BUSINESS at OECD

Business at OECD (BIAC)

Regulatory Sandboxes for Privacy Analytical Report

November 2020

Acknowledgements

The Regulatory Sandboxes for Privacy project is a *Business at OECD* contribution to the review of the OECD Privacy Guidelines.

We would like to thank *Business at OECD* Members, the OECD and the Singapore Personal Data Protection Commission – Infocomm Media Development Authority for their support of this project, including the development of this Analytical Report and the September 23, 2020 Project Roundtable.

We extend a special thanks to Paula Bruening, President, Casentino Strategies LLC, for serving as consultant to this project and the principal drafter of this Report, working together with *Business at OECD* Members, OECD Secretariat and Government Experts.

Contents

Introduction 3

Regulatory Sandboxes for Privacy – an Overview 4

Key Characteristics of Regulatory Sandboxes 6

Experience of Regulator-run Privacy Sandbox Initiatives 6

Information Commissioner's Office, UK 7

Association of Southeast Asian Nations (ASEAN) and GSMA – Regulatory Pilot Space 9

Singapore Personal Data Protection Commission – Infocomm Media Development Authority 11

Potential of Regulatory Sandboxes for Privacy 13

Benefits for Companies 13

Benefits for the Market and the Public 14

Benefits for Regulators 16

Challenges 18

What's Needed to Make Regulatory Sandboxes for Privacy Work 19

Infrastructure and Resources 19

Governance 20

Regulatory Clarity 21

Requirements Specific to Cross-border Regulatory Sandboxes for Privacy 22

Conclusion: Future Work on Regulatory Sandboxes for Privacy 24

Introduction

Rapid changes in technology, data driven innovation, and cross-border data flows have prompted the need for agility, flexibility, enhanced public-private cooperation, and coordination of privacy policy and regulation. Response to the Covid-19 pandemic further highlights these trends.

The *Business at OECD* (BIAC) project on regulatory sandboxes was launched in 2020 as a contribution to the review of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("the Guidelines").[1] The project also aims to inform the broader discussion about how regulatory sandboxes for privacy can enhance the agility of regulators working within existing privacy and data protection frameworks. In doing so, it may contribute to efforts to develop approaches to data protection policy and regulations that advance the dual goal of protecting privacy and promoting innovation.

To facilitate this work, on September 23, 2020 *Business at OECD*, together with OECD and the Singapore Personal Data Protection Commission - Infocomm Media Development Authority, convened experts from business and regulatory bodies to participate in a Roundtable on regulatory sandboxes. The goal of the Roundtable was to facilitate discussion about essential questions related to how regulatory sandboxes for privacy can promote greater data sharing within countries and across borders, and further regulatory approaches that enhance data protection and privacy while fostering innovation. Proceedings of this Roundtable contribute substantially to this report. The report also benefits from the views of *Business at OECD* Members, and Delegates of the OECD Committee on Digital Economy Policy (CDEP) Working Party on Data Governance and Privacy (DGP).

The regulatory sandbox for privacy project is further prompted by the overarching need to understand how to apply existing regulation, frameworks and policies to new digital technology and data innovation that may not fit easily into existing regimes. Innovation in digital technology and data use makes possible transformative, beneficial change across government, civil society, and business. But innovation also poses challenges to companies seeking to comply with regulatory frameworks, and to regulators seeking to enforce them.

The review of the Guidelines includes two focus areas of particular relevance to this project: (1) the impact of emerging digital technologies, and (2) implementation and enforcement. The OECD Guidelines note that Member countries should establish and maintain privacy enforcement authorities with the governance, resources, and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial, and consistent basis. Taken together, these two areas of review suggest the importance of innovative tools and approaches like regulatory sandboxes for privacy to advancing relevant and effective privacy policy approaches and regulation.

[1] OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

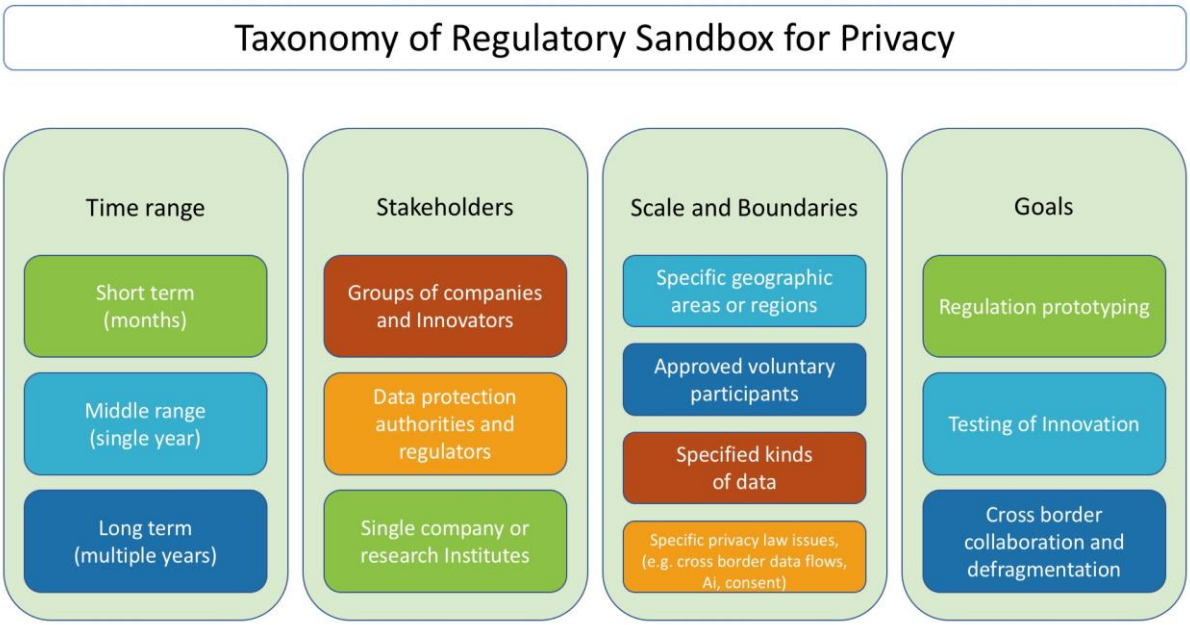
Many tools in law and policy are available to regulators to protect privacy and the rights of individuals over their data. As is highlighted by the OECD Going Digital Toolkit Policy Note, regulatory sandboxes represent just one of these.[2] As a safe space for experimentation – to test the application of regulation, to investigate how regulation works, and to understand how challenging policy questions might be addressed - they can assist companies and regulators in understanding how innovation sits within existing law and regulation and help them chart a path towards new policy. They can enhance privacy-by-design efforts by making it possible to fully assess the risks introduced by new technology, determine how they might be mitigated and build in privacy protections during the innovation process. Examples presented at the 23 September Roundtable, and highlighted in this paper, show how regulatory sandboxes can also encourage trust between different regulators within a country, or among several countries.

