11 October 2018

CIPL Response to the ICO call for views on creating a "Regulatory Sandbox"

"It's not a choice between privacy or innovation"

Summary

The Centre for Information Policy Leadership (CIPL)[1] warmly welcomes the ICO's initiative in developing the "Regulatory Sandbox" concept. Our response sets out the key features of the concept—essentially a supervised safe space for piloting and testing innovatory products, services, business models or delivery mechanisms in the real market, using the personal data of real individuals.

Alongside actual and hypothetical examples of where Sandbox participation might be or have been useful, we identify the main benefits of the approach—for organisations, for the ICO itself, for individuals and for the economy and society at large.

There will be challenges in the implementation of the Sandbox, not least arising out of a statutory framework which does not explicitly accommodate this concept. But the challenges are not insurmountable and we set out various practical suggestions to maximize the prospects of success. We attach particular importance to the need for clear, objective and transparent criteria for participation—stressing the importance of an innovative element and regulatory uncertainty—and the need for the ICO to clarify the relationship with data protection impact assessments (DPIAs).

Organisations will have some anxieties, especially relating to commercial confidentiality and the risks of adverse enforcement action. Our response sets out some safeguards which we urge the ICO to adopt. In particular, CIPL considers that information disclosed into the Sandbox must only be used as the basis for an enforcement action in exceptional circumstances and that the ICO must give some benefit of the doubt where—during testing in a real-life scenario in the supervised space—genuine uncertainty arises about compliance.

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 65 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

Regulatory Sandbox

CIPL warmly welcomes the ICO's initiative in developing the "Regulatory Sandbox" concept and is very pleased to provide this response to the current call for initial views.

In our 2017 paper, **Regulating for Results**,[2] CIPL proposed that, for maximum effectiveness, data protection authorities (DPAs) should give the "Leadership" function the top strategic priority—helping and guiding organisations which are seeking to comply, while dealing firmly with those who are not even trying. A key part of regulatory Leadership involves "Constructive Engagement" with accountable organisations where there is a spirit of trust and mutual co-operation between DPAs and organisations which share the commitment to the same results.

Our paper (on pages 37-41) explored what "Constructive Engagement" means in practice and stressed the mutual interest of regulators and regulated entities in securing genuine data protection for individuals alongside data innovation and the growth of the digital economy. "In other words"—CIPL's paper argued—"effective and results-based regulators and accountable organisations can work more alongside each other as two essential pillars of modern data protection".

Several examples of activities and techniques were identified to bring Constructive Engagement to life, including the need to "create space for responsible innovation". This was described in terms of building compliance solutions co-operatively, with the involvement of multifunctional teams including designers, technology engineers, behavioural economists and marketing and customer relationship experts, as well as legal and privacy experts.

We put forward (on page 39) the Regulatory Sandbox in the following terms as a specific option for DPAs to consider:

[2] "Regulating for Results – Strategies and Priorities for Leadership and Engagement", 10 October 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement__2_.pdf.

The Regulatory Sandbox – Space for Responsible innovation

Constructive engagement includes creating space for responsible innovation by accountable organisations. How might this be achieved?

The "Regulatory Sandbox" model being developed by the UK's Financial Conduct Authority may prove an interesting way to enable regulated companies to experiment and innovate in a "safe haven" overseen by the regulatory body.

The regulatory sandbox allows businesses to test innovative products, services, business models and delivery mechanisms in the real market, with real consumers.

The sandbox is a 'supervised space' that is claimed to provide organisations with:

- reduced time-to-market at potentially lower cost; and
- appropriate consumer protection safeguards built in to new products and services

The sandbox offers tools such as restricted authorisation, individual guidance, waivers and no enforcement action letters. The FCA closely oversees trials using a customised regulatory environment for each pilot.

Sandbox tests are expected to have a clear objective (e.g. reducing costs to consumers) and to be conducted on a small scale, so firms will test their innovation for a limited duration with a limited number of customers. It is arguable that technical innovation is impacting on data protection to an even greater extent than financial services. This model may be particularly well suited and well received in the data protection community, where there is increasing recognition that compliance has to be treated as an iterative process.

