Centre for Information Policy Leadership

Hunton Andrews Kurth LLP

Centre for Information Policy Leadership

Roundtable on the Regulatory Sandbox

19 February 2019

London

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

Opening Remarks

Bojana Bellamy, President, CIPL

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

Agenda

- 10:00 AM **Registration**
- 10:30 AM **Opening Remarks**
- 10:40 AM **ICO Regulatory Sandbox Strategic Policy**
- 11:00 AM **Regulatory Sandboxes - Constructive Engagement in Practice**
- 11:15 AM **ICO Draft Operating Model for a Regulatory Sandbox**
- 11:45 AM **Open Discussion with Working Lunch Served at 13.00**
- 16:00 PM **End of Roundtable**

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

ICO Regulatory Sandbox Strategic Policy

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

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

Regulatory Sandboxes
Constructive Engagement in Practice

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

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

ICO Draft Operating Model for a Regulatory Sandbox

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

Regulatory Sandbox
Beta Operating Model

Chris Taylor, ICO Head of Assurance
(Sandbox, Codes, Certification, eIDAS)

ico.
Information Commissioner's Office

In this presentation...

- Purpose
- Meet the team
- What is the Beta phase?
- Our target operating model
- Confidentiality
- Links to DPIAs
- Introduction to the afternoon

ico.
Information Commissioner's Office

Purpose

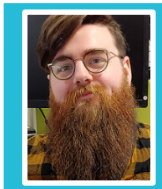
- to support the safe use of personal data in innovative products and services that can be shown to be in the public interest
- to help develop a shared understanding of what compliance in particular innovative areas looks like
- to support the UK in its ambition to be an innovative economy.

ico.
Information Commissioner's Office

Meet the Team

Chris Taylor
(Head of Assurance)

Claire Chadwick
(Group Manager)



Sam Evans
(Senior Case Officer)

Sarah Smith
(Senior Case Officer)

Steven Stafford
(Senior Case Officer

ico.
Information Commissioner's Office

What is the Beta phase?

- A flexible test of our Sandbox across 2019-20
- Working with around 10 organisations of various sizes and levels of DP maturity across any and all sectors
- Working with those organisations to define, agree, execute and monitor bespoke sandbox plans
- Sandbox plans can contain a number of mechanisms: advisory, adaptive, anticipatory

ico.
Information Commissioner's Office

Sandbox Mechanisms

Informal Advisory Mechanisms

- Flexible – informal advice/steers designed around each participant and the objective of their plan:
  - phased or iterative informal steers – from idea, concept to prototyping
  - informal supervision of product or service testing
  - process design walkthroughs – step by step walkthroughs of proposed processing activity leading to informal advice
  - drop-in or workshops with design and development teams at an early stage in order to inform very early thinking;
  - informal steers on risk mitigation at design stage;

- Principle of honest shared challenge – mitigating risk, supporting DP by design and default

