Centre for Information Policy Leadership
Hunton Andrews Kurth

8 March 2019

Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice

"It's not a choice between privacy or innovation"[1]

"A Sandbox is essentially 'Supervised Privacy by Design'"[2]

1. Summary

What is a "Regulatory Sandbox"? How could it contribute to high standards of data protection and privacy and promote innovation? What are the challenges and problems? What safeguards are needed? Why would regulators and organisations want to participate in a Sandbox?

In this white paper, the Centre for Information Policy Leadership (CIPL)[3] sets out the key features of the concept. Essentially, it is a supervised "safe space" set up by a Data Protection Authority (DPA) for piloting and testing innovatory products, services, business models or delivery mechanisms of participating organisations in the real market, using the personal data of real individuals.

We identify the main benefits of the approach—for organisations, for DPAs, for policymakers, for economic and social progress and for individuals.

There will be challenges, not least where legislative frameworks do not explicitly accommodate the Sandbox concept. But the challenges are not insurmountable and we set out various practical suggestions to maximise the prospects of success. We attach particular importance to the need for clear, objective and transparent criteria for participation—notably an innovative element and regulatory complexity or uncertainty.

Prospective participants will have some anxieties—especially around commercial confidentiality and the risks of adverse enforcement action—and our response sets out some safeguards which we suggest DPAs should put in place. In particular, CIPL considers that information

[1] Elizabeth Denham, CBE, UK Information Commissioner.
[2] Participant at CIPL Roundtable on the Regulatory Sandbox, 19 February 2019.
[3] 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 74 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.

disclosed into the Sandbox should only be used as the basis for enforcement action in exceptional circumstances and there will need to be some tolerance where—during testing in a real-life scenario in the supervised space—new uncertainties arise about compliance.

As with any novel concept, there will also be risk and concerns on both sides as to why regulators and organisations would invest in the Sandbox process and concept. Some may ask, what is the "return on investment" of considerable time and resources? CIPL believes that the direct, short-term and indirect, long-term benefits to all will ultimately prevail over any concerns and reservations. CIPL especially sees the potential of the Sandbox to address and resolve some of the more challenging aspects of deploying innovative technologies, services and projects in the modern information age, against the backdrop of less agile and more traditional regulatory frameworks. The Sandbox provides an opportunity for accountable organisations and innovative regulators to work and learn together in a collaborative fashion to enable all the benefits of the digital transformation of our society and economies and the protection of individuals' privacy and personal data.

2. The Rise of Regulatory Sandboxes

The Regulatory Sandbox concept originated with financial services. In brief, the financial regulatory body establishes and oversees a forum where organisations can experiment and test innovative products, services, business models and delivery mechanisms in a live market with real consumers. It is a supervised "safe haven" which encourages and supports innovation in ways which will comply with legislative and other requirements. Such a supervised space can provide organisations with reduced time-to-market for new products and services, combined with assurance that they have built in appropriate safeguards.

In this laboratory environment each Sandbox participant is expected to have clear objectives (such as reducing costs to consumers) and to carry out its testing on a small scale, with innovations being tested for a limited duration with a limited number of customers.

The most progress with the Sandbox concept has been made by the UK's Financial Conduct Authority (FCA) which announced its programme at the end of 2015.[4] In October 2017, the FCA published a very helpful and encouraging "Lessons Learned" report.[5] Since then, the regulatory and expert data privacy community has started to explore the Sandbox concept in the context of data protection. There have been a series of significant developments to date:

[4] The usage of the Regulatory Sandbox for Fintech innovations has since expanded to other jurisdictions. For example, in January 2018, Taiwan passed its Financial Technology Development and Innovation Experimentation Act which provides for the creation of a Regulatory Sandbox that allows Fintech start-ups to develop and test out their products and services without endangering the rights of individuals. In addition, the Australian Securities and Investments Commission has created a Sandbox framework that allows eligible Fintech businesses to test certain specified services for up to 12 months without an Australian financial services or credit licence.

[5] 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.

- In 2017, the Singapore Personal Data Protection Commission published a Guide to Data Sharing that set out details of how a proposed Regulatory Sandbox will work—so that accountable businesses "are not held back from deploying technological and business innovations". Since then a programme set up to support innovative data-driven start-ups includes a Regulatory Sandbox, with strong incentives for participation.

