



DATASPHERE  
INITIATIVE

# Sandboxes and Artificial Intelligence:

*Opportunities, experiences and recommendations*

**Working Paper**

July 2024

## About the Datasphere Initiative

The Datasphere Initiative is a think and do tank that catalyzes meaningful dialogues and co-creates actionable and innovative approaches to respond to data challenges and harness opportunities across borders. Our mission is to equip organizations to responsibly unlock the value of data for all.

For more information, visit [www.thedatasphere.org](http://www.thedatasphere.org) or contact [info@thedatasphere.org](mailto:info@thedatasphere.org).

## Acknowledgements

This policy brief was authored by Adam Zable, Fellow at the Datasphere Initiative, with contributions from Lorraine Porciuncula, Executive Director and Mariana Rozo-Paz, Policy, Research and Project Management Lead at the Datasphere Initiative. The team is also thankful to Sam Jungyun Choi for her insights and comments. The Policy Brief counted with editorial and design support from Sophie Tomlinson, Director of Partnerships and Communications and Barbara Miranda, Design Thinking Lead of the Datasphere Initiative.

## About this Working Paper

This working paper is a preliminary research output to be used as input for discussions in the context of the inaugural meeting of the Global Sandbox Forum on 22-23 July, 2024. A final version will be published in September 2024 and will include insights of the exchanges, acknowledging additional contributors.

## Executive Summary

This policy brief explores the potential of sandboxes as important tools for the regulation and development of AI and data-driven technologies. Sandboxes offer a valuable solution for experimental and anticipatory governance of AI, providing secure environments in which innovators and regulators can come together to safely experiment with new technologies, practices, and business models. Sandboxes can enable iterative testing, reduce uncertainty, enhance competition, and foster collaboration between innovators and regulators. The brief reviews the diverse implementations of sandboxes on AI applications, from regulatory to operational, and highlights their potential to foster innovation while ensuring compliance with regulations and align with societal values and ethical standards. Policy recommendations include enhancing capacity building among stakeholders, standardizing data governance frameworks, integrating privacy-enhancing technologies, supporting cross-sectoral and cross-border sandboxes and establishing a Global Sandboxes Forum. These measures aim to create robust, adaptive, and collaborative sandbox frameworks that address the complexities of AI development and deployment.

## Introduction

Artificial Intelligence (AI) relies on vast data to function effectively, identifying patterns, making predictions, and performing tasks traditionally requiring human intelligence. Generative AI (GenAI) creates new content, driven by large data inputs and advances in algorithms, computational power, and machine learning. AI offers unprecedented opportunities to enhance human welfare by transforming productivity, human capability, and decision-making, impacting sectors like healthcare<sup>1</sup>, supply chain management<sup>2</sup>, and education<sup>3</sup>. However, realizing these benefits will depend on how effectively we manage substantial risks and potential harms associated with AI.

As AI's potential to influence political narratives and electoral outcomes grows, global unease increases.<sup>4</sup> AI's integration into healthcare, finance, education, and entertainment raises ethical, legal, and social issues, with concerns about systemic biases, job displacement, and privacy. Built on the collective data of society, GenAI not only reflects, but amplifies these challenges related to trust, intellectual property, and information integrity.

Central to these challenges is data governance, essential for AI functionality. GenAI systems use massive, varied datasets, which can be incomplete or biased<sup>5</sup>, leading to unjust outcomes.<sup>6</sup> Moreover, the lack of transparency in how data is sourced and used exacerbates these problems.<sup>7</sup> Data governance involves policies guiding data processing, protection, and value creation throughout its lifecycle.<sup>8</sup> Robust data governance can mitigate GenAI risks, fostering trust and maximizing societal benefits.<sup>9</sup> Effective data governance can address issues of bias by promoting diverse and representative datasets<sup>10</sup>, ensure accountability through documentation and auditing of data processes<sup>11</sup>, and safeguard privacy by changing the default mode of data collection from opt-out to opt-in.<sup>12</sup> Ultimately, data governance should serve to not only address

---

<sup>1</sup> Saraswat et al (2022), [Explainable AI for Healthcare 5.0: Opportunities and Challenges](#) IEEE Access.

<sup>2</sup> Dash et al (2019), [Application of Artificial Intelligence in Automation of Supply Chain Management](#), Journal of Strategic Innovation and Sustainability.

<sup>3</sup> Bhutoria (2022), *Personalized education and Artificial Intelligence in the United States, China, and India: A systematic review using a Human-In-The-Loop model*, Computers and Education: Artificial Intell.

<sup>4</sup> Bell and Korinek (2024), [AI's economic peril to democracy](#) Brookings, / Nick Robins-Early (2023), [Disinformation reimagined: how AI could erode democracy in the 2024 US elections](#), The Guardian.

<sup>5</sup> Wachter and Mittelstadt (2019), [A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI](#), Columbia Business Law Review.

<sup>6</sup> Ferrara (2023), [Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies](#), University of Southern Carolina.

<sup>7</sup> Center for Research on Foundation Models (2024), [The Foundation Model Transparency Index](#), Stanford University.

<sup>8</sup> Organisation of Economic Cooperation and Development (2024), [Framework for Anticipatory Governance of Emerging Technologies](#), OECD Science, Technology and Industry Policy Papers.

<sup>9</sup> Aaronson (2024), [Data Disquiet Concerns about the Governance of Data for Generative AI](#), CIGI Papers.

<sup>10</sup> Verhulst and Schuur (2023), [Interwoven Realms: Data Governance as the Bedrock for AI Governance](#), Medium, Data and Policy Blog.