Finally, it is important to note that the emergence of COVID-19 and attempts by governments, businesses, and the healthcare sector to address the spread of the disease, develop therapeutics and vaccines, and mitigate the social and economic consequences of the pandemic, highlight the need to address barriers that may impede rapid innovation. Coping with the spread of COVID-19 has accelerated digital transformation and the centrality of data to all sectors - at the local, regional, and national level – and the need to identify ways to unleash innovation while respecting regulatory safeguards. The pandemic underscores the urgent need for enhanced cooperation among governments, business, and policymakers to engage in evidence-based policymaking that would address issues of global scope.

Regulatory Sandboxes for Privacy – an Overview

Regulatory sandboxes can generally be defined as a controlled environment wherein for some predetermined period of time and for a defined use case, a close collaboration between firms and a regulator enables firms to test new data uses, technologies and applications while receiving regulatory guidance. Companies that participate in sandboxes benefit from an understanding about the approach a regulator will take to assess whether privacy-by-design and other regulatory requirements have been effectively implemented. At the same time, regulatory sandboxes enable regulators and governments to understand the implications of different policy choices and build trust in the use of data in cross-regulatory and cross-border scenarios.

[2] Regulatory sandboxes represent just one of many tools available to address data protection and privacy in emerging technology. For example, as regulators work to overcome the challenges that innovative technologies and data uses present to current approaches to regulation, policymakers have explored risk-based approaches to regulation. They have also relied on outcome or performance-based regulation, which focuses on whether an organization meets specified outcomes or objectives established by regulation rather than the means by which these might be achieved. "The role of sandboxes in promoting flexibility and innovation in the digital age," OECD Going Digital Toolkit Policy Note, 2020, https://goingdigital.oecd.org/toolkitnotes/the-role-of-sandboxes-in-promoting-flexibility-and-innovation-in-the-digital-age.pdf.



There is no one-size-fits all approach to regulatory sandboxes for privacy. How a sandbox is designed and scoped will depend upon many factors. As noted above (See Chart above), sandboxes may be organized around the following:

- *The time period during which organizations will participate* – A key step in setting up the regulatory sandbox for privacy is determining its beginning and end date. Setting these outer boundaries clarifies for companies the period during which they may benefit from the specific regulatory guidance that makes testing possible.

- *The participating stakeholders* – The stakeholders that participate in the regulatory sandbox for privacy will vary depending on the technology, data use or data flows being tested. In some cases, sandboxes may include stakeholders that are governed by more than one regulatory scheme and wish to explore and understand how data protection compliance may be affected by the requirements of other laws and regulations. In some cases, companies will participate as facilitators or by providing resources to support the regulatory sandbox.

- *The boundaries and scope of participation* – Regulatory sandboxes for privacy may also be organized around, for example, a certain kind of data, a particular issue or set of issues or a particular regulatory question.

- *The goals of the regulatory sandbox* – Participants' and regulators' goals for regulatory sandbox testing may vary. For example, in some cases, companies may seek guidance about how to implement a particular technology or data use within the boundaries of law or regulation. In others, regulators and companies may wish to explore ways to share data across borders while complying with regulatory obligations. In still others, regulators and companies may wish to investigate existing law and policy to understand how they may be adapted or changed to better serve the emerging data and technology environment.

Key Characteristics of Regulatory Sandboxes

As was illustrated by presentations at the September 23 Roundtable and related use cases, regardless of their design, regulatory sandboxes generally share a number of key characteristics:

- Regulatory sandboxes are used to test genuine innovation, whether new digital technology or the innovative use of an existing technology. In some cases, this can include potential novelty to a relevant jurisdiction or marketplace.[3]
- Applicants to participate in regulatory sandboxes are asked to demonstrate the benefit to consumers of their innovative technology or data use.[4]
- A technology or data use must raise a demonstrable need or readiness for sandbox testing. Companies are able to identify a particular regulation or legal uncertainty about how a regulation applies that constrains their ability to innovate.[5]
- Sandbox testing takes place in particular geographic location, industry sector or over a defined period of time.[6]
- Safeguards are implemented in a way that limits any potential negative consequences of regulatory sandbox participation.[7]
- An existing regulatory sandbox framework or support infrastructure is provided by a sufficiently resourced regulator.[8]
- A methodology and engagement tools facilitate productive interactions between regulator and companies.[9]
- The sandbox ideally results in concrete outputs that capture the lessons learned from the regulatory sandbox program to ensure they promote improved law and policy.[10]

Experience of Regulator-run Privacy Sandbox Initiatives

The following are examples of sandboxes for privacy run by regulators, including the UK Information Commissioner's Office (ICO); The Association of Southeast Asian Nations (ASEAN) Regulatory Pilot Space Launched developed jointly with the GSMA; and the Singapore Personal Data Protection Commission – Infocomm Media Development Authority.

---

[3] Comments of Yeong Zee Kin, Assistant Chief Executive (Data Innovation and Protection Group) of the Infocomm Media Development Authority of Singapore (IMDA) and Deputy Commissioner of the Personal Data Protection Commission (PDPC) at the September 23, 2020 Roundtable; "Sandbox assessment criteria indicators," UK Information Commissioner's Office, https://ico.org.uk/media/for-organisations/documents/2618128/sandbox-criteria-indicators.pdf.

[4] "Sandbox assessment criteria indicators," Ibid.

[5] The role of sandboxes in promoting flexibility and innovation in the digital age," OECD Going Digital Toolkit Policy Note, 2020, pp. 10-11. https://goingdigital.oecd.org/toolkitnotes/the-role-of-sandboxes-in-promoting-flexibility-and-innovation-in-the-digital-age.pdf.

[6] Ibid, p. 9-10.

[7] Ibid., p. 10.

[8] Ibid.

[9] See Facebook use case, pp. 16, and 21.

[10] UK Information Commissioner's Office, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/combining-privacy-and-innovation-ico-sandbox-six-months-on/

Information Commissioner's Office, UK

Developing the Regulatory Sandbox

The UK ICO describes its regulatory sandbox as a service of the ICO to support organizations that are creating products and services which use personal data in innovative and safe ways. In the regulatory sandbox, participants have the opportunity to engage with the ICO sandbox team, and to draw upon wider ICO expertise and advice about mitigating risks and building in "data protection by design."[11]

The ICO developed its regulatory sandbox through a process of engagement that involved assessing the extent to which existing legal powers would support the implementation and management of a sandbox project. It reviewed similar mechanisms that already existed globally and drew upon the findings of a report issued by Nesta, a UK-based organization, that discussed how regulators can encourage innovation.[12] It also issued a formal call for input from the public on regulatory sandboxes and reached out to stakeholder bodies that represent innovators. It looked to the work of the Centre for Information Policy Leadership on constructive engagement and regulatory sandboxes.[13]

Based on this outreach, the ICO drafted internal discussion papers and convened workshops to determine how the regulatory sandbox would be structured and how it would work. It also decided on how to describe the sandbox and communicate with the public about it.