- CIPL's 2017 paper Regulating for Results[6] proposed that for maximum effectiveness, DPAs should give the "Leadership" function the top strategic priority. Constructive engagement with regulated entities is needed to encourage a spirit of trust and mutual co-operation. This is even more important given that rapid technological developments, digitalisation and datafication of our societies and economies require innovative regulatory approaches, in addition to traditional laws, regulations and regulatory policies. This paper identified the Sandbox concept—"creating space for responsible innovation"—as a potential example of constructive engagement and innovative regulatory and oversight policy in practice.

- In December 2017, the Finnish Ministry of Economic Affairs and Employment published a report on Finland's national AI strategy which notes that a framework which ensures the availability of data must be created and that a "regulatory sandbox" experimentation environment can be created as one way to encourage data sharing.[7]

- In 2018, the Singapore Personal Data Protection Commission (PDPC) used the Sandbox in order to test possible changes to Singapore's Personal Data Protection Act (PDPA).[8]

- In the UK, the Information Commissioner's Office (ICO) announced in its Technology Strategy 2018–2021[9] the intention of establishing a Regulatory Sandbox—"to enable organisations to develop innovative digital products and services, whilst engaging with

[6] "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.

[7] Finland's Age of Artificial Intelligence, Ministry of Economic Affairs and Employment of Finland, December 2017, available at http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160391/TEMrap_47_2017_verkkojulkaisu.pdf?sequence=1&isAllowed=y at page 44.

[8] See Speech by Dr Yaacob Ibrahim, Minister for Communications and Information at the Personal Data Protection Seminar 2017, available at https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2017/7/personal-data-protection-seminar-2017 at paragraph 18 ("The PDPC is also prepared to work with companies who adopt accountability practices to create regulatory sandboxes to allow us to understand how our proposed changes to the PDPA might work in practice so that we can fine-tune the details before we amend the PDPA. This will enable companies who are ready to continue to be innovative and competitive").

[9] 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.

the regulator…". It is of some significance that this initiative received top-level political endorsement, including at the WEF 2018 Summit in Davos.[10]

- In 2018, the ICO carried out a public consultation on creating a Regulatory Sandbox which generated 65 responses, which were summarised in a paper published in November 2018.[11] The paper outlined how the ICO intends to proceed in the light of the "overwhelmingly positive response". The ICO has since published a further discussion paper on how the Sandbox will work, during a pilot programme, or "beta phase", from March 2019 to September 2020.[12]

- In Malta, specific legislation[13] has paved the way for a Regulatory Sandbox for testing Artificial Intelligence against pre-determined functional outputs.

- In India, a 2018 consultation on Privacy, Security and Ownership of Data in the Telecom Sector by the Telecom Regulatory Authority of India (TRAI) asked whether a data sandbox should be set up to allow regulated companies to create anonymised data sets which can be used for the development of newer services.[14] This topic was then identified for "further deliberations" after implementation of the data privacy law.[15]

- In December 2018, the European Commission announced its "Coordinated Plan on Artificial Intelligence", involving some €1.5 billion between 2021 and 2027, for experimenting and testing Artificial Intelligence technology. The Annex elaborates how testing facilities "may include regulatory sandboxes…in selected areas where the law provides regulatory authorities with sufficient leeway".[16]

---

[10] 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/.

[11] ICO's call for views on building a sandbox: summary of responses and ICO comment, available at https://ico.org.uk/media/about-the-ico/consultations/2260322/201811-sandbox-call-for-views-analysis.pdf.

[12] See Sandbox Beta Phase Discussion Paper, UK Information Commissioner's Office, January 2019, available at https://ico.org.uk/media/2614219/sandbox-discussion-paper-20190130.pdf.

[13] Malta Digital Innovation Authority Act, available at http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=12873&l=1.

[14] See TRAI Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector, 9 August 2017, available at https://trai.gov.in/sites/default/files/Consultation_Paper%20_on_Privacy_Security_ownership_of_data_09082017.pdf at page 24, question 6.

[15] See TRAI Recommendations on Privacy, Security and Ownership of the Data in the Telecom Sector, 16 July 2018, available at https://www.trai.gov.in/sites/default/files/RecommendationDataPrivacy16072018_0.pdf at page 58.

