Centre for Information Policy Leadership
Hunton & Williams LLP

27 April 2017

CIPL MADRID WORKSHOP KEY TAKEAWAYS

On 6 and 7 March 2017, CIPL held its 3rd major workshop of the GDPR Implementation Project focusing on the issues of transparency, consent and legitimate interest. The workshop was held in the historic premises of Telefónica with more than 140 participants from industry, DPAs, national governments, the European Commission, the EDPS, and academia.

The Workshop also included a special session on the Commission's Communication on cross border data flows, an update of the state-of-play of the implementation of the GDPR in the Member States, as well as a discussion on the key challenges for industry in becoming GDPR-ready.

The key takeaways were:

1. GDPR Certification and Cross-Border Transfers

- The Commission intends to work on expanding the existing data transfer mechanisms and developing new ones. This includes: a) expanding transfers covered by BCR, b) development of processor to processor model clauses and c) building bridges between cross-border transfer mechanisms, such as BCR and GDPR certifications and APEC CBPR.

- The Commission takes the GDPR certifications seriously and intends to commission a study to examine different existing certifications in the EU and elsewhere.

2. The GDPR Revolution

- The GDPR significantly changes data protection obligations and requires a fundamentally new and systematic approach to compliance.

- It is incorrect to say the GDPR represents merely an evolution. It clearly represents a revolution. The principles may be the same, but our world has become digital and technological developments and the facts on the ground to which data protection principles are applied have changed.

- If we don't acknowledge this, we won't understand the challenges of implementation.

3. DPAs need practical examples from industry to develop appropriate guidance

- Industry input on WP29 GDPR guidance can be made more effective by providing concrete practical examples and evidence to the WP29, as this is what they need most.

- This will be particularly important in respect of forthcoming guidance on profiling and consent and in respect of legitimate interest processing, as well as in relation to the proposal for ePrivacy Regulation.

4. Member States' GDPR Implementation

- Member States vary greatly in the progress of their national implementation of the GDPR.

- The Commission is keen to keep a tight rein on harmonisation and ensure Member States implementing laws do not go beyond the GDPR. The Commission is organising monthly meetings with Member States representatives to discuss the status of national implementation, in addition to bilateral discussions.

- Industry has specific concerns that harmonisation will not be achieved in areas where Member States have a margin of maneuver, in particular regarding a) children's age of consent (Art. 8), b) processing of special categories of data (including biometric and genetic data) (Art. 9), c) the exemption for scientific and historical research purposes and statistical purposes (Art. 89), and d) employees' data processing (Art. 88).

- The Commission should drive full transparency regarding the progress of national implementation, by publishing all national implementing drafts and final laws in one place, as well as a brief overview of the state of implementation in each country. Such information would also incentivise Member States that lag behind.

- There is concern that some Member States will not be able to have their implementing legislation ready in time. Ideally, national laws should be adopted by the end of 2017, enabling stakeholders to adapt to new national legal requirements in time.

5. DPA Must be Well Resourced

- The GDPR places a much higher burden and additional responsibilities on DPAs but does not specify how funding will be provided.

- Some DPAs expect an increase of their staff; other DPAs don't expect that their staff will be increased.

- DPAs identified the need for more training of staff, including English language courses.

- CIPL's **smart data protection project** could facilitate greater DPA effectiveness even with limited resources.

6. Implementation by May 2018 and Industry/DPA Relationship and Dialogue

- Since it is unrealistic for organisations to meet all GDPR requirements by May 2018, organisations must prioritise compliance, based on the risk-based approach and accountability. Organisations must be able to show good faith and demonstrate that they have commenced their compliance programs, even if they are not completed by May 2018. The WP29 should recognise good faith efforts.

- For the industry to prioritise in a sensible manner, the WP29 must first clarify their priorities and especially establish processing where there is likely "low risk". This would particularly help SMEs to spend their resources most effectively.

- Communications, consultations and engagement on guidance development between companies and DPAs/WP29 need to be more nimble, expeditious and efficient. DPA guidance should provide objectives rather than solutions, leaving sufficient flexibility for organisations to implement appropriately.

- One-size-fits all and "industry-wide solutions" are not necessarily helpful or even possible in view of the great variety of industry sectors.

7. GDPR Transparency

- The growing gap between legal transparency and user-centric transparency (with long privacy notices as an obvious example) must be addressed. Transparency in the GDPR is

intended to be user-centric.

- Transparency should be context-specific, considering the possibilities of new technologies and avoiding information overload. Transparency tools should be interactive, innovative and embedded in technology and products.

- Individuals should be primarily provided with information that enables informed choices, and some information should possibly be given to individuals only "on demand".

- Icons may have limited usefulness and application, though they may hold promise for specific contexts. Some organisations are interested in developing their own icons for specific applications. Icons should be developed by industry and not by regulators and they should be based on research and evidence.

8. GDPR Consent & Legitimate Interest

- Consent, legitimate interest and the other grounds for processing) have equal status under the GDPR and are equally appropriate when used in the right context.

- Consent should be used as legal ground for processing in situations where individuals have a genuine choice to decide the use of their personal data and where the withdrawal of consent is possible.

- Consent under GDPR requires a higher bar and stricter requirements. In some instances, other grounds for processing may be more appropriate.

- Legitimate interest as a ground for processing is an effective and accountable tool for protecting individuals. It requires a case-by-case balancing test that considers both the risks and the benefits of processing for individuals, third parties and society.

- Although direct marketing is mentioned as an example of legitimate interest in the GDPR recital, DPAs stressed that it must still be ascertained in each case based on the balancing test that a controller performs.

- The biggest concern for organisations is that DPAs will not accept the outcomes of their risk/benefits balancing in connection with legitimate interest. That concern must be addressed by DPAs.

9. Alignment between GDPR and ePrivacy Regulation

- It is important to bring proposed ePrivacy Regulation into alignment with the GDPR on the issues of consent and legitimate interest.

- Industry fears that the broad scope of ePrivacy Regulation and stricter rules for the use of data will result in much of the modern processing activities in the digital ecosystem being excluded from the application of the more progressive and flexible GDPR requirements.