EU Data Protection's Paradigm Shift

From Directive to Regulation

ERNST & YOUNG
Quality In Everything We Do
EU Data Protection’s Paradigm Shift
From Directive to Regulation

Author: Lindsey Lynch | Risk Manager, Advisory Services | Ernst & Young The Netherlands

As technological times evolve into a whirlwind of cloud computing, social networking and online services, traces of personal information are continuously collected and stored. Nowadays, privacy concerns are stepping into the compliance spotlight as the previous data protection principles move towards more restrictive and enforceable rules. The future shift from Directive to Regulation has executive management worried about compliance questions becoming more urgent: do our organizations have control over the technologies and processes in place which collect, use and store personal and sensitive data? Moreover, are we prepared for this shift from Directive to Regulation?

What’s changing: Shift from Directive to Regulation

As of January 2012, a major turn was undertaken by the European Commission in an effort to devise a single uniform data protection policy which applies to the European Union as a whole. With the aim of raising the bar and strengthening individual privacy rights, the rules will define consistent EU protection standards for EU member states collectively. This was a necessary shift as the previous Directive left room for member states to interpret the guidelines inconsistently and introduce inefficient measures in an effort to comply.

Although the main principles from the 1995 Directive will still apply, the new Regulation is more focused on enforcing and standardizing the control that data subjects have over their personal data. Under stringent EU legislation, personal data can only be collected subject to strict conditions, for legitimate purposes only. Therefore, organizations which manage personal data must respect the rights of the data subjects in the collection, storage and maintenance of sensitive personal data. The European Commission’s new slogan is that “protecting your data is a personal fundamental right, the free flow of personal data – a common good!” This change will prompt organizations to create more transparency in the way they manage their privacy programs in the responsibility domain.

While most organizations have introduced policies outlining how Personal Identifiable Information (PII) is processed, this will not be sufficient when it comes to complying with the proposed Regulation. Going forward, organizations will be moving in the direction of having structured and documented procedures, in other words a data protection framework that demonstrates how personal data is safeguarded. This will provide stakeholders with the confidence that PII is properly treated in line with their expectations and allows organizations to demonstrate compliance with the Regulation in the future.

Data Privacy

The rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal data.

- **Data Subject**: individual to whom personal data relates.
- **Data Controller**: person (individual/company/organization) that determines the purpose for and manner in which personal data is, or will be, processed.
- **Data Processor**: individual who processes personal data on behalf of a data controller.
- **Personally Identifiable Information (PII)**: any information that can be used to identify, contact, or locate a data subject.

Organizational Impact & Consequences

Due to the shift from Directive to Regulation some major changes are expected, which will have a significant impact on EU companies. A few of these changes are summarized below.

Single set of data protection rules in the EU

Under the new proposal, there will be a single set of privacy rules, which will be valid and enforceable across the European Union. This means that organizations will be answering to a single data protection authority in the EU. Additionally, these rules will apply to companies established outside the EU if they offer goods or services within the EU or process personal data of EU citizens.

Increased fines

Penalties for data privacy breaches will come into effect, which means fines from the Data Protection Authority could be as high as two percent of global annual revenue. Consequences of a data protection breach can attract a high level of attention from all stakeholders and supervising authorities. Public press statements could lead to a loss of customer confidence. Obviously, a loss of customer trust in an organization’s brand and reputation, accompanied by a material fine, could have a significant impact on an organization’s current and future success in the market.

Right to be forgotten

The ‘right to be forgotten’, or the right that a data subject holds to request that their information be deleted completely from wherever it is stored by the data controller, will come into effect. In order for an organization to manage the deletion process, it must first be able to manage the collection and storage of the sensitive data. In other words, organizations should have an established understanding where all the data flows and is stored in order to take the steps necessary to delete it from all the respective locations.
Mandatory Data Protection Officer
What used to be an optional Data Protection Officer under the Directive will now become obligatory under the proposed Regulation. It will require that, if you are a public company, if data processing is your main business or if you have more than 250 employees, you must have a Data Protection Officer to manage the organization’s data protection program. Additionally, Data Protection Officers must comply with the qualifications needed to perform this role and possess the skills necessary to carry out the job. They must be independent of management and have the task of making sure that the organization complies with the Regulation on behalf of management.