How the Sandbox Works

On its website, the ICO invites expressions of interest to participate in the sandbox from organizations that operate under UK data protection law and that intend to or are in the process of developing innovative products and services using personal data. While in its early stages the ICO encouraged a broad mix of participants of all sizes and across all sectors, going forward it plans to target the work of the sandbox on innovations that align with its current areas of focus, which include health, central government, finance, education, and law enforcement.[14] Applicants to participate in the sandbox are required to meet a set of published criteria,[15] including:

- How innovative is the product or service?
- Will the product or service provide a potential demonstrable benefit to the public?
- Can the ICO provide the resource and capabilities required to support the sandbox?
- How viable is the organization's proposed sandbox plan?

[11] "The Guide to the Sandbox," The UK ICO, https://ico.org.uk/for-organisations/the-guide-to-the-sandbox/.
[12] "Renewing Regulation: 'anticipatory regulation' in an age of disruption, Nesta, March 2019, https://www.nesta.org.uk/report/renewing-regulation-anticipatory-regulation-in-an-age-of-disruption/.
[13] "Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice," the Centre for Information Policy Leadership, March 8, 2019, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_regulatory_sandboxes_in_data_protection__constructive_engagement_and_innovative_regulation_in_practice__8_march_2019_.pdf
[14] For example, in 2020-2021, the ICO sought project involving technologies and data uses for which the UK's age appropriate design code was a consideration and those related to data sharing, particularly in the areas of health, central government, finance, higher and further education or law enforcement.
[15] "Sandbox criteria indicators," UK ICO, https://ico.org.uk/media/for-organisations/documents/2618128/sandbox-criteria-indicators.pdf.

Applicants' expressions of interest are assessed on the basis of their responses to these questions.[16]

Participating organizations are provided with a statement of regulatory comfort, which articulates the approach the data protection authority will take should something go wrong, for example, should a breach occur. Organizations are given assurances that assuming they rectify the problem and take required steps, the ICO's default is not to take corrective action. Such regulatory comfort is not a workaround, however, and compliance with the law is expected.

Companies are also provided with informal advice regarding the plan for the sandbox activity, the goals for the exercise, and how the work will be conducted. This planning builds in flexibility to accommodate the non-linear path innovation often takes. The ICO appoints a single point of contact charged with providing the organization with support and advice throughout the planning stage.

The ICO's sandbox activity ends with the issuance of an exit report that provides a factual, transparent account of what happened in the sandbox and that is redacted as necessary to maintain confidentiality.[17] The exit report discusses what was learned, sets out key data protection considerations and generalizable learnings that the ICO wishes to make available to the public.[18] In some cases, if the ICO believes it is appropriate and the organization finds it useful, the ICO may provide a further statement of regulatory comfort. That statement does not serve as a rubber stamp nor as an endorsement of compliance. Rather, it states that based on the information available to it, the ICO finds no breach of regulation or non-compliance.

[16] UK Information Commissioner's Office, "Sandbox Assessment Criteria Indicators," https://ico.org.uk/for-organisations/the-guide-to-the-sandbox/how-will-the-ico-assess-applications-for-the-sandbox/.
[17] The ICO has published two exit reports on its Regulatory Sandbox engagements. "Regulatory Sandbox Final Report: Heathrow Airport Ltd.: A summary of Heathrow Airport's participation in the ICO's Regulatory Sandbox Beta," June 2020, https://ico.org.uk/media/for-organisations/documents/2618024/heathrow-airport-ltd-regulatory-sandbox-final-report.pdf; and "Regulatory Sandbox Final Report: Jisc: A summary of Jisc's participation in the ICO's Regulatory Sandbox Beta," June 2020, https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/07/jisc-regulatory-sandbox-final-report.pdf.
[18] Comments of Christopher Taylor, Head of Assurance (Supervision) Information Security Office (ICO) UK ICO, Roundtable on Regulatory Sandboxes, 23 September 2020.

Novartis participation in the UK ICO Regulatory Sandbox

Novartis is exploring the use of voice technology in the healthcare setting as a tool to make patient care easier for both health care professionals and patients. It is working with healthcare professionals and third-party technology providers to design its voice technology solution.

Through its participation in the UK ICO Regulatory Sandbox, Novartis seeks to understand the data privacy risks associated with the use of voice in a clinical setting, and what controls are needed to address those risks. Specifically, the Sandbox project explores such issues as the risks related to use of data by third parties and how can those risks be appropriately addressed. In addition, the Sandbox project focuses on questions related to secondary use of data, processing of biometric data, automated decision making, and how the integrity and quality of data used in voice technology for healthcare can be ensured. It also explores the legal bases for processing special category data and issues related to transparency and how patients effectively can be provided with necessary information about the use of data in voice technology.

Key steps in the sandbox project included ongoing discussion with the ICO, and collaboration on concepts and issues. In addition, Novartis conducted a data protection impact assessment and identified safeguards; performed an analysis of data privacy roles; mapped data flows; and developed transparency information.

Novartis' engagement demonstrates how the Regulatory Sandbox for privacy can promote open and collaborative sharing of information between companies and regulators, and practical exploration of the risks and legal uncertainties raised by voice technology used in the healthcare setting. Going forward, such insights could improve regulatory guidance and approaches as regulators address the privacy concerns these technologies raise. Ideally, companies, regulators and the public should be informed of the benefits of the sandbox and its role in both promoting innovation and addressing risk.

Association of Southeast Asian Nations (ASEAN) and GSMA – Regulatory Pilot Space

The ASEAN Regulatory Pilot Space (RPS) is intended to support two complementary purposes: to allow companies to demonstrate to themselves and to policymakers that cross-border data flows are possible between countries that usually do not allow data flow; and to enable ASEAN Member States, regardless of their existing data privacy and cybersecurity laws, to test the impact of different policy solutions on cross-border data flows in a controlled environment and for a predefined amount of time.

In order to achieve this, the RPS is designed to ensure that personal data is protected appropriately and that participating organizations commit to meeting predefined standards. It is intended to allow Member States to evaluate different ways to address cybersecurity concerns in a way that will not delay the development of the digital society. The RPS can also be viewed as a possible stepping-stone for countries that do not have well-established data protection regimes

or mechanisms to better understand how such laws work or to test the planned implementation of new data protection laws.[19] In this way, it is hoped that the RPS will encourage and promote policies that facilitate the flow of data between participating ASEAN countries while raising the level of data protection across the region.