ico.
Information Commissioner's Office

Sandbox Mechanisms

Adaptive

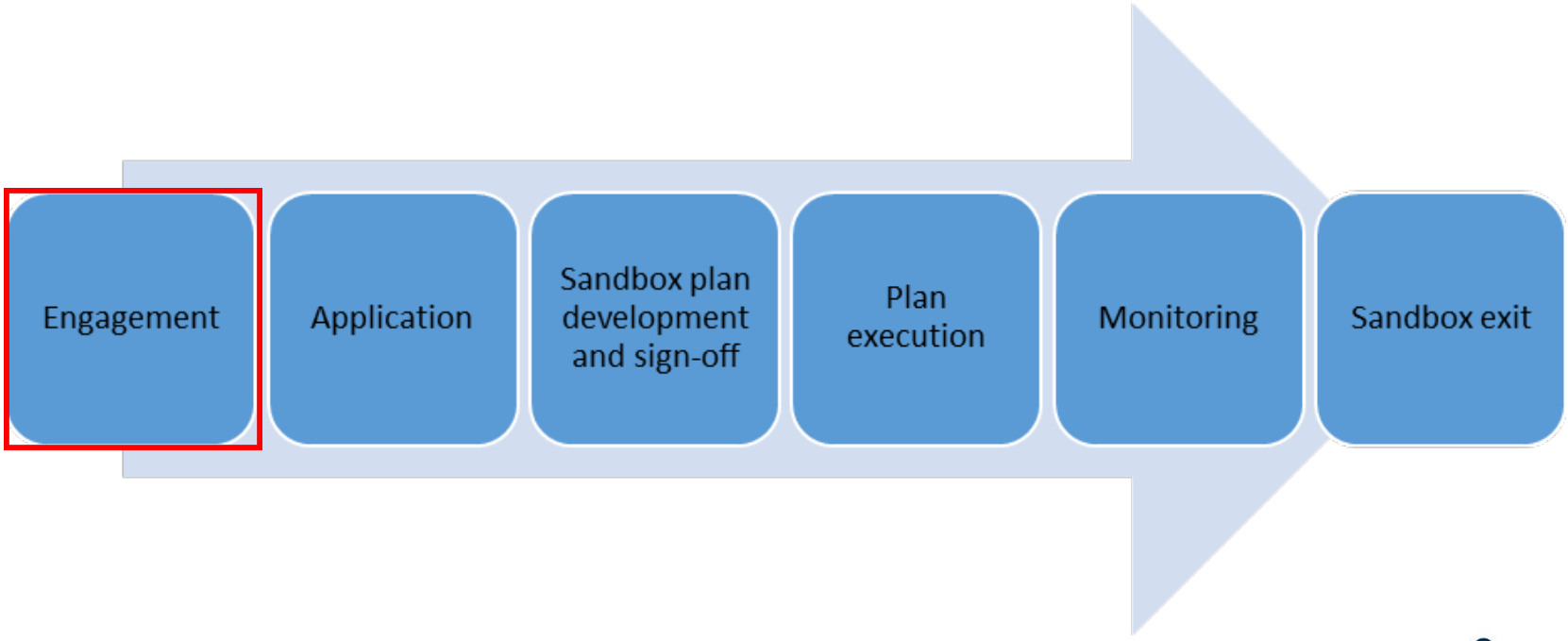
- GDPR/DPA18 applies – this is not about relaxing legal requirements. But we do have some discretion:
  - Comfort from enforcement – for all on entry
  - Letter of regulatory comfort – if needed/applicable on exit
- Could also look to inform the guidance we give to government on future provisions based on specific use case

Anticipatory

- Using participant's product/service use case to develop specific guidance on compliance in a particular area for wider use
- Using participant's product/service use case to consider what future regulatory provisions or approaches may be needed

ico.
Information Commissioner's Office

How will we run the sandbox?