[16] Annex to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Coordinated Plan on Artificial Intelligence (COM(2018) 795 final), 7 December 2018, available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56017.

- There are some parallels with the Sandbox principle in the United States. It is common for companies with an innovation to "run it by" the FTC or other regulators on an informal basis prior to rollout. Rules made under the Children's Online Privacy Protection Act (COPPA) provide a more formal opportunity for companies to apply to the FTC for approval of new methods of parental consent. This takes the form of a written application for public comment and approval.[17]

- In the EU context, there are also some parallels with the procedures for Binding Corporate Rules (BCR) which in practice have involved extensive (and mutually welcome) dialogue between DPAs and applicant companies.

Relevant examples from the Financial Conduct Authority

The FCA "Lessons Learned" report recorded that 146 applications were received for the first two 6-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.

3. Benefits

A Regulatory Sandbox in data protection 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 more rapidly and to an even greater extent than on financial services. Given the remarkable transformation of our societies and economies as part of the fourth industrial revolution, it is critical that every country and government works to ensure this digital change takes place in a way which enables the benefits but minimises the risks. In the context of data protection, this means enabling data-driven innovation while ensuring responsible use of data and protection of individuals' rights and interests. All

[17] COPPA Rule §312.12 (Voluntary Commission Approval Processes).

stakeholders are being challenged to achieve this balance—governments and policymakers, legislators, regulators and public and private sector organisations that depend on the use and processing of personal data. Across the data protection community, compliance is increasingly treated as an iterative and agile process, with feedback loops and improvements along the way.

We identify the following benefits of a Regulatory Sandbox:

(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 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;
- Recognition as a market leader and an accountable and responsible business that deploys accountability and corporate digital responsibility in practice; and
- An opportunity to build a relationship and constructively engage with a data protection regulator.

(ii) Benefits to the DPA

- Improved effectiveness through a targeted programme of constructive engagement;[18]
- 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 fulfil the DPA's leadership function by asserting its influence at critical stages;
- Reasonable assurance that innovative products will be compliant;
- Access to intelligence about cutting-edge research and development and about the direction of travel of innovation, allowing the DPA to better target its resources;
- Improved "bottom-up" know-how to feed into guidance and/or future legislation; and
- Reduced likelihood that other regulators (e.g. financial services) will reach unhelpful conclusions on data protection/privacy issues within their own Sandbox schemes.

[18] See CIPL paper on "Regulating for Results", *op. cit.*

(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;
- Improved assurance that innovation is taking place in a responsible and accountable manner;
- There is also considerable scope to deploy the Sandbox approach in such "quality of life" areas as medical research, healthcare service and delivery, employment, transport, policing, telecommunications, targeting of social benefits, etc.

(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, as part of the Sandbox process.
- Consumers (and patients, travellers, citizens and employees) overwhelmingly value new products and services that deliver convenience and real value for them.
- They will benefit even more where privacy safeguards have been tailor-made and scrutinised, with confidence that their data will be used responsibly and protected.
- More generally, everyone benefits where medical and similar research can proceed responsibly in ways which avoid uncertainties about data protection compliance.

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 transparency requirements under the GDPR, and many have continuous efforts underway to find the best way of communicating complex information about data processing. A Sandbox would allow for testing of new language, presentation or settings and lead to continued innovation in this field, with immediate benefits for consumers.

- 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 minimises data collection and retention, pseudonymises 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 (1) projects focused on Artificial Intelligence which enable innovative businesses to test and pilot AI responsibly and (2) 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 and use of data.

- At a recent DPIA seminar, CIPL members suggested that a company which is developing a privacy risk framework could put it forward as a Sandbox project. There is a clear need for consensus on how to assess the likelihood and severity of risks and harms to fundamental rights and freedoms of individuals. A Sandbox project, preferably with a real-life scenario, could be an excellent step towards alignment between industry and regulators.

- At CIPL's Roundtable on the Regulatory Sandbox, held in London, in February 2019, numerous further suggestions were made, including:
  - personalised medicine and other health initiatives;
  - identifying societal harms on social media;
  - online recruitment and facilitation of home-working;
  - tagging of offenders;
  - airport biometric checks;
  - supermarket trolley assessment;
  - identifying personalised gambling threats;
  - facial recognition experiments; and
  - online banking identity checks.

