy, and measures need to remain in place to protect data from breaches.

GDPR and sovereign states

The European team behind the GDPR worked hard to ensure the regulation could help make Europe more competitive as a region providing a one-stop shop for data protection across Europe. But the final GDPR document includes a large amount of buy-in at the country-by-country level (each country can layer its own regulation on top of the GDPR after it has been adopted if the regulation does not impede the requirements of European law).

Furthermore, it will be the appointed DPAs in each country that will police and guide interpretation of the regulations on a country-by-country (or in some cases region-by-re-gion) basis. The thought is, as a result, that local data protection requirements will vary slightly by country – just how, in many cases, it is too early to tell, but some countries have provided indications of the direction they are likely to take.

German DPAs

German DPAs (Germany has 10 DPAs, each representing a different region), for example, are reviewing their take on cloud computing and trans-border transfers of personal data.

They are concerned that more international transfers of German personal data are taking place, and as a result have already sent questionnaires to 500 German companies covering the types of services and products used for such activities and the legal ground behind each transfer. It is mostly focusing on marketing, recruiting, cloud storage, internal communications systems and intra-group data transfer.

The idea is to find out how companies comply with European data protection law, but responses can also lead to ongoing investigations and eventually administrative fines of up to €300,000. The questionnaire is also focusing on the US Privacy Shield, and contractual clauses and other mechanisms used for transfer of data.

French DPA

The French DPA (called CNIL – commission nationale de l'informatique et des libertés) has also launched a public consultation on four priority topics related to the GDPR. It is collecting questions and concerns from organizations and individuals in regard to the GDPR's interpretation, to gather insight to take to the Article 29 Working Party on where further guidance might be required.

The CNIL is focusing on a number of areas, including data portability (benefits and limitations), the privacy impact assessments (the scope of the obligation, who should be involved in conducting assess-ments), certifications (who will issue these, what products and services they will include, and specific SME needs for certification) and the requirement for a DPO (qualifications required, how one is resourced, and what tasks or powers they should have).

Its efforts tie in with the CNIL's 'digital safe' label, which it says certifies organizations for offering a secure digital storage location only accessed by particular users.

Similar to Germany, the French government is expected to push local buy-in for regulatory purposes, promoting sovereign storage of data as the only true way the government can have control over the protection of data.

Complications due to international differences?

Many companies are concerned that added complexity could come about due to the international differences that will be seen through DPA and government involvement in regulation on top of GDPR.

Controllers are first regulated by, and answer to, the DPA or other lead supervisory authority for their main or single establishment. They then cooperate with all other concerned authorities – for example, where cross-border transfers are concerned.

This follows a cooperation procedure that involves a lengthy decision-making process, and there is the right to refer the case to the European Data Protection Board, while provisional measures can be adopted to protect the rights and freedoms of data subjects in the interim.

It will be up to controllers and processors to choose which member state will be their lead supervisory authority (and this could change from customer to customer), which means careful consideration will need to be given to all guidance issued in coming years.

High demand for DPOs

One of the biggest initial (and ongoing) costs for companies adhering to the GDPR will be the new requirement for a DPO – a specialist in privacy protection. Last estimates by the International Association of Privacy Professionals show that 'at least' 75,000 DPOs could be required globally (keeping in mind that companies from around the world will be dealing with European data for various reasons).

The requirement is for public authorities and companies processing personal data at a large scale (meaning most small businesses are exempt) to have a DPO with privacy law knowledge that is independent of the organization.

These positions are already common in France, Sweden and Germany, but demand in other markets could mean these positions are pushed to a premium, and questions will remain as to whether there are enough suitable candidates to go around.

The estimates for DPOs

In Europe estimates by the International Association of Privacy Professionals are that roughly 11,800 nonfinancial, private sector enterprises will require a DPO. And in the US, about 9,000 US companies will need to hire for the position.

Questions will be raised as to the role of the DPO

To date, 40% of companies questioned say they plan to make their current privacy leader a DPO, but 50% say they will appoint someone on the privacy leader's team or train someone within the organization.

So far, fewer than 10% of IAAP members say they will outsource the role. (It is important to note that these responses are from members, many of which are already aware of privacy issues.) We suspect there will be many companies just starting to consider this requirement and needing guidance from their DPA – their buy-in to what the role will require could be crucial.

The IAAP says that, in most cases, the average privacy office in a company has only existed for six years, and so far, the GDPR states that a DPO requires 'sufficient expert knowledge.