<sup>11</sup> Brundage et al (2018), [The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation](#), arxiv.

<sup>12</sup> King and Meinhardt (2024), [Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World](#), Stanford Institute for Human-Centered Artificial Intelligence.

the immediate risks associated with AI's use of data but also anticipate future implications for society.

**In this complex landscape, sandboxes stand out as important tools for experimental and anticipatory governance of AI and data that underpins it.** Countries all over the world are implementing sandboxes for AI, providing secure environments where organizations can test and refine new technologies and business models under controlled conditions. As of 2024, research by the Datasphere Initiative shows that at least 19 countries have implemented or are developing national sandboxes for data or AI (see Appendix). Sandboxes offer an important opportunity to iterate and refine AI governance and the data that underpins these technologies.

This policy brief explores the potential of sandboxes to address the multifaceted challenges of AI. By enabling iterative testing and refinement, sandboxes ensure that as data-driven technologies like AI evolve, they do so within governance frameworks that maximize societal benefits and minimize risks.

## Current Challenges in AI Regulation

The rapid expansion of AI technologies has heightened public awareness of a host of regulatory challenges that policymakers are struggling to address. AI's capability to influence public opinion, automate decisions, and generate content at scale presents complex challenges which intersect with crucial areas of public concern like the spread of misinformation, deepening digital divides, and rising inequality, which can all collectively erode democratic structures. As these technologies become increasingly integrated into the critical infrastructure of various sectors — from public service delivery and healthcare to military and commercial decision-making — the need for comprehensive and adaptive governance frameworks becomes urgent. Here we highlight just some of the legal, socioeconomic, and ethical challenges facing policymakers as they look to govern AI.

### *Legal and Regulatory Challenges*

The rapid pace of AI technology development, exemplified by the frenetic evolution of GenAI, poses significant challenges to existing regulatory frameworks, which often lag behind technological advancements.

GenAI developers typically train their models on data gathered through extensive scraping of the open internet, presenting complex legal questions involving copyright and personal data protection laws.<sup>13</sup> The practice of web scraping can result in the infringement of intellectual property rights, both by training models on copyrighted material without permission and by generating content that may replicate or closely resemble copyrighted works.<sup>14</sup> Web scraping also holds implications for data protection laws; for example, if a model is trained on sensitive

---

<sup>13</sup> Tiedrich (2024), [The AI data scraping challenge: How can we proceed responsibly?](#), OECD

<sup>14</sup> Holloway, Cheng, and Dickenson (2024), [Will copyright law enable or inhibit generative AI?](#), World Economic Forum.

commercial or personal data, there is currently no way for the model to subsequently ‘unlearn’ that data, as required by some data protection laws.<sup>15</sup>

The global nature of AI development further complicates regulation, as the essential computational infrastructure, expertise, and data often flow across national borders. This necessitates an unprecedented level of international cooperation to avoid a fragmented global regulatory landscape. Such coordination is currently lacking, with fundamental issues like the definition of AI itself still lacking a commonly agreed standard with clearly defined terms.<sup>16</sup> Regulatory strategies and data governance frameworks also differ significantly between regions.<sup>17</sup> Inconsistent regulatory environments can stifle innovation by SMEs and create competing standards, erecting barriers to new entrants and limiting data sharing crucial for advanced AI development. They can also place companies in regions with stringent AI regulations at a competitive disadvantage, increase compliance costs significantly, and enable AI developers to “forum shop” or exploit regulatory differences for the most beneficial regulations. While there are promising initial efforts, such as the Council of Europe Convention on AI, much more international coordination is needed to harmonize regulations, balance protection from harm with scientific innovation, and ensure the global adoption of AI technologies.<sup>18</sup>

### **Socioeconomic Challenges**

AI's rapid integration into various sectors raises numerous societal issues. In public services and law enforcement, the use of AI intensifies concerns over systemic biases and potential discrimination. In the global workforce, AI raises critical issues around job displacement, the need for reskilling workers, and the future of employment.<sup>19</sup>

AI's ability to generate content at scale, particularly through GenAI, complicates the information landscape by making it difficult to distinguish between real and fabricated content.<sup>20</sup> This can undermine trust and accountability, especially during elections, when actors can misuse unregulated systems to manipulate and misinform, threatening the integrity of democratic processes.

The impact of AI on competition is another significant socioeconomic concern. As AI technology becomes more advanced, the potential for monopoly control over information and technology increases.<sup>21</sup> Large corporations with access to vast amounts of data and computational power

---

<sup>15</sup> Falconer (2023), [Privacy in the age of generative AI](#), Stack Overflow;

<sup>16</sup> Marsden (2017), [Artificial Intelligence Defined: Useful list of popular definitions from business and science](#), digitalwellbeing.org.

<sup>17</sup> Benizri et al (2023) [A Comparative Perspective on AI Regulation](#), Lawfare.

<sup>18</sup> Council of Europe (2024), [The Framework Convention on Artificial Intelligence](#), Council of Europe.

<sup>19</sup> Korinek and Juelfs (2022), [Preparing for the \(non-existent?\) future of work](#), Brookings Center on Regulation and Markets.

<sup>20</sup> Ofcom (2024), [Future Technology and Media Literacy: Understanding Generative AI](#)

<sup>21</sup> Price (2023), [Allowing big tech to monopolize AI is risky business](#), Digital Content Next.

can dominate the market, stifling innovation and creating barriers for smaller entities.<sup>22</sup> Furthermore, the increasing prevalence of partnerships among key players could reinforce or extend existing market power positions across the value chain.<sup>23</sup> This concentration of power raises questions about fairness, accessibility, and the overall health of the competitive landscape.