The possible use of the sandbox model in this context was raised by the former Secretary-General of the CNIL in an article in *Les Echos* in early 2017.[3]

There have been a number of developments since our paper was published:

- In October 2017 the UK Financial Conduct Authority published a very helpful and encouraging "Lessons Learned" report[4];
- Singapore's Personal Data Protection Commission's Guide to Data Sharing set out details of how its Regulatory Sandbox will work—so that accountable businesses "are not held back from deploying technological and business innovations"; and

[3] Y. Padova, "L'innovation, l'autre arme du Brexit", LesEchos.fr, 31 January 2017, available at https://www.lesechos.fr/idees-debats/cercle/cercle-165613-linnovation-lautre-arme-du-brexit-2061519.php.

[4] Regulatory sandbox lessons learned report, Financial Conduct Authority, October 2017, available at https://www.fca.org.uk/publication/research-and-data/regulatory-sandbox-lessons-learned-report.pdf.

- The ICO's Technology Strategy 2018-2021[5] announced the intention of establishing a Regulatory Sandbox—"to enable organisations to develop innovative digital products and services, whilst engaging with the regulator…." It is of some significance that this initiative received top-level political endorsement, including at the WEF 2018 Summit in Davos.[6]

Relevant examples from the Financial Conduct Authority

The FCA "Lessons Learned" report recorded that 146 applications were received for the first two six-month cohorts. 50 were accepted and 41 tested.

- One firm is testing a Distributed Ledger Technology platform that enables consumers to pay, log-in and verify their identity using biometrics.
- Another proposition uses facial recognition technology to feed into the risk profiling assessment used by a financial adviser.
- A data-sharing experiment between a large firm and a Fintech company successfully provided a product which increased customers' savings through analysis of current account transactional data.
- A number of firms have used the Sandbox to test Robo-Advice models.

<u>Benefits</u>

A Regulatory Sandbox can simultaneously address two inevitable uncertainties—the uncertainties of innovation ("what is this going to deliver?") and the uncertainties of principles-based regulation ("will this processing be fair?"). As noted above, technical innovation is impacting on data protection regulation and compliance more rapidly and to an even greater extent than on financial services. Across the data protection community, compliance is increasingly treated as an iterative and agile process, just like software and technology development.

Against this background, the benefits of a Regulatory Sandbox—as a mutually beneficial laboratory—should be obvious. However, it is worth summarising them—not least to stress

[5] Technology Strategy 2018-2021, UK Information Commissioner's Office, available at https://ico.org.uk/media/about-the-ico/documents/2258299/ico-technology-strategy-2018-2021.pdf.

[6] 2018 speech in Davos, Matt Hancock, the Secretary of State for Digital, Culture, Media and Sport, 25 January 2018, available at http://www.ukpol.co.uk/matt-hancock-2018-speech-in-davos/.

that the benefits accrue both to organisations and to the ICO itself. There are also much wider social and economic benefits and, perhaps most important of all, benefits to individuals whose personal data is being processed.

(i) Benefits to Organisations

- Reductions in regulatory uncertainty and the time in getting new ideas to market;
- Incentives—especially for SMEs—to innovate (or proceed further with an innovation) with better confidence about the eventual regulatory environment;
- The opportunity to participate in frank and confidential discussions about the implications and acceptability of a technological or other innovation;
- The ability to build mutual trust and constructive dialogue with key data protection regulators, including the Lead DPA in the context of the GDPR;
- The ability to develop ground-breaking products/services in a live market with a degree of assurance that the experimental and testing phases are unlikely to fall foul of regulatory requirements;
- A degree of confidence that a new product or service can then be launched without the prospect of regulatory challenge or enforcement action;
- Early warning, from a trusted, independent and authoritative source, that a particular feature will not be acceptable;
- The ability, at a relatively early stage, to modify a feature to ensure acceptability;
- In extreme cases, the opportunity to abandon a product, service or feature before excessive expenditure of time, effort and money;
- For public sector organisations specifically, the ability to deliver more efficient and cost-effective innovative government services, which are compliant, socialised and acceptable to multiple stakeholders and a wider public opinion (in other words avoiding the lost opportunity of some past initiatives, such as the government's care.data).