Developing the Regulatory Pilot Space

The RPS is the result of a policy dialogue between ASEAN and GMSA,[20] designed to explore aspects of the digital economy across the region. That discussion quickly began to focus on data protection, the ASEAN Data Protection Framework and cross-border data flows.[21]

GSMA produced a report on cross-border data flows and regional privacy frameworks,[22] bearing in mind the overlap of APEC and ASEAN in terms of member states and that APEC already had in place a cross- border privacy rules system. The report reflected the high level of awareness that already existed across the region and a desire not to duplicate efforts. It also recognized the significant variation in the levels of data protection laws across the ASEAN region – some have very mature, established data protection regimes, while some have no data protection law at all – and persistent concerns about data localization and data sovereignty.

As ASEAN considered what could serve as a long-term solution to data protection in the region it considered the utility and feasibility of a practical, safe space to explore questions about regulation and gave GSMA the go-ahead to develop the RPS. While regulatory sandboxes had been used in the financial sector, it was seen as novel to establish a regulatory sandbox in the context of data privacy, as only the UK ICO and the Singapore Infocomm Media Development Authority had embarked on similar projects.[23]

How the RPS Works

Implementing the RPS in the ASEAN region presented its own unique challenges. Experimentation in the RPS would involve more than one country or economy, and more than one data protection authority. It would also involve the engagement of countries and economies not yet comfortable with cross-border data flows.

Therefore, in designing the RPS, it was important to recognize that it would involve at least two participants, two countries, and two data protection authorities. The architecture of the RPS is

[19] "The Regulatory Pilot Space for Cross Border Data Transfers" GSMA, https://www.gsma.com/asia-pacific/resources/rps/

[20] GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organizations in adjacent industry sectors. https://www.gsma.com/aboutus

[21] Framework on Personal Data Protection, ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN), https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf .

[22] "Regional Privacy Frameworks and Cross-Border Data Flows: How ASEAN and APEC can Protect Data and Drive Innovation," GSMA, September 2018, https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf .

[23] Comments of Boris Wojtan, Director of Privacy, GSMA at the 23 September 2020 Roundtable.

designed around the *Participating Member State* and the *RPS Host*. It is governed by the terms of a *Memorandum of Understanding* that establishes a Joint Supervisory Committee.

The *Participating Member State* may wish to explore how to facilitate data flows but lack the mechanisms necessary to readily make them possible. It also may have in place data localization requirements but be willing to waive strict enforcement of relevant rules within the RPS. An applicant based in the Participating Member State that wishes to transfer data to a recipient in another ASEAN country acting as the RPS Host must meet eligibility criteria. It must submit a proposal for consideration by a supervisory committee and enter into contractual obligations with the data recipient.

In response to a proposal, the *RPS Host* must meet eligibility criteria that include: 1.) an existing data privacy or equivalent law; 2.) a functioning data privacy or equivalent supervisory authority; and 3.) a mature rule of law with courts and enforcement bodies able to take enforcement actions. The RPS host is required to have in place an established data protection authority that meets eligibility criteria, and that is empowered and willing to administer an RPS and take enforcement actions. The organization receiving the data must be able to provide a high level of information security and meet eligibility criteria. It must also agree to fulfill minimum contractual obligations set out in the RPS rules.[24]

It is envisioned that the Memorandum of Understanding will incorporate a *foundation document* setting out rules that: define the purpose and scope of the RPS for cross-border data flows; articulate eligibility requirements for all parties engaged in the RPS; establish requirements for minimum safeguards to be implemented and demonstrated by the applicant; define relevant commitments of each participant; and set the rules of cooperation governing administration of the RPS, participation and extraction of benefits. It should also establish a joint committee to consider proposals and supervise activities within the scope of the proposal.[25]

Singapore Personal Data Protection Commission – Infocomm Media Development Authority

Singapore's implementation of regulatory sandboxes for privacy built on the joint effort of the Infocomm Media Development Authority (IMDA) and the Personal Data Protection Commission's (PDPC) Data Collaborative. The Collaborative brought together six data contributors to test and validate concepts related to public and private data sharing and the fusion of public and private data sets. The Trusted Data Sharing Framework that guided that work forms the foundation for the processes of the regulatory sandbox for privacy, which is structured around three phases:

- *Engagement* - In the engagement phase, companies identify areas of interest and provide plans to innovate with data. Companies are encouraged to be as transparent as possible and to present working prototypes and blueprints for how a technology or system is to be built. Regulators look for sufficient detail to encourage constructive discussion.

[24] Ibid.
[25] Ibid.

- *Providing Guidance* - In many cases the company's involvement ends at the engagement stage, because the DPA is able to provide sufficient assurances to provide the regulatory certainty necessary to move forward with development and implementation. If the company proceeds with implementation that comports with the facts revealed and guidance provided, they can benefit from a level of assurance they are on the right compliance path. If later it deviates in some way, the company can engage in additional discussions with the DPA, or assume risk and continue with implementation.

  In other instances, additional consultation and testing may be necessary before guidance is offered. In either case, IMDA/PDCP provide either general or practical guidance to enhance clarity and understanding and reduce uncertainty about application of regulation to the innovative use or technology. In some cases, when findings are useful and have a broader relevance to the rest of industry, IMDA/PDCP may, with the company's approval, redact its findings and publish its policies, interpretations and position.

- *Policy Prototyping* - In some cases, compliance concerns cannot be addressed by interpretation or a sharpening of policy. In such instances, regulators, companies and the public engage in an exercise in *co-creation* of guidance, wherein a particular question is opened for consultation about what guidance is necessary and would help companies innovate within the spirit and requirements of the law. In some cases, the new policy may be considered as an amendment to law.

Singapore Datathon

The purpose of the Datathon was to support data collaboration between the public and private sectors that aimed to address two key social well-being issues: financial outcomes and health outcomes. The data collaboration involved the fusion of public and private sector data sets and allowed businesses and their data partners to explore and pilot innovative use of data in a safe environment in consultation with IMDA and PDPC. The Datathon also sought to reduce uncertainty about compliance with existing and anticipated policies in order to limit companies' risk of non-compliance and mitigate consumers' risk of privacy violation. Due to the sensitivity of the data, the Data Regulatory Sandbox was particularly useful to explore the pseudonymisation and fusing of data as tools to protect individuals and promote trust.

Keys to the Datathon's success were an appreciation of the strategic objectives of the data collaborations, and the combined effort of IMDA, PDPC and industry to develop a detailed process for the work. It was also important to have an open discussion about the mitigation of potential risks and possible safeguards that could be implemented to retain consumer trust.

Through the Datathon, collaborators gained regulatory clarity about whether consent is required to process and disclose pseudonymized data for data fusion and to anonymize the fused datasets. As a result, both the regulators and data collaborators in the Datathon demonstrated how regulatory uncertainty can be resolved. They also established an industry practice that is practical from the perspective of the private sector businesses and acceptable from the perspective of the regulator. The published case study and the practical guidance produced by the Datathon provided other businesses with similar regulatory clarity.

