FROM BLUEPRINT TO REALITY

Implementing AI Regulatory Sandboxes under the AI Act

Nathan Genicot

VUB LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY RESEARCH GROUP

FARI AI FOR THE COMMON GOOD INSTITUTE BRUSSELS

The report was written by Nathan Genicot within the interdisciplinary Research Group on Law, Science, Technology & Society (LSTS) of the Vrije Universiteit Brussel (VUB) and funded by the Brussels FARI AI Institute for the Common Good (ULB-VUB).

For contact with the author: nathan.genicot@vub.be

Please cite this publication as:
N. Genicot, *From Blueprint to Reality: Implementing AI Regulatory Sandboxes under the AI Act*, FARI & LSTS Research Group (VUB), Brussels, 2024.

Date: December 2024 (Version 1.0)

Contents

Executive Summary

Artificial intelligence (AI) regulatory sandboxes are a mechanism introduced in the recently adopted Artificial Intelligence Act (AI Act) to foster the development of innovative AI systems within the European Union (EU). By 2 August 2026, each Member State of the EU will be required to have at least one AI regulatory sandbox in place. This report explores this new legal framework and reviews existing related practices. It aims to enhance the understanding of the rules introduced by the AI Act, and highlight key issues that must be addressed to ensure the effective and timely implementation of AI regulatory sandboxes at the national level.

The notion of regulatory sandboxes emerged about ten years ago in the financial sector. It is generally defined as a controlled environment in which companies can test innovative products under the guidance of a competent regulator, and where regulatory requirements may be relaxed, particularly through the granting of individual exemptions. **In recent years, the instrument gained popularity within the EU**, with both the European Commission and the Council of the EU promoting it as a policy instrument. Several EU regulations adopted in 2024 covering various sectors, from net-zero technologies to cyber resilience, include provisions for the establishment of regulatory sandboxes.

Among these, the AI Act stands out as the most ambitious, notably by making the introduction of regulatory sandboxes mandatory in every Member State. Article 3(55) of the regulation defines AI regulatory sandboxes as "***a concrete and controlled framework*** *set up by a* ***competent authority*** *which offers providers or prospective* ***providers*** *of AI systems the possibility to develop, train, validate and test, where appropriate in real world conditions, an* ***innovative AI system****, pursuant to a sandbox plan for a limited time* ***under regulatory supervision***". The provisions on AI regulatory sandboxes raise multiple questions.

A first question is which types of AI systems AI regulatory sandboxes are intended for. The AI Act states that sandboxes must be open to any provider of an AI system meeting specified eligibility and selection criteria. However, since one of the main aims of the sandbox is to assist participants with compliance obligations, it suggests that AI systems subject to the regulation's requirements should be their primary focus. This would be in line with the AI Act's risk-based approach, according to which requirements and obligations imposed on AI systems depend on the level of risk they pose to health, safety, and fundamental rights. While AI systems posing an unacceptable risk are banned, high-risk systems are permitted but subject to most of the AI Act's requirements, low-risk systems face minimal or no obligations, whereas general-purpose AI systems are governed by a specific regime. High-risk AI systems are, therefore, the most logical candidates for participation in a sandbox, as this category is primarily subject to the obligations outlined in the AI Act.

A second question concerns the *national competent authorities* responsible for operating the sandbox. Under the AI Act, this term refers either to *market surveillance authorities* – responsible for post-market surveillance of AI systems, monitoring the risks to health, safety, and fundamental rights posed by AI systems once they have been placed on the market or put into service – or to *notifying authorities*, which are responsible for designating and monitoring notified bodies. Market surveillance authorities might seem better suited for this role, as operating AI regulatory sandboxes primarily involves advising providers on regulatory compliance – a task that aligns directly with their mandate to monitor AI systems' compliance with the AI Act.

As a third point, the issue of possible exemptions from regulatory requirement demands careful analysis. While the AI Act does not explicitly state that derogations are allowed, participants are granted a form of regulatory flexibility through limited sanctions: as long as they respect the sandbox plan and act in good faith, no administrative fines shall be imposed by the competent authority. As a matter of fact, however, the requirements and obligations set out in the AI Act – along with associated fines for non-compliance – only apply after AI systems have been placed on the market or put into service, whereas sandbox participation is to occur before such stage. This raises questions about the practical effect of this rule. Importantly, if other authorities responsible for EU or national legislation beyond the AI Act are involved in supervising an AI system in the sandbox and provide advice on compliance, no administrative fines will be imposed for violations of that legislation either: if a participant complies with the sandbox plan but infringes another EU or national law, they should not be penalised. The legality of this provision may be questionable in some cases, as it is doubtful that the AI Act has the authority to limit the supervisory powers of authorities exercised under other national or EU laws. To ensure the effectiveness of this exemption from fines, the relevant laws would therefore need to be amended accordingly by the competent legislator.

A fourth issue concerns the implications of testing in real world conditions. This mechanism involves the temporary testing of an AI system in real-life settings to gather reliable and robust data and to assess and verify the system's conformity with the requirements of the regulation. This procedure is distinct from AI regulatory sandboxes and may be carried out either within or outside them. When testing high-risk AI systems in real world conditions, the process must be conducted under the supervision of a market surveillance authority and is subject to specific rules and conditions. Crucially, this testing does not qualify as placing the AI system on the market or putting it into service under the AI Act. As a result, it allows high-risk AI systems to be tested in real world conditions without being subject to most of the requirements that apply to these systems under the AI Act, making this mechanism closely akin to a regulatory exemption.

A final question is whether an AI regulatory sandbox can be linked to testing facilities, meaning that the sandbox would not only facilitate compliance with the AI Act but would also support the development of AI systems through access to technical infrastructure. In this regard, the AI Act states that sandboxes should be linked to other EU-funded services,

such as testing and experimentation facilities and European digital innovation hubs. However, a review of AI regulatory sandboxes established by data protection authorities before the adoption of the AI Act shows that none of them provide technical infrastructure. Establishing connections between regulators and testing facilities might pose challenges, especially given the need to avoid conflicts of interest or confusion between their respective missions.

To ensure the effective implementation of AI regulatory sandboxes by Member States, several recommendations can be made. First, the European Commission should clarify the roles and responsibilities of the authorities involved in sandbox operations, particularly addressing the ambiguity between market surveillance authorities and national competent authorities in the upcoming implementing acts. Second, Member States should design the supervision of regulatory sandboxes in tandem with the supervisory framework of the AI Act. In this regard, it might be prudent to designate a central authority to coordinate the various AI regulatory sandboxes that may be established at the local or sectoral level, ensuring uniform procedures and effective communication. Third, Member States should evaluate whether legislation beyond the AI Act could be amended to support the effective testing of AI systems. This could involve, on the one hand, enabling the non-imposition of administrative fines for participants who successfully took part in an AI regulatory sandbox (thereby making the exemption from fines provision effective) and, on the other hand, introducing experimental clauses to permit temporary derogations from specific legal requirements. Finally, Member States should consider how to build bridges with technical infrastructures while ensuring no conflict of interest or confusion between the roles of regulators and technical service providers. This could be achieved by establishing a single one-stop shop with two channels: one dedicated to legal compliance within regulatory sandboxes, and the other offering resources and support from various AI ecosystem instruments to aid in AI system development.

Introduction

Artificial intelligence (AI) regulatory sandboxes are a mechanism introduced in the recently adopted Artificial Intelligence Act (AI Act) to foster the development of innovative AI systems.[1] This report explores the legal framework established for these sandboxes and reviews existing related practices.

Regulatory sandboxes emerged around ten years ago in the financial sector and have grown in popularity over time, including in the European Union (EU), which is actively promoting their adoption across a variety of sectors. This notion refers to a controlled environment in which innovative products can be tested under the supervision of a regulatory authority, often with a relaxation of regulatory requirements, particularly through the granting of individual exemptions.

Under the AI Act, AI regulatory sandboxes are intended to facilitate the development and testing of AI systems before they are placed on the market or put into service, with regulatory oversight from national competent authorities. The regulation requires each Member State to set up at least one such sandbox by 2 August 2026.

Understanding the exact nature of the mechanism introduced by the AI Act is essential, as the notion of regulatory sandboxing covers different realities. While some regulatory sandboxes are essentially forums for discussion between regulators and developers of innovative projects, others are less focused on this regulatory dialogue and have the primary mission of granting legal exemptions that allow economic actors to test products that are currently not permitted under applicable law. In addition, some regulatory sandboxes provide, alongside legal guidance, a technical infrastructure for the development and testing of new technological solutions. This diversity makes it critical to appreciate where the AI Act's regulatory sandboxes sit in this landscape.

Against this backdrop, this report seeks to clarify the legal regime governing AI regulatory sandboxes, as set out in the AI Act, and to identify the key challenges that must be addressed to enable their effective implementation by Member States.

The report is divided into two parts.

The **first part** focuses on the rules introduced by the AI Act on regulatory sandboxes. The first section briefly explains what regulatory sandboxing is. The second section discusses the growing use of regulatory sandboxes as a legal instrument by the EU and details other EU legislation, recently adopted or under discussion, that foresees the creation of such sandboxes. The third section examines the AI Act, outlining its key principles, its supervisory

[1] Article 57(1) of the Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L.

framework, and analysing the provisions of its Chapter VI which specifically cover AI regulatory sandboxes and 'testing in real world conditions'. The final section identifies key challenges and outstanding issues that must be addressed by either the European Commission or Member States to ensure the proper implementation of AI regulatory sandboxes.

The **second part** is devoted to a review of existing AI regulatory sandbox projects that have already been launched by EU Member States prior to the adoption of the AI Act. While the focus is on the EU, a few initiatives from non-EU countries that were considered relevant are also described. It looks in particular at sandboxes relating to AI, which have been created by different data protection authorities. Drawing on published documents, this review provides an overview of existing initiatives and offers insights into how the AI Act's regulatory sandboxes could build upon them.

Acknowledgements

This report was conducted as part of interdisciplinary research carried out in collaboration with FARI, the LSTS Research Group, and the AI Lab (VUB). The report benefitted from valuable discussions and comments on earlier versions provided by Gloria González Fuster, Antoine-Alexandre André, Martin Canter and Thiago Moraes, as well as from fruitful exchanges with Yailen Martinez Jimenez, Yordanka Ivanova, Alexandra Papageorgiou, Rocco Saverino, and participants of the CAIRNE & FARI workshop on AI regulatory sandboxes, held on 19 November. Part II of the report also benefited from the research assistance provided by Roxane Van der Bruggen during her internship at FARI. Any errors or shortcomings in the report remain the sole responsibility of the author.

Part I - Regulatory sandboxing and its role in the AI Act

1. Regulatory sandboxing in a nutshell

The notion of *regulatory sandboxes* emerged about ten years ago.[2] It is generally defined as a controlled environment in which companies can test innovative products under the guidance of a competent regulator, and with a relaxation of regulatory requirements (notably through the granting of individual exemptions).[3] The term '*sandbox'* comes from computer science, where it refers to separate virtual environments in which software or codes can be tested without risking damage to other operational systems.[4] Regulatory sandboxes are often described as a policy tool that balances the pursuit of innovation with the need to ensure that appropriate safeguards are in place to protect safety and consumer interests.[5]

The first regulatory sandbox was launched in 2015 in the United Kingdom (UK) by the Financial Conduct Authority (FCA) to promote innovative products (i.e. mostly FinTech products).[6] Many of the participants in the sandbox were start-ups developing solutions based on technologies such as blockchain, distributed ledgers or data analytics, and aimed at facilitating operations such as cross-border transactions, payment processing, consumer behaviour analysis, provision of log-in solutions, claims processing automation, etc.[7] In the wake of the FCA, many countries around the world launched their own financial regulatory sandboxes.[8] Many regulatory sandboxes were also created in other areas. In the energy sector, regulatory sandboxes have been created, notably by many European countries, to encourage the development of new technological solutions such as smart

[2] D. Zetzsche et al., "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation", *Fordham Journal of Corporate & Financial Law*, 1 January 2017, vol. 23, no. 1, p. 64.

[3] *Ibid*. p. 64; H.J. Allen, "Regulatory Sandboxes", *The George Washington Law Review*, 2019, vol. 87, no. 3, p. 592.

[4] S. Philipsen, E.F. Stamhuis, M. De Jong, "Legal enclaves as a test environment for innovative products: Toward legally resilient experimentation policies", *Regulation & Governance*, 2021, vol. 15, no. 4, p. 1132; E. Gromova, E. Stamhuis, "Real-Life Experimentation with Artificial Intelligence", *in* J. Temperman, A. Quintavalla (eds.), *Artificial Intelligence and Human Rights*, Oxford University Press, 2023, p. 552. It is also used in areas such as video games and cybersecurity.

[5] Financial Conduct Authority, *Regulatory sandbox*, November 2015, online https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf (retrieved on 4 November 2024).

[6] S. Appaya, H.L. Gradstein, M.N. Haji, *Global Experiences from Regulatory Sandboxes*, Washington, D.C., World Bank, Fintech Note | No. 8, 2020, p. 5, online http://documents.worldbank.org/curated/en/912001605241080935/Global-Experiences-from-Regulatory-Sandboxes (retrieved on 4 October 2024).