A lack of transparency around how leading-edge models are trained exacerbates these challenges, making it difficult to ensure accountability and trust in AI systems. This opacity makes it difficult to address issues such as “hallucinations,” where GenAI produces fabricated content. Such unreliable outputs pose significant challenges for determining liability and ensuring the reproducibility of scientific results.<sup>24</sup>

### ***Ethical***

Researchers have long raised ethical concerns regarding bias and fairness in AI systems.<sup>25</sup> When an AI system is trained using historical data that reflects societal biases, such as those related to gender or race, these biases can be perpetuated in the AI's decisions.<sup>26</sup> Incomplete or unrepresentative data can also lead to incorrect or unfair predictions. This is particularly concerning in sensitive areas like recruitment and law enforcement, where biased AI decisions can have significant societal impacts.<sup>27</sup> Furthermore, the lack of transparency in how data is sourced and used intensifies these ethical issues, making it difficult to ensure accountability and fairness in AI applications.

GenAI, trained on diverse datasets from various sources, heightens the risk of embedding biases and inaccuracies in AI systems.<sup>28</sup> The extensive use of web scraping to collect necessary data for GenAI also raises ethical questions about the consent of data subjects and the rights of content creators, whose work may be used without proper attribution or compensation.<sup>29</sup>

**Navigating these challenges requires developing regulatory approaches that are dynamic and adaptable as the technologies they aim to govern.** This includes creating frameworks that respond to current AI capabilities and are flexible enough to evolve with future

---

<sup>22</sup> Staff in the Bureau of Competition & Office of Technology (2023), [“Generative AI Raises Competition Concerns”](#), Federal Trade Commission

<sup>23</sup> Competition & Markets Authority (2024) [AI Foundation Models Update paper](#), Government of the United Kingdom.

<sup>24</sup> Aaronson and Thakur (2024), [We Need to Talk about AI Reproducibility](#), Centre for International Governance Innovation.

<sup>25</sup> Zou and Schiebinger (2018), [AI can be sexist and racist — it’s time to make it fair](#), Nature.

<sup>26</sup> Reagan (2021), [Understanding Bias and Fairness in AI Systems](#), Towards Data Science.

<sup>27</sup> NAACP (2024), [Artificial Intelligence in Predictive Policing Issue Brief](#), NAACP.

<sup>28</sup> Ferrara (2023), [Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies](#), arxiv.

<sup>29</sup> Aaronson (2024), [Data Disquiet Concerns about the Governance of Data for Generative AI](#), CIGI Papers.



technological developments. In this environment, sandboxes emerge as a key governance and experimentation tool. Regulatory sandboxes allow for real-world experimentation within a controlled regulatory environment, providing a means of overcoming the limitations of traditional regulation.<sup>30</sup> Operational sandboxes, meanwhile, enable experimentation with data models and practices, allowing stakeholders to test and refine data handling techniques in a secure setting.<sup>31</sup> Sandboxes for AI can help build the agile, iterative governance framework necessary for a systemic approach to governance.

## The Potential of Sandboxes for AI

Sandboxes, originally adapted by financial technology (FinTech) regulators from the enclosed software testing environments used by programmers, have evolved into crucial tools for the exploration and regulation of data-driven technologies like AI.<sup>32</sup> Sandboxes can be divided into two main types: regulatory and operational.

Regulatory sandboxes offer a collaborative, time-bound setting where innovators can test novel technologies and practices within existing regulatory frameworks under the supervision of regulators, before the new product or service is offered to the wider market. When developed with appropriate guardrails, this model is beneficial for assessing new technologies while minimizing risks to the broader economy.<sup>33</sup> Regulatory sandboxes are not merely theoretical spaces but dynamic environments where real-time interaction occurs between innovators and regulators, helping to refine both technology and business models.

Operational sandboxes, on the other hand, are secure platforms where datasets and other resources are pooled and accessed by various stakeholders to explore new data applications. They enable collaborative analysis and testing of data in a controlled environment.<sup>34</sup>

Sandboxes can operate at various levels of governance—local, national, and international. Local sandboxes address community-specific needs and contexts, like [Zurich's AI sandbox](#), which assesses and implements AI projects while granting participants access to new data sources.<sup>35</sup> National sandboxes are the most common type seen today. In 2024, research by the Datasphere Initiative identified 19 countries that have implemented or are developing national sandboxes for data or AI, including 15 regulatory sandboxes, two operational, and two hybrid or

---

<sup>30</sup> Organisation for Economic Cooperation and Development (2024), [Framework for Anticipatory Governance of Emerging Technologies](#), OECD Science, Technology and Industry Policy Papers.

<sup>31</sup> Datasphere Initiative (2022), [Sandboxes for data: creating spaces for agile solutions across borders](#), Datasphere Initiative.

<sup>32</sup> Datasphere Initiative (2022), [Sandboxes for data: creating spaces for agile solutions across borders](#), Datasphere Initiative.

<sup>33</sup> United Nations Department of Economic and Social Affairs (2021), [Sandboxing and experimenting digital technologies for sustainable development](#), Future of the World Policy Brief.

<sup>34</sup> Datasphere Initiative (2022), [Sandboxes for data: creating spaces for agile solutions across borders](#), Datasphere Initiative.