Public sector example where the Sandbox might have been useful

In 2017 the ICO announced[19] 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[20] 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

[19] 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/.

[20] 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.

4. Hesitations

Despite the benefits, there will be concerns from many organisations which may well deter participation, or at least cause some to hesitate.

Concerns are likely to focus on:

- Fears that participation may not be entirely voluntary;
- Threats to brand or corporate reputation;
- Wasted upfront investment if not selected for participation;
- Incompatibility or reliability of timelines, especially where swift and agile responses will be needed from the DPA;
- Inadequate technical know-how within the DPA;
- Handling changes to a product or service during the lifetime of Sandbox participation;
- 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;
- Fears that the DPA may propose unrealistic or poorly informed refinements to manufacturing practices or key processes;
- Risks that information shared in good faith will lead to adverse enforcement action;
- Risk and concern that the Sandbox may not yield results or would be unduly burdensome and a drain on resources;
- In the context of the EU and the GDPR, uncertainties about the relationship between the Sandbox and Data Protection Impact Assessments (DPIAs);
- Uncertainty about the international scope of a Sandbox process; and
- Difficulties in getting senior leadership buy-in and agreement to engage in the Sandbox, due to perceived risks.

Most of these concerns reflect the reduced control when any sort of joint endeavour is attempted, but will be more acute when the relationship is with the regulatory body. The key to success will be mutual trust, and this will need to exist and be nurtured at all times. Recognising and responding to concerns, and mutual awareness of expectations and constraints, will all be fundamental.

Sandbox participation must be seen as a win-win opportunity. In the next three sections, CIPL suggests ways forward to make the Sandbox concept work in the privacy/data protection context, while addressing these predictable concerns. These cover the practicalities (in terms of both principles and procedures) needed to create and operate a Sandbox, the Criteria for participation and the Safeguards which must be built in from the outset. Separate sections then address the more specific concerns about DPIAs and the international dimension.

5. Practicalities of Setting Up the Sandbox

CIPL recognises that each DPA must operate within its own legal framework. As far as CIPL is aware, none of the existing laws explicitly accommodate the Sandbox concept. Some impose various duties on DPAs which may not be easily reconciled with a formal Sandbox. The challenge may be especially acute where organisations wish to test and develop something with the live data of "real" customers (even a limited number for a limited time). Moreover, DPAs cannot normally grant exemptions, or feed results into new legislation. Nor can they easily use waivers or "No Enforcement" or "Comfort" letters. Lastly, there is not the same prior-authorisation framework as is common for the regulation of financial services which can provide scope for limited or conditional authorisation for Sandbox purposes.

Ideally, relevant laws would explicitly authorise the DPA to oversee a Sandbox programme and facilitate their deployment, but this is not likely to happen in the short term.

The various challenges are not insurmountable. CIPL believes that, in fact, DPAs have considerable scope to rely upon the powers and discretions available to them to be able to launch and operate a Sandbox and to address predictable concerns. An approach which incorporates the following features may maximise the prospects of success:

- Clear, objective and transparent criteria for types of innovative projects, initiatives and technologies 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 and explicit availability of the Sandbox to organisations outside of the financial sector (given that the Sandbox concept has been mostly utilised in this sector to date).

- Speedy acceptance and assessment processes which will work fast for rapidly changing markets.
- Commitment to a realistic and agreed timescale.
- Clear labelling and ring-fencing of Sandbox participants.
- Complete agreement about the respective roles and responsibilities.
- Maximum clarity about likely "outputs"—preferably with the aim of a "regulatory comfort" letter or similar document.
- Outputs which include influence on future guidance and learning of benefit to non-participants.
- Clarity about rules on publicising or otherwise sharing outcomes of a Sandbox and when such activities are appropriate (e.g. for educational purposes or in cases of impact on the wider marketplace or specific industry).
- Clear and explicit operating rules and procedures which spell out 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.
- Acknowledgement that Sandbox experiences may be bespoke and not "one-size-fits-all".
- A degree of informality and flexibility to reflect diversity of participants, issues brought to the Sandbox 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 and a reiterative compliance process must be permitted.
- A strong commitment that the Sandbox will **not** be the DPA's only form of constructive engagement—it is vital that the traditions of approachability, dialogue, pragmatic guidance and advice continue to flourish.
- Consideration of how to collaborate with other national regulators who may also be using a Sandbox process for the same project, in the context of their regulatory powers and area. It is very likely that a Fintech project or a financial services project involving Blockchain technology or big data deployment may be introduced into the financial regulator Sandbox and a data privacy Sandbox.