Potential of Regulatory Sandboxes for Privacy

Regulatory sandboxes for privacy promise significant benefits to all stakeholders – companies, regulators, the market and consumers. At the same time, they raise challenges that will need to be addressed if those benefits are to be realized.

Regulatory sandboxes for privacy are anticipated to enhance the ability of principles-based regulation to respond to uncertainties introduced by new technologies, new data uses, and rapid innovation. They enable regulators to consider the practical application of the law in new or novel use cases where norms of compliance may not yet be established.

When used to help bring projects that benefit the public into compliance before they are introduced in the market, regulatory sandboxes themselves may serve the public interest. Moreover, they represent a more efficient and effective use of resources than bringing expensive enforcement and legal action later, when non-compliance is discovered.[26] Regulatory sandboxes for privacy may be tailored to help speed and enhance development of data-driven solutions to address global crises, such as COVID-19. Regulatory sandboxes can serve in gathering evidence about the functioning of digital markets and the impact of regulation, including whether regulatory requirements affect digital and traditional sectors in the same way.

Because companies participate at early stages in the development process, regulatory sandboxes for privacy can serve as an important tool in assessing risk and in carrying out privacy- by-design. Ideally, they promote the dual goals of robust innovation and regulatory compliance, so that they promote a win-win outcome for companies and regulators.

Benefits for Companies

- *A safe space for testing regulation and policy* - Regulatory sandboxes provide companies with a real world, safe space to test their innovation against applicable regulation and policies. They enable companies to engage in positive and collaborative engagement with regulators.[27] Regulatory sandboxes can also serve as a platform to seek guidance from more than one regulator where multiple – and sometimes overlapping or even conflicting – requirements may apply.

- *Company access to guidance and advice* – Regulatory sandboxes provide the opportunity for companies to benefit from the guidance and advice they receive from regulators and other industry participants in the sandbox.

- *Reduced regulatory uncertainty* - Regulatory sandboxes for privacy enhance the ability of companies to develop innovative products and services by providing them with a degree of assurance that experimental and testing phases will not run afoul of regulatory

[26] Comments of Chris Taylor, Head of Assurance (Supervision) Information Commissioner's Office UK, at September 23, 2020 Roundtable.
[27] Comments of Knut Mager, Head, Global Public Policy, Novartis, at the September 23, 2020 Roundtable.

requirements. Regulatory sandbox testing can enable companies to identify features or applications that may not be acceptable early and provide the opportunity to modify them. In doing so, the Regulatory sandbox can reduce the time required to bring new ideas to the market by lowering the risk of introducing innovation that is then challenged by regulators or rejected by consumers.

- *Enhanced capacity for compliance* - Regulatory sandboxes for privacy can enhance companies' capacity for compliance, particularly in the case of startups and small businesses. Sandbox participation can serve as an element of risk assessment and privacy-by-design, helping companies meet their accountability obligations under applicable data protection laws and frameworks. Regulatory sandboxes particularly can assist startups in this regard, by not only helping them to comply with law, but encouraging and providing the opportunity for adherence to voluntary frameworks.[28]

- *Opportunities for business development* - Regulatory sandboxes may provide enhanced networking and business development opportunities for start-ups and small businesses. Reduced regulatory uncertainty and the ability to conduct testing can help facilitate financing for innovative firms.[29]

- *Enhanced incentives to innovate* - Confidence that new technology or application complies with privacy law and regulation can provide companies with greater incentives to innovate.

- *Reduced time to market* - For companies, regulatory flexibility can enable live-market testing and market entry that otherwise may not have been possible, enabling companies to introduce new innovations to the market more quickly.

Benefits for the Market and the Public

- *Enhanced data sharing and cross-border data flow* – Regulatory sandboxes for privacy may encourage more data sharing and enhanced cross-border data flows, promoting digital competitiveness across regions and among companies.[30]

- *Clearer guidance for all interested parties* - When appropriate, the results of regulatory sandbox testing can be shared with the public, so that regulators and innovators across the market can benefit from sandbox findings. In such cases, the findings can provide clarity and guidance for all interested parties, not only the regulatory sandbox

[28] Comments of Arianne Jimenez, Privacy and Public Policy Manager, Asia Pacific, Facebook, at the September 23, 2020 Roundtable.
[29] "The role of sandboxes in promoting flexibility and innovation in the digital age," OECD Going Digital Toolkit Policy Note, 2020, https://goingdigital.oecd.org/toolkitnotes/the-role-of-sandboxes-in-promoting-flexibility-and-innovation-in-the-digital-age.pdf.
[30] Comments of Chris Taylor, Head of Assurance (Supervision) Information Commissioner's Office UK, at the September 23, 2020 Roundtable.

participants.[31] As a forum for direct engagement between regulators and innovators, regulatory sandboxes can improve understanding of compliance issues among all stakeholders.[32]

- *Opportunity for evidence-based policymaking* - Because they enable real-world testing and collaboration, regulatory sandboxes for privacy can foster evidence-based policymaking that promotes innovation while protecting the privacy interests of consumers.

- *A venue for co-created policymaking* – Regulatory sandboxes can provide an additional venue through which regulators can consult with industry to co-create policy.

Facebook Experimental Governance Programs:
Regulatory Sandbox on Notice and Consent

Given the rapid advancement of new and emerging technologies and the difficulty of fully understanding and anticipating its effects, there is a need for effective policies to govern their development and use. Bringing together governments and tech companies, Facebook has been implementing experimental governance programs in order to help inform how policy around emerging technologies can be co-developed, tested, and adopted on a global scale. Through regulatory sandboxes, Facebook has contributed to the evaluation and improvement of existing legal frameworks, while through policy prototyping programs, it has supported the co-creation and testing of new governance frameworks.

As Singapore was updating its Personal Data Protection Act and drafting Advisory Guidelines on the Enhanced Consent Framework, Facebook, in collaboration with the Singapore Infocomm Media Development Authority (IMDA), ran a Regulatory Sandbox project focused on issues surrounding notice and dynamic consent. The project was part of a larger startup incubator program called Facebook Accelerator - Singapore.

The Project sought to enable participating startups to co-create, with the guidance of a regulator and assistance from industry experts, ways to demonstrate how concepts such as notice and dynamic consent can be implemented in innovative products and services. It also allowed participants to test and identify the challenges of existing and proposed legal requirements on notice and consent, and explore ways to address them. Finally, it sought to produce evidence-based policy recommendations that could inform the policy-making process.

***** For further information on the Notice and Consent Regulatory Sandbox within the Facebook Accelerator - Singapore, please see this resource: https://www.ttclabs.net/Insights

[31] See Novartis use case, p. 9.
[32] See Facebook use case, p. 21.