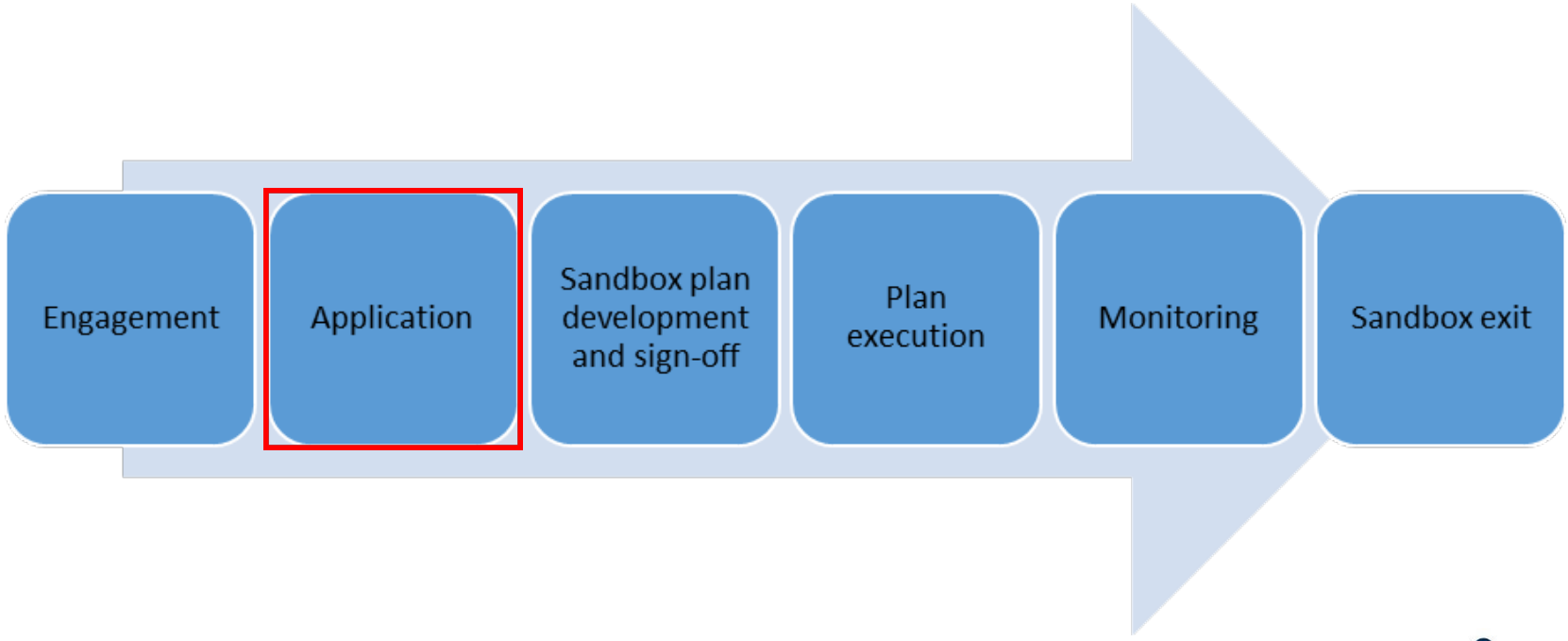
ico.
Information Commissioner's Office

Engagement

- Call for views, stakeholder discussions, FCA input, discussion workshop
- Building the sandbox openly and transparently – listening to potential participants and adapting our approach
- Also have a team now in place and ready to answer queries throughout application phase: sandbox@ico.org.uk
- Aim to help and support organisations understand the application process to ensure good quality relevant applications – engage early
- Published discussion paper end Jan
- This roundtable!

ico.
Information Commissioner's Office

How will we run the Sandbox?