<sup>35</sup> Zurich (2024), [Innovation Sandbox for Artificial Intelligence \(AI\)](#).



uncategorized.<sup>36</sup> While few cross-border sandboxes exist today, they hold immense potential to facilitate international collaboration and harmonize regulations across jurisdictions. For example, the EU has created a cross-border operational sandbox, the [Europeana Metis Sandbox](#), which provides a secure, collaborative environment to allow cultural heritage institutions and aggregators to pool and test datasets to improve data quality, aggregation, and workflow processes.<sup>37</sup>

The diversity within sandbox implementations reflects a spectrum of objectives, from strict compliance to fostering innovation, and varies widely globally. For regulatory sandboxes, some are designed to align innovators with existing regulations, enhancing the oversight capabilities of regulators without intending regulatory change. Others, especially those aimed at fostering scientific and industrial innovation, may temporarily relax certain regulations to encourage experimentation (see Box 1). Operational sandboxes, too, vary widely in their objectives, scope, and impact (see Box 2).

### Box 1: Regulatory Sandboxes in the EU and South Korea

In the **European Union**, the 2023 AI Act requires member states to establish AI sandboxes as part of its comprehensive strategy to regulate artificial intelligence across the Union. Article 57 of the Act details how these sandboxes are intended to provide a controlled testing environment in which innovators and regulators will work together to identify risks and ensure compliance with relevant EU regulations, including the AI Act itself. While the sandboxes do aim to foster innovation and competitiveness, their primary focus is on enhancing legal certainty, facilitating regulatory compliance, and promoting the sharing of best practices. The insights gained from these sandboxes are intended to better enable regulators to effectively apply the Act to emerging sectors and use cases, but they are not necessarily meant to influence policy amendments.<sup>38</sup>

In contrast, **South Korea**, their approach to sandbox initiated under the ‘5 Regulatory Innovation Acts’ of 2019 and further developed in subsequent years, emphasizes economic growth and technological innovation. South Korea’s sandbox system offers a flexible regulatory environment that encourages testing and quick adaptation to technological needs. This approach explicitly shifts the regulatory paradigm from a traditionally restrictive framework to one that prioritizes innovation by permitting activities unless they are explicitly prohibited.<sup>39</sup> Today, five different government agencies in South Korea each operate their own sandbox, in industrial convergence, regulation free zones (regional innovation), ICT, fintech, and smart city.<sup>40</sup>

<sup>36</sup> This does not include the numerous fintech sandboxes that exist around the world. Moreover, some countries have more than one sandbox.

<sup>37</sup> Europeana (2022), [Metis Sandbox Training](#), Europeana Knowledge Base.

<sup>38</sup> EU Artificial Intelligence Act (2024), [Article 57: AI Regulatory Sandboxes](#), Future of Life Institute.

<sup>39</sup> Heonyoung Kwon (2019), “한국형 규제샌드박스의 현황과 향후 과제 [[Current status and future challenges of Korean regulatory sandbox](#)], KISO Journal

<sup>40</sup> European Chamber of Commerce in Korea (2020), [Guide to the Regulatory Sandbox](#), European Chamber of Commerce in Korea.

## Box 2: Operational Sandboxes in Australia and Colombia

In **Australia**, the Australian Competition and Consumer Commission launched the Consumer Data Right (CDR) Sandbox to help participants test and improve their data sharing solutions under the Consumer Data Right legislation. Its primary objective is to enhance the quality of data sharing offerings, reduce barriers for businesses, and foster innovation in the early stages of software development. The scope of this sandbox is relatively narrow at present, focusing on the financial and energy sectors the CDR covers, but the government intends to continuously expand the CDR to other sectors. Its impact is primarily on helping companies comply with data sharing regulations, improving their data sharing services, and ultimately empowering consumers with greater control over their personal data.<sup>41</sup>

In contrast, in **Colombia**, the Ministry of Information Technology and Communications launched the Data Sandbox Collaborative Space in 2021 to enable public entities to carry out pilot projects in analytics and Big Data. It aims to leverage Big Data technologies to address public sector challenges and foster innovation within government entities by providing a secure environment for public entities to develop and refine solutions to public and citizen problems. This operational sandbox allows public entities to pool data resources, experiment with data-driven solutions, and enhance their capabilities in handling large-scale data through the use of advanced Big Data technologies.<sup>42</sup>

The scope and intended impact of the Colombian sandbox are wider than those of Australia's. While the Australian sandbox focuses only on CDR data sharing, Colombia's sandbox addresses critical societal issues such as identifying flood-prone areas, monitoring rural land markets, and estimating poverty through a multidimensional index. The Australian sandbox aims to improve compliance and service quality in data sharing under the CDR regulatory framework, whereas the Colombian sandbox aims to enhance the data handling capabilities of public entities and promote collaborative experimentation to improve public services and inform policy decisions.

**The experimental nature of sandboxes can be invaluable for testing innovative approaches to the governance of emerging technologies.** They provide a controlled setting to experiment with and understand the implications of new technologies and data practices. This hands-on approach allows for real-time problem-solving and adaptation, which is crucial in a rapidly evolving digital landscape.

Regulatory sandboxes have demonstrated significant benefits in sectors like fintech over the past decade and these advantages are increasingly being applied to other [areas](#) of technology and policy.<sup>43</sup> They **reduce uncertainty, facilitate market entry, and enhance competition** by providing a structured environment where businesses can engage with regulators and receive

<sup>41</sup> Commonwealth of Australia (2024), [Consumer Data Right Sandbox](#).