[7] See https://www.fca.org.uk/firms/innovation/regulatory-sandbox/accepted-firms, accessed 4 October 2024.

[8] S. Appaya, H.L. Gradstein, M.N. Haji, *Global Experiences from Regulatory Sandboxes*, *op. cit.* note 6; A. Attrey, M. Lesher, C. Lomax, *The role of sandboxes in promoting flexibility and innovation in the digital age*, Paris, OECD, OECD Going Digital Toolkit Notes, 2020, online https://doi.org/10.1787/cdf5ed45-en (retrieved on 4 October 2024).

meters, smart charging of electric vehicles or electricity storage.[9] In the healthcare sector, countries like the UK, Japan, the United States of America, and Singapore have established regulatory sandboxes to support the development and deployment of innovative digital health solutions.[10] In the transport sector, regulatory sandboxes have been established to facilitate the testing and development of technologies such as autonomous vehicles and drones.[11] Several data protection authorities have also established sandboxes in recent years.[12]

Depending on the country and field of application, the functioning and nature of regulatory sandboxes can differ. They typically exhibit the **following characteristics**, though not all to the same extent.

- **Innovation-driven:**

Regulatory sandboxes are typically established to foster innovation, particularly that driven by emerging technologies.[13] They often aim to support start-ups in developing their products and bringing them to market, making them somewhat similar to incubators.[14] However, they can also aim to drive technological advancements in public services, as exemplified by the CNIL's sandbox, which supports AI projects for public sector applications.[15]

- **Supervision by an authority and regulatory dialogue**

A regulatory sandbox is overseen by a competent authority (and often created on its own initiative). For example, in the financial sector, sandboxes are supervised by authorities such as the UK FCA or the Dutch Authority for the Financial Markets. In the energy sector, regulators such as the British Office of Gas and Energy Markets (Ofgem) and the French *Commission de Régulation de l'Energie* play similar roles. Health regulatory sandboxes are managed by government bodies such as Singapore's Ministry of Health. In data protection, data protection authorities like the Information Commissioner's Office (ICO) in the UK,

[9] F. Gangale et al., *Making energy regulation fit for purpose. State of play of regulatory experimentation in the EU: insights from running regulatory sandboxes*, Luxembourg, Publications Office of the European Union, EUR no. 31438, 2023; Z. Aydın, O. Yardımcı, "Regulatory sandboxes and pilot projects: Trials, regulations, and insights in energy transition", *Engineering Science and Technology, an International Journal*, August 2024, vol. 56, p. 101792.
[10] E. Leckenby et al., "The Sandbox Approach and its Potential for Use in Health Technology Assessment: A Literature Review", *Applied Health Economics and Health Policy*, November 2021, vol. 19, no. 6, p. 863.
[11] A. Attrey, M. Lesher, C. Lomax, *The role of sandboxes in promoting flexibility and innovation in the digital age*, *op. cit.* note 8, p. 20.
[12] See Part II of the report.
[13] D. Zetzsche et al., "Regulating a Revolution", *op. cit.* note 2, p. 68.
[14] S. Ranchordás, "Experimental Regulations and Regulatory -Sandboxes – Law Without Order?":, *Law and Method*, 2021, p. 5.
[15] Commission nationale de l'informatique et libertés, "'Sandbox': CNIL launches call for projects on artificial intelligence in public services", 28 July 2023, online https://www.cnil.fr/en/sandbox-cnil-launches-call-projects-artificial-intelligence-public-services (retrieved on 6 December 2024).

Datatilsynet in Norway, or the French *Commission nationale informatique et libertés* (CNIL) oversee their respective sandboxes.

A key aspect of regulatory sandboxes is that they provide a space for **close dialogue between the authorities and regulated parties**, where companies explain the technological solutions they are developing and the authorities provide bespoke guidance on how to comply with the law.[16] This mutual exchange is supposed to benefit both sides: regulated actors gain a clearer understanding of legal requirements and their resulting obligations, while regulators gain insights into emerging technologies and ensure that regulations effectively achieve their objectives.

- **Regulatory flexibility**

Regulatory sandboxes are traditionally described as offering regulatory flexibility for selected participants by easing certain regulatory requirements and reducing the risk of sanctions.[17]

In this sense, regulatory sandboxes are associated to experimental law, which refers to the temporary testing of a law or policy instrument in a limited space in order to evaluate its effects.[18] The experimental nature of regulatory sandboxes lies in the fact that, on a case-by-case basis, they allow private or public actors to test new technological solutions within a temporarily relaxed regulatory framework. This regulatory flexibility is intended to strike a balance between safety, on the one hand, and innovation which risks being hindered by overly strict laws, on the other.[19] A parallel has been drawn between regulatory sandboxes and clinical trials: both involve testing products under strict conditions before they are placed on the market.[20]

---

[16] S. Ranchordás, "Experimental Regulations and Regulatory -Sandboxes – Law Without Order?", *op. cit.* note 14, p. 5; S. Philipsen, E.F. Stamhuis, M. De Jong, "Legal enclaves as a test environment for innovative products: Toward legally resilient experimentation policies", *op. cit.* note 4, p. 1132.

[17] D. Zetzsche et al., "Regulating a Revolution", *op. cit.* note 2, p. 64; A. Attrey, M. Lesher, C. Lomax, *The role of sandboxes in promoting flexibility and innovation in the digital age*, *op. cit.* note 8, p. 6.

[18] On the subject, see: S. Ranchordás, "Experimental Regulations and Regulatory -Sandboxes – Law Without Order?", *op. cit.* note 14; Conseil d'État, *Les expérimentations : comment innover dans la conduite des politiques publiques ?*, Paris, 2019; S. Ranchordás, *Constitutional sunsets and experimental legislation: a comparative perspective*, Cheltenham, Edward Elgar Publishing Limited, 2014; G. Van Dijck, R. Van Gestel, "Better Regulation through Experimental Legislation", *European Public Law*, 2011, vol. 17, no. 3, p. 539.

[19] T. Buocz, S. Pfotenhauer, I. Eisenberger, "Regulatory sandboxes in the AI Act: reconciling innovation and safety?", *Law, Innovation and Technology*, 2023, vol. 15, no. 2, p. 357.

[20] Financial Conduct Authority, *Regulatory sandbox*, *op. cit.* note 5, p. 9; D. Zetzsche et al., "Regulating a Revolution", *op. cit.* note 2, p. 68; T. Buocz, S. Pfotenhauer, I. Eisenberger, "Regulatory sandboxes in the AI Act: reconciling innovation and safety?", *op. cit.* note 19, p. 357. Granting exemptions involves differentiating between those who benefit from them and those who do not, which may violate the principle of equal treatment. See on this subject: S. Ranchordás, "Experimental Regulations and Regulatory -Sandboxes – Law Without Order?", *op. cit.* note 14, p. 13; T. Buocz, S. Pfotenhauer, I. Eisenberger, "Regulatory sandboxes in the AI Act: reconciling innovation and safety?", *op. cit.* note 19, p. 382.

However, the nature of this regulatory flexibility varies considerably from one regulatory sandbox to another, depending on the legal regime governing the area concerned. In highly regulated sectors such as finance and energy, individual exemptions allow start-ups, for example, to test innovative products without prior authorisation or a licence.

In addition, regulatory flexibility depends directly on the powers that the regulator holds under the law establishing it. In some cases, the authorities setting up a sandbox already have the power to authorise temporary derogations from the law, because the law gives them considerable discretionary powers. However, in other cases, the legislator must intervene to explicitly confer such powers on the authority.[21] In the case of data protection sandboxes, the General Data Protection Regulation (GDPR)[22] does not authorise exemptions to be granted, which therefore limits the room for manoeuvre of data protection authorities. This has led the CNIL in France to state that its data protection sandbox was not a regulatory sandbox but just a sandbox as "*it does not allow the removal of legal constraints, even temporarily, because personal data law does not allow it*".[23] However, many other data protection authorities speak of regulatory sandboxes, although they do not grant legal exemptions either. While the ability of regulatory sandboxes to deviate from the law is often presented as one of their essential characteristics, this is not always the case. As explained in more detail below, the AI Act provides for a mixed regime which allows AI systems to be tested in real world situations while being guaranteed not to incur administrative fines.

The experimental dimension of regulatory sandboxes also lies in the fact that the sandbox process is supposed to inform the legislator and, where appropriate, indicate how existing law should evolve in the light of social and technological developments.[24]

- **Entry and exit requirements**

Participation in the sandbox is subject to public **eligibility criteria**. Applicants must generally demonstrate how innovative and fit for purpose their proposed product is.[25] They must also show that they have the necessary resources in terms of finance and skills to participate effectively in the sandbox process. Additionally, participation sometimes

[21] T. Buocz, S. Pfotenhauer, I. Eisenberger, "Regulatory sandboxes in the AI Act: reconciling innovation and safety?", *op. cit.* note 19, p. 364.
[22] Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.
[23] Commission nationale de l'informatique et libertés, *"Sandbox": CNIL launches call for projects on artificial intelligence in public services*, *op. cit.* note 15. See also Part II of the report, 'France', p. 40.
[24] B. Laurent et al., "The Test Bed Island: Tech Business Experimentalism and Exception in Singapore", *Science as Culture*, 3 July 2021, vol. 30, no. 3, p. 383.
[25] D. Zetzsche et al., "Regulating a Revolution", *op. cit.* note 2, p. 69.

necessitates regulatory uncertainty, meaning that there must be a question or ambiguity regarding the application or interpretation of the law in relation to their project.[26]

Once they have been selected, the participants must agree with the authority on a testing plan that defines the rules and procedures that will be followed during participation in the sandbox. It is only if the participant complies with the rules and implements the required safeguards defined in the plan that the legal exemptions will apply (if they apply). The competent regulator is generally empowered to exclude a participant from the sandbox if the testing plan is not respected, or for other specified conditions (such as too high risk of violation of fundamental rights).[27]

- **Testing environment**

Regulatory sandboxes are often described as '*testing environments*' where participants can test their products with reduced risk. From the participants' perspective, the risk of being sanctioned by the authority is minimised, while from the point of view of individuals and society, the risks are contained because the product is either not yet deployed or is deployed in a very limited way. In some cases, the testing environment involves real technical infrastructure that participants can use. In this sense, regulatory sandboxes share similarities with other concepts such as testbeds and living labs. Each of these frameworks promotes the testing and experimentation of innovative technologies and encourages dialogue and collaboration between various stakeholders, including public authorities, companies, and sometimes citizens[28].

Testbeds are dedicated environments designed purely for technical testing. Unlike regulatory sandboxes – which sometimes provide both regulatory guidance and a technical framework for product testing – testbeds focus solely on the technical aspects, enabling participants to trial their technologies without addressing regulatory compliance considerations. **Living labs** emphasise *co-participation* and local engagement, placing citizens and residents at the heart of the innovation process. In living labs, the community actively participates in designing and testing products, giving these initiatives a distinctive community-centered approach to product development.

[26] *Ibid*. p. 71.
[27] *Ibid*. p. 77.
[28] See S. Arntzen *et al.*, *Testing innovation in the real world: real-world testbeds*, Nesta, October 2019, https://media.nesta.org.uk/documents/Testing_innovation_in_the_real_world.pdf (last consulted on 6 December 2024); European Commission, 'Regulatory learning in the EU Guidance on regulatory sandboxes, testbeds, and living labs in the EU, with a focus section on energy', SWD(2023) 277/2 final, 28 August 2023.

2. Regulatory sandboxes as an EU legal instrument

The inclusion of regulatory sandboxes in the AI Act is not an isolated initiative. It illustrates a broader willingness of EU institutions to promote the use of regulatory sandboxes as a policy instrument. In March 2020, the European Commission published the communication *'An SME Strategy for a Sustainable and Digital Europe'* in which regulatory sandboxes are described as enabling "*innovative solutions not already foreseen in regulations or guidelines to be live-tested with supervisors and regulators*".[29]

In the wake of this Communication, the Council of the EU adopted in November 2020 conclusions on '*Regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age*'.[30] As part of its will to promote "*efficient regulatory instruments*", the Council underlines the need for a regulatory framework that is "*evidence-based*" and "*future-proof*". Flexibility and experimentation are presented as key elements to reach this objective. Noting that regulatory sandboxes are increasingly used, the Council highlights that they "*can provide the opportunity for advancing regulation through proactive regulatory learning, enabling regulators to gain better regulatory knowledge and to find the best means to regulate innovations based on real-world evidence, especially at a very early stage, which can be particularly important in the face of high uncertainty and disruptive challenges, as well as when preparing new policies*". The Council therefore calls "*on the Commission to organise, in cooperation with Member States, an exchange of information and good practices regarding regulatory sandboxes between Member States*".

