Centre for Information Policy Leadership
Hunton & Williams LLP

Byline

April 1, 2016

How to build a cathedral in two years

by Bojana Bellamy and Markus Heyder

Originally appeared on the IAPP's Privacy Perspectives

EU Regulators Urge Industry to Help Flesh Out the GDPR

Perhaps the most encouraging takeaway from the first workshop on implementing the new General Data Protection Regulation (GDPR) organized by the Centre for Information Policy Leadership (CIPL) in Amsterdam, was that the EU Commission, Member States ministries and data privacy regulators all agree with industry that implementing the GDPR over the next two years will be a significant task for all involved and will require close collaboration between themselves and industry.

Let's work together

The sentiment of having to face the implementation challenge together was clearly and repeatedly expressed by workshop participants from the Article 29 Working Party (WP 29) and the European Commission: "It would be impossible and not smart" for the data protection authorities to interpret the GDPR alone, said Isabelle Falque-Pierottin, Chair of the Article 29 Working Party. "We will work with industry and civil society to build this up from the ground. We must associate all stakeholders. ... We need you and your inputs." When asked about the correct process for providing input, she said "please use all the channels you have, and send us your ideas and criticisms. ... The industry must be proactive and bring ideas to the WP29." (For Isabelle Falquie-Pierottin's written remarks, please click here.)

Karolina Mojzesowicz, the head of Data Protection Reform Sector at the European Commission, concurred: "We are always here and will always listen. Please approach us. I can't over-invite you to approach us with your issues, questions and solutions."

Both Falque-Pierottin and Mojzesowicz also announced plans for stakeholder input events. As to the WP29, it might organize a "Fablab" on the GDPR in June 2016, to provide a forum for stakeholders "to bring proposals, tools, innovations and also criticisms" regarding the WP29's planned guidance on GDPR implementation, which, according to Falque-Pierottin, the WP29 seeks to develop "in close cooperation with [industry]." Similarly, Mojzesowicz noted that in September 2016, the Commission will hold a "large stakeholder event on the needs of businesses, NGO's and others."

The day-long workshop clearly illustrated the broad range of opportunities, challenges and unanswered questions raised by the GDPR. Nevertheless, while acknowledging the hard work ahead, Falque-Pierottin championed a "can do" attitude. "We have no choice," she said. "Step by step we can win."

Let's prioritize

To accomplish this, Falque-Pierrotin confirmed the WP29's four initial implementation priorities for 2016 and said that the group will "put flesh on the bones" and provide guidance on these priorities. These priorities are:

- The role of the Data Protection Officer (DPO)
- The role of risk and high risk processing
- Data portability
- Certifications

This list of priorities will be reviewed periodically and amended, said Falque-Pierottin, including based on industry input about what's most important.

She also emphasized that, in parallel, the WP29 will be working on the new governance model for the GDPR, which includes setting up the European Data Protection Board (EDPB), developing the "one stop shop", defining "lead authority" and other issues relating to cooperation among the European data protection authorities. In fact, she called it the WP29's "top priority," noting that "the regulation will be a failure" if the issues around EDPB governance and DPA cooperation are not worked out.

The four priorities align well with some of the priorities that industry so far has identified, though they leave out important issues, such as profiling, the application of consent, legitimate interest-based processing, transparency, pseudonymization and anonymization, and the role of organizational accountability for both controllers and processors. Of course, some of the issues can be addressed in the context of the current priorities – pseudonymization, anonymization and accountability can be addressed in the context of risk, and accountability is also linked to certifications and the role of the DPO.

Let's not reinvent the wheel and let's provide solutions

It will be important for industry to come together and speak to EU regulators with a unified voice where possible. Also, industry would be well advised to offer concrete and usable solutions rather than just to articulate problems. Both of these items, in fact, were key asks from the regulators at the workshop: "Don't just engage in individual dialogue; bring us solutions," said Jacob Kohnstamm, the chair of the Dutch DPA. "We don't have time."

Indeed, the two-year implementation period is not that long. We should not use it to re-invent the wheel. For example, there already is well-established and sound guidance on some of the new GDPR issues, such as accountability and the role of DPOs. After all, while the GDPR intends to bring change, even significant change in some cases, it also builds on existing foundations of privacy law and practice. Where these foundations include sound guidance, it is incumbent upon industry to bring this to the attention of the WP29 in a constructive manner to ensure continuity and consistency. Certainly other important issues, such as the role of risk and how to assess and mitigate risks to individuals without unnecessarily sacrificing societal benefits of data processing, will require further development and guidance by and for all stakeholders, despite the fact that a substantial amount of work has already been done on that front as well.

Further, certifications, seals, and codes of conduct have a prominent role in the GDPR. As Falque-Pierottin pointed out, organizations and DPAs have high expectations for these mechanisms. They are regarded as potential tools to help translate the new requirements into effective and practical compliance.

However, there are many unanswered questions here, too. For example, should certifications be product-based or program-based? The unequivocal answer from industry was that they should primarily be program based, as certifications and seals formalize and demonstrate externally a comprehensive privacy and accountability program within an organization. Also, what are their roles in the cross-border context? The industry consensus was that certifications, seals and codes of conduct can and must be used as mechanisms to enable cross-border data flows and they must be able to interoperate with accountability mechanisms outside the EU, such as the APEC Cross-Border Privacy Rules (CBPR).

Let's also focus on harmonization and the goals of the Digital Single Market

The complexity of the task ahead is heightened by two additional moving parts: the GDPR's goal of harmonizing data protection across Europe and the objectives of Europe's Digital Single Market (DSM) initiative.

With significant leeway for further implementation left to Member States, harmonization under the GDPR, of course, might seem less than certain. However, it remains of utmost importance both to industry and the Commission. Mojzesowicz repeatedly stressed: "Our aim is full harmonization, consistent with Recitals 7 and 8. Whatever goes on at the member state level should not undermine harmonization." She left no doubt that the Commission intends to be "the guardian" of harmonization.

As to the DSM, there was much discussion about the need to implement the GDPR with an eye to the DSM goals of digital competitiveness and innovation. Any guidance coming from the WP29 must be "future proof," industry representatives told the DPAs at the workshop. Indeed, as Bojana Bellamy observed, in this day and age, where data is the driver of economic and social prosperity, DPAs must embrace a new dual role of ensuring data protection and innovation; and Falque-Pierottin agreed: "Yes, we need to preserve innovation and we don't want a prescriptive text," she said.

Let's build a cathedral in two years

That was music to the ears of the participants. But, somewhat dauntingly, Falque-Pierottin also likened the GDPR "to a kind of cathedral – huge and a bit complex." That sure put the GDPR "to-do" list into perspective for privacy officers, DPAs, the EU Commission and the Member States. Building a cathedral has, in the past, taken anywhere between 25 to 600 years. Clearly, these new cathedral builders have their work cut out for them over the next two years, despite the preexisting foundations in data protection law and practice. High time to prioritize, organize, pool resources and get busy.

Bojana Bellamy is President and Markus Heder is Vice President and Senior Policy Counselor of Hunton & Williams LLP's Centre for Information Policy Leadership, a preeminent global privacy and information policy think tank located in Washington, DC and London. Bojana can be reached at bbellamy@hunton.com. Markus can be reached at mheyder@hunton.com.