(ii) Benefits to the ICO

- Insights (otherwise largely unobtainable) into upstream technological developments to get an early indication of how data protection requirements are likely to impact upon a very fast-moving playing-field;
- The ability to fulfill the ICO's leadership function by asserting its influence at critical stages;
- Reasonable assurance that innovative products will be compliant;
- Building trust and constructive dialogue with key private and public sector organisations involved in the data economy and society;
- Access to intelligence about cutting-edge research and development and about the direction of travel of innovation, allowing the ICO to better target its resources;

- Improved "bottom-up" know-how to feed into ICO or EDPB Guidance and/or future legislation.

(iii) Social and Economic Benefits

- Economic prosperity depends upon the success of the digital economy and in a rapidly-changing environment there are obvious benefits if innovative products and services which are known to comply with regulatory requirements can be swiftly brought to market;
- There is also considerable scope to deploy the Sandbox approach in such "quality of life" areas as medical research, transport, policing, telecommunications, targeting of social benefits, etc.;
- Reduces the reticence risk that many organisations face when considering innovative, cutting-edge technologies while at the same time being concerned with high regulatory enforcement risks.

(iv) Benefits to Individuals

- The fundamental rights and freedoms of individuals will be better protected with appropriate safeguards where an innovative product or service (which many will struggle to understand) has been scrutinised, and perhaps modified and even socialised, as part of the Sandbox process;
- Consumers overwhelmingly value new products and services—as do patients, travelers and citizens;
- Everyone benefits where medical and similar research can proceed responsibly in ways which avoid uncertainties about data protection compliance.

An informal Sandbox

Following a series of discussions, Google gave assurances to the ICO in July 2008 that enabled the launch of Street View—namely that privacy would be protected by blurring faces and vehicle licence plates.

On April 23, 2009, the ICO ruled that, although Google Street View carries a small risk of privacy invasion, it should not be stopped. It ruled that Google Street View (with faces and licence plates blurred) did not contravene the Data Protection Act, as an image of a house held on Street View is not a data protection matter.

Since then Street View has been permitted in most European countries, provided that the same safeguards are in place.

Examples (actual or hypothetical) from CIPL members where Sandbox participation might have been (or still be) helpful

- Several CIPL members offer photo storage applications with useful features allowing the grouping of similar pictures together, organising them into albums, and more. Innovations in this type of product could benefit from Sandbox testing.

- All CIPL members have to comply with notice requirements under the GDPR, and many have continuous efforts underway to find the best way of communicating complex information about data processing to individuals in many different contexts. A Sandbox would allow for testing of new language, presentation, settings or user-design led solutions and lead to continued innovation in this field, with immediate benefits for individuals.

- One CIPL member offers a number of technologies aimed at improving the performance of mobile devices. These include software applications that:
  - improve location performance by providing data which enables devices to determine their location more quickly and accurately and conserve battery power;
  - improve security by identifying malware behaviour and alerting third-party security applications installed on the same device; and
  - improve quality of service such as reducing dropped-calls or improving battery performance by collecting telemetry data.

  While the CIPL member minimizes data collection and retention, pseudonymizes the information it collects and makes no attempt to personally identify users, the member would have valued a Regulatory Sandbox as these technologies were being developed to explore design choices to meet data protection compliance obligations.

- Another member has identified projects focused on artificial intelligence which enable innovative businesses to test and pilot AI responsibly, as prime examples of where a Sandbox approach would be beneficial for all.

- A CIPL member suggested that the Sandbox could be useful for initiatives involving innovative access to data—aligned to the broader topic of "Data Trusts"—enabling business and research institutions to develop, test and agree terms and conditions for access, sharing and use of data.

- It is understood that some companies have paused medical research and development out of uncertainty over the GDPR provisions relating to scientific research. A Sandbox would be an ideal environment for them to continue pursuing beneficial research while receiving guidance about compliance.

Public sector example where the Sandbox might have been useful

In 2017 the ICO announced[7] that the Royal Free Hospital in London had not complied with the Data Protection Act when it provided the sensitive medical data of around 1.6 million patients to DeepMind, an artificial intelligence company, as part of a clinical safety initiative. Although successful outcomes had been reported, the NHS Trust which ran the hospital was required to commit to various changes to ensure future compliance with the law.