In 2021, the **Better Regulation toolbox** – a comprehensive European Commission handbook which aims to improve the quality of EU legislation by ensuring a transparent and efficient decision-making process – added regulatory sandboxes as an emergent policy instrument.[31] Regulatory sandboxes are defined as "*schemes that enable firms to test innovations in a controlled real-world environment, under a specific plan developed and monitored by a competent authority*" (see *Tool #69. Emerging Methods and Policy*

[29] European Commission, "*An SME Strategy for a Sustainable and Digital Europe*" (Communication) COM(2020) 103 final, p. 9. That same year, the OECD published a policy note on regulatory sandboxes (A. Attrey, M. Lesher, C. Lomax, *The role of sandboxes in promoting flexibility and innovation in the digital age*, *op. cit.* note 8). In addition, the Commission already considered the establishment of AI regulatory sandboxes as early as 2018 in its coordinated plan on AI (See European Commission, "Annex to the Coordinated Plan on Artificial Intelligence" (Communication) COM(2018) 795 final, p. 8).

[30] Council of the European Union, 'Conclusions on regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age' (2020) C 447/1.

[31] Accessible here: https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/better-regulation/better-regulation-guidelines-and-toolbox_en.

Instruments).[32] Various key characteristics of regulatory sandboxes (which echo those highlighted above) are detailed:[33]

The product, service, or business model tested should represent a "*genuine innovation*" not yet available in the market. It must offer societal or consumer benefits, addressing unmet needs or supporting policy goals like environmental protection or financial stability. The innovation must be ready to be tested, and the specific legal obstacles to testing that should be lifted must be identified. The sandbox must present clear boundaries – including applicable legislation, sectors, test duration, and exit conditions – to ensure legal clarity and enable outcome assessment. Lastly, appropriate safeguards must be in place within the sandbox to uphold policy objectives and legal requirements, such as safety standards when testing autonomous technologies.

In line with this approach, the **New European Innovation Agenda** presented in 2022 by the European Commission also insists on the importance of creating "*responsible regulatory frameworks that facilitate experimentation by innovators, ensure public acceptance and enable learning and adaptation by regulators in new domains*"[34]. The European Commission emphasises the need for "*experimentation spaces*", a notion which encompasses regulatory sandboxes, testbeds and living labs.

Besides the AI Act, four EU regulations adopted in 2024 (or currently under discussion) provide for the implementation of regulatory sandboxes: the Interoperable Europe Act,[35] the Net-Zero Industry Act,[36] the Cyber Resilience Act,[37] and the Proposed regulation on the authorisation and supervision of medicinal products for human use.[38] Prior to these, no other regulatory sandboxes had been explicitly introduced in EU legislation.[39] They are

[32] European Commission, 'Better regulation toolbox' (2023), https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=BR%20toolbox%20-%20Jul%202023%20-%20FINAL.pdf.
[33] See *Ibid.*, p. 559.
[34] European Commission, "A New European Innovation Agenda" (Communication) COM(2022) 332 final p. 8.
[35] Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act) [2024] OJ L.
[36] Regulation (EU) 2024/1735 of the European Parliament and of the Council of 13 June 2024 on establishing a framework of measures for strengthening Europe's net-zero technology manufacturing ecosystem and amending Regulation (EU) 2018/1724 [2024] OJ L.
[37] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) [2024] OJ L.
[38] European Commission, "Proposal for a Regulation of the European Parliament and of the Council laying down Union procedures for the authorisation and supervision of medicinal products for human use and establishing rules governing the European Medicines Agency, amending Regulation (EC) No 1394/2007 and Regulation (EU) No 536/2014 and repealing Regulation (EC) No 726/2004, Regulation (EC) No 141/2000 and Regulation (EC) No 1901/2006" COM(2023) 193 final (Proposed regulation on medicinal products).
[39] This statement is based on a search in EUR-Lex. Only regulatory sandboxes for which an explicit legal regime is laid out in an EU legislative act are listed, excluding instances where a simple mention to the concept is

presented here in chronological order, from the earliest to the most recent. Lastly, a European Commission initiative – the Pan-European blockchain regulatory sandbox – is briefly discussed.

- **Interoperability regulatory sandboxes**

Adopted in March 2024, the *Interoperable Europe Act* is an EU Regulation which aims to ensure cross-border interoperability between the IT systems used by the public services of all Member States and by EU institutions, in order to guarantee a genuine European digital Space and European digital services.[40] Documents issued in one Member State, such as university diplomas, social security details or vaccination certificates, should, for example, be able to be used in other Member States without further formalities.

The Regulation provides for the creation of interoperability regulatory sandboxes to act as hubs for the development of innovative interoperable solutions.[41] Interoperability regulatory sandboxes shall be operated under the responsibility of the participating EU entities or national public sector bodies and shall be subject to authorisation by the European Commission. Participation in the interoperability regulatory sandbox shall be based on a specific plan elaborated by the participants detailing the project and the risk mitigation measures.[42]

In addition to the European Commission, other national or local supervisory authorities may be involved in supervising an interoperability regulatory sandbox if the project falls within their remit. The only type of supervisory authority explicitly mentioned in the Regulation are data protection authorities, which must intervene as soon as personal data is being processed. Article 12(6) of the Interoperable Europe Act authorises the processing of personal data in the sandbox for purposes other than that for which it has initially been lawfully collected, subject to various conditions. The AI Act contains a very similar provision for AI regulatory sandboxes, which will be discussed further below. The underlying aim of interoperability regulatory sandboxes is to facilitate the development of innovative solutions by allowing data processing.

made. Nor does it include regulatory sandboxes that have been implemented by Member States because national authorities have spontaneously decided to do so. See also the staff working document published the European Commission on this subject: European Commission, 'Regulatory learning in the EU Guidance on regulatory sandboxes, testbeds, and living labs in the EU, with a focus section on energy', SWD(2023) 277/2 final, 28 August 2023, p. 16.

[40] Recitals 1-3 of the Interoperable Europe Act.

[41] They are defined as "a controlled environment set up by a Union entity or a public sector body for the development, training, testing and validation of innovative interoperability solutions, where appropriate in real world conditions, supporting the cross-border interoperability of trans-European digital public services for a limited period of time under regulatory supervision" (Article 2(14) of the Interoperable Europe Act).

[42] Article 12(3) of the Interoperable Europe Act.

The Interoperable Europe Act does not provide for the possibility of derogating from the law in these sandboxes.[43] Participants in the sandbox remain liable under EU and national law on liability for any damage caused during their participation in the interoperability regulatory sandbox.[44]

- **Net-zero regulatory sandboxes**

The *Net-Zero Industry Act* has been adopted in June 2024. This regulation aims to enhance the internal market by ensuring a secure and sustainable supply of net-zero technologies, scaling up their manufacturing and supply chains, supporting climate neutrality and decarbonisation, and fostering quality jobs and competitiveness in the EU.[45] It provides for the creation of net-zero regulatory sandboxes, described as "*an important tool to promote innovation in the field of net-zero technologies and regulatory learning*".[46] They are defined as "*a scheme that enables undertakings to test innovative net-zero technologies and other innovative technologies in a controlled real-world environment, under a specific plan, developed and monitored by a competent authority*".[47]

Member States may establish a net-zero regulatory sandbox either at their own initiative or at the request of any company, organisation or consortium that develops innovative net-zero technologies and fulfils certain eligibility and selection criteria.[48] The setting up of these sandboxes is therefore not compulsory. The European Commission will adopt implementing acts defining the eligibility criteria and selection procedure, the whole sandbox process, as well as the terms and conditions applicable to the participants.[49]

The sandbox must be supervised by a competent authority – not further defined – which must exercise its supervisory powers "*in a flexible manner within the limits of the relevant law, adapting existing regulatory practices and using their discretionary powers when implementing and enforcing legal provisions to a specific net-zero regulatory sandbox project, with the objective of removing barriers, alleviating regulatory burden, reducing regulatory uncertainty, and supporting innovation in net-zero technologies or other innovative technologies*".[50] The regulation adds that competent authorities "*shall consider whether to grant derogations or exemptions in national law to the extent allowed by relevant Union law*" while ensuring that "*the net-zero regulatory sandbox plan respects the requirements of Union law and the key objectives and essential requirements of national law*".[51] The possibility of granting regulatory exemptions does not concern the rules

[43] See Article 12(4) of the Interoperable Europe Act: "Participation in the interoperability regulatory sandboxes shall not affect the supervisory and corrective powers of any authorities supervising those sandboxes".
[44] Article 12(5) of the Interoperable Europe Act.
[45] Article 1 of the Net-Zero Industry Act.
[46] Recital 100 of the Net-Zero Industry Act.
[47] Article 3(22) of the Net-Zero Industry Act.
[48] Article 33(1-2) of the Net-Zero Industry Act.
[49] Article 33(3) para. 2 of the Net-Zero Industry Act.
[50] Article 33(4) of the Net-Zero Industry Act.
[51] Article 33(5) of the Net-Zero Industry Act.

contained in the Net-Zero Industry Act itself – which in fact contains few restrictive rules – but any relevant national rules (if it is legally possible). Although the Regulation encourages the granting of legal exemptions, it does not appear to provide a sufficient legal basis on its own, as evidenced by the fact that it specifies that derogations and exemptions are granted to the extent allowed by relevant EU law.

The competent authorities must also monitor risks to health, safety or the environment and suspend the testing process if a significant risk is identified, until it has been mitigated.[52] Participants in the sandbox remain liable for any material harm caused to third-party as a result of the sandbox testing.[53]

- **Cyber resilience regulatory sandboxes**

The *Cyber Resilience Act*, adopted on 23 October 2024, aims to establish cybersecurity requirements for products with digital elements, covering their design, production, use, and market surveillance.[54] It enables Member States to establish cyber resilience regulatory sandboxes, to be operated by market surveillance authorities.[55] Such sandboxes should foster innovation and competitiveness for businesses, contribute to improve legal certainty for all actors that fall within the scope of this Regulation, and facilitate and accelerate access to the Union market for products with digital elements.[56] They shall "*provide for controlled testing environments for innovative products with digital elements to facilitate their development, design, validation and testing for the purpose of complying with this Regulation for a limited period of time before the placing on the market*".[57] These regulatory sandboxes shall not affect the supervisory and corrective powers of the competent authorities. The text does not mention any possibility of legal exemption or any other form of regulatory flexibility.

- **Regulatory sandboxes for medicinal products**

A Proposal for a Regulation on the authorisation and supervision of medicinal products for human use was published in 2023 by the European Commission and is currently being negotiated between the Council and the European Parliament. The aim of this text is to amend EU pharmaceutical legislation in order to improve access to medicines, including by making the environment for research, development and production of medicines in the EU more attractive, innovation-friendly and competitive.[58]

[52] See details in Article 33(5) of the Net-Zero Industry Act.
[53] Article 33(6) of the Net-Zero Industry Act.
[54] Article 1 of the Cyber Resilience Act.
[55] Article 33(2) of the Cyber Resilience Act.
[56] Recital 97 of the Cyber Resilience Act.
[57] Article 33(2) of the Cyber Resilience Act.
[58] See the "Reasons for and objectives of the proposal" in the Explanatory Memorandum of the Proposed regulation on medicinal products.

The proposal provides for the establishment of regulatory sandboxes which enable "*the testing of innovative technologies (..) especially in the context of digitalisation or the use of artificial intelligence and machine learning in the life cycle of medicinal products from drug discovery, development to the administration of medicinal products*".[59] They would be created specifically when medicinal products cannot be developed "*in compliance with the requirements applicable to medicinal products due to scientific or regulatory challenges arising from characteristics or methods related to the product*".[60] These regulatory sandboxes offer a controlled environment where targeted derogations from certain EU legislation – namely this Regulation on medicinal products, the revised Directive 2001/83/EC on the Community code relating to medicinal products for human use and the Regulation (EC) 1394/2007 on advanced therapy medicinal products – could be granted.

The creation of a sandbox begins with a recommendation from the European Medicines Agency, in which are identified the types of medicines that could benefit from this flexibility because of challenges relating to their characteristics or their development methods.[61] The Agency then establishes a sandbox plan tailored to these needs and the European Commission, by means of implementing acts, decides on the set up of a regulatory sandbox.[62] The implementing acts shall define the modalities and conditions for the operation of regulatory sandboxes, including eligibility criteria, as well as the procedures for application, selection, participation, and exit, along with the rights and obligations of participants.[63] Once created, a regulatory sandbox is supervised by the national competent authorities, who are responsible for overseeing compliance with the requirements of the regulation.[64]

This potential future category of regulatory sandbox differs from interoperability or cyber resilience regulatory sandboxes in that it allows derogations from some EU legislative acts. The aim of this sandbox is not so much to help participants understand the law through a close dialogue between regulators and regulated entities, but to allow them to develop medicinal products that cannot be developed under current legislation.[65] It also differs from the net-zero regulatory sandbox in that, in this case, the European legislation from which the regulatory sandbox allows for exemption is clearly identified.