<sup>42</sup> Ministry of Information and Communications Technologies, [Data Sandbox Collaborative Space](#), Government of Colombia

<sup>43</sup> Appaya and Haji (2020), [Four years and counting: What we've learned from regulatory sandboxes](#). World Bank Blogs.

tailored feedback on compliance requirements. This **enables companies to refine their technologies and business models** with greater confidence. Additionally, sandboxes offer a **platform for iterative testing and adaptation**, allowing innovators to adjust their approaches based on real-time insights and regulatory advice, which accelerates the development process and helps ensure market readiness. For regulators, they offer direct exposure to advanced technologies and business models, **preparing them for future challenges**. Additionally, they can help regulators develop more informed and adaptive regulatory frameworks, foster industry collaboration, and build capacity within regulatory bodies.<sup>44</sup>

**In terms of data governance, both operational and regulatory sandboxes provide a unique venue to address the specific challenges associated with both personal and non-personal data.** They allow stakeholders to explore innovative data practices and uses that do not fit neatly within traditional regulatory frameworks. Operational sandboxes enable stakeholders to access pooled data resources to explore new uses of data, while regulatory sandboxes can help clarify regulatory parameters and improve regulators' abilities to respond to sectoral needs. This flexibility is crucial in a landscape where data flows across borders and data-driven technologies evolve rapidly, helping to ensure that data governance keeps pace with technological advancements and societal needs. Sandboxes can also support AI development by facilitating rights-respecting data sharing and access by incubating technologies such as Privacy-Enhancing Technologies (PETs).<sup>45</sup>

Sandboxes represent an invaluable tool for managing the challenges posed by AI technologies. **By enabling developers and regulators to collaboratively test new systems and datasets, sandboxes help ensure that AI technologies are safe, compliant, and aligned with societal values before their widespread deployment.** This collaborative approach is essential, especially since a single regulatory body, perspective, or set of cultural values cannot effectively govern AI — a technology that transcends borders and sectors. For example, a competition regulator addressing monopolistic practices cannot alone tackle the ethical, social, and economic implications of AI. Additionally, concepts like transparency vary significantly across cultures, making it impractical for one country to adopt another's AI governance framework wholesale.

**Sandboxes bridge the gap between rapid technological innovation and the slower pace of regulatory evolution, facilitating innovation while ensuring safety and compliance.** They can build trust between regulators within a country or between countries, and can also build public trust not only by giving consumers greater assurance that novel practices that emerge from the sandbox have been subjected to regulatory scrutiny, but also by identifying when these practices are not compliant with regulations and intervening to prevent their

---

<sup>44</sup> Datasphere Initiative (2022), [Sandboxes for data: creating spaces for agile solutions across borders](#), Datasphere Initiative.

<sup>45</sup> Datasphere Initiative (2022), [Sandboxes for data: creating spaces for agile solutions across borders](#), Datasphere Initiative.

proliferation in the marketplace.<sup>46</sup> As AI and other data-driven technologies continue to integrate into various global sectors and applications, the strategic use of sandboxes could become a cornerstone of the effective governance of data and emerging technologies in general.

## Case Studies and Experiences

Several initiatives have demonstrated the effectiveness of sandboxes in addressing the challenges of AI as a data-intensive technology. This section highlights three examples from Norway, France, and Singapore.

### **Norway's Regulatory Sandbox for Artificial Intelligence**

<p><i>Context</i></p>	<p>The Norwegian Data Protection Authority, Datatilsynet, established its Regulatory Sandbox in 2020 under the National Strategy for Artificial Intelligence. Initially funded through supplemental appropriations in the National Budget, the sandbox became a permanent fixture with the 2023 National Budget.<sup>47</sup> Its primary goal at first was to stimulate “privacy-friendly” innovation in AI.<sup>48</sup> The rationale for this initial focus on AI stemmed from its vast potential to transform public and commercial sectors and improve the general population’s quality of life. The Norwegian government established the sandbox as a proactive measure to address the significant challenges regarding AI’s personal data usage, providing a controlled environment to develop compliant and ethical AI solutions.</p> <p>While data was always a primary focus of the sandbox, its first three iterations were dedicated entirely to developing responsible and ethical AI solutions that complied with data protection regulations. However, recognizing that data protection challenges and the need for privacy-friendly solutions extend across various technological advancements, the government subsequently expanded the sandbox’s scope.<sup>49</sup> Now in its fifth iteration, the sandbox supports projects addressing not only AI but also regulatory uncertainties in complex data sharing, the GDPR’s provisions on automated decision-making, and secondary data uses, among other topics.<sup>50</sup></p>
<p><i>Objectives</i></p>	<p>Norway's Regulatory Privacy Sandbox has three main objectives: stimulating privacy-friendly innovation and digitalization, enhancing the Norwegian Data Protection Authority's expertise in new technologies, and ensuring that technological</p>

<sup>46</sup> Organisation for Economic Cooperation and Development (2022), [Harnessing the power of AI and emerging technologies](#), OECD Digital Economy Papers.

<sup>47</sup>Lystad (2022), [Datatilsynet jubler: sandkassa får permanent støtte \[The Norwegian Data Protection Authority rejoices: the sandbox receives permanent support\]](#), Computerworld.

<sup>48</sup> Datatilsynet (2024), [Doorkeeper. exit report: Intelligent video monitoring with data protection as a primary focus](#), Norwegian Data Protection Authority.

<sup>49</sup> Markussen (2023), [Evaluation of the Norwegian Data Protection Authority's Regulatory Sandbox for Artificial Intelligence](#). Norwegian Data Protection Authority.

<sup>50</sup> Datatilsynets (2021), [How to apply to join the sandbox?](#), Norwegian Data Protection Authority.