- *Better outcomes for consumers* - Regulatory sandboxes can enhance the trust and confidence necessary for innovation across the marketplace. Regulators can use sandboxes to prevent or stop activity that may be non-compliant. While the goal of the sandbox is to support public interest in innovation, if a technology or data use cannot be deployed in compliance with regulation, the sandbox can deliver that regulatory outcome at an earlier stage in the development process. Preventing a company from falling outside the bounds of regulation early on can be an important regulatory benefit for consumers.[33]

- *An opportunity to identify law and regulation that should be revisited and updated* - Regulatory sandboxes can signal the existence of legal gaps and shortcomings that need to be assessed after the sandbox experiment has been completed. Regulatory sandbox testing also may reveal the limitations in existing laws that need to be revisited.

- *Enhanced trust between regulators and companies* - Regulatory sandboxes can help facilitate dialogue between regulators and market players. Including regulators in the companies' product development process may help to build mutual trust.

Benefits for Regulators

- *Greater agility in regulation* - By providing an opportunity to investigate and understand the application of law early in the development of digital products and services, regulatory sandboxes can introduce greater agility into the regulation process.

- *Increased capacity for cooperation among regulators* - Regulatory sandboxes can benefit regulators by fostering collaboration that enhances their understanding of regulatory regimes outside their home country and increases their capacity for cross-border cooperation.

- *Regulator education* - Regulatory sandboxes can help facilitate dialogue with new market players, including those from other sectors, so that regulators are up-to-date and aware of developments at the frontier of innovation.[34] This interaction between regulators and companies can help regulators understand industry needs and focus their attention on those areas where regulatory clarity is crucial. Such collaboration can lead to learning opportunities for regulators and access to real world examples and cases. Such access can support policy prototyping and evidence-based policymaking that eventually results in better regulation and laws.[35]

---

[33] Comments of Chris Taylor, Head of Assurance (Supervision) Information Commissioner's Office UK, at the September 23, 2020 Roundtable.

[34] "The role of sandboxes in promoting flexibility and innovation in the digital age," OECD Going Digital Toolkit Policy Note, 2020, pp. 11-12, https://goingdigital.oecd.org/toolkitnotes/the-role-of-sandboxes-in-promoting-flexibility-and-innovation-in-the-digital-age.pdf.

[35] Comments of Yeong Zee Kin, Assistant Chief Executive (Data Innovation and Protection Group) of the Infocomm Media Development Authority of Singapore (IMDA) and Deputy Commissioner of the Personal Data Protection Commission (PDPC) at the September 23, 2020 Roundtable.

Additional Country Examples - Steps Toward Regulatory Sandboxes for Privacy

Government agencies and ministries have taken first steps toward use of Regulatory Sandboxes for privacy.

- In December 2018, the European Commission announced its "Coordinated Plan on Artificial Intelligence, an initiative to experiment and test AI technology. The Annex to the announcement notes how testing facilities "may include regulatory sandboxes. . . in selected areas where the law provides regulatory authorities with sufficient leeway."
- In 2017 the Singapore Personal Data Protection Commission (PDPC) published a Guide to Data Sharing that articulated details of how a proposed Regulatory Sandbox would work. It used the Sandbox to test possible changes to Singapore's Personal Data Protection Act (PDPA).
- In December 2017, the Finnish Ministry of Economic Affairs and Employment reported on Finland's national AI strategy, noting that a Regulatory Sandbox can serve as one way to encourage data sharing.
- European Commission "Coordinated Plan on Artificial Intelligence" announcement notes that testing facilities "may include regulatory sandboxes . . . in selected areas where the law provides regulatory authorities with sufficient leeway."
- Malta passed the Malta Digital Innovation Authority Act, specifically paving the way for use of a Regulatory Sandbox to test artificial intelligence.
- The Colombian government, in partnership with CAF, developed a Regulatory Sandbox on AI; the Colombian Communications Regulation Commission evaluated Regulatory Sandboxes as a means to support rural connectivity.
- The Telecom Regulatory Authority of India's Consultation[1] on Privacy, Security and Ownership of Data in the Telecom Sector identified the use of anonymized data sets in Sandboxes as a tool in development of newer services for further consideration.
- The Danish Financial Supervisory Authority (DFSA – Finanstilsynet) has embarked on a sandbox initiative targeting Denmark's most innovative fintech startups. The FT Lab is designed to offer selected companies a platform to test their technologies in a secure environment. It is intended to provide a basis for testing innovative financial products and services, and to promote their development. It also is designed to enable the DFSA to better understand Fintech and to support the use of new technology in the financial sector. It enables pilot testing of new technologies in a limited market environment under regulatory supervision, but without the need to be licensed. The project enables low-cost testing to ensure regulatory compliance and security checks for financial operations including cryptocurrencies and blockchain based systems.

Challenges

Implementation and participation in regulatory sandboxes for privacy raise challenges for regulators and companies. Without the necessary authority, appropriate resources and clarity about what rules apply to companies, implementation of regulatory sandboxes for privacy may lack credibility and a clear sense of the benefits they offer. Regulatory sandboxes for privacy will not be viewed favorably by companies with assurances that participation in regulatory sandboxes will not compromise their proprietary interests or open them to discriminatory treatment by regulators.

It will be important to meet the challenges faced by regulators and companies to maintain trust in the utility and fairness of regulatory sandboxes for privacy. These challenges include:

- *Lack of regulatory authority* - Legislative frameworks may not explicitly accommodate regulatory sandboxes for privacy. Clarity about regulators' authority to implement and engage in regulatory sandboxes will be needed for their successful deployment and to avoid the risk of undermining the credibility of regulators.

- *Application of regulations in cross-sectoral innovation* - In many cases, data and technology innovation will be governed by more than one regulatory scheme. Regulatory sandboxes for privacy will need to be able to help companies navigate regulations that may overlap or, in some cases, conflict.

- *Company concerns about regulatory clarity* - Lack of clarity about the circumstances under which companies might face enforcement actions based on their activities or information shared while in the sandbox could discourage some participants. The approach a regulator may take in case of a privacy breach or violation should be established at the outset to provide all participants with clarity and enable fulsome discussion.

- *Preserving intellectual property interests* - Companies may be discouraged from participating over concerns about compromise to intellectual property interests should information about innovative products and services shared while participating in the sandbox fall into the hands of competitors or enter the public domain prematurely.

- *Discriminatory treatment* - Concerns that regulatory sandboxes for privacy might, in the absence of safeguards, open companies to favorable or discriminatory treatment, or that sandboxes might be accessible only by certain players or industry sectors, might discourage some participants. It will be important to mitigate against excluding smaller companies with fewer resources from participation in sandboxes.[36] However, it may be that smaller companies, rather than larger, better resourced businesses would be more likely to participate in sandbox testing.[37]

[36] Comments of JoAnn Stonier, Chief Data Officer, Mastercard, at the September 23, 2020 Roundtable.
[37] Comments of Chris Taylor, Head of Assurance (Supervision) Information Commissioner's Office UK, at the September 23, 2020 Roundtable.