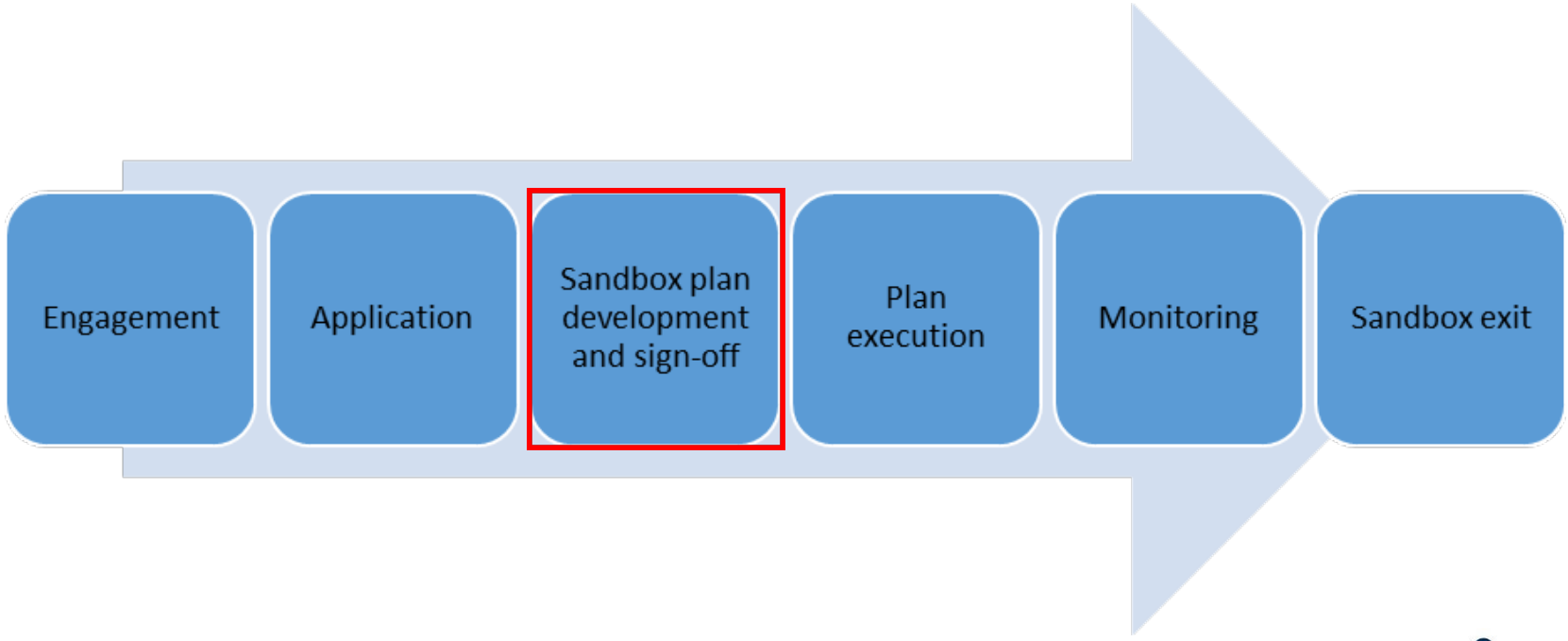
ico.
Information Commissioner's Office

Application process

- Aiming to open applications on line end of March/early April: full guidance, FAQs, example case studies, example terms and conditions, application forms, criteria indicators
- Aim to close end of May – we have made this window longer in response to feedback
- Application via simple word form
- Open and transparent process assessing applications against
  - Threshold criteria: innovation, public benefit, Sandbox plan viability – as per indicators in the discussion paper
  - Other factors (e.g. DP challenges, mixture of orgs, our own resources)
- Applications assessed by internal ICO panel
- Organisations notified end of June/early July

ico.
Information Commissioner's Office

How will we run the Sandbox?



ico.
Information Commissioner's Office

Sandbox Plan Development

- On accepting ICO will then work with participants to design and agree a bespoke plan that will define that participants experience in the sandbox and how we will work together.

