

Centre for Information Policy Leadership (CIPL) Roundtable

**CIPL Roundtable on the Regulatory Sandbox
- Under Chatham House Rule -**

Hunton Andrews Kurth LLP, Meeting Rooms 3 & 4
30 St Mary Axe
London EC3A 8EP

19 February 2019 | 10:00 – 16:00

AGENDA

10:00 **Registration and Coffee**

10:30 **Opening Remarks**

- ❖ Bojana Bellamy, President, Centre for Information Policy Leadership

10:40 **ICO Regulatory Sandbox Strategic Policy**

- ❖ Simon McDougall, Executive Director for Technology Policy and Innovation, UK Information Commissioner's Office

11:00 **Regulatory Sandboxes – Constructive Engagement in Practice**

- ❖ Richard Thomas, Global Strategy Advisor, Centre for Information Policy Leadership

11:15 **ICO Draft Operating Model for a Regulatory Sandbox**

- ❖ Chris Taylor, Head of Assurance, UK Information Commissioner's Office

11:45 **Open Discussion with Working Lunch Served at 13.00**

Participants will discuss key questions around the operation and function of the Regulatory Sandbox. The questions below aim to facilitate a structured discussion to dissect some of the most common, open and unresolved questions relating to the Sandbox concept.

16:00 **End of Roundtable**

Questions for Discussion

1. What are the benefits to organisations, DPAs, society and the economy and individuals of the Regulatory Sandbox?
2. What are the expectations surrounding a Regulatory Sandbox pilot programme (e.g. the ICO Sandbox beta phase) for both the DPA and organisations?
3. The ICO Sandbox beta phase is open to about 10 organisations of different types and sizes across the private, public and third sectors – Will this also be the case once the Sandbox becomes a permanent part of the ICO regulatory toolkit? Does the ICO intend to allow newly formed companies or startups who may not have a history of demonstrated accountability the chance to participate?
4. The ICO Sandbox beta phase will particularly welcome applications regarding products and services that address specific data protection challenges central to innovation (e.g. use of personal data in emerging/developing technologies, complex data sharing, building good user experience and trust, perceived limitations on rules around automated decision-making, machine learning and AI or utilising existing data for new purposes). Are there other specific challenges the ICO should consider? Should any of the existing challenges be modified?
5. The ICO lists several threshold eligibility criteria for entry into the Sandbox – are these the full set of criteria that will be used to make the assessment or are there others that participants should be thinking about? Are there any other criteria the ICO should consider in assessing applications?
6. What is the ICO looking for when assessing organisational data protection maturity and accountability as a criterion for entering the Sandbox? How can organisations ensure they are in the best position to meet this criterion?
7. The threshold eligibility criteria include looking at the ICO's resources and capabilities and determining whether they can take on a Sandbox project. What are the expectations around participant resources? Will participation be costly or require organisations to budget for their participation?
8. Is the application process and timing for the ICO Sandbox beta phase realistic for organisations?
9. What are the main barriers to entry for organisations to participate in the Sandbox? How can we address these?
10. Once an organisation enters the Sandbox, the ICO will provide support in the form of advisory, adaptive and anticipatory mechanisms. What other mechanisms could the ICO provide to support organisations in the Sandbox as they test their new innovations?
11. The ICO plans to utilise two flexible mechanisms to provide assurance to organisations around fears of adverse enforcement action through participation in the Sandbox – comfort from enforcement for participants on entry and letters of negative assurance on exit. Will these mechanisms be beneficial to participants? Are there other methods of assurance the ICO should

consider to support innovators in achieving compliance/provide assurances around concerns of adverse enforcement action?

12. The ICO wants the Sandbox to push its understanding of what compliance looks like so it can anticipate what changes to regulatory approaches may be needed in the future. What areas might this be most useful in? What kinds of outputs might be produced as a result?
13. With respect to protecting commercially sensitive information, IP and other business proprietary information, the ICO lists certain safeguards including sharing sandbox participant information among ICO staff members only where necessary, adhering to obligations under S.132 of the DPA 2018 and treating FOIA requests on a case by case basis, considering whether any exceptions apply. What additional steps can the ICO or organisations themselves take to minimise any risks to confidential information and commercial concerns?
14. If an organisation who is ultimately accepted into the Sandbox decides to end the process before testing is complete, are there any consequences, including in terms of how they are viewed by the regulator? Would such organisations be expected to provide detailed reasons as to why they have decided to end the testing?
15. If a participating organisation uses another non-participating organisation's technology as part of its innovation, could a finding of non-compliance on the part of the participating organisation in the sandbox indirectly implicate the non-participating organisation, in particular, if the issue is linked to the non-participating organisation's technology?
16. In regular cases of non-compliance (i.e. not in the context of the Sandbox), could mandatory Sandbox participation provide a corrective measure in lieu of other enforcement action?
17. Is there scope to expand the Regulatory Sandbox beyond the participation of individual companies (i.e. have sectoral, or industry wide Sandboxes for multiple companies engaged in a common innovation, or cross-border Sandboxes)?
18. What is the relationship between the Sandbox and Data Protection Impact Assessments (DPIA)? Does the ICO's approach to handling the interface between DPIAs and Sandbox participation appear effective?
19. What safeguards will exist for individuals who are test subjects in the Regulatory Sandbox and will such individuals know they are part of a testing phase?
20. What are the challenges of the Regulatory Sandbox for the DPA? How can we address these?
21. How can we socialise the Regulatory Sandbox concept beyond the UK? Are there any negative connotations or preconceptions about the Sandbox in certain countries to be aware of?