	<p>advancements benefit society while safeguarding individual rights.<sup>51</sup> Datatilsynet aims to build public trust by developing and implementing technological solutions within a governance framework that emphasizes accountability, transparency, explainability, and the protection of fundamental rights. Datatilsynet provides tailored guidance to selected projects, develops best practices based on insights gained, and facilitates collaboration and networking among participants and external experts.</p>
<i>Stakeholder engagement</i>	<p>The sandbox emphasizes broad stakeholder engagement, involving diverse participants from both private and public sectors. The selection process involves a rigorous evaluation of applications by an internal interdisciplinary group within the Norwegian Data Protection Authority, which interviews all applicants.<sup>52</sup> An external reference group, comprising members from Innovation Norway, the Norwegian Computing Centre, the Equality and Anti-Discrimination Ombud, and Tekna (a union for graduate technical and scientific professionals), assists in assessing the public benefit of potential projects.<sup>53</sup> The final selection is made by a steering committee composed of the Authority's management. Supporting stakeholders play a crucial role, with Datatilsynet coordinating with other sandbox-managing entities within the Norwegian government and being part of a European sandbox network that includes the British ICO and French CNIL. Datatilsynet has also engaged with authorities in several other countries interested in the Norwegian sandbox and has shared experiences with master's students and doctoral fellows who have written assignments about the sandbox.<sup>54</sup></p> <p>Datatilsynet actively engages the public and stakeholders through its website, where it publishes project plans, final reports, and other relevant sandbox news. The agency also maintains a sandbox newsletter and a podcast series called SandKasten, in which it shares insights from ongoing sandbox projects. Furthermore, Datatilsynet organizes workshops and seminars to disseminate learnings from the sandbox and has leveraged both national and international media, participating in over 30 conferences and events.<sup>55</sup></p>
<i>Reporting</i>	<p>Datatilsynet publishes experiences from both ongoing and completed projects, sharing insights that can benefit other organizations and contribute to broader understanding and improvement in privacy practices.<sup>56</sup> An example from their website can illustrate how projects that successfully navigate the sandbox conclude with the development and refinement of a product or service that complies with privacy regulations and incorporates feedback and insights gained during participation. Take Doorkeeper, a</p>

<sup>51</sup> Datatilsynets (2021), [How to apply to join the sandbox?](#), Norwegian Data Protection Authority.

<sup>52</sup> Datatilsynets (2021), [How to apply to join the sandbox?](#), Norwegian Data Protection Authority.

<sup>53</sup> Markussen (2023), [Evaluation of the Norwegian Data Protection Authority's Regulatory Sandbox for Artificial Intelligence.](#), Norwegian Data Protection Authority.

<sup>54</sup> Datatilsynets (2021), [Årsrapport for 2021 Spesielt om regulatorisk sandkasse for ansvarlig kunstig intelligens \[Annual report for 2021 Especially about the regulatory sandbox for responsible artificial intelligence\]](#), Norwegian Data Protection Authority.

<sup>55</sup> Datatilsynets (2021), [Årsrapport for 2021 Spesielt om regulatorisk sandkasse for ansvarlig kunstig intelligens \[Annual report for 2021 Especially about the regulatory sandbox for responsible artificial intelligence\]](#), Norwegian Data Protection Authority.

<sup>56</sup> Datatilsynet (2024), [Reports](#), Norwegian Data Protection Authority.

	Norwegian start-up that developed an intelligent video monitoring system. Through the sandbox, Doorkeeper addressed regulatory challenges, explored alternative designs, and implemented data minimization and robust security measures. This collaboration ensured their solution not only complied with data protection laws but also set a precedent for privacy-friendly innovations in the security industry, exemplifying how sandbox participation can lead to the successful integration of privacy principles in technological advancements. <sup>57</sup>
<i>Impact assessment</i>	In 2023, Datatilsynet partnered with an external consulting company to assess the sandbox's impact and effectiveness. The evaluation revealed that the sandbox successfully met the needs of participating entities and generated valuable insights into AI, data protection, and ethical technology use. Key recommendations from the evaluation included enhancing the sandbox's technical expertise, improving communication strategies to reach a broader audience, and fostering systematic collaboration with other public and private actors. While the sandbox was generally well-received, the evaluation highlighted areas for improvement, such as providing more detailed final project reports, streamlining internal processes for faster project approval, and recruiting a more diverse range of projects <sup>58</sup>
<i>Risk management</i>	Notably, this sandbox ensured protections for previously-existing intellectual property, allowing participants to retain ownership of any IP they bring into the sandbox collaboration. As a risk-assessment practice, this is an interesting example of an active responsible practice.

**France’s Personal Data Sandbox and its AI iteration**

<i>Context</i>	The French data protection authority, CNIL, launched its personal data sandbox in 2021 to provide focused support to innovative projects that prioritize data privacy from their inception. CNIL offers direct engagement through its legal and technical teams to clarify regulatory requirements, provide practical advice, and audit developed solutions to ensure GDPR compliance. <sup>59</sup>
<i>Objectives and scope</i>	Each year, CNIL invites applications from organizations developing products and services within a selected sector, contrasting with Norway's broader approach that accepts any project dealing with data or AI as outlined in its guidelines. The French sandbox’s first iteration focused on innovations in the field of digital health, and its second on educational digital tools (EdTech). The latest edition targets the integration of artificial intelligence in public services. As with Norway’s sandbox, this choice was driven by a recognition of AI’s significant potential to transform public sector operations. According to the CNIL, AI can significantly improve service delivery by

<sup>57</sup> Datatilsynet (2024), [Reports](#), Norwegian Data Protection Authority.

<sup>58</sup> Markussen (2023), [Evaluation of the Norwegian Data Protection Authority’s Regulatory Sandbox for Artificial Intelligence](#), Norwegian Data Protection Authority.