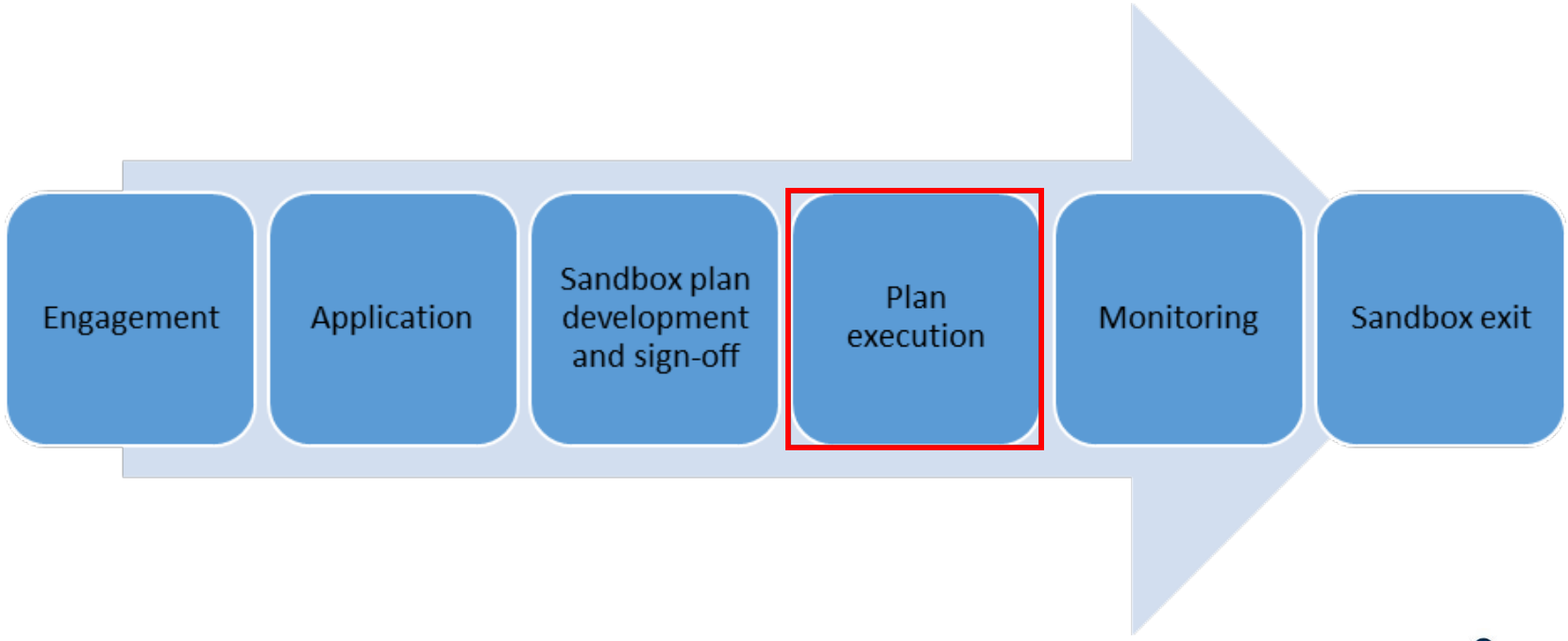
- It will cover:
  - Agreed mechanisms and objectives
  - Timeline and expected outcomes
  - Risk assessment
  - Monitoring arrangements
  - Resource commitments

- Discussion will start asap and we will seek to sign off those plans as soon as feasible so that activity can start – all underway by end September at the latest and with a maximum length through to Sept 2020

- We are as open to short focussed engagements as we are to more complex longer engagements

ico.
Information Commissioner's Office

How will we run the Sandbox?