Mandatory Data Privacy Impact Assessments
Under the proposed Regulation, Data Privacy Assessments (DPIAs) will be a requirement for organizations that perform data processing going forward. DPIAs should be conducted by data controllers and processors prior to processing personal data. These assessments can be a great starting point in assessing where an organization stands in terms of its data protection program. A DPIA should include safeguards and mechanisms for ensuring the protection of PII. For example, an evaluation of how the data will be processed and further if the process involves risks for the data subject and PII being exposed in any way.

Increased accountability and responsibility
The new Regulation proposes increased responsibility and accountability for the processors of personal data. The draft EU Regulation states, in Article 22, that "the controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation".

Although the Regulation is still in the drafting stages and not expected to be finalized before 2014, companies are looking to brace themselves now by considering where they stand with their current data protection programs and taking the necessary measures to prepare for compliance in order to avoid the steep consequences in the future.

Assessment considerations: Is your organization ready for the shift from Directive to Regulation?

- Does the organization have cohesive and accurate accounting of its processes that use personal identifiable information, and of the controls and compliance environments that govern the information’s use?
- Does the organization have a statement of business rules related to the use and protection of personal identifiable information which is understood by the people who use the personal identifiable information (employees, agents and customers)?
- Have roles and responsibilities been defined regarding accountabilities and authorities for the use and protection of personally identifiable information? Has the organization formally established a governance structure and roles and responsibilities to ensure that it maintains compliance with its policies and applicable laws and regulations?
- Is an overall approach for managing privacy risk and compliance in place across the organization which addresses the use of technologies and deals with cross-border and multi-jurisdictional challenges?
- Have third-party risk management processes been considered for privacy risks, including performing due diligence during the selection process, putting controls in place – both contractually and for the secure transfer of the information – and building a solid basis of confidence that the third parties using the personal identifiable information can protect it and govern its use?

Preparation: Governance is Data Protection’s Future State
In order for management to have robust governance over data protection, its goal should be to proactively identify the risks and give proper assurance that controls are in place in order to demonstrate future compliance as the Directive shifts into a Regulation. However, due to the uncertainty of what the end product will be after the Regulation is finalized, many organizations are currently holding back on addressing compliance to the Regulation now.

What organizational front runners are opting for instead is taking a good look as to how their organizational data protection is currently structured and operating by performing a data protection program assessment. In so doing, an organization will gain a clear understanding of how sensitive data flows through the company in the various scenarios, paired with a clear overview of the processes (or the lack thereof) in place to control the data. This will allow an organization to quickly and efficiently react, once the Regulation comes into effect, in order to comply.

The challenge that clearly lies ahead will be whether the organization identifies all the areas, or scope, in which the data protection rules will be applied and implemented at a future stage and, of course, what the final Regulation will look like. However, having a structured understanding and overview of the organization’s current program will give companies significant leverage, as a starting point, to cope with the future state of data protection in the EU.
Contacts

**Tonny Dekker**  |  Risk Leader Belgium and The Netherlands  
+31 88 4071004  
Tonny.dekker@nl.ey.com

**Lindsey Lynch**  |  Risk Manager  
+31 88 4071528  
Lindsey.lynch@nl.ey.com

**Nora Boukadid**  |  EMEIA Lead Data privacy  
+31 88 4073082  
Nora.boukadid@nl.ey.com

**Peter Kits**  |  IT and Privacy Law Specialist  
+31 88 4070018  
Peter.kits@hollandlaw.nl

Ernst & Young

Assurance | Tax | Transactions | Advisory

**About Ernst & Young**
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 167,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

© 2013 Ernst & Young LLP.  
All rights reserved.

www.ey.com/nl