Lastly, this regulatory sandbox is intended to promote "*regulatory learning*". A Recital in the proposed Regulation adds in this regard: "*the learning stemming from a regulatory sandbox*

[59] Recital 133 of the Proposed regulation on medicinal products.
[60] Article 113(1)(a) of the Proposed regulation on medicinal products. The text defines regulatory sandbox as "a regulatory framework during which it is possible to develop, validate and test in a controlled environment innovative or adapted regulatory solutions that facilitate the development and authorisation of innovative products which are likely to fall in the scope of this Regulation, pursuant to a specific plan and for a limited time under regulatory supervision." (Article 2(12) of the Proposed regulation on medicinal products).
[61] Article 113(1)(4) of the Proposed regulation on medicinal products.
[62] Article 113(5-7) of the Proposed regulation on medicinal products.
[63] Article 115(3) of the Proposed regulation on medicinal products.
[64] Article 113(2) al. 2 of the Proposed regulation on medicinal products.
[65] Article 113(1)(a) of the Proposed regulation on medicinal products.

should inform future changes to the legal framework to fully integrate the particular innovative aspects into the medicinal product regulation. Where appropriate, adapted frameworks may be developed by the Commission on the basis of the results of a regulatory sandbox".[66]

- The **Pan-European blockchain regulatory sandbox** for innovative use cases involving Distributed Ledger Technologies (DLT)

This last initiative is worth mentioning, although its status as a regulatory sandbox is questionable. It is an initiative of the European Commission, funded through the Digital Europe Programme which provides funding for projects in areas such as AI, supercomputing, and the use of digital technologies across the economy and society. This sandbox aims to "*establish a pan-European framework for regulatory dialogue*" and "*brings together national and EU regulators and authorities with providers of innovative blockchain/DLT applications in both the private and public sector to identify possible issues and solutions from a legal & regulatory perspective in a safe and confidential environment*"[67]. Managed by a consortium led by the law firm Bird & Bird, it is to be operational from 2023 to 2026, with 20 projects selected each year.[68] A first *Best Practices report* was published in 2023.[69]

The facilitated dialogue is intended to bring together participants who are developing DLT projects and various national and European regulators who have competence in related regulatory areas.[70] The sandbox does not focus on one regulation in particular; the idea is to encourage dialogue around all the possible regulatory areas affected by the selected DLT projects.[71] The consortium managing the sandbox, which is not a regulatory authority, has no power other than that of facilitating this dialogue.[72] The aim is to help companies and innovators understand the law and how to comply with it, and possibly to help regulators familiarise themselves with new disruptive technologies.

---

[66] Recital 135 of the Proposed regulation on medicinal products.
[67] European Commission, Bird & Bird, OXYGY, *European Blockchain Sandbox: Best Practices Report. 1st cohort, part A.*, LU, Publications Office, 2024, p. 6, online https://data.europa.eu/doi/10.2759/841857 (retrieved on 5 November 2024).
[68] The selection criteria are available here: Anonymous, "EU Regulatory Sandbox - Selection criteria for website", no date, online https://ec.europa.eu/digital-building-blocks/sites/display/EBSISANDCOLLAB/Key+documents?preview=/634979024/710119244/Selection%20criteria%20-%20Version%202.0%20(23.01.2024).pdf (retrieved on 5 November 2024).
[69] European Commission, Bird & Bird, OXYGY, *European blockchain sandbox*, *op. cit.* note 68 'Distributed Ledger Technology' is defined in the report as a technology that enables the operation and use of distributed ledgers, and 'Distributed Ledger' as an information repository that keeps records of transactions and that is shared across, and synchronised between, a set of DLT network nodes using a consensus mechanism. Blockchain is a type of DLT.
[70] *Ibid.* p. 8.
[71] *Ibid.* p. 10.
[72] *Ibid.* p. 14.

The fact that the sandbox is not run by a regulator (and *a fortiori* that it does not involve the granting of legal exemptions) is remarkable given that this is a key feature of regulatory sandboxes, raising doubts as to whether it actually qualifies as such. Nor does it provide any technical infrastructure. The 2023 *Best Practices Report* stressed in this sense that this sandbox is essentially a "*confidential and informal dialogue*" but that it should also serve as a bridge to other national regulatory sandboxes, such as those to be created under the AI Act.[73]

[73] *Ibid*. p. 15.

3. Regulatory sandboxes in the AI Act

This third section focuses on regulatory sandboxes under the AI Act. It first presents the fundamental principles of the AI Act (3.1.), then describes how this regulation will be supervised and implemented at national level (3.2.), and finally analyses the legal regime of AI regulatory sandboxes as defined in the AI Act (3.3.).

3.1. Key principles of the AI Act

The AI Act is both general in its scope of application, since in principle it covers all types of AI systems, and **risk-based**, since the level of requirements and obligations imposed on the AI system depends on the risk the system poses to health, safety and fundamental rights. AI systems which present a risk deemed too substantial are banned, those that present a high risk are subject to a series of legal requirements, and those with a low risk are subject to minimal or no requirements.

Prohibited AI practices include uses such as real-time biometric identification, social scoring or emotional recognition at work or in an educational institution.[74] **High-risk AI systems** are of two types. First, different AI systems are listed in Annex III of the AI Act. Without being exhaustive, it comprises AI systems used to recruit new employees or assess their performance once they have been hired, to select and rate insurers for life and health insurance, to assess the eligibility of citizens for public assistance benefits, to assess the risk of recidivism or to assess the risk of illegal immigration. Second, AI systems that are used as a safety component of a product (or are themselves a product) covered by the Union harmonisation legislation listed in Annex I, and that require third-party conformity assessment pursuant to this legislation are also classified as high-risk. This includes the use of AI in products such as toys, lifts or medical devices.[75] Other types of AI systems that present a **lower risk**, such as chatbots or systems that generate content such as images or audio, are subject to limited obligations, including the obligation to inform the person with whom the AI system interacts that the content is produced by an AI system.[76]

Most of the requirements contained in the AI Act relate to high-risk AI systems and fall on the providers of such systems. These include establishing a risk management system, drafting technical documentation which demonstrates compliance with the AI Act, maintaining a data governance framework (which notably aims to control the quality and representativeness of the data used to feed the AI model), ensuring that a human oversees the AI system and its outputs, etc.[77] As the AI Act's requirements largely concern high-risk AI

[74] See Article 5 of the AI Act.
[75] The classification rules for high-risk AI systems are contained in Article 6 of the AI Act which refers to the Annexes of the regulation.
[76] See Article 50 of the AI Act. This report does not cover the specific rules contained in Chapter V of the AI Act which concern general-purpose AI models (such as GPT developed by OpenAI or GEMINI by Google).
[77] See Chapter III of the AI Act.

systems, participation in AI regulatory sandboxes should be of particular interest to those types of AI systems.

The AI Act aligns with the New Legislative Framework (NLF), which guides EU legislation on product safety.[78] In this sense, the AI Act requires providers of high-risk AI systems a **conformity assessment** before placing their systems on the market or putting it into service.[79] In some limited cases, the conformity assessment will have to be carried out by a third-party body, referred to in the AI Act as a *notified body*. In most cases, however, this conformity assessment will take the form of a self-assessment: providers shall evaluate themselves whether their systems comply with the requirements of the AI Act.[80] Once this self-assessment is successfully completed, the supplier must affix a CE mark to the system and issue an EU declaration of conformity.[81] In accordance with the NLF approach, providers will have the option of following harmonised standards as part of their conformity assessment, which will lead to a presumption of conformity with the AI Act requirements.[82]

This logic of self-assessment differs from that observed in highly regulated sectors such as pharmaceuticals or financial services, where economic operators must receive a licence to operate and/or obtain *ex ante* authorisation before placing a product on the market. This is particularly relevant in relation to regulatory sandboxes, as in both of these regulatory sectors a regulatory sandbox allows the need for such prior approval to be avoided.[83] In the case of the AI Act, the situation is different and more akin to data protection regulation, given the limited role of regulators at the *ex ante* stage.

---

[78] Recital 9 of the AI Act.

[79] For an explanation of the NLF approach in the context of the AI Act: M. Veale, F.Z. Borgesius, "Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach", *Computer Law Review International*, 2021, vol. 22, no. 4, p. 97.

[80] The subtleties of conformity assessment are contained in Article 43 of the AI Act, a key principle being that conformity assessment for all the high-risk AI systems listed in Annex III can be carried out through the internal control procedure (with the exception of biometric systems described in point 1, which are subject to slightly more demanding rules).

[81] Article 16(h) and 48 of the AI Act. CE marking is a cornerstone of the EU's harmonisation legislation. Affixing the CE mark to a product indicates that it complies with all applicable legal requirements under EU law, allowing the product to circulate freely within the EU.

[82] Harmonised standards are technical standards which are adopted by European standardisation organisations on the basis of a request made by the Commission for the application of Union harmonisation legislation. They are currently being negotiated. On the role of harmonised standards in the AI Act: J. Soler Garrido et al., *Analysis of the preliminary AI standardisation work plan in support of the AI Act*, Luxembourg, Publications Office of the European Union, JRC technical report no. 31518 EN, 2023, online https://publications.jrc.ec.europa.eu/repository/handle/JRC132833 (retrieved on 7 November 2024), DOI:10.2760/5847; M. Gornet, W. Maxwell, "The European approach to regulating AI through technical standards", *Internet Policy Review*, 2024, vol. 13, no. 3.

[83] On the distinction between regulatory sandboxes in licensing and in non-licensing regimes, see T. Moraes, "Regulatory sandboxes as tools for ethical and responsible innovation of artificial intelligence and their synergies with responsive regulation", *The Quest for AI Sovereignty, Transparency and Accountability*, FGV - Direito Rio, 2024, online https://vlex.com.br/vid/regulatory-sandboxes-as-tools-1034960669 (retrieved on 26 August 2024).

3.2. The supervisory framework of the AI Act

To understand which authorities will operate AI regulatory sandboxes, it is first necessary to detail the broader supervisory framework of the AI Act. Apart from general-purpose AI models for which the European Commission is competent,[84] and for AI systems put into service or used by EU institutions and agencies for which the European Data Protection Supervisor (EDPS) is competent,[85] the supervision and enforcement of the regulation will be carried out at national level.

The AI Act speaks of **national competent authorities** which refers either to a **notifying authority** or a **market surveillance authority**.[86] Notifying authorities are responsible for designating and monitoring the bodies that carry out third-party conformity assessment (notified bodies).[87] Market surveillance authorities are responsible for the post-market surveillance of AI systems covered by the AI Act,[88] in accordance with the regime set out in the Regulation 2019/1020 on market surveillance and compliance of products (Market Surveillance Regulation).[89] They must monitor the risks to health, safety and fundamental rights posed by AI systems once they have been placed on the market or put into service, and have various powers, including access to the source code of a high-risk AI system and carrying out testing procedures.[90] If an AI system is deemed to pose a risk, the market surveillance authority will examine whether the AI system complies with the AI Act and, in case of non-compliance, will take all appropriate measures (including, if necessary, withdrawal from the market or prohibition of the AI system).[91]

Unlike other pieces of legislation such as the GDPR, the AI Act does not require a unique independent authority to be set up, and leaves Member States considerable leeway in organising supervision. The selection of notifying and market surveillance authorities is left to the discretion of the Member States. They may designate an existing public body or create a new one, with a minimum of one authority for each role, although more than one authority may be designated.[92] The European Data Protection Board (EDPB) published in July 2024 a statement in favour of designating **data protection authorities** as the main market surveillance authorities.[93] However not all countries will follow this path. Spain has created a new authority – the *Agencia Española de Supervisión de la Inteligencia Artificial* –

[84] Regarding the supervision and enforcement of general-purposes AI models, see Chapter V of the AI Act.
[85] Article 3(48), 70(9) and 74(9) of the AI Act.
[86] Article 3(48) of the AI Act.
[87] Articles 3(19) and 28 of the AI Act.
[88] Articles 3(26) and 74 of the AI Act.
[89] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 OJ L 169/1.
[90] Article 74(13) of the AI Act.
[91] For exact details, see Article 79 of the AI Act.
[92] Article 70 of the AI Act.
[93] European Data Protection Board, 'Statement 3/2024 on data protection authorities' role in the Artificial Intelligence Act framework' (2024), <https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf> accessed 13 November 2024.

specifically dedicated to the supervision of the AI Act.[94] Italy intends to designate existing authorities – the *Agenzia per l'Italia Digitale* and the *Agenzia per la cybersicurezza nazionale* – as the main competent authorities.[95] In the Netherlands, two authorities – the data protection authority and the Dutch Authority for Digital Infrastructure – have been asked by the Minister for Economic Affairs and Climate Policy and the Minister for Digitisation to investigate how the supervision of the AI Act could be organised.[96] In a document published in May 2024, they suggest that the Dutch data protection authority should serve as the Market Surveillance Authority for most high-risk AI areas listed in Annex III, working in collaboration with domain-specific supervisors.[97] For instance, the Dutch Labour Authority would be associated to the supervision of high-risk AI systems used in the field of employment, workers' management and access to self-employment.[98] Member States must designate their notifying and market surveillance authorities by 2 August 2025.[99]

However, for certain AI systems, the AI Act reduces Member States' flexibility by indicating which authorities will have to serve as market surveillance authorities. First, for all high-risk AI systems covered by the legislation listed in Annex I.A (such as toys, lifts, etc.), the existing market surveillance authorities should also play the same role for the purposes of the AI Act.[100] Second, specific authorities are explicitly designated by the AI Act to oversee certain high-risk systems listed in Annex III: for high-risk systems used by financial institutions regulated by Union financial services law (e.g. credit scoring systems used by banks), the market surveillance authority is the relevant national authority responsible for the financial supervision of those institutions (e.g. financial markets authority, national bank);[101] similarly, for high-risk systems used for law enforcement purposes, border management and justice and democracy, the market surveillance authority must be the data protection authority.[102]

In addition to that, the AI Act also gives to the **authorities protecting fundamental rights** (which must be designated by the Member States) the power to verify whether AI systems

---

[94] "Agencia Española de Supervisión de la Inteligencia Artificial | España Digital 2026", no date, online https://espanadigital.gob.es/lineas-de-actuacion/agencia-espanola-de-supervision-de-la-inteligencia-artificial (retrieved on 7 December 2024).