> *"The Trust did carry out a privacy impact assessment, but only after DeepMind had already been given patient data. This is not how things should work…The vital message to take away is that you should carry out your privacy impact assessment as soon as practicable, as part of your planning for a new innovation or trial. This will allow you to factor in your findings at an early stage, helping you to meet legal obligations and public expectations…**New cloud processing technologies mean you can, not that you always should**…Changes in technology mean that vast data sets can be made more readily available and can be processed faster and using greater data processing technologies. That's a positive thing, but just because evolving technologies can allow you to do more doesn't mean these tools should always be fully utilised, particularly during a trial initiative."* **(Elizabeth Denham, Information Commissioner)**

Participation in a Regulatory Sandbox may have avoided some of the problems which were encountered in this situation, perhaps if the hospital had agreed with the ICO how best to share limited volumes of patient data for medical research on a pilot or trial basis before the bulk transfer.

Machine learning in the criminal justice system – A future candidate for the Sandbox?

A recent study[8] published by the Royal United Services Institute and the Centre for Information Rights, University of Winchester calls for measures to regulate computerised decision-making in policing.

Issues include a lack of transparency and the choice of data to train artificial intelligence

[7] See Royal Free – Google DeepMind trial failed to comply with data protection law, UK ICO, 3 July 2017, available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/.

[8] A. Babuta *et al*., Machine Learning Algorithms and Police Decision-Making – Legal, Ethical and Regulatory Challenges, RUSI Whitehall Report 3-18, September 2018, available at https://rusi.org/publication/whitehall-reports/machine-learning-algorithms-and-police-decision-making-legal-ethical.

systems, the report notes. Reliance on police arrest data, for example, is "particularly problematic" as it may reflect the fact that a particular neighbourhood—or racial group—has been disproportionately targeted by police in the past. If that data then informs systems that predict future crimes, it can create a feedback loop "whereby the predicted outcome simply becomes a self-fulfilling prophecy".

The report argues that "it is essential that such experimental innovation is conducted within the bounds of a clear policy framework, and that there are sufficient regulatory and oversight mechanisms in place to ensure fair and legal use of technologies within a live policing environment".

It recommends that any trials using predictive policing tools must be comprehensively and independently evaluated before moving ahead with large-scale deployment.

Practicalities

The principles and procedures which will be used to create and operate the ICO's Sandbox will be important, but will be challenging.

CIPL recognises that the ICO must operate within a statutory framework which itself reflects the GDPR regime. This does not explicitly provide for the Sandbox concept, although it allows for an increasingly active and wide role for the DPA. It also imposes various duties on the ICO which may not be easily reconciled. The challenge may be especially acute where organisations wish to test and develop something with "real" customers (even a limited number for a limited time). Moreover, ICO cannot grant exemptions or anticipate feeding results into new legislation (as in Singapore). Nor can it easily use waivers or "No Enforcement" letters (as with the FCA). Lastly, there is no authorisation regime (as with the regulation of financial services) which provides scope for limited or conditional authorisation for Sandbox purposes (apart from the prior consultation for the DPIAs where the high risk cannot be mitigated).

These challenges are, however, not insurmountable. We believe that in fact the ICO has considerable scope to rely upon the powers and discretions which are available to it under the GDPR.

An approach which incorporates the following features may maximize the prospects of success:

- Clear, objective and transparent criteria for innovations which qualify for entry into the Sandbox programme—not least to avoid any risks of anti-competitive "favouritism". The approach to criteria is elaborated below.
- Covering new business models as well as technological innovation;
- Accessible to both private and public sector organisations;
- As "open" as possible—especially to SMEs and multinational companies;

- Acceptance and assessment processes must be speedy, to work fast for rapidly-changing markets;
- Acceptance should be accompanied by commitment to a realistic and agreed timescale;
- Clear labelling and ring-fencing of Sandbox participants (as with FCA's successive "cohorts");
- Maximum clarity about likely "outputs"—including influence on future guidance and learning of benefit to non-participants;
- "Rules" which spell out procedures, the nature of "safe space supervision", safeguards to protect the rights of individuals in the pilot, likely stages of interaction, anticipated outcomes and exit conditions;
- But rules which are not bureaucratic, rigid or "one-size-fits-all";
- A degree of informality and flexibility to reflect both diversity of participants and the speed of technological developments;
- Clear points of contact, preferably via dedicated case officers with expertise to understand both technological and privacy issues;
- An explicit recognition in suitable language that—while not tolerating obvious or serious non-compliance—supervision of Sandbox testing means that a degree of regulatory relaxation must be permitted;
- A strong commitment that the Sandbox will **not** be the ICO's only form of constructive engagement—it is vital that the traditions of approachability, dialogue, pragmatic guidance and advice continues to flourish;
- Clarity about the relationship between the Sandbox facility and DPIAs—which are required (inter alia) where "new technologies…[are] likely to result in a high risk to rights and freedoms". This point is also elaborated below.
- Commitment to confidentiality and commercial sensitivities involved in new projects and technologies, including consideration on how the FOI rules to which the ICO is subject may (or may not) apply and impact the discussions and content of the Sandbox.