6. Criteria for Acceptance into the Sandbox

As stated above, it will be essential to have criteria for participation which are clear, objective and transparent. It is not yet possible to propose a comprehensive set of criteria, but they are likely to include:

- Identifiable benefits for individuals or the public interest;

- Genuinely innovative, cutting-edge projects (not a routine short-cut to getting free legal advice or an assurance of compliance);
- Real need for Sandbox testing, especially where there is:
    - regulatory uncertainty (probably for both the DPA and the organisation); and/or
    - a clear element of experimentation where a "live" environment is needed;
- Contributing to the development of the digital economy and society and supporting wider governmental strategies for innovation and digital leadership;
- Contributing to one or more of the regulatory objectives (e.g. free flow of information, greater transparency, responsible data sharing between sectors);
- No obvious breach or threat to individuals' rights;
- Workable arrangements for the DPA's "supervision"; and
- Readiness and viability to engage and test.

In order to foster wide acceptance and competition, it is also important that each DPA 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. In the early years at least, DPAs should prioritise proposals with a clear social benefit.

More generally, admission to the Sandbox should be offered as a specific incentive to maximise accountability. It is important to link the Sandbox to accountability, as a way of encouraging and incentivising best practices and good behaviours among regulated organisations. Accountable organisations should be able to engage in a Regulatory Sandbox, as an additional regulatory incentive. Of course, accountability is an evolving process and a journey; hence, a commitment to accountability may be a sufficient criterion for some organisations, especially SMEs and start-ups.

Participation might also be made available on a sectoral basis. Here, a group of organisations which are facing similar issues as their technologies develop on broadly similar paths may come together with a joint proposal. This approach could be especially attractive for public sector bodies, for start-ups or with coalitions like the Partnership on AI. In the EU context, there is also scope for Sandbox use by companies that are engaging together with a Code of Conduct under Article 40 of the GDPR.

Finally, although this may not strictly be a criterion, we can foresee situations where the DPA 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.

7. Safeguards

DPAs have to be aware of the likely concerns of prospective participants and the potential barriers to entry. These will be even more exaggerated in the Sandbox pilot phase and its early years of functioning as organisations may be reluctant to be "guinea pigs" for Sandbox experimentation. Some may justifiably ask "What's in it for us?" and this dynamic needs to be addressed by the regulator.

Some of the suitable safeguards to address these concerns could be, for example:

- Assurance 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 in respect of information received by the DPA from a Sandbox participant, as well as protection of intellectual property rights. This also includes appropriate procedures in case of Freedom of Information Act requests;
- Confirmation (backed up with explicit assurances and some separation of functions) that while participants must comply with the law without expectations of exemptions—the DPA 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 or where the conditions for participation have not been respected;
- The use of regulatory discretion 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; and
- Failure to follow a recommendation would not automatically be used to justify enforcement action, without further investigation and contact with the organisation.

It will also be important not to neglect safeguards to protect the interests of individuals whose data is processed in any Sandbox. It can be expected that this will naturally be a prime concern for the supervising DPA. Safeguards will be needed, for example, to ensure that:

- Appropriate consents, where necessary, have been obtained or other legal grounds apply for the processing in question;

- Individuals have been adequately informed and their rights are not imperilled; and

- A Sandbox experiment takes account of any risks to individuals and is stopped for further consideration and deliberation if high risks become apparent.

It would not be practicable for any liabilities to be suspended where individuals have a right of action for a violation which occurs in the context of a Sandbox experiment. But that is likely to act as a rational constraint on the experiment and provide a safeguard in itself.

8. Relationship with Data Protection Impact Assessments

Although the GDPR does not explicitly contemplate any Sandbox mechanism, its risk-based approach is broadly consistent with the approach. Sandbox participants engaged in otherwise "high-risk" processing would be able nevertheless to engage in processing because their Sandbox participation will have required appropriate mitigations and voluntary regulatory oversight. Equally, if the Sandbox experience demonstrates that the risks cannot be adequately mitigated then the project will probably need to be abandoned or radically changed.