<sup>59</sup> CNIL (2021), [Bac à sable » données personnelles de la CNIL : appel à projets 2021 \[CNIL personal data “sandbox”: 2021 call for projects\]](#), CNIL.



	improving efficiency, reducing administrative burdens, and enhancing user accessibility. It can assist public officials in optimizing time management, prioritizing tasks, and maximizing the utility of data. The sandbox addresses the challenges related to AI systems relying on substantial volumes of personal data, ensuring innovations comply with strict data protection standards while improving public service delivery. <sup>60</sup>
<i>Outcomes and engagement</i>	Throughout their participation, sandbox projects receive ongoing feedback and support from CNIL, with findings and recommendations published on its website afterwards to foster broader compliance and innovation. Previous recommendations from the digital health and EdTech sandboxes emphasized data minimization, clear data retention policies, robust anonymization to protect privacy, and transparency in data processing. <sup>61</sup> However, the analysis of the sandbox program and communication of its broader impacts remain somewhat constrained, with limited engagement beyond the participating organizations. This may restrict the application of insights gained to broader sectoral technology development or regulatory adjustments.

**Singapore’s Generative AI Evaluation Sandbox for Trusted AI**

<i>Context</i>	Singapore's Generative AI Evaluation Sandbox, spearheaded by the Infocomm Media Development Authority (IMDA) and established in 2023 in partnership with the AI Verify Foundation, illustrates a unique approach to sandbox implementation that diverges from traditional frameworks. This initiative brings together major multinational companies to evaluate trusted AI products using a newly crafted Evaluation Catalogue developed by the IMDA. The Catalogue delineates standardized methods and benchmarks specifically for Large Language Models (LLMs), setting foundational criteria for GenAI evaluation. <sup>62</sup>
<i>Objective</i>	The collaboration between IMDA and the AI Verify Foundation seeks to forge a common standard for GenAI evaluations that not only mitigates risks but also fosters safe adoption, thereby enhancing assessment capabilities across the AI ecosystem. The sandbox is tailored to pinpoint and address the particular gaps in GenAI assessments, and develop benchmarks for model performance, focusing especially on domains relevant to the unique needs of Singapore.
<i>Engagement</i>	The sandbox involves a diverse array of participants, including model developers, application developers, and third-party testers, as well as the Singapore Personal Data Protection Commission.
<i>Reporting</i>	Given how recent the GenAI Evaluation Sandbox is, detailed public information about the sandbox remains scarce.

<sup>60</sup> CNIL (2023), [Digital health and EdTech: the CNIL publishes the results of its first “sandboxes”](#), CNIL.  
<sup>61</sup> CNIL (2023), [“Sandbox”: CNIL launches call for projects on artificial intelligence in public services](#), CNIL.  
<sup>62</sup> Infocomm Media Development Authority (2023), [First of its kind Generative AI Evaluation Sandbox for Trusted AI by AI Verify Foundation and IMDA](#), Infocomm Media Development Authority.



## Conclusion

**As these case studies demonstrate, sandboxes hold significant potential in regards to AI governance and, by extension, data governance.** Nevertheless, their development and implementation present significant challenges that must be addressed to fully leverage their benefits. The inherently global nature of AI, characterized by technology inputs and outputs frequently crossing national borders, complicates regulatory oversight by any single national sandbox operator. Additionally, AI resists regulation from a singular perspective due to its broad and interconnected applications.

Sandboxes are typically developed in silos, meaning that one regulatory body often crafts a framework from scratch without leveraging lessons learned from previous implementations in other jurisdictions. This approach can lead to inefficiencies and unnecessary duplication, compounding the already substantial resources and time required to set up and run a sandbox. For example, while a sandbox might be effective within its own country, the lack of knowledge sharing and collaboration with other countries means that best practices and successful strategies are not disseminated, limiting the overall effectiveness and innovation potential globally.

As noted above, sandboxes often require significant investment in terms of time and expertise to manage complex technologies and ensure compliance under regulatory regimes which often lack clarity in their application (hence the technology's inclusion in the sandbox in the first place). They are usually designed to address specific, narrowly defined problems, limiting their ability to handle cross-sectoral issues or adapt to rapidly evolving AI technologies that span multiple regulatory domains. The experimental nature of sandboxes also means that they are typically not suited for large-scale deployment without significant modifications. These challenges underscore the need for careful planning, robust design, and clear objectives when implementing sandboxes.

**Addressing these challenges effectively requires a collective, coordinated effort that transcends individual organizations or jurisdictions. At present, such international collaboration is lacking.** The establishment of a Global Sandboxes Forum could facilitate this collaborative approach, offering a platform for stakeholders worldwide to share experiences, strategies, and regulatory practices. Such a forum would foster global dialogue and capacity building, promote the harmonization of sandbox frameworks, and help mitigate the resource burdens by pooling expertise and efforts. Ultimately, this could enhance the scalability and adaptability of sandboxes, making them more effective tools for managing the complexities of AI regulation across different sectors and regions.

## ***Policy Actions and Recommendations***

To fully leverage the potential of sandboxes in AI and data governance, policymakers, governments, the private sector, international organizations and other stakeholders should focus on the following areas.

