Centre for Information Policy Leadership
Hunton & Williams LLP

6 July 2017

CIPL – Senior Leaders Working Session on Smart Data Protection

Dublin – 14th June 2017

CIPL hosted this working session primarily to stimulate feedback on the latest draft of its 'Smart Data Protection' Discussion Paper. The draft examines the expanding role of DPAs (especially under the GDPR) and raises questions about how DPAs can maximize their effectiveness in a world of limited regulatory resources and how DPAs and regulated entities (accountable organisations) can effectively engage in a constructive dialogue as a means of achieving the best regulatory outcomes for all.

The event was attended by around 60 key stakeholders – with senior representatives from DPAs, businesses, national governments and academics.

Overall Summary

The working session unanimously welcomed the subject of regulatory effectiveness. This is a joint goal of both regulators and regulated entities and essential in the area of data privacy regulation which is closely linked to data innovation and digital economy and growth. There was agreement that accountable organisations and effective and outcome-based regulators are two essential pillars of smart data protection. It was agreed that the Data Protection community (regulators and regulatees) could learn much from other regulatory fields. There was a consensus about the importance of seeking clear outcomes and focusing on the spirit of regulation, rather than compliance for its own sake. A broad goal can be expressed in terms of ensuring that a good quality of life flows from genuine, human-centred, privacy in a world where widespread use of data is universally popular. Constructive dialogue and engagement between DPAs and those they regulate (bringing to life Art.57(1)(d) of the GDPR) is vital and both sides could do much to assist the other.

The draft CIPL paper is on the right lines, but should be revised further before its launch in Hong Kong in September. In particular, it needs to:

i. Build more on what DPAs are already doing;

ii. Emphasise more the purpose of the paper which is to give a constructive contribution to the development of strategies by independent DPAs in view of the significant new challenges; and

iii. Say more about the constructive dialogue between accountable and responsible organisations and DPAs and how organisations can provide helpful input which will not be seen as self-serving.

Regulatory effectiveness should also be addressed within the framework of a wider context which recognizes the contributions of a rich network of stakeholders outside the direct regulator / regulatee relationship.

6 July 2017

Noteworthy points

- Accountable organisations and well-resourced and effective DPAs are both cornerstones for the success of the GDPR, and any regulatory framework.
- GDPR inevitably means a new regulatory eco-system based on clear expectations, risk assessments and priorities.
- The extremely limited resources available to DPAs is a very real issue. Only a few have so far secured any significant increases. Wider skills are also needed.
- There are serious concerns about the risks of an uncontrollable tsunami of complaints, requests for information, breach notifications, prior consultations, applications for cross-border and other authorisations, etc. – all of which will require immediate regulatory attention.
- Transparent strategies setting out priorities, expectations and working methods will help DPAs discharge their various regulatory duties (leader / advisor, policemen / enforcer, complaint handler, authoriser, etc.) and help organisations to "get it right first time".
- Regulatory conversations and constructive dialogue are especially needed where there are no common opinions on what the "right thing" is, or even what should be prevented. This is even more needed in light of the new GDPR requirements and the new reality of ever-changing technology to which both existing and unfamiliar requirements will be applied
- Compliance is a journey and an on-going goal. Just like with reiterative software and technology development, compliance solutions should be reiterative, evolve and subject to constant feedback and improvement. Regulators should allow the evolving notion of compliance, allowing for failures and improvements. They should work collaboratively with regulated entities on this joint goal.
- Effective regulation involves monitoring and changing behaviours, and sometimes cultures, not just ensuring the formalities and paperwork are in order.
- Bridge-building approaches based more on co-regulation, accountability, corporate digital responsibility and "regulated self-assurance" are likely to prove more effective than a "Command & Control" approach. This approach has been proven to work in many other areas of regulation and is starting to emerge in data privacy regulation too.
- Organisations should be positive in helping DPAs to develop a better understanding of the landscape they regulate, including being ready to explain and demonstrate their business models, processes and technology solutions.
- Many compliance solutions can be built jointly, in a collaborative environment, with multiple stakeholders, including DPAs and regulated companies, but also experts and technologists. Design thinking is an example of how some data privacy requirements and apparent compliance challenges can be made scalable and developed bottom-up, including by those who create user interfaces and user-centric products and services.
- There should also be space for responsible innovation by accountable organisations. In addition to design thinking collaborative processes, another recent development the

"sandbox" concept - being developed by financial regulators in the UK - may prove an interesting model to enable regulated companies to experiment and innovate in confined parameters and a "safe haven" by regulators.

- Greater reliance upon DPOs, privacy management programs (accountability), Codes of Conduct, Certification schemes and pressures from well-informed data subjects will promote self-compliance and reduce pressures on DPAs.
- Education and digital literacy of individuals is an important goal for both DPAs and regulated organisations. Organisations should proactively educate individuals, which will not only promote digital trust and confidence, but help alleviate regulatory burden for all stakeholders.
- Organisations tend to move in herds, following the benchmarks of sector leaders and competitors, especially where an approach has secured some sort of regulatory endorsement. DPAs could probably do more to exploit this tendency, e.g. promoting acceptable templates and encouraging specific "best in class" behaviours. This would help improve market standards and be especially useful for SMEs and start-ups, which don't have sophisticated and well-resourced privacy functions.
- Corporate leadership will take data protection and privacy more seriously if DPAs create and communicate clear incentives for good faith privacy management and compliance programs, such as potential mitigation in enforcement, enabling cross-border data transfers, enabling wider use of data (big data and analytics) or data innovation initiatives.
- Business and governmental organisations should be open – and do much more to explain, showcase and develop best practice.
- The ethical dimension is important - legislation works best where the rules are openly reinforced by ethical values and are made fairly, applied fairly and correspond to widespread moral values. Ethical business practices and ethical regulation go hand in hand.
- Sanctioning should not only be limited to fines, but include wider tools, including reputational aspects and ordering powers. 'Naming and shaming' techniques may prove valuable. Finally, there could be a "traffic light" approach, identifying organisations as green, yellow or red.
- DPAs are starting to leverage and look for assistance from other regulatory authorities (e.g. consumer protection and competition authorities).
- Enforcement through sanctions works best as a last resort mechanism, rather than a "First Stop" instrument. But media and political pressures will expect tough enforcement for the worst and repeated infringements. A risk-based approach is essential for identifying priorities.
- There should be maximum consistency of EU DPAs enforcement and regulatory strategies and priorities - possibly included in EDPB guidelines. This is just as important for the functioning of Digital Single Market and data protection as a fundamental right across the EU, as standardising and harmonising rules and

guidance. There is a recognition that this will not be easy or quick to achieve, especially where regulatory cultures differ.

- It is essential that there is not only consistency, but also transparency in respect of DPAs' enforcement and fining strategies, as well as complaint handling and breach notification handling strategies.
- There may be scope for DPAs to improve practical co-ordination - e.g. sharing expertise and further foster transparency of their work and decision making. Technology should be able to help here.
- Performance indicators may help to measure and demonstrate effectiveness, and also influence and ultimate success. There may be value in developing common metrics, although this is not an easy task, especially how to measure influence and outcomes.
- Cooperation at European level may enable all EU DPAs to leverage each other's skills and strengths, and adopt best practices that some of the EU DPAs have already developed.