Criteria for Acceptance into the Sandbox

As stated above, it will be essential to have criteria for participation which are clear, objective and transparent. On the one hand, the criteria will raise the profile of the scheme and effectively spell out incentives for participation. On the other hand, they will enable the ICO to select participants objectively and rationally if (as with the FCA) there is over-subscription. A list of possible Sandbox scenarios would also be helpful, especially in the early days.

It is not yet possible to propose a comprehensive set of criteria, but they are likely to include:

- identifiable consumer or public interest benefit;

- genuinely innovative and exceptional projects (not a routine short-cut to ensuring compliance);
- real need for Sandbox testing, especially where there is:
  - regulatory uncertainty; and/or
  - a clear element of experimentation where a "live" environment is needed;
- contributing to the development of the digital economy and society;
- contributing to one or more of the regulatory objectives (e.g. free flow of information, "open data" for research);
- no obvious breach or threat to individuals' rights;
- workable arrangements for ICO "supervision";
- ready to test.

It is also important—not least to foster competition—that the ICO ensures diversity of participation, with the Sandbox open to all—private, public and voluntary sectors; large, medium and small enterprises; incumbents and new entrants.

There is a case for accommodating some projects that will require a very short timeframe with a need for quick and actionable feedback.

More generally, there is merit in offering admission to the Sandbox as an incentive to maximise accountability. Certainly, there is a case for the ICO to give some priority to those organisations which manifestly present a high degree of accountability and are able to demonstrate such accountability.

Although this may not be currently contemplated, we can also see merit in participation being available on a sectoral basis. A group of organisations which are facing similar issues as their technologies or practices develop on broadly similar paths, may come together with a joint proposal to the ICO. This could be done in ways which in fact facilitate ICO supervision. This approach could be especially attractive for public sector bodies, for start-ups or with coalitions like the Partnership on AI.

Finally, although this may not strictly be a criterion, we can foresee situations where the ICO itself may wish to propose Sandbox participation as a corrective measure, or even an alternative to enforcement action. This may, for example, arise where there is a real blocking-point and/or genuine disagreement about the application of a data protection requirement which cannot be easily resolved without supervised testing.

<u>Relationship with Data Protection Impact Assessments</u>

As noted above, it will be important for the ICO to be clear about the relationship between the Sandbox facility and DPIAs. Organisations will be aware that the ICO's 2018 Regulatory Action Policy states that "breaches involving novel or invasive technology…without having done a full

Data Protection Impact Assessment and taken appropriate mitigating action…can also expect to attract regulatory attention at the upper end of the scale".

We believe that DPIAs and the Sandbox are two different concepts, with different objectives and present different avenues for organisations. Therefore, they should not be confused. It can be argued that a DPIA is not intended for a genuinely experimental exercise, even where live data is used. In any event, the DPIA should take place, where appropriate, "prior to processing". This should be interpreted purposively so that Sandbox testing—normally with only pilot data and under "supervision"—can happen at an earlier stage. Satisfactory testing, with or without any modification, can thus anticipate a DPIA and—with better information—may in fact make it easier to conduct any subsequent assessment. In some cases, it may be possible to replace it altogether. In any event, it should be made clear that the Sandbox can be used for a product or development whether or not it would require a DPIA.