[95] R. Saverino, "Regulatory (Mis)Alignment: Between Data Protection and AI Authorities", *unpublished paper*, p. 9.

[96] See Dutch Data Protection Authority, Dutch Authority for Digital Infrastructure, *2nd (interim) advice on the Dutch supervisory structure for the AI Act*, 16 May 2024, online https://www.autoriteitpersoonsgegevens.nl/en/documents/second-interim-advice-on-supervisory-structure-ai-act (retrieved on 6 December 2024).

[97] *Ibid*. p. 4

[98] *Ibid*.

[99] Article 70(2) of the AI Act.

[100] Article 74(3) of the AI Act. The second paragraph of the same provision adds that in appropriate circumstances "Member States may designate another relevant authority to act as a market surveillance authority, provided they ensure coordination with the relevant sectoral market surveillance authorities responsible for the enforcement of the Union harmonisation legislation listed in Annex I".

[101] For exact details, see Article 74(6) and (7) of the AI Act.

[102] For exact details, see Article 74(8) of the AI Act.

covered by this regulation violate fundamental rights by requiring access to certain documents and even by asking a market surveillance authority to organise the testing of a high-risk AI system through technical means.[103] The following table summarises the key he key elements of the supervisory framework:

<table>
<tr><th colspan="4">SUPERVISION OF THE AI ACT AT THE NATIONAL LEVEL</th></tr>
<tr><td rowspan="5">National competent authorities
(Articles 3(48) and 70 of the AI Act)</td><td>Notifying authorities
(Articles 3(19) and 28 of the AI Act)</td><td colspan="2">To be designated at the discretion of the Member States</td><td>Responsible for designating and monitoring notified bodies</td></tr>
<tr><td rowspan="4">Market surveillance authorities
(Articles 3(26) and 74 of the AI Act)</td><td colspan="2">To be designated at the discretion of the Member States, except for certain high-risk AI systems where the AI Act directly designates the authority:</td><td rowspan="4">Responsible for the post-market surveillance of AI systems covered by the AI Act</td></tr>
<tr><td>National authority responsible for the financial supervision of those institutions
e.g. financial markets authority, national bank</td><td>High-risk systems used by financial institutions regulated by Union financial services law
e.g. credit scoring systems</td></tr>
<tr><td>Data protection authority</td><td>High-risk systems used for law enforcement purposes, border management and justice and democracy (+ biometrics in these areas)
e.g. polygraphs</td></tr>
<tr><td>Existing market surveillance authorities under other NLF legislation</td><td>High-risk AI systems covered by the legislation listed in Annex I.A
e.g. toys, lifts</td></tr>
<tr><td></td><td>Authorities protecting fundamental rights
(Articles 77 of the AI Act)</td><td colspan="2">To be designated at the discretion of the Member States</td><td>Has the power to examine whether AI systems violate fundamental rights</td></tr>
</table>

[103] Article 77 of the AI Act. Each Member State was expected to notify the European Commission of the authorities they had designated as 'Authorities protecting fundamental rights' by 2 November 2024 (Article 77(2) of the AI Act).

3.3. AI regulatory sandboxes

This section analyses the provisions relating to AI regulatory sandboxes, contained in Chapter VI of the AI Act '*Measures in support of innovation*'. At this stage, several uncertainties remain as to their interpretation.[104] The European Commission will adopt implementing acts to further specify these provisions.[105]

3.3.1. Definition, objectives and actors

AI regulatory sandboxes are defined as "*a concrete and controlled framework set up by a competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real world conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision*".[106]

This definition aligns with the traditional characteristics of regulatory sandboxes: supervision of the sandbox by an authority, limited duration, innovative nature of the product required, existence of a sandbox plan. All these aspects are further detailed in article 57 and 58 of the AI Act.

The establishment of sandboxes by Member States must pursue the following objectives:[107]

(a) improve legal certainty and thus regulatory compliance;
(b) support the sharing of best practices;
(c) foster innovation and competitiveness;

---

[104] Several works have already been published on the issue of regulatory sandboxes in the AI Act (often discussing the Commission's initial proposal or the versions amended by the European Parliament or the Council). See *inter alia*: S. Ranchordás, "Experimental Regulations for AI: Sandboxes for Morals and Mores", *Morals & Machines*, 2021, vol. 1, no. 1, p. 86; J. Truby et al., "A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications", *European Journal of Risk Regulation*, 2022, vol. 13, no. 2, p. 270; T. Buocz, S. Pfotenhauer, I. Eisenberger, "Regulatory sandboxes in the AI Act: reconciling innovation and safety?", *op. cit.* note 19, p. 357; E. Gromova, E. Stamhuis, "Real-Life Experimentation with Artificial Intelligence", *op. cit.* note 4; H. Burden, S. Stenberg, *Sustainable AI and Disruptive Policy – AI Regulatory Sandboxes*, RISE Research Institutes of Sweden AB, 2023, online https://diva-portal.org/smash/record.jsf?pid=diva2%3A1835556&dswid=-7488 (retrieved on 12 December 2024); K. Yordanova, N. Bertels, "Regulating AI: Challenges and the Way Forward Through Regulatory Sandboxes", *in* H. Sousa Antunes et al. (eds.), *Multidisciplinary Perspectives on Artificial Intelligence and the Law*, Springer, 2024, vol. 58, p. 441; T. Moraes, "Regulatory sandboxes as tools for ethical and responsible innovation of artificial intelligence and their synergies with responsive regulation", *op. cit.* note 84; A. Papageorgiou, *Addressing the Challenges arising from the Implementation of Regulatory Sandboxes under the AI Act*, Master Thesis, KU Leuven, 2024, online https://repository.teneo.libis.be/delivery/DeliveryManagerServlet?dps_pid=IE21041849& (retrieved on 9 December 2024).

[105] See Articles 58 and 60(1) para. 2 of the AI Act.

[106] Article 3(55) of the AI Act. All the provisions relating to AI regulatory sandboxes mention 'providers or prospective providers', since the sandbox is open to both. For simplicity, the following pages will only refer to 'providers'.

[107] Article 57(9) of the AI Act.

(d) contribute to evidence-based regulatory learning;
(e) facilitate and accelerate access to the Union market for AI systems (in particular for SMEs).

The AI Act states that Member States must ensure that their **national competent authority** set up at least one national regulatory sandbox, to be operational by 2 August 2026.[108] As explained, the notion of national competent authority refers either to the market surveillance authority or to the notifying authority.[109] The role of notifying authorities is to designate and control notified bodies which performs third-party conformity assessment, while market surveillance authorities are responsible for monitoring AI systems that are placed on the market or put into service by providers and used by deployers. Since operating AI regulatory sandboxes consists of interacting with providers, particularly by providing them legal guidance, it seems more logical for market surveillance authorities to assume this role.

Additional AI regulatory sandboxes may also be established at regional or local levels or jointly with the competent authorities of other Member States.[110]

Where an AI system being tested involves the processing of personal data, data protection authorities must also be associated to the supervision of the sandbox.[111] The same applies to other national authorities where the AI system being tested in the sandbox falls within their supervisory remit.[112] However, as has been seen, it is entirely possible for the data protection authority to be the market surveillance authority under the AI Act, and therefore responsible for operating an AI regulatory sandbox, regardless of whether personal data is processed in that sandbox.

In the Netherlands, the document already mentioned, published by the Dutch Authority for Digital Infrastructure and the Dutch data protection authority, recommends that these two authorities coordinate sandbox activities.[113] The document suggests that: "*For each test situation, there will then be a competent authority to lead the specific project. This ensures that the competent authority that may encounter the AI system and its provider later in its supervision is also competent to take decisions in the context of the sandbox*".[114] The document also recommends that all potentially competent supervisory authorities should be asked by default about their participation in a sandbox project.[115]

---

[108] Article 57(1) of the AI Act.
[109] Articles 3(48) and 70 of the AI Act.
[110] Articles 57(1) and (2) of the AI Act.
[111] Article 57(10) of the AI Act.
[112] Article 57(10) of the AI Act.
[113] Dutch Data Protection Authority, Dutch Authority for Digital Infrastructure, *2nd (interim) advice on the Dutch supervisory structure for the AI Act*, *op. cit.* note 97, p. 12.
[114] *Ibid.* p. 13.
[115] *Ibid.* p. 13.

The EDPS may also establish and operate an AI regulatory sandbox for EU institutions, bodies, offices and agencies.[116]

3.3.2. Sandbox process

The regulatory sandbox must be open to any provider of an AI system who fulfils eligibility and selection criteria.[117] It can be assumed that providers of high-risk AI systems, in particular, are targeted, given that one of the main aims of AI regulatory sandboxes is to improve regulatory compliance and that this category of AI system is primarily subject to the obligations outlined in the AI Act. This view was embraced in Spain, where an AI regulatory sandbox pilot was launched in 2022. The royal decree adopted for this purpose states that regulatory sandboxes were open to high-risk AI systems.[118]

The European Commission will further define the selection criteria for participating in the sandbox and the whole process of testing in its implementing acts.[119]

- **Selection**

The selection criteria shall be transparent and fair, and national competent authorities must inform applicants of their decision within three months of the application.[120] Access to the AI regulatory sandboxes is in principle free of charge for small and medium enterprises (SMEs).[121] Procedures, processes and administrative requirements for application, selection, participation and exiting the AI regulatory sandbox must be simple, easily intelligible, and clearly communicated in order to facilitate the participation of SMEs, including start-ups, with limited legal and administrative capacities. This also aims to avoid fragmentation between Member States. Participation in an AI regulatory sandbox set up by a Member State or by the EDPS is mutually and uniformly recognised and produces the same legal effects throughout the Union.[122]

- **Sandbox plan and testing**

The competent authority and the provider of an AI system must agree on a specific sandbox plan which describes the objectives, conditions, timeframe, methodology and requirements for the activities carried out within the regulatory sandbox.[123]

Once a sandbox plan has been agreed, the testing starts. During the testing, the competent authority provides "*guidance, supervision and support within the sandbox with a view to identifying risks, in particular to health, safety and fundamental rights, testing, mitigation*

[116] Article 57(3) of the AI Act.
[117] Article 58(2)(a) of the AI Act.
[118] As well as to general-purpose AI models, which are not discussed in this report. See Part 2 of the report, 'Spain', p. 52.
[119] Article 58(1) of the AI Act.
[120] Article 58(2)(a) of the AI Act.
[121] Article 58(2)(d) of the AI Act.
[122] Article 58(2)(g) of the AI Act.
[123] Article 3(54) and Article 57(5) of the AI Act.

measures, and their effectiveness in relation to the obligations and requirements of the AI Act and, where relevant, other Union and Member States legislation supervised within the sandbox".[124] It provides guidance to providers on regulatory expectations, fulfilling the requirements and obligations of the AI Act, and supporting compliance with conformity assessment obligations.[125]

Any significant risks to health, safety and fundamental rights identified during the testing phase must result in an adequate mitigation. National competent authorities are authorised to temporarily or permanently suspend the testing process and participation in the sandbox if effective mitigation measures cannot be implemented.[126] They must inform the AI Office of such decision.[127]

- **Written proof and exit report**

At the conclusion of the testing phase, and upon request of the provider of the AI system, the competent authority issues a written proof of the activities successfully completed in the sandbox. The competent authority prepares an exit report detailing the activities carried out, along with the related results and learning outcomes. Providers may use these documents – the exit report and the written proof – to demonstrate compliance with the AI Act during the conformity assessment process or other market surveillance activities. The exit reports and written proofs issued by the national competent authority must be positively taken into account by market surveillance authorities and notified bodies, with the aim of reasonably accelerating conformity assessment procedures.[128] In other words, while a successful **participation to a sandbox** will be a positive element in assessing conformity of the AI system with the AI Act, it **does not automatically lead to full compliance**.

- **Annual reports**

National competent authorities must submit to the AI Office and to the European AI Board, annual reports, starting one year after the establishment of the AI regulatory sandbox.[129] The reports will detail the progress and outcomes of sandbox implementation, covering best practices, incidents, lessons learned, and recommendations for their setup, as well as potential revisions to this Regulation and other relevant EU laws (in line with the regulatory learning objective).[130] These reports will be made public either in full or in summary form only. The fact that abstracts may be published instead of the full reports risks undermining one of the interests of the sandbox, which is precisely to enable non-participants to learn from the sandbox process.