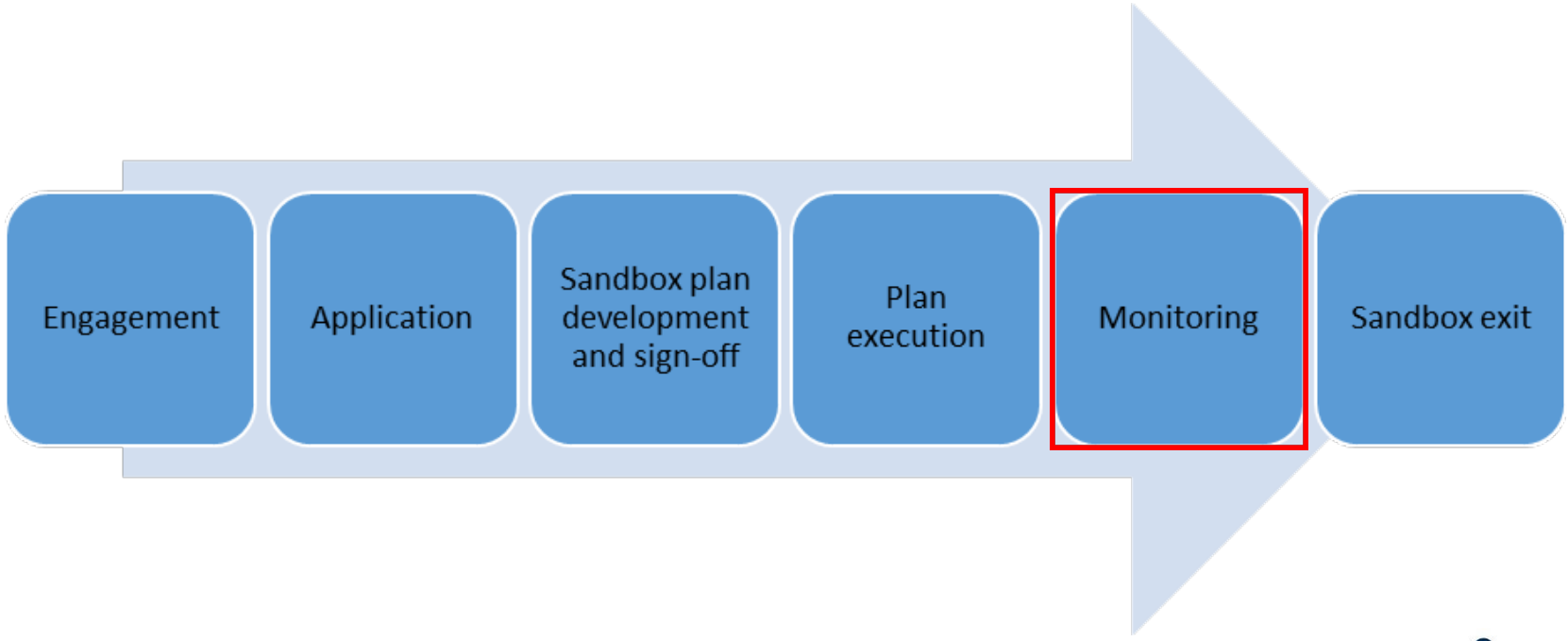
ico.
Information Commissioner's Office

Plan Execution

- This will differ depending on the nature of the plan agreed – but is in effect a partnership project with the participant in line with the pre-agreed plan
- Plans could be very different for each organisation, with different mechanisms, start dates and specific objectives
- Our emphasis is to be flexible and responsive as new issues or challenges emerge
- Plans will be able to change – defined change control process

ico.
Information Commissioner's Office

How will we run the Sandbox?



ico.
Information Commissioner's Office

Monitoring

- Monitoring will be designed as per the plan as relevant to the sandbox participant taking account of the risks involved in the project with greater frequency and intensity of monitoring for higher risk projects:

- In all cases we would expect there to be three formal meetings:

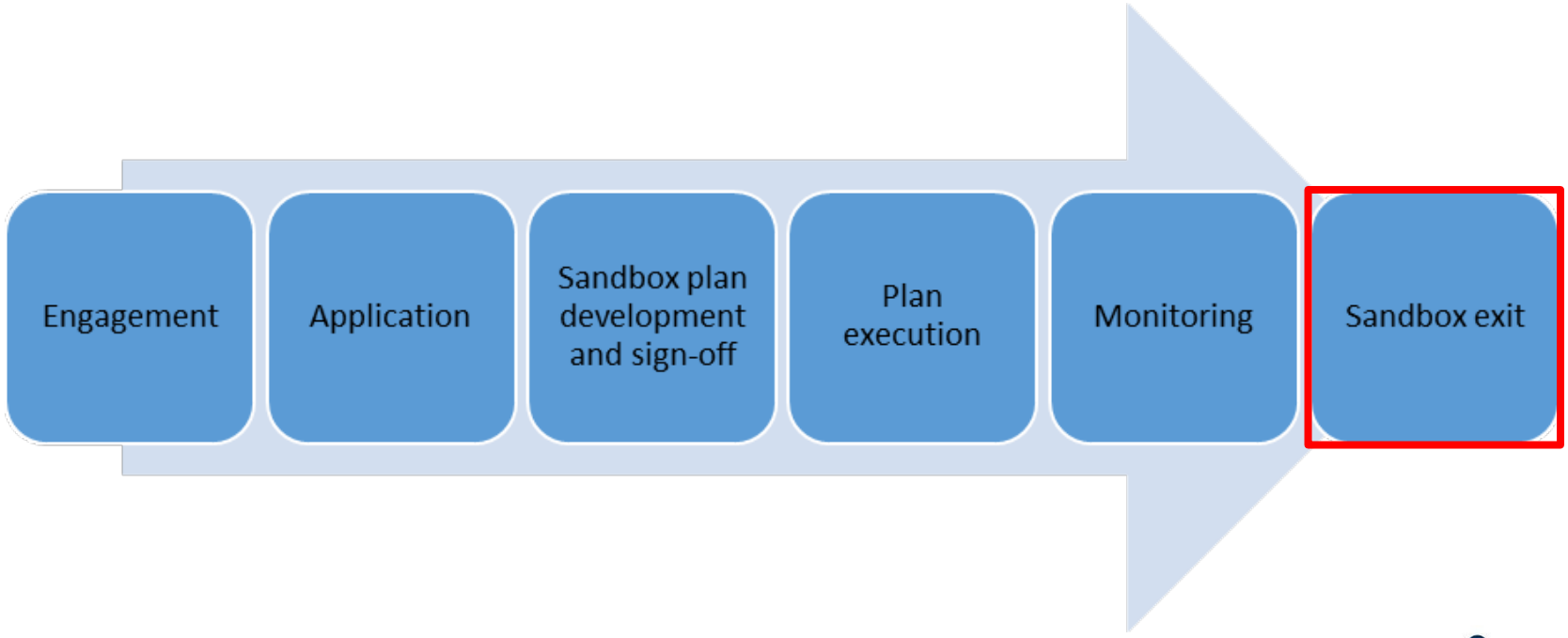
  - Plan kick off meeting: to talk through practical arrangements, confirm timescales of activity and mutual expectations