- *Strain on resources of regulators and companies* - Implementing, monitoring and participating in regulatory sandboxes for privacy impose costs on companies and regulators. The cost of operating a sandbox can reach $1 million US for regulators. The need to allocate resources may preclude some companies from participating.

- *Compromise to trust* - To be trusted, regulatory sandboxes for privacy will need to adhere to effective rules and governance that encourage transparency and credibility.

- *Complexity* - When multiple authorities and/or countries are involved, the perceived complexity of the regulatory sandbox for privacy could prevent its full implementation or deter potential participants.

- *Fragmentation of approaches* - Divergence in approaches to sandboxes among countries could limit the ability of regulators to run sandboxes across sectors and across borders. Lack of a harmonized approach to sandbox implementation could compromise the trust necessary to derive the benefits of regulatory sandboxes for privacy.

What's Needed to Make Regulatory Sandboxes for Privacy Work

To best serve companies, regulators and consumers, regulatory sandboxes for privacy require infrastructure and resources to ensure their smooth operation. Governance measures are also essential to promote fairness and trust as participants apply for, participate in, and leave the sandbox environment. Clarity about how regulation applies in the sandbox, and how violation of regulations will be addressed, will be critical to preserving the sandbox as a safe space to test the application of law and policies to new digital technologies and to motivate companies to participate.

Infrastructure and Resources

- *Application Process* - Roundtable participants noted that important to the success of the sandbox is a clearly established, publicly accessible process by which companies apply to participate. A transparent application process encourages broad participation and public trust in the regulatory sandbox for privacy process and ensures that the sandbox is available to companies of a range of sizes, industry sectors and maturity levels. In some cases, data protection authorities may wish to better understand and test the application of regulation to certain kinds of innovative data use or technologies. In such instances, they may encourage applications by companies that can help them achieve those goals.

- *Technical arrangements for data sharing* - Because the sandbox involves the sharing of data, technical arrangements are necessary to ensure that data is transferred as needed and with the appropriate protections in place. Technical arrangements should address how data is received, stored, accessed, secured and disposed of.[38]

[38] Comments of Yeong Zee Kin, Assistant Chief Executive (Data Innovation and Protection Group) of the Infocomm Media Development Authority of Singapore (IMDA) and Deputy Commissioner of the Personal Data Protection Commission (PDPC) at the September 23, 2020 Roundtable.

- *Resources for regulators and companies* - Establishing, managing and participating in a regulatory sandbox imposes costs on regulators and companies. Regulators will need appropriate funding to support operation and monitoring of the sandbox; companies will need to allocate resources specifically dedicated to their participation in the sandbox.

- *Communications and publishing* - In some cases, regulators will wish to publish the findings and outcomes of the sandbox process. When publication is appropriate, regulators will need the support necessary to publish sandbox results.

- *Incentives for participation* - To participate in a regulatory sandbox for privacy, companies must invest time and resources. It will be important to understand what measures would provide necessary incentives to encourage companies to engage in regulatory sandbox testing.

Governance

- *Eligibility criteria* - Regulators need clearly articulated criteria against which to evaluate participant applications and determine what projects are appropriate for the sandbox. Roundtable participants noted that sandbox applicants were required to meet established eligibility criteria. These tended to include: the benefit of the innovation to the public; how innovative the product or service is understood to be; whether the product or service will provide a potential demonstrable benefit to the public; the viability of the sandbox plan; whether there are sufficient resources and capabilities to support the sandbox to completion; whether the project provides increased clarity; and guidance for all interested parties.

- *Clearly defined start and end dates for sandbox projects* - Regulators and companies will need to establish and clearly understand the period of time during which the sandbox is active. Doing so defines for companies the period during which the assurances provided to sandbox participants with respect to regulation apply.

- *Established criteria for assessing and evaluating outcomes* - Criteria against which regulatory sandbox findings are evaluated should be clearly articulated. In addition to providing a tool to assess sandbox outcomes, these criteria also can help regulators and companies determine whether, in light of sandbox findings, a technology should be brought to market.

- *Established requirements for data safeguards and companies' responsibilities to protect data security and confidentiality* - Data used in the sandbox will need to be protected from loss, breach, compromise or inappropriate access. Requirements for how data will be secured while used in the sandbox will be needed to promote trust.

- *Protection of intellectual property rights* - To participate confidently in the sandbox, companies will need assurances that their intellectual property in the sandbox will be protected and their protections under patent or trade secret law will not be compromised.

- *Guidance to address cross-jurisdictional issues* - Digital technologies and data innovation occurs across all industry sectors. Regulators and companies participating in the sandbox will require guidance about how to address cross-jurisdictional issues that may arise in a sandbox project that involves more than one regulatory regime, *e.g.*, data protection and telecommunications law, or data protection and financial services law.

- *Protection of individuals' data* - While sandboxes are intended to enable companies to test the application and the limits of regulation when applied to innovative technologies and data use, individuals' data must still be protected. Protections for individuals' rights in their data, and transparency about the existence of regulatory sandboxes for privacy and how they work are needed to make the space safe for individuals. But protections should not fully replicate every aspect of the extant law and regulation in a way that limits the ability to experiment and innovate.

- *Criteria and rules for when and how outcomes are made public* - In some cases, regulators - and companies – may want to make the outcomes of the sandbox available to the public to allow innovators across the market to benefit. Criteria should be established to determine when broad publication is appropriate, and what steps should be taken to protect confidentiality and intellectual property interests.

Regulatory Clarity

- To participate in the regulatory sandbox with confidence, and to extract the greatest benefit from it, companies need clarity about their responsibility to comply with regulation and how regulators will address failures to meet obligations. If the regulatory sandbox for privacy is to provide a safe space to test the application and boundaries of regulation, it will be important to determine what assurances companies need that their participation in the sandbox, in and of itself, does not expose them to a regulatory enforcement action.[39]

- Regulators will also need to determine what assurances are appropriate, and how they can be articulated to companies clearly. However, the assurances provided to sandbox participants no longer apply when sandbox testing ends, and they do not apply to other activities. A goal of the regulatory sandbox for privacy is to develop guidance, not provide immunity for participants.[40]

[39] Comments of Boris Wojtan, Director of Privacy, GSMA, at the September 23, 2020 Roundtable.
[40] Ibid.

Facebook Experimental Governance Programs:
Policy Prototyping on AI Transparency and Explainability

Facebook, in collaboration with the Singapore IMDA, established a policy prototyping program to test specific concepts, processes and strategies on AI explainability and transparency. This is part of a global initiative aimed at developing and testing governance frameworks to inform future rule and lawmaking on AI. As an empirical program, it is meant to provide evidence-based policy input to improve existing governance frameworks and inform policy-making processes. This program's primary objective is to recommend clarifications and improvements for the specific AI explainability elements of Singapore's Model AI Governance Framework and its companion document, the Implementation and Self-Assessment Guide for Organizations (ISAGO).