Safeguards

It is important that the Sandbox approach addresses some of the real concerns that are likely from prospective participants. In the time available for this response, CIPL has not been able to conduct a comprehensive survey amongst its members. In any event, the organisations would probably need more details from the ICO before giving meaningful answers. But it can be predicted that their main concerns will focus on:

- Fears that participation may not be voluntary, or that there may be an increased pressure for organisations to take part in the Sandbox, even with potential "implicit" negative consequences for those that don't take part;
- Risks that information about innovative products and services (sometimes even mere headline descriptions) will fall into the hands of competitors or enter the public domain prematurely;
- Risks that information shared in good faith with the ICO will lead to adverse enforcement action.

Suitable safeguards on the following lines will be needed to address these concerns:

- Assurance from the ICO that no organisation will be compelled to participate in the Sandbox, or will suffer any disadvantage just because it fails to participate or withdraws early;
- Very strong security and confidentiality assurances in respect of information received by the ICO from a Sandbox participant;
- Regular and strong internal and external reminders that section 132 of the 2018 Act makes it a criminal offence for ICO personnel to disclose commercially confidential information which has been provided to the Commissioner;

- A preliminary consideration of how FOI requirements may or may not apply to the Sandbox information and content in general, with additional consideration in particular cases of Sandbox application;
- A confirmation, backed up with explicit assurances, that—while participants must comply with the law without expectations of exemptions—the ICO will observe the principle, in line with the presumption against self-incrimination, that information shared in the course of a Sandbox exercise should not be used to prejudice anyone;
- Accordingly, information disclosed into the Sandbox will only be used as the basis for enforcement action in exceptional circumstances, for example where there has been deception or mis-representation;
- The ICO is prepared to use its discretion constructively to give some benefit of the doubt where—during testing in a "real-life" scenario in the "supervised space"—genuine uncertainty arises as to whether or not an innovation involves non-compliance;
- Assuming that the feature is removed or modified before the main launch, enforcement action will not follow where supervised testing in fact reveals non-compliance;
- Failure to follow a recommendation received in the Sandbox would not automatically be used to justify enforcement action.

Facebook working with the IMDA and PDPC in Singapore

Facebook, in partnership with Singapore's Infocomm Media Development Authority (IMDA), has unveiled "Startup Station Singapore", a six-month programme to support innovative data-driven start-ups that are developing the next generation of business solutions. The programme aims to help establish a model of data innovation for Asia and the rest of the world.

As part of their collaboration, this accelerator will include a Regulatory Sandbox, where IMDA, working with Facebook, will support the start-ups by providing support in defined areas of interest, including forward-looking regulatory provision for AI/machine learning and data portability.

The initiative is seen by Facebook and IMDA as a good example of industry-government collaboration—both in its goals of supporting innovative data-driven start-ups and in developing better and more effective regulation. Start-ups are often innovation leaders, but their fledgling business models can be vulnerable to poorly designed or administered regulation, especially where they operate at the forefront of technology frontiers.

As it is focused on data-driven start-ups across a range of different verticals, a key focus for the Sandbox will be the question of accessibility, with strong incentives for start-ups to participate. This is particularly critical as many start-ups have limited development resources to deploy and must choose where and how they invest with great care.

Going Forward

CIPL hopes and expects that the ICO's Regulatory Sandbox initiative will be a great success. It is quite possible that—as with the FCA—interest will be significantly higher than might be initially expected. Even if there has to be a strict process to select participants, that in itself will demonstrate the demand for such a facility. We also anticipate that other DPAs around the world will want to follow the ground-breaking leadership of Singapore and the UK. This approach could be specifically incentivised by the EDPB, too. Finally, there may also be scope, at least in due course, to have cross-border Sandboxes with counterpart DPAs, or joint Sandboxes with other regulatory bodies (e.g. the FCA or energy or telecommunications regulators).

We hope that all the above comments will be helpful as the ICO scheme is developed. This is an initial call for views and inevitably there will still be many unknowns. We very much hope that, in the spirit of dialogue which must characterise any Sandbox initiative, the ICO will continue to engage with relevant stakeholders as the architectural process continues and the building blocks are put in place.

CIPL certainly stands ready to help in any way it can. In particular, we hope we can co-host a small by invitation only roundtable with the ICO in London at some point in the next few months to take forward Sandbox thinking. We will also publicise the ICO initiative and our response, including to other DPAs with whom we are in contact.

If you have any questions or would like additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; or Sam Grogan, sgrogan@huntonAK.com.