1. **Support the development of cross-regulatory, cross-sectoral, cross-border sandboxes for AI:** Given the multiple origins of AI training data and the interconnected nature of policy impact of AI applications, there is a need for sandboxes that can handle cross-sectoral and transversal policy issues. Regulatory bodies should consider developing sandboxes that can adapt to the evolving nature of AI technologies and address challenges that span multiple regulatory domains, ensuring collaboration among different regulatory agencies in the same jurisdiction. Similarly, cross-border sandboxes should be established to foster interoperability of regulations and promote international cooperation among regulatory agencies of different countries, ensuring that AI innovations can thrive in a consistent and supportive global environment.
2. **Foster common data governance frameworks:** Many AI providers already have, and many laws already require, robust data governance policies that address data quality, provenance, and lifecycle management for data that is processed within the scope of sandbox operations. However, these frameworks are rarely harmonized. There is a need to standardize data governance frameworks to ensure consistency and interoperability across different jurisdictions. A common minimum framework would facilitate more effective data sharing and collaboration, enhancing the overall effectiveness of AI sandboxes.
3. **Integrate privacy-enhancing technologies (PETs) in AI sandboxes:** Encourage the use of PETs and advanced anonymization techniques within AI sandboxes to protect individual privacy and ensure compliance with data protection regulations. This includes technologies like differential privacy, homomorphic encryption, and federated learning, which allow AI systems to process and analyze data without compromising user privacy.
4. **Establish a Global Sandboxes Forum:** A dedicated global platform should be created to foster international collaboration and knowledge sharing. This platform would enable regulatory bodies, industry stakeholders, and academic institutions to exchange experiences and best practices. Regular conferences and workshops should be organized to discuss developments, challenges, and innovations in AI and data governance sandboxes. A repository of case studies, guidelines, and tools should be developed for global access.
5. **Enhance capacity building:** Policymakers and stakeholders must be equipped with the tools and knowledge to effectively run sandboxes and address regulatory issues holistically. Training programs and educational initiatives should be developed to build capacity among regulators, industry participants, and civil society. These programs should focus on the unique challenges posed by AI technologies, including ethical considerations, data governance, and compliance with evolving regulations.

## Annex: Sandboxes for AI and Data Around the World

Name of Sandbox	Country	Competent Authority	Years of Operation	Type	Topic/Focus
Consumer Data Right Sandbox	Australia	Australian Competition and Consumer Commission	2022-	Operational	Technical solutions to data sharing under the Consumer Data Right
AI Regulatory Sandbox	Brazil	Brazilian National Data Protection Authority	In development	Regulatory	Machine learning (ML)-driven technologies, including generative AI
AI Regulatory Sandbox	Chile	Ministry of Economy, Development and Tourism	In development	Regulatory	Experimenting with new uses of AI within the framework of the National AI Policy
Sandbox on privacy by design and by default in Artificial Intelligence projects	Colombia	Superintendence of Industry and Commerce	Uncertain	Regulatory	AI projects in the design stage which involve the processing of personal data
Data Sandbox Collaborative Space	Colombia	Ministry of Information Technology and Communications	2021-	Regulatory	Pilot projects in Analytics and Big Data, empowering public entities to leverage Big Data technologies in a collaborative environment
Regulatory Sandbox on AI	Denmark	Danish Data Protection Authority	In development	Regulatory	Data protection
Data Protection [Panel and] Sandbox	Estonia	Ministry of Economic Affairs and Communications	Uncertain	Other	Projects that are a priority in the development of the digital state; data processing that impacts fundamental rights
Europeana Metis Sandbox	European Union	Deutsche Digitale Bibliothek (German Digital Library)	In Beta testing since 2022	Operational	Data aggregation, quality evaluation, and workflow enhancement for cultural heritage projects
CNIL Personal Data Sandbox	France	National Commission on Informatics and Liberty	2021-	Regulatory	projects developing innovative goods or services linked to the processing of health data (first edition); EdTech (second edition); Projects involving the use of AI in public services (third edition)
Regulatory Sandbox	Japan	Cabinet Secretariat, Secretariat of New Form of Capitalism Realization	2018-	Regulatory	Cutting-edge technologies and business models in any sector

		Headquarters			
AI Sandbox	Malaysia	Ministry of Science, Technology and Innovation	In development	Unknown	Unknown
Regulatory Sandbox for artificial intelligence	Norway	Norwegian Data Protection Authority	2020-	Regulatory	Developing AI solutions that comply with data protection regulations (1st, 2nd, and 3rd editions); projects addressing regulatory uncertainties in complex data sharing, the GDPR's provisions on automated decision-making, secondary data uses, etc (4th, 5th editions)
Regulatory Sandbox System	Republic of Korea	Ministry of Trade, Industry and Energy	2019-	Regulatory	New products and service models that surpass existing laws and systems through convergence of AI, big data, IoT, etc.
Data and Privacy Regulatory Sandbox	Saudi Arabia	Saudi Authority for Data and Artificial Intelligence	2023-	Regulatory	Solution/service/business model that falls under Data and Privacy laws and regulations or is a PET (Privacy Enhancing Technology) solution
Privacy Enhancing Technology Sandbox	Singapore	Infocomm Media Development Authority (IMDA)	2022-	Regulatory	Projects using PETs to collaborate on data
Generative AI Evaluation Sandbox for Trusted AI	Singapore	Infocomm Media Development Authority (IMDA)	2023-	Regulatory	Evaluation and Testing of trustworthy generative AI
Regulatory Sandbox on Artificial Intelligence	Spain	Secretary of State for Digitalization and Artificial Intelligence, Ministry of Economic Affairs and Digital Transformation	In development	Regulatory	Artificial Intelligence
Regulatory sandbox on data protection	Sweden	Swedish Authority for Data Protection	2023-	Regulatory	topics related to "gray area issues" in data protection law
ico Regulatory Sandbox	United Kingdom	Information Commissioner's Office	2020-	Regulatory	Various