[124] Article 57(6) of the AI Act.
[125] Articles 57(6-7) and 58(2)(e) of the AI Act.
[126] Article 57(11) of the AI Act.
[127] *Ibid*.
[128] Article 57(7) para. 2 of the AI Act.
[129] Article 57(16) of the AI Act.
[130] *Ibid*.

3.3.3. Limitations on fine imposition and liability regime

As previously discussed, regulatory sandboxes typically involve a certain level of regulatory flexibility, with the overseeing authority being accommodating to participants, in particular by granting legal exemptions. However, some regulatory sandboxes, such as the EU interoperability regulatory sandbox or several data protection regulatory sandboxes, do not allow exemptions to be granted.

As regards the AI Act, the possibility of exempting participants from certain normally applicable rules is not explicitly provided for either. However, participants are granted a form of regulatory flexibility through limited sanctions: as long as participants respect the sandbox plan and the terms and conditions for their participation and follow in good faith the guidance given by the national competent authority, **no administrative fines shall be imposed by the competent authority**.[131]

While this measure is intended to allow providers to develop their products without fear of penalties, the question arises as to its effect in practice. Indeed, **the requirements and obligations set out in the AI Act** (along with the fines in case of non-compliance) **only apply *after the AI systems have been placed on the market or put into service***.[132] However, participation in a sandbox takes place precisely before AI systems reach this stage.[133]

Importantly, Article 57(12) also states that if other authorities responsible for European or national legislation are involved in the supervision on an AI system in the sandbox and provide advice on compliance, no administrative fine shall be imposed for that legislation either. The rationale of this provision is that if a participant in an AI regulatory sandbox complies with the sandbox plan but infringes another EU or national law, this participant should not be penalised. This includes data protection: if personal data is processed in the sandbox in breach of the GDPR but the participant complies with the sandbox plan and follows in good faith the guidance provided, the data protection authority should not fine the participant.

The legality of this provision may be questionable in some cases, as it is doubtful that the AI Act has the authority to limit the supervisory powers of national authorities exercised under

---

[131] Article 57(12) of the AI Act. See also T. Buocz, S. Pfotenhauer, I. Eisenberger, "Regulatory sandboxes in the AI Act: reconciling innovation and safety?", *op. cit.* note 19, pp. 368-369.

[132] Article 2(8) of the AI Act states that "This Regulation does not apply to any research, testing or development activity regarding AI systems or AI models *prior to their being placed on the market or put into service*. Such activities shall be conducted in accordance with applicable Union law. Testing in real world conditions shall not be covered by that exclusion". The issue of testing in real world conditions is the subject of specific provisions which are discussed below. This view is shared by Burden and Stenberg: H. Burden, S. Stenberg, *Sustainable AI and Disruptive Policy – AI Regulatory Sandboxes*, *op. cit.* note 105, p. 13.

[133] "AI regulatory sandboxes established under paragraph 1 shall provide for a controlled environment that fosters innovation and facilitates the development, training, testing and validation of innovative AI systems for a limited time *before their being placed on the market or put into service* pursuant to a specific sandbox plan agreed between the providers or prospective providers and the competent authority." (Article 57(5) of the AI Act).

other national or EU laws. In the case of the GDPR, the AI Act explicitly stipulates that "*this Regulation does not seek to affect the application of existing Union law governing the processing of personal data, including the tasks and powers of the independent supervisory authorities competent to monitor compliance with those instruments*".[134] This provision of the AI Act may conflict with other European or national rules. And one of the particularities of the AI Act is that its scope is extremely broad, since AI systems can be integrated into toys, medical devices, or used by banks, insurance companies, public services, etc. All these areas are governed by various specific rules.

The rule that no administrative fines should be imposed, even those not related to the supervision of the AI Act, should therefore rather be seen as an invitation to regulators who often have certain discretionary powers when deciding to impose a fine. Ultimately, it seems more prudent for Member States to consider the different regulators likely to be involved in a regulatory sandbox and to adopt a national law that would specify the conditions under which they should or should not impose a fine.

With regard to damage that may be caused to a third party during participation in a sandbox, the **provider remains liable** under applicable EU and Member States liability legislation.[135] Although it is common practice not to exempt participants from civil liability in regulatory sandboxes, this provision has been criticised for potentially deterring developers of AI systems from joining an AI regulatory sandbox.[136] An important question is whether compliance with the testing plan will prevent a participant from being deemed to be in breach of duty (and therefore liable under a fault-based liability regime). Compensation schemes, such as insurance, could be implemented to limit the risk to participants while protecting affected individuals from potential harm.[137]

3.3.4. Specific legal regime governing the processing of personal data

The AI Act provides for a specific legal regime for the processing of personal data: in some circumstances, personal data lawfully collected for other purposes may be processed solely for the purposes of developing, training and testing certain AI systems in the sandbox.[138]

---

[134] Recital 10 of the AI Act.

[135] Article 57(12) of the AI Act.

[136] J. Truby et al., "A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications", *op. cit.* note 105, pp. 285-287; T. Buocz, S. Pfotenhauer, I. Eisenberger, "Regulatory sandboxes in the AI Act: reconciling innovation and safety?", *op. cit.* note 19, pp. 384-385. See also E. Gromova, E. Stamhuis, "Real-Life Experimentation with Artificial Intelligence", *op. cit.* note 4, pp. 563-565.

[137] See J. Truby et al., "A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications", *op. cit.* note 105, p. 270; T. Buocz, S. Pfotenhauer, I. Eisenberger, "Regulatory sandboxes in the AI Act: reconciling innovation and safety?", *op. cit.* note 19, p. 357.

[138] Article 59 of the AI Act. There is a similar provision in the Interoperable Europe Act regarding interoperability regulatory sandboxes.

A number of conditions must be met to do this. First, AI systems shall be developed for safeguarding substantial public interest in one or more of the following areas: public safety and public health, protection of the environment, energy sustainability, transport systems and mobility, critical infrastructure and networks, public administration and public services. Second, the data processed are necessary for complying with the requirements for high-risk AI systems where those requirements cannot effectively be fulfilled by processing anonymised, synthetic or other non-personal data. Third, different measures aimed at safeguarding the rights of data subjects must be taken. More details can be found in Article 59 of the AI Act.[139]

3.3.5. Testing in real world conditions

The AI Act also provides for the possibility to test AI systems in real world conditions. This mechanism is distinct from regulatory sandboxes. It is defined as "*the temporary testing of an AI system for its intended purpose in real-world conditions outside a laboratory or otherwise simulated environment, with a view to gathering reliable and robust data and to assessing and verifying the conformity of the AI system with the requirements of this Regulation and it does not qualify as placing the AI system on the market or putting it into service within the meaning of this Regulation provided that all the conditions laid down in Article 57 or 60 are fulfilled*".[140]

When the testing in real world conditions concerns **high-risk AI systems** listed in Annex III of the AI Act, Article 60 and 61 set out specific rules and conditions.[141] These include: establishing a real-world testing plan – defined as "*a document that describes the objectives, methodology, geographical, population and temporal scope, monitoring, organisation and conduct of testing in real-world conditions*"[142] – approved by the market surveillance authority;[143] registering the testing in the EU databases;[144] limiting the testing to the time necessary to achieve its objectives and, in any case, to a maximum of six months, with the possibility of a six-month extension;[145] informing subjects participating in testing in real world conditions about the nature, purpose and conditions of the test, and obtaining

[139] This provision is not supposed to contradict the GDPR which contains strict rules regarding the further processing of personal data. However, as discussed by A. Papageorgiou, the legality of this provision is doubtful as it does not fully comply with Article 23(2) of the GDPR. See A. Papageorgiou, *Addressing the Challenges arising from the Implementation of Regulatory Sandboxes under the AI Act*, *op. cit.* note 105, pp. 19 and following pages.

[140] Article 3(57) of the AI Act. Two elements of this definition are curious. First, the fact that it mentions articles 57 to 59 – which concern AI regulatory sandboxes – whereas testing in real world conditions does not necessarily take place within a regulatory sandbox. Second, the fact that it does not mention Article 61, which directly concerns testing in real world conditions.

[141] Article 60 of the AI Act.

[142] Article 3(53) of the AI Act.

[143] Article 60(4)(a-b) of the AI Act.

[144] See exact details in Article 60(4)(c) of the AI Act.

[145] Article 60(4)(f) of the AI Act.

their consent to participate in it.[146] Throughout the entire process of testing in real world conditions, the market surveillance authority monitors the activities to ensure compliance with the AI Act and may suspend or terminate the testing or require the provider to modify any aspect of it as needed.[147] The provider remain liable for any damage caused during the testing in real world conditions.[148]

This mechanism has significant implications: it allows a high-risk AI system to be tested in real-life settings without being subject to the requirements outlined in Chapter III of the AI Act.[149] According to the definition of testing in real world conditions, the system under testing is not considered to have been placed on the market or put into service, and the AI Act only applies to systems that have reached this stage. Thus, while the AI Act does not explicitly describe it this way, **the mechanism closely resembles a regulatory exemption**. However, an important nuance must be noted: the prohibition of certain AI practices under Article 5 of the AI Act continues to apply during testing in real world conditions.[150]

The exact interaction between regulatory sandboxes and testing in real world conditions is not easy to understand from the wording of the AI Act.[151] The more plausible interpretation is that testing in real world conditions of high-risk AI systems can occur either within an AI regulatory sandbox (as outlined in Articles 57(5), 58(4) and 76(2) of the AI Act) or outside of it. When conducted within an AI regulatory sandbox, Articles 57 to 59 apply, offering benefits such as legal guidance, exemption from administrative fines and the possibility of further processing of personal data. Conversely, testing in real world conditions may also take place independently of AI regulatory sandboxes. In such cases, providers do not have to meet all the requirements imposed by the AI Act, but do not benefit from the services provided by the sandbox. This table summarises this reading of the rules applicable to testing in real world conditions.[152]

PROVISIONS GOVERNING TESTING IN REAL WORLD CONDITION		
	High-risk AI systems	**Non high-risk AI systems**
Inside the regulatory sandbox	Articles 57-61 and 76 of the AI Act	Article 57-59 of the AI Act
Outside the regulatory sandbox	Articles 60-61 and 76 of the AI Act	Unclear, but not of much interest as there are few requirements for non high-risk AI systems under the AI Act

[146] See details in Article 60(4)(i) and 61 of the AI Act. See the other conditions in Article 60 of the AI Act.
[147] See Article 60 and 76 of the AI Act.
[148] Article 60(9) of the AI Act.
[149] This chapter concerns high-risk AI systems.
[150] Article 60(1) of the AI Act.
[151] The European Commission must adopt implementing acts that will hopefully clarify the situation (Article 60(1) para. 2 of the AI Act).
[152] This is an interpretation of the provisions of the AI Act, although they sometimes contradict each other.

Another uncertainty concerns the authority responsible for these two mechanisms. AI regulatory sandboxes must be operated by national competent authorities, whereas testing in real world conditions is overseen by market surveillance authorities. The rationale appears to be that testing in real-world conditions involves greater risk, as it affects real subjects, and therefore requires the oversight of market surveillance authorities. However, as noted, the AI Act defines national competent authorities as either notifying authorities or market surveillance authorities, and it seems more natural for market surveillance authorities to operate sandboxes. If true, this would mean that regulatory sandboxing and real world testing are the responsibility of market surveillance authorities. The table below attempts to make sense of the wording of the AI Act.

AUTHORITIES OPERATING AI REGULATORY SANDBOXES AND TESTING IN REAL WORLD		
National competent authorities (NCAs)	Member States ensure that their national competent authorities establish at least one **AI regulatory sandbox** at national level (Article 57(1) of the AI Act)	*Remark: NCAs are either MSAs or notifying authorities. MSAs seems better suited to this role.*
Market surveillance authorities (MSAs)	Market surveillance authorities shall have competences and powers to ensure that **testing in real world conditions** is in accordance with this Regulation. (Article 60 and 76 of the AI Act)	
Data protection authorities (DPAs)	Data protection authorities must be involved when the AI systems being tested involve the **processing of personal data**. (Article 57(10) of the AI Act)	*Remark: DPAs are also mandatorily MSAs for certain high-risk AI systems (see previous table) and may be designated as such for other high-risk AI systems as well.*
Other national authorities	Any national authority must be associated when the AI systems tested fall within its **supervisory remit**. (Article 57(10) of the AI Act)	

3.3.6. Regulatory sandboxes and other testing environments

The AI Act stipulates that AI regulatory sandboxes must facilitate the involvement of other relevant actors within the AI ecosystem, including **European Digital Innovation Hubs** (EDHIs) and **Testing and Experimentation Facilities** (TEFs).[153] Article 58(3) specifies that participants in the sandbox, in particular SMEs and start-ups, shall be directed where relevant to value-adding services such as those offered by EDIHs and TEFs.

