GDPR: Personal Data, Global Impact

Sheila M. FitzPatrick
Chief Privacy Officer
NetApp

proximus

With new requirements for organizations and new rights for individuals, there is no doubt that the European Union's General Data Protection Regulation will deeply impact every organization, regardless of whether or not they have operations in Europe. We have asked Sheila FitzPatrick, one of the world's leading experts in data protection laws, to share with us her insights and experience on how to best apprehend the changing landscape of data protection and prepare for what appears to be a profound shift in the way enterprises handle personal data.

"If you have access to personal data of any EU citizen, provide a service to EU citizens, employ EU citizens, capture EU citizens' personal data, you will have to comply with the new regulation, even if you don't have a physical presence in the EU", says Sheila FitzPatrick. This makes de facto the GDPR a global data protection compliance challenge, and time is running out to meet it as the new data protection regulation will come into effect in May 2018. "And if you violate the regulation, the sanction can be up to €20 million or 4 % of your global annual revenue, whichever is highest. So, this new regulation is quite extensive and it will have a particular impact on data processors, data centers, cloud services providers and their customers", she adds.

The new European regulation introduces a massive change in the way organizations are collecting, processing, accessing, using, storing, or transferring personal data. Many businesses will need to understand their obligations under the GDPR and adapt their services, contracts and processes accordingly. Those that get on top of understanding the importance of compliance and the basis of that compliance will gain a competitive edge over other players in the market.

Creating Trust by Design

One of the most important changes introduced by the European legislator is the **broadened definition of personal data**. Under GDPR, any data that might identify an individual is now considered personal data. "Unique identifiers, location data, biometric data, genetic data and data relating to the cultural or economic aspects of an individual now come within the remit of the law. Even an IP address will be considered as personal data", Ms. FitzPatrick underlines.

The GDPR principle of **data minimization** is more stringent than the previous European data protection regulation. "If personal data are not an absolute must for managing the business - or employment - relationship, companies should refrain from collecting them", Sheila FitzPatrick recommends. Not only must data controllers - the individual or the legal person who controls and is responsible for the keeping and use of personal information - restrain from keeping data for any longer than necessary, but they must also avoid altering the use of the data they have collected without requesting the explicit and freely-given consent from the data subject - the individual who originates the data - for the new or extended usage. Data subjects have a new **right to be forgotten** and organizations must have in place clear processes for deleting individual

data subjects on request. "Enterprises will have to ensure transparency around the justification for collecting, storing and processing personal data, what they are going to do with them and whether those data will be transferred outside of the country of origination. And If you don't imperatively need to collect personal data, don't do it: use aggregate, statistical or anonymous data instead", Sheila FitzPatrick advises. Under the GDPR, organizations will have to get the balance right between retaining data for discovery purposes and data minimization.

The right to be forgotten - or right of erasure – will pose a serious challenge to every organization. This is why, when designing solutions, engineers and developers need to think about the ability to destroy the data when they are no longer needed. Depending on the application or what the cloud services provider offers, deleting every bit of personal data may be difficult since the information can be copied, backed-up and redistributed into multiple places. "It means that whenever you develop a new application or implement a new system that will likely have an impact on personal data, you must conduct a **Privacy Impact Assessment** in order to determine if using those data is well-founded with regard to the service that you provide", says Sheila FitzPatrick. The PIA should provide a clear picture of the location of all the data in the organization and map out every data flow. However, any investment in resources to automate data discovery ahead of GDPR will pay dividends later on by reducing discovery overhead cost.

The crippling fines for transgressing GDPR pose a major risk to any company. Top management needs to take a lead on driving within the organization the **privacy by design** approach mandated by the new regulation. This means that any initiative to redesign business processes or collect new data must be thought of with GDPR compliance in mind from the start.

Security doesn't Guarantee Privacy. But it Helps

The GDPR requires public authorities processing personal information to appoint a **data protection officer** (DPO), as well as other entities, when core activities require regular and systematic monitoring of data subjects on a large scale or consist of processing on a large scale of special categories of data. According to a study by the International Association of Privacy Professionals (IAPP), this requirement means that, in Europe and the US alone, 28,000 DPOs will have to be appointed in the next two years.

The new legal framework also introduces the concept of **personal data breach** into the European law for the first time, and specifies notification requirements to both the supervisory authority and affected data subjects. "In the event of a personal data breach, data controllers must notify the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it", Sheila FitzPatrick explains, adding that "if the controller has determined that the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, it must also communicate information regarding the personal data breach to the affected data subjects". And when a data processor experiences a personal data breach, they must in turn notify the controller. One question that Sheila FitzPatrick is frequently asked is "what is the difference between privacy and security?" Actually, if **privacy** and **security** are inter-twined they are not identical, far from it. "You can have world-class security and absolutely no privacy", she says. "As an analogy, you can compare data privacy with a wheel, where the entire wheel represents the full life-cycle of the data. Security is just one spoke of that wheel and if you only take that specific spoke into account, the wheel is going to break. Of course, security is extremely important because you need to lock down your data. But if all you do is encrypting data that you should never have collected, you don't comply with your privacy obligations".

Choosing a Trusted Cloud Services Provider

Although the GDPR is primarily a legal and compliance issue, technology and tools will play a pivotal role in helping organizations maintain compliance with the GDPR requirements. The GDRP separates responsibilities and duties of data controllers and processors, obligating controllers to engage only those processors that provide sufficient guarantees to implement appropriate technical and organizational measures to meet the GDPR's requirements and protect data subjects' rights.

The GDPR extends the liabilities associated with processing data. Companies that provide services based on processing data on behalf of their customers – and potential sub-contractors of those providers - must understand clearly their responsibilities and the rights of data subjects.

"You need a partner that can help you navigate through the challenges of putting data in the cloud from a data privacy prospective. You can't just make the decision based on cost, flexibility, and scalability only: you have to put data privacy into that equation. By doing so, you will not only avoid heavy financial penalties, you will also help your organization achieve new competitive advantages", Sheila FitzPatrick concludes.

Sheila M. FitzPatrick has over thirty years' experience as an international employment and data protection attorney. She is considered one of the world's leading experts in data privacy laws and works closely with the US Government, Council of the European Union and national data protection agencies in Europe, Asia/Pacific, and The Americas.

Ms. FitzPatrick currently works with NetApp as their global Data Governance and Privacy Counsel and Chief Privacy Officer. She is responsible for NetApp's worldwide data privacy compliance program that includes responsibility for compliance with global laws related to data protection, data sovereignty, cybersecurity, data breach notification, cloud computing and records management.

NetApp is considered a role model with regards to GDPR because the company has taken a data privacy first approach and has gone to the extent of implementing Binding Corporate Rules (BCRs) in every country of operation. NetApp has built a robust, proactive, global data privacy compliance program - rather than a US-centric approach - that has positioned the corporation as a trusted advisor in the data privacy space.

Appendix: **European Commission's GDPR Infographic**

This infographic published by the European Commission offers an overview of the General Data Protection Regulation, including what information constitutes personal data, the reason for the change, companies' obligations and the cost of non-compliance:
http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_en.htm

More information?

Get in touch with your usual Proximus contact person or surf to **www.proximus.be/gdpr**