Throughout the 6-month program, the 12 participating companies are developing an AI explainability solution while providing comprehensive insights about their experience in building and delivering that AI explainability solution in accordance with the policy guidance. We will be continuing to collect empirical information over the next months, planning the dissemination of final results in early 2021.

Sandboxes and prototyping programs allow companies to help shape policy, inform future laws, and to operate with regulatory guidance that promotes innovation. This collaboration enables companies and regulators to engage in long-term planning. Ideally, experimental governance allows for iterative development as the regulatory model is developed over time. The sandbox and the prototyping programs revealed the importance of actively engaging regulators and technologists, and identified several risks that emerge when that engagement does not occur:

- Policy is directed in a way that does not match the needs of companies and other participants in the ecosystem;
- The experimental governance exercise has little or no impact on subsequent regulation;
- High-value, impactful projects do not develop;
- The sandbox becomes a vehicle for companies to be exempted from certain rules without an emphasis on innovation; and
- Policies are developed that are difficult or impossible to implement and do not reflect people's attitudes toward and use of new technologies.

Requirements Specific to Cross-border Regulatory Sandboxes for Privacy

International sandboxes may raise unique questions and therefore have different requirements, outlined as follows:

- *A multinational framework* – A framework may be needed to assist in creating and running sandboxes that involve the use of data that is transferred and shared across borders. Such

a multinational instrument would articulate the role of DPAs and establish measures to be taken to promote cooperation between authorities in administering the sandbox and extracting benefits.

- *Clear definitions of roles and responsibilities* – Cross-border regulatory sandboxes for privacy benefit from clear articulation of roles and responsibilities among regulators. This is particularly important when the level of maturity of privacy law and regulation differs from country to country, and in situations where not every participating country will have a data protection authority. It also will be important to establish which authorities will take part in and how they will collaborate. Finally, established criteria by which it is determined what countries will participate and what roles they will take in the regulatory sandbox will foster credibility and trust.

- *International Cooperation* – Cross-border regulatory sandboxes will only function well if participating countries establish agreed-upon responsibilities, particularly with respect to implementation of safeguards. They also will require clear articulation of the manner in which the parties will participate in the benefits and outcomes of the sandbox. Cooperation also will be necessary to coordinate sandbox activities across authorities and preserve an environment conducive to innovation. Memoranda of Understanding may serve as one arrangement for such cooperation.

- *Incentives and assurance* – It may be necessary for data protection authorities to articulate incentives to encourage participation. For companies, such incentives may include the opportunity to test an idea so as to speed its introduction to the market or to reach an operational efficiency more quickly, knowing that they do not inadvertently expose themselves to sanctions in the process. For data protection authorities and countries, the incentive may lie in the opportunity to engage in policy prototyping; to better align law and practice in a region or globally; or to facilitate the responsible flow of data.

- *Safeguards for countries when data protection laws vary in levels of maturity* - Safeguards may be needed to when sandboxes involve sharing data between countries and economies whose privacy laws and protections are at varied stages of development. In cases where a country may not have a data protection authority in place, it will be important to determine what authority can participate in the regulatory sandbox. Agreed upon criteria will be needed to support that determination.

Data Sandboxes

Data sandboxes are recognized as a tool to explore data sets and extract new insights from them and may provide relevant experience and perspective for regulatory sandboxes for privacy. They are isolated environments in which data is accessed and analyzed, and analytic outputs are exported. Because data sandboxes are a highly controlled environment, they enable innovators access sensitive and proprietary data while assuring the privacy and intellectual property rights of rights holders. They can function through technical means or through physical onsite presence with the data holders.*

Organizations' experience with Data Sandboxes can provide important insights about the governance necessary to make Regulatory Sandboxes for privacy work safely and successfully. Data Sandbox implementation, participation and process are guided by established processes and criteria. This governance guides the participants from the application, preparation of data and determination of its fitness for use; testing; evaluation of outcomes and publication, as appropriate, of results.

Because data in the sandbox is often sensitive and proprietary, companies engaged in a sandbox must take steps to be transparent, to secure the data, and to comply with data protection law and regulation. Companies that implement data sandboxes conduct due diligence to clearly understand who should participate, the goals of the Sandbox project, and whether the data to be used is fit for concept. Significantly, implementers of data sandboxes consider the potential outcomes of the project, their anticipated benefits and risks, and their impact on society. Such thoughtful governance is established and followed to promote credibility and trust.

*See OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, https://doi.org/10.1787/276aaca8-en, pp. 33-34.

Conclusion: Future Work on Regulatory Sandboxes for Privacy

The OECD's evidence-based approach to policy analysis and development, and its capacity to convene experts across relevant sectors and disciplines positions it uniquely to engage in future work on regulatory sandboxes for privacy.

This project has raised a number of questions for consideration in future OECD work related to governance and digitalization, and implementation of the OECD Privacy Guidelines.

Questions that may be considered in future OECD work related to regulatory sandboxes for privacy:

- How can regulatory sandboxes for privacy help companies carry out the risk assessment and mitigation necessary for privacy by design and compliance with accountability requirements
- Can codes of conduct serve regulatory sandboxes for privacy?
- What is the role of regulation? Can regulatory sandboxes for privacy operate within existing regulatory schemes? Or is additional regulation necessary?
- What are the particular challenges regulators and companies face when establishing and operating in international privacy sandboxes? How can these be addressed so that they can be used more widely?
- How can use of sandboxes be encouraged and promoted? What incentives can motivate regulators and innovators to participate in them?
- What can companies and regulators reasonably expect to achieve through the use of regulatory sandboxes?
- How can existing data sandbox projects help us understand how to design and benefit from regulatory sandboxes for privacy?
- How can regulatory sandboxes for privacy be deployed in non-discriminatory ways?
- What are current outcomes of existing regulatory sandboxes? What questions might they raise about the potential risk of regulatory arbitrage?

Regulatory sandboxes for privacy are an important tool to advance the introduction of new and emerging technologies in the marketplace. They allow innovators and regulators to ensure that regulatory frameworks are well aligned with new product and service developments and address needs of relevant stakeholders. Initiatives to explore the possibilities of regulatory sandboxes in the privacy space demonstrate their benefits in this respect.

Business would welcome further OECD work to develop an evidence base and guidance for policy makers focused on regulatory sandboxes for privacy. This work would benefit policy makers and innovators both across sectors and policy disciplines.

Business at OECD
13-15 Chaussée De La Muette
75016 Paris
France
contact@biac.org | @BusinessAtOECD | www.businessatoecd.org

Established in 1962, *Business at OECD* stands for policies that enable businesses of all sizes to contribute to growth, economic development, and societal prosperity. Through *Business at OECD*, national businesses and employers' federations representing over 7 million companies provide and receive expertise via our participation with the OECD and governments promoting competitive economies and better business.