These two instruments, currently funded under the Digital Europe Programme, are designed to offer spaces for testing and experimenting with digital technologies and AI, as well as to "*help SMEs and public administrations to take up AI*".[154] EDIHs act as one-stop shops that

[153] Article 58(2)(f) of the AI Act. See also Article (3) of the AI Act.
[154] European Commission, "Fostering a European Approach to Artificial Intelligence" (Communication) COM (2021) 205 final p. 8.

assist companies and public sector organisations in addressing digital challenges and enhancing their competitiveness.[155] Hundreds of EDIHs operate across the EU. TEFs, on the other hand, are "*specialised large-scale reference sites open to all technology providers across Europe to test and experiment at scale state-of-the art AI solutions*".[156] There are currently four TEFs in operation, deployed across multiple sites in different countries, and active in sectors such as smart cities and communities,[157] agriculture,[158] manufacturing,[159] and healthcare.[160] Additionally, the European Union is developing a Data Strategy – particularly through the creation of European Data Spaces – which aims to "increase the availability of and facilitate access to high-quality data for AI startups and the science and innovation community".[161]

More recently, the European Commission also created AI factories which refer to "*open ecosystems formed around European public supercomputers and bringing together key material and human resources needed for the development of generative AI models and applications*".[162]

The underlying idea is that AI regulatory sandboxes should not only facilitate compliance with the AI Act but also support the development of AI systems by providing access to training, technical expertise, testing facilities, and infrastructure. Since the EU has already invested significant funding in initiatives designed for these purposes, the goal is not to recreate everything from scratch but to establish connections between regulatory sandboxes and these instruments.

[155] See "European Digital Innovation Hubs | Shaping Europe's digital future", no date, online https://digital-strategy.ec.europa.eu/en/activities/edihs (retrieved on 16 December 2024).
[156] Anonymous, "Sectorial AI Testing and Experimentation Facilities under the Digital Europe Programme | Shaping Europe's digital future", 17 May 2023, online https://digital-strategy.ec.europa.eu/en/activities/testing-and-experimentation-facilities (retrieved on 16 December 2024)
[157] See https://citcom.ai/.
[158] See https://www.agrifoodtef.eu/.
[159] See https://ai-matters.eu/.
[160] See https://tefhealth.eu/home. See also "Sectorial AI Testing and Experimentation Facilities under the Digital Europe Programme | Shaping Europe's digital future", 17 May 2023, online https://digital-strategy.ec.europa.eu/en/activities/testing-and-experimentation-facilities (retrieved on 16 December 2024).
[161] European Commission, "Communication on boosting startups and innovation in trustworthy artificial intelligence", COM(2024) 28 final, p. 3. See European Commission, "Staff Working Document on Common European data spaces", SWD(2024) 21 final.
[162] European Commission, "Communication on boosting startups and innovation in trustworthy artificial intelligence", COM(2024) 28 final, p. 4.

4. Key challenges and outstanding issues for the implementation of AI regulatory sandboxes

This last section briefly identifies and discusses four key challenges that will need to be addressed, either by Member States or by the European Commission in its implementing acts, to ensure proper implementation of AI regulatory sandboxes under the AI Act.

- ***Recommendation 1: Clarifying the rules for authorities operating AI regulatory sandboxes***

As shown in the above analysis, the establishment of AI regulatory sandboxes is highly dependent on the broader national supervisory framework of the AI Act, which is itself partly left to the discretion of each Member State. The regulation is slightly unclear about the exact nature of the authorities that can operate regulatory sandboxes and the role of market surveillance authorities. It states that competent authorities (which can also be local or regional) should operate sandboxes, and that market surveillance authorities should monitor testing in real world conditions. However, national competent authority refers to either a market surveillance authority or a notifying authority. Perhaps it would have been simpler to designate market surveillance authorities as solely responsible for operating the sandboxes.

One way to give an effective interpretation to these rules is to consider that an authority designated as a market surveillance authority under the AI Act for certain types of high-risk AI systems can supervise all types of high-risk AI systems in a sandbox, even those for which it has not been designated as the market surveillance authority. Consider the following scenario: a Member State designates multiple existing authorities – such as a ministry, a telecom authority, etc. – as market surveillance authorities for overseeing the different kinds of high-risk AI systems. This Member State also wishes to assign the data protection authority, designated as a market surveillance authority only where required by the AI Act, to operate a general AI regulatory sandbox covering all types of high-risk AI systems. Would the AI Act permit this setup? It seems that it would. However, if testing in real world conditions were conducted for a certain type of high-risk AI system, the market surveillance authority responsible for this type of AI system would need to be involved, as required by Article 60 of the AI Act. This would explain why the AI Act distinguishes between the operation of regulatory sandboxes by national competent authorities and the monitoring of testing in real world conditions by market surveillance authorities.

To resolve these ambiguities, the European Commission could clarify the role and responsibilities of the various authorities involved in the operation of a sandbox in the upcoming implementing acts.

- ***Recommendation 2: Creating a national supervisory framework that meets legal requirements without organisational burden***

In addition to national competent authorities and market surveillance authorities, the AI Act requires the involvement in the sandbox of any other national authority where the AI system being tested falls within their supervisory remit. This complex supervisory framework differs from existing regulatory sandboxes in fields like energy, finance, or data protection, which are managed by the respective energy, financial, or data protection authorities.

Since the AI Act covers very different types of AI systems, various authorities may be competent, even for the same AI system.[163] For example, a credit scoring system used in banking may require oversight by the financial markets authority, the central bank and – if personal data is being processed – the data protection authority. Bringing together representatives from the various competent authorities for each AI system tested in the sandbox could be challenging. Each Member State will therefore have to develop a *modus operandi* that meets the requirements of the AI Act without being too cumbersome from an organisational point of view.

It would therefore be beneficial to designate a central authority to coordinate the various AI regulatory sandboxes that could be established at the local or sectoral level, ensuring uniform procedures and effective communication. This is the approach that the Netherlands and Germany seem to be adopting.[164] The choice of authority depends on each Member State's specific context. However, in many cases, it would be logical **for data protection authorities** to play a key role, particularly for high-risk AI systems listed in Annex III, given their experience with AI regulatory sandboxing and the likely numerous interactions between the AI Act and the GDPR.[165]

- ***Recommendation 3: Introducing regulatory flexibility in other legislation***

The AI regulatory sandboxes under the AI Act contain regulatory flexibility in that, firstly, no administrative fines are imposed to participants in the sandbox (provided that the sandbox rules are properly met) and, secondly, AI systems tested in real world conditions are deemed not to be placed on the market or put into service, implying that most of the requirements of the AI Act do not apply.

The exemption from fines is also intended to apply to legislation beyond the AI Act that may govern AI systems being tested. As previously noted, this is only feasible if the national authority has sufficient discretion or if a law explicitly authorises it. Beyond the issue of

[163] K. Yordanova, N. Bertels, "Regulating AI: Challenges and the Way Forward Through Regulatory Sandboxes", *op. cit.* note 105, p. 450.
[164] For The Netherlands, see Dutch Data Protection Authority, Dutch Authority for Digital Infrastructure, *2nd (interim) advice on the Dutch supervisory structure for the AI Act*, *op. cit.* note 97; For Germany, see below 'Germany: The Regulatory Sandboxes Strategy', p. 42.
[165] On sandboxes set up by data protection authorities, see Part II of the report.

fines, conducting real world testing of AI systems may sometimes require obtaining individual authorisations or derogations from an authority, unrelated to the AI Act. This could be the case, for example, with drones under aviation law or autonomous vehicles under traffic regulations.

Member States should therefore map national laws likely to affect AI systems regulated by the AI Act and identify where regulatory flexibility could be introduced to facilitate proper testing in real world conditions. Where applicable, experimental clauses could be added to laws to allow temporary exemptions from specific rules. Germany is currently discussing a federal regulatory sandbox law that would create a legal framework for the adoption of experimental clauses in specific areas.[166] This could once again serve as an inspiration for other countries.

- ***Recommendation 4: Building bridges between AI regulatory sandboxes and existing testing infrastructures***

The objective of establishing connections between AI regulatory sandboxes and other instruments – such as TEFs, EDIHs, or AI factories – designed to foster AI development may prove challenging. As outlined in Part II of the report, existing AI regulatory sandboxes created by data protection authorities in recent years have not offered technical infrastructure, indicating that data protection authorities do not regard this as part of their mandate.

Authorities may lack awareness of these instruments as well as the expertise to guide providers of AI systems effectively. More importantly, there is a need to avoid conflicts of interest or confusion about the authorities' roles. Although a regulatory sandbox aims to establish a dialogue between regulators and regulated parties, the regulator nonetheless occupies a position of authority by virtue of the supervisory powers it holds. It could appear incongruous for a market surveillance authority to provide technical support to AI providers while simultaneously ensuring they meet legal requirements.

For these reasons, Member States will need to devise procedures that facilitate connections with testing facilities while avoiding conflicts of interest. Assigning this mission to an entity separate from market surveillance authorities could be a more effective approach to providing these services. Overall, **a single one-stop shop could be established, operating through two distinct channels: one focusing on legal aspects and compliance within regulatory sandboxes, and the other guiding participants toward resources and support offered by various instruments within the AI ecosystem to aid in the development of AI systems**.

[166] See below 'Germany: The Regulatory Sandboxes Strategy', p. 42.

Part II – A review of existing AI regulatory sandboxes and related initiatives

This second part provides a mapping of existing AI regulatory sandbox projects launched by EU Member States prior to the adoption of the AI Act.[167] While the focus is on the EU, a few relevant initiatives from non-EU countries are also included. Particular attention is given to initiatives led by data protection authorities, which have been especially proactive in the development of AI regulatory sandboxes.

The mapping is based on publicly available documents and does not aim to be exhaustive. It offers an overview of existing initiatives, as opposed to announced projects in vague terms, such as those outlined in national AI strategies. Descriptions are concise and synthetic, providing essential information by country.

Sector-specific sandboxes – such as those in finance, energy, health, or transport – are excluded from this analysis (even though they may involve AI-driven products). For each country, the description covers the context of the sandbox's creation, the key actors involved in its management, the applicable legal framework, and the funding sources that enabled its establishment and operation.

[167] See also A. Attrey, M. Lesher, C. Lomax, *The role of sandboxes in promoting flexibility and innovation in the digital age*, *op. cit.* note 8; OECD, *Regulatory sandboxes in artificial intelligence*, OECD Digital Economy Papers, no. 356, 2023, online https://www.oecd-ilibrary.org/science-and-technology/regulatory-sandboxes-in-artificial-intelligence_8f80a0e6-en (retrieved on 13 December 2024).

1. Denmark

Context

In autumn 2023, the Danish data protection authority and the Danish Digital Agency set up a regulatory sandbox for AI that aims to promote the development of GDPR-compliant AI solutions. In the future, this regulatory sandbox should also be used as an AI regulatory sandbox within the meaning of the AI Act.

Key Actors

- Datatilsynet, the Danish data protection authority
- The Danish Digital Agency

Legal Framework

The sandbox is organised under the remit of the two Danish Authorities. Participation in the sandbox does **not entail any legal exemption**: participants in the sandbox must comply with the GDPR and all relevant data protection legislation.

Funding

Participation in the sandbox is **free** but **no financial support** is provided to participants. Participants must therefore have sufficient resources to attend meetings and carry out the work required.

Sandbox framework

- **Eligibility criteria**
  - Open to **companies** (established in Denmark) and **public authorities**
  - The project must involve **AI**
  - The project must involve the processing of **personal data** (but in the future the sandbox will be opened to projects that do not involve such processing but fall within the scope of the AI Act)
  - The project must **benefit society**
  - The project must be **innovative**
  - The project must benefit from participation in the sandbox (there are some **regulatory challenges** that have been identified)

- **Testing Process**
  - The normal duration is **6 months**
  - At the end of the sandbox process, the results are communicated so that other interested parties can benefit from them.
  - Completion of the sandbox process does not imply product approval from Datatilsynet and the Digital Agency.

- Various meetings and workshops are organised during the testing process between the participants and the officials responsible for the sandbox.

- **Nature of the support**

The support is mainly legal. **No technical infrastructure is provided** for participants. The sandbox initially focuses on GDPR and Danish data protection laws. Guidance may cover data protection impact assessment, data protection by design solutions and other data protection challenges. However, it is expected that **guidance on the AI Act** will also be provided in the future.

- **Results**

In July 2024, the data protection authority and the Digital Agency have selected 2 participants among 23 applications (coming both from companies and public authorities). Both projects are AI assistants, one developed by an insurance company, the other by a public-private partnership including municipalities.

References

- "To AI-projekter udvalgt til første runde af den regulatoriske sandkasse", https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/jul/to-ai-projekter-udvalgt-til-foerste-runde-af-den-regulatoriske-sandkasse, 8 July 2024.
- "To AI-projekter udvalgt til første runde af den regulatoriske sandkasse", https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/regulatorisk-sandkasse.
- "Ny regulatorisk sandkasse for AI", https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2024/mar/ny-regulatorisk-sandkasse-for-ai, 5 March 2024.

