How to deal with the new requirements of the Privacy Regulation?

24 February 2016

On 15 December 2015, the final text of the EU General Data Protection Regulation (GDPR) has been made available. The expectations are that the GDPR will be formally adopted in April 2016 and will come into force two years and twenty days after the date of publication. Organizations should start preparing now, but there are still a lot of questions and concerns with regard to the practical approach of the GDPR.

In this context, ADM organized a session on how to deal with the new requirements of the GDPR, where six discussion groups each covered a different topic that organizations must know about. For each of the topics, you will find below the major concerns / reflections made by the participants during the session.

Transparency and Consent

One of the discussion groups covered the topic of transparency and consent. The participants voiced concern about the behaviour of Google and Facebook, as they appeared somehow reluctant that something would really change in the behaviour of those big companies with the introduction of the GDPR, especially in the way they collect consent. In general, the attendants were not aware of the changes that the GDPR will bring on consent and transparency requirements and are not yet working on the review of their privacy notices or consent mechanisms. Several participants indicated that they would first need to create an overview of what everyone in the organization is doing with personal data and put that in an inventory, before they would be able to update their privacy notice.

Data Subject Rights

Another discussion group covered the data subject rights, and in particular the right to be forgotten and the right of data portability. Here, the participants had a feeling of unease and a lack of preparedness to handle the various data subject rights. Most participants realize that they had not come into contact with the various data subject rights so far. However, this might change in the future with the increasing privacy awareness in Belgium and the attention in the press. Participants hoped that additional guidance would be made available on several topics, including the right of data portability and restriction (e.g. how to do this technically) and the right of erasure (or to be forgotten) (e.g. what to do with old systems and back-up tapes).

International Data Transfers and Managing Service Providers

In a third discussion group, questions and concerns were raised on international data transfers and managing service providers, a hot topic due to the invalidity of the Safe Harbor regime since October 2015. The GDPR continues the current data transfer mechanisms (and expands a few), but also puts a lot more emphasis on taking accountability over its service providers. In this context, it is important make a clear distinction between three types of actors, being controllers, processors and joint-controllers. In every relationship between these different actors, a set of contractual clauses is needed, also within a company group. In addition, under the GDPR, the emphasis in such clauses is put more and more on the individual. On international data transfers, data protection authorities are now heavily pushing for the use of EU model contracts or Binding Corporate Rules (for intragroup transfers). We will see how the EU-US Privacy Shield (Safe Harbor 2.0) will have an impact.

Data Breach Notification

Data breach notification is another hot topic under the GDPR that was covered by one of the discussion groups. First, the participants stated that the new regulation is unclear with regard to the data breach notification duty, for example how the concepts "without undue delay" and "where feasible" should be interpreted. As a second conclusion, companies should understand the advantage of having a data breach notification procedure, even though the implementation of such a procedure takes a lot of work and time. This means that companies need to take preventive actions, put preventive systems in place, and make practice policies or e-learnings for example, to enable a quick and efficient response.

Privacy Impact Assessments and Privacy by Design

Questions that were raised in a fifth group, focused on data privacy impact assessments (PIAs) and privacy by design. The experience of the participants was very diverse. On the one hand, certain companies see DPIAs as a lot of work, where on the other hand there are companies that perform PIAs at the start of every project. Considering PIAs are a good tool for demonstrating Accountability, integrating privacy impact assessments in other risk assessments of project or software development phases, will be a focus point of many organizations in the coming years.

Privacy Responsibilities and Data Protection Officers

In a last discussion group, participants took a look at privacy responsibilities, and in particular the role of Data Protection Officers (DPO). Participants indicated the following:

- more clarification is needed on the conditions in which the appointment of a DPO is necessary (e.g. what is "on a large scale").
- Considering the GDPR requirements, larger organisations would likely need a full-time DPO.
- Many participants have not yet taken a decision and are looking into the options for appointing a DPA. Many suggested that the role of a DPO should be located within the risk/quality department, the compliance department, internal audit or in the legal department. The link was made to the "informatieveiligheidheidsconsultent" who currently often deals with data protection, but whose role is not the same as the DPO's. Several questions were asked on the independence of the DPO, such as when the DPO would be located in the IT department.
- In order to monitor DPOs and compliance with the GDPR, DPA investigations could be launched or specific seals and certification programmes should be developed.
- The GDPR and the appointment of a DPO will help to get things moving in the right direction within the organisation where the leadership may not have prioritising privacy issues.

Conclusion

Most participants expressed that the high fines could be used for encouraging privacy compliance within their organization. Even though several organizations did not start preparing yet for the entering into force of the GDPR or are on 'stand-by' to see how things will develop, most participants believe that the GDPR will help to get things moving in the right direction with regard to privacy.

Thanks

The discussion session on 24 February and the above write-up was made possible by:

- **Allen & Overy** – Filip Van Elsen, Tine Carmeliet
- **Deloitte** – David Lenaerts, Chris Senior; Georgia Skouma, Dessislava Vitcheva
- **Thomas More Hogeschool** - Peter Berghmans