  - Mid-point evaluation and stock take to review progress

  - Sandbox wash-up meeting at end of sandbox participation

ico.
Information Commissioner's Office

How will we run the Sandbox?



ico.
Information Commissioner's Office

Sandbox Exit

- End point will be defined in original plan – and kept under review
- At the end of the sandbox process SCOs will hold a wash-up meeting with the organisation to evaluate the process, seek feedback, and in order to populate a sandbox exit report.
- The report will summarise the process and the key activity that was undertaken and whether initial objectives have been met. A common format for this report will be created.
- If pre-agreed as part of the sandbox plan and following that meeting we may issue a letter of regulatory comfort

ico.
Information Commissioner's Office

Confidentiality

- ICO sandbox team is bound by strict obligations of confidentiality by Section 132 of the DPA 2018
- Includes confidential information that relates to an identified or identifiable individual or business provided as part of the sandbox process
- We are subject to the Freedom of Information Act 2000 (FOIA) and so are legally required to respond to any FOIA requests we receive, which may include requests for information provided to us in relation to the sandbox.
- Treat on a case by case basis but will particularly consider the following exemptions:
  - Section 41 (information provided in confidence)
  - Section 36 (conduct of public affairs)
  - Section 43 (commercial interests)

ico.
Information Commissioner's Office

Links to DPIAs

- Requirements to undertake a DPIA remain:
  - Flag at application and tell us how you plan to mitigate the risk – revisit in plan development
  - Sandbox team can work with you on risk mitigation, but wont formally review or comment on DPIAs
- If new high risk processing is part of your plan (e.g. live testing) then we will need assurance that risk has been mitigated before new processing can start
- If residual risk remains high, and you want to proceed usual DPIA requirement to consult will kick in and usual process will need to be gone through – sandbox participation will then be paused
- Once outcome of that process has been given we may restart sandbox depending on what that outcome is

ico.
Information Commissioner's Office

Changes

- Longer application window
- Removal of DP Maturity as an assessment criteria – though will still require information and outcome of checklist to tailor support
- Requirement to tell us what the specific DP issue is that means the participant needs the Sandbox
- Introduction of chance for sandbox team to clarify factual matters on applications
- Additional DP challenges: security in innovative environments, big data
- Clarified approach to collaborative applications (possible but will need single lead org)

ico.
Information Commissioner's Office

Keep in touch

sandbox@ico.org.uk

Subscribe to our e-newsletter at www.ico.org.uk
or find us on…

@iconews

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

Discussions

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

Questions (1)