As noted above, it will be important for DPAs enforcing the GDPR to be clear about the relationship between the Sandbox facility and Data Protection Impact Assessments (DPIAs). There is an opportunity for some really creative methodologies here, but also a need for pragmatic flexibility.

A DPIA is required by the EU GDPR where, *inter alia*, "new technologies…[are] likely to result in a high risk to the rights and freedoms of natural persons". Prior consultation with the DPA is required in cases where high risks cannot be mitigated. It is very possible that many Sandbox scenarios may actually be "high risk" and even unmitigated high risk.

A DPIA is required "prior to processing". CIPL believes that this should be interpreted purposively and flexibly so that Sandbox testing—normally with only pilot data and under "supervision" with suitable guarantees—could happen at an earlier stage in suitable cases. This would be consistent with the need for prior consultation to mitigate risks. Satisfactory testing, with or without any modification, would thus anticipate a DPIA and—with better information—may then make it easier to conduct any subsequent assessment. A DPIA should be seen primarily as a means of assessing risk, and should never be a pre-condition for participation. In some cases, it may be possible to integrate Sandbox participation with the DPIA or replace it altogether. In other cases, Sandbox participation could be the result of a DPIA—i.e. as a means of verifying that risks have been suitably mitigated. Occasionally, it may be wise to repeat a DPIA after Sandbox participation.

In any event, it should be made clear that the Sandbox can be used for a product or other innovation whether or not it would require a DPIA. Regulators should also take the realistic view that very often the very cases brought into the Sandbox will be complex and involve high-risk processing, which sometimes cannot be mitigated easily, but which justifies trials, experiments and go-to-market due to its benefits and overall positive impact. This may especially be the case where there is low likelihood of a high risk materialising.

9. The International Dimension

The progress which the UK ICO makes with the "beta phase" of its Sandbox pilot programme will be watched closely by other DPAs and by commercial and public organisations. CIPL is pleased that the ICO's discussion paper[21] for this phase largely matches the approach adopted here.

The ICO pilot programme, inevitably, will be a national exercise with no immediate impact outside UK borders. Assuming it is a success, however, it is very likely that multinational companies, that are developing and deploying their products, services and technologies for global business and global customers, will want ways to be found to ensure any Sandbox initiative can be extended on a more international scale. Sandboxes are likely to be particularly attractive for large, multinational organisations at the forefront of new products, services and technology. But no such company will wish to be involved with numerous highly similar exercises in different jurisdictions.

Equally, it can be anticipated that other DPAs around the world will wish to learn from, and capitalise upon, early experiences and then co-operate internationally without pointless duplication.

There are various possibilities here, including:

- Any DPA conducting a Sandbox programme should share its approach and outcomes (positive and negative) with as many other DPAs around the world as possible;
- Any Sandbox exercise should be able to draw upon evidence from trials in other countries;
- Where a Sandbox initiative involves cross-border processing across two or more regulated countries, the DPA should involve other relevant DPAs as much as possible, perhaps with scope for a cross-border mechanism for appropriate cases; and
- Arrangements should, in due course, be put in place—broadly in line with the EU's consistency mechanism—for there to be a "lead" DPA for each initiative, with at least a presumption that the outcome of that initiative will be recognised and accepted by other DPAs.

10. Going Forward

CIPL hopes and expects that the Regulatory Sandbox concept will develop into a great success for DPAs and organisations alike. Even where there has to be a strict process to select participants, that in itself will demonstrate the demand for such a facility.

As interest in the Sandbox concept develops, the International Commissioners' Conference would be a good forum for further exposure and evaluation, as will regional forums such as the

[21] *Supra* note 12.

Asia Pacific Privacy Authorities (APPA) Forum. There may also be opportunities for coordinating bodies, such as the European Data Protection Board or the APPA Forum, to develop guidance.

Funding to support Sandbox initiatives might also be secured from such sources as the EU's Coordinated Plan on Artificial Intelligence.

New laws—possibly a comprehensive federal privacy framework in the US—might also make provision for a Sandbox mechanism.

We hope that this paper will be helpful as DPAs develop their own schemes and organisations consider whether to participate. In the spirit of dialogue which must characterise any Sandbox initiative, CIPL and its members stand ready to engage with lawmakers and DPAs across the world as the architectural processes are developed and the building blocks are put in place.

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.