1. **Benefits** of Sandbox - to organisations, DPAs, society and the economy and individuals?
2. **Expectations** surrounding Sandbox pilot programme for both the DPA and organisations?
3. **Scope of the Sandbox** - ICO pilot welcomes 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). What type of projects; technologies; innovations; unclear legal norms; challenging trade-offs; conflicts of laws? **Provide some examples of hypothetical cases for Sandbox.**
4. **Threshold eligibility criteria for entry** into the Sandbox – ICO lists Innovation, Public interest, Organisations accountability and maturity. Are these the right criteria? **Provide examples.** Any **other criteria** the ICO should consider in assessing applications? What is the ICO looking for **when assessing organisational data protection maturity and accountability** as a criterion for entering the Sandbox? How can organisations meet this criterion and what they may have to demonstrate? Does the ICO intend to allow SMEs or **startups** who may not have a history of demonstrated accountability the chance to participate? The pilot is open to 10 organisations of different types and sizes in private, public and third sectors – will this also be the case and will there be a limited number **once the Sandbox becomes a permanent part of the ICO regulatory toolkit**?
5. **Process, resources, timing** - What are the expectations around participant resources? Will participation be costly or require organisations to budget for their participation? Is the application process and timing for the beta phase realistic for organisations?

Questions (2)

6. **Barriers to entry for organisations** to participate in the Sandbox – what are they and how can we address them? How to "sell" Sandbox internally?

7. Addressing the fears of enforcement – comfort letter from enforcement for participants on entry and letters of negative assurance on exit. Will these be beneficial to participants? Any **other methods** of assurance the ICO should consider?

8. Early exit from Sandbox - 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?

9. Protecting IP, commercially sensitive and business proprietary information- the ICO lists safeguards including restricted sharing of information with other ICO staff; adhering to obligations under S.132 of the DPA 2018; and considering exceptions to FOIA requests on a case by case basis. What additional steps can the ICO or organisations themselves take to minimise any risks to confidential information and commercial concerns?

10. In 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 ? 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?

11. **Sandbox and Data Protection Impact Assessments** (DPIA) - what is the relationship? Does the ICO's approach to the interface between DPIAs and Sandbox participation appear effective?

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

Questions (3)

12. **Participating organisation uses another organisation's technology** as part of its innovation – does this implicate the other organisation in the Sandbox? Could a finding of non-compliance indirectly implicate the non-participating organisation, in particular, if the issue is linked to the non-participating organisation's technology?

13**. Expanding the Sandbox** to sectors/ industries (multiple companies engaged in a common innovation) or cross-border sandboxes with multiple DPAs – are these viable and useful?

14. **Sandbox as a corrective measure in case of non-compliance - could mandatory Sandbox** participation be used to provide a corrective measure in lieu of other enforcement action?

15. **Safeguards for individuals** who are test subjects in the Regulatory Sandbox ? Will they know they are part of a testing phase?

16. **Challenges of the Sandbox for the DPA**? How can we address these?

17.. **Socialisting the Sandbox concept beyond the UK**? Would this be helpful? Where is it most likely to succeed? Are there any negative connotations or preconceptions about the Sandbox in certain countries to be aware of? How to promote cross-border Sandboxes?

Contacts

Bojana Bellamy
President
Centre for Information Policy Leadership
BBellamy@huntonak.com

Markus Heyder
Vice President & Senior Policy Advisor
Centre for Information Policy Leadership
MHeyder@huntonak.com

Nathalie Laneret
Director of Privacy Policy
Centre for Information Policy Leadership
NLaneret@huntonak.com

Sam Grogan
Global Privacy Policy Analyst
Centre for Information Policy Leadership
SGrogan@huntonak.com

Centre for Information Policy Leadership
www.informationpolicycentre.com

Hunton Andrews Kurth Privacy and Information Security Law Blog
www.huntonprivacyblog.com

FOLLOW US ON LINKEDIN
linkedin.com/company/centre-for-information-policy-leadership

FOLLOW US ON TWITTER
@THE_CIPL