2. France

3.1. The CNIL's sandbox

Context

In 2021, the *Commission Nationale de l'Informatique et des Libertés* (CNIL) – the French data protection authority – has created a 'sandbox' which is defined as a "*mechanism designed for actors initiating innovative projects*" and aimed at bringing "*CNIL's support and expertise on emerging legal and technical issues*" (CNIL, 2023b). The focus is on the compliance with data protection legislation, in particular the GDPR.

The CNIL precises that it is not a *regulatory* sandbox but just a sandbox since "***it does not allow the removal of legal constraints**, even temporarily, because personal data law does not allow it*" (CNIL, 2023a). However, other countries have set up similar sandboxes which do not allow legal exemptions either, but are nevertheless referred to as 'regulatory' sandboxes.

In 2021, the CNIL opened a first sandbox on health, and in 2022 on education (Edtech). On 28 July 2023, the CNIL launched a call for projects on **AI in public services**.

Key actor

- The French data protection authority (**CNIL**)

Legal framework

The sandbox is implemented under the remit of the CNIL as part of its innovation and foresight activities. **Participation in the sandbox does not exempt projects from GDPR compliance**. Instead, it assists participants in navigating and implementing GDPR requirements effectively.

Funding

The CNIL offers guidance for **free** but the selected organisations must ensure they have enough resources to participate in a useful way to the sandbox.

Sandbox Framework

- **Eligibility criteria:**
  - Projects related to the use of AI in public services.
  - Open to public bodies and private bodies "*provided that the project is carried out with one or more public actors*" or that "*the project is specifically intended to fulfil a need identified by several public actors*".
  - Projects that are under development (and therefore not already deployed).

A pre-selection is made by a committee composed of external personalities and members of the CNIL. The president of the CNIL then selects four winning projects.

- **Testing Process:**

The sandbox lasts several months and is divided in three phases: 1) the 'support phase' (6 months) which consists in identifying the issues that must be addressed. Workshops, trainings and other types of exchanges may be organised; 2) the 'implementation phase' where the participating organisations implement the recommendation made by the CNIL; 3) the 'phase of return to the ecosystem' where the CNIL summarises the work and recommendations made on the different selected projects.

- **Sectors concerned**

Use of AI in public services (2023). Two sandboxes had been launched before in the field of health (2021) and education (2022), but they were not specifically dedicated to AI.

- **Nature of the support**

The support is mainly **legal**. **No technical infrastructure is provided** for participants.

- **Results**

The call is now closed and the procedure is ongoing. The CNIL states that "*it has received more than twenty applications, mostly from public actors and mainly for **generative AI tools for various use cases** such as ecology, relations between users and administrations, employment and health*" (CNIL, 2023b).

Four projects have been selected:

- Albert: assisting [civil servants] in the search for information and helping them to formulate specific responses to users;
- Personal Job Intelligence Advice: conversational tool, based on a language model, aimed at helping *Pôle Emploi* advisors to propose a personalised support adapted to the needs of job seekers;
- Ekonom IA: aims to monitor citizens' water consumption in order to provide them with information and recommendations on how to minimise their consumption;
- RATP project: aims to detect specific events by analysing video images.[168]

References

- CNIL, 2023a, "Personal data sandbox: CNIL launches a call for projects on artificial intelligence in public services", 21 July 2023.
- CNIL, « Accompagnement renforcé » : la CNIL lance un nouveau dispositif innovant d'accompagnement, 20 February 2023.
- CNIL, 2023b, "Artificial Intelligence and Public Services "sandbox" : the CNIL supports 8 projects", 04 December 2023.

[168] RATP is responsible for operating the public transport system in Paris and its suburbs.

3.2. Experimentation with augmented cameras under French law on the Olympic Games

In addition to the CNIL's sandbox, it is also worth mentioning the French law that has been adopted in the context of the 2024 Olympic Games (*loi n° 2023-380 du 19 mai 2023 relative aux Jeux Olympiques et Paralympiques de 2024*).This law contains a provision (Article 10) allowing, on an experimental basis and until 31 March 2025, the algorithmic processing of images collected by video systems for the purpose of ensuring the security of sporting, recreational or cultural events. The processing can only be aimed at detecting, in real time, predetermined events such as the use of a weapon or abandoned objects. Facial recognition however is not allowed under this law. The law contains safeguards and requirements in terms of data governance, human oversight, record keeping, etc. that clearly echo the AI Act.

This law is related to regulatory sandboxes in the sense that it is an **experimental legislation**, limited in time and space. An evaluation of the experimentation will be carried out and published in the form of a report.

References

- Antonin Guillard et Vincent Louis, « La loi « jeux olympiques » : l'arbre de l'expérimentation algorithmique cache la forêt de l'extension sécuritaire », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 18 septembre 2023, consulté le 26 août 2024. URL : http://journals.openedition.org/revdh/18490.

3. Germany: The Regulatory Sandboxes Strategy

Context

In 2018, The Germany Economic Affairs Ministry ("BMWK") adopted the '***Regulatory Sandboxes Strategy***' and set up a few months later a 'Regulatory Sandboxes Coordinating Office' in charge of implementing this strategy. In 2019, the Ministry published a report *Making space for innovation. The handbook for regulatory sandboxes*. The regulatory sandboxes strategy aims "*to systematically establish regulatory sandboxes as an instrument of economic and innovation policy in Germany and thereby to make a contribution towards a new digital regulatory framework*" (Federal Ministry, 2019, p. 15).

While various initiatives related to sandboxes and experimental legislation already existed in Germany, this strategy intends to favour the gathering and sharing of information and good practices. The handbook describes the steps required to set up a regulatory sandbox which could thus be followed by any German authority willing to create a sandbox.

Although these regulatory sandboxes strategy does not specifically concern AI, it is worth examining because it could have a direct impact on the AI regulatory sandboxes that will have to be created under the AI Act. In addition, regulatory sandboxes are described as key in **Germany's AI strategy** (2020).

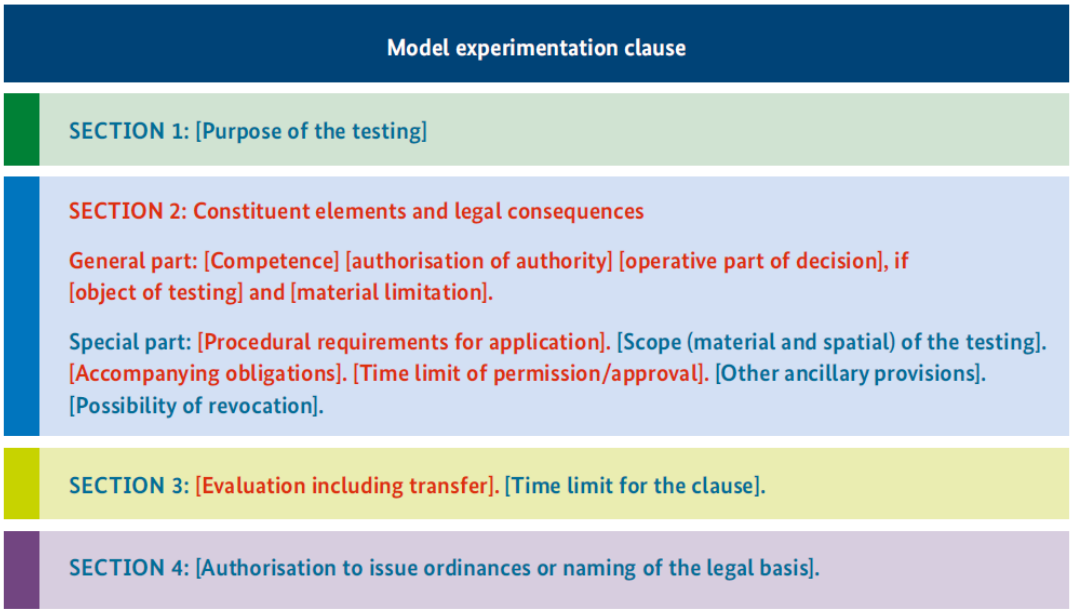
Key actors

- The **BMWK** oversees the '*Regulatory Sandboxes Strategy*'.
- Various national or local public bodies can be in charge of a regulatory sandbox.
- A **Network of Regulatory Sandboxes** has been created as part of the Strategy. It counts hundreds of members coming from various backgrounds.

Legal framework

The handbook sees the possibility of relaxing the rules as an essential characteristic of regulatory sandboxes. In this sense, it insists on the importance of **legal exemptions** which allow innovators to test products without having to comply with all the normally applicable rules. The handbook recalls that the German Basic Law (i.e. the Constitution) requires that every regulatory sandbox abide by the legal principles of legality, precision and equality. Several German laws (whether federal or local) contain **experimental clauses** which may allow identified authorities to create a regulatory sandbox and grant exemptions to participants. For instance, the 'Carriage of Passengers Act Section 2 subsection 7' states that *"In order to allow for the practical testing of new modes or means of transport, the licensing authority may, upon request on a case-by-case basis, authorise exemptions from the provisions of this Act or from provisions adopted on the basis of this Act for a maximum period of four years, insofar as they do not conflict with public transport interests."* (Federal Ministry, 2019, p. 71).

In 2020, Federal Ministry for Economic Affairs and Energy published another report, *New flexibility for innovation Guide for formulating experimentation clauses*, which specifically addresses the issue of experimentation clause for the creation of regulatory sandbox. The report proposes a model for experimentation clause.



Source: BMWK, 2020, p. 11

The 2021 Governmental coalition agreement calls for the adoption of a federal law establishing a general framework for regulatory sandboxes. A **concept note** detailing this future regulatory sandbox law has been published by the BMWK in 2021. According to the OECD, **a federal regulatory sandbox law** is expected to be effective in 2025 (OECD, 2024, p. 99).

The idea is to create a legal framework with common principles that pave the way for the adoption of experimental clauses in specific areas. The concept note stresses the need for the law to clearly define basic principles such as transparency, equal access, public interest, to ensure that experimental clauses specify a clear timeframe for testing, and that the power of the competent authority is clearly defined, as well as the purpose of testing and the criteria for evaluating the results of testing. It is also provided that a **central one-stop shop** shall be created to help with the creation of regulatory sandboxes.

Funding

Many regulatory sandboxes have received dedicated funding. Living laboratories for the energy transition, for example, have been set up and funded with €100 million a year for the period 2019-2022 (Federal Ministry, 2019, p. 34). A test bed for autonomous driving has been set up in Baden-Württemberg with public funding of €2.5 million.

Sectors

Regulatory sandboxes have already been created in various sectors including autonomous driving, urban development, delivery robots, drones, energy, health, digital identities.

References

OECD, *OECD Artificial Intelligence Review of Germany* (Organisation for Economic Co-operation and Development 2024) <https://www.oecd-ilibrary.org/science-and-technology/oecd-artificial-intelligence-review-of-germany_609808d6-en> accessed 13 August 2024

Federal Ministry for Economic Affairs and Climate Action (BMWK), Regulatory Sandboxes – Enabling Innovation and Advancing Regulation, September 2022.

Federal Ministry for Economic Affairs and Climate Action (BMWK), Neue Räume, um Innovationen zu erproben Konzept für ein Reallabore-Gesetz, September 2021.

Federal Ministry for Economic Affairs and Energy (BMWi), New flexibility for innovation Guide for formulating experimentation clauses, December 2020.

German Federal Government, Strategie Künstliche Intelligenz der Bundesregierung - Fortschreibung, 2020.

Federal Ministry for Economic Affairs and Energy (BMWi), Making Space for Innovation, The handbook for regulatory sandboxes, July 2019.

4. Luxembourg

Context

In May 2024, the Luxembourg data protection authority announced the launching of '*Sandkëscht'*, a regulatory sandbox on AI. The goal is to help innovators to develop AI systems compliant with the GDPR.

Key Actor

The *CNPD*, *Commission nationale pour la protection des données* (i.e. the data protection authority)

Legal framework

The sandbox is organised under the remit of the CNPD. Participation in the sandbox does **not entail any legal exemption** from the GDPR.

Sandbox framework

- **Eligibility criteria**
  - It is open to both public and private organisations.
  - The participant must be established in Luxembourg.
  - Projects must be centered on the development, integration, or use of new technologies, including AI.
  - Projects must address challenges in data protection and raise uncertainties as to the interpretation.
  - Projects must provide benefits for individuals or society in general

- **Testing Process**

According to the *Charte de participation*, the participation in the sandbox is divided into three phases.

1) First, the definition of the objectives and expected results, establishment of a roadmap, setting of deadlines and duration of participation, development of an exit plan.
2) Implementation and monitoring of the measures.
3) Validation of good practices and completion of an exit report.

The length of participation may vary but should be between **9 and 18 months**.

Participants must have the necessary resources to carry out the test. If this is not the case, CNPD may terminate participation.

- **Nature of the support**

The support is mainly **legal**. **No technical infrastructure is provided** for participants. The FAQ precises that "*The CNPD is not intended to provide an IT or technical architecture for testing. The project leader assumes full responsibility for its information system and other architecture elements throughout the experiment*".

References

- Sandkëscht, https://cnpd.public.lu/fr/professionnels/outils-conformite/sandbox.html
- Charte de Participation au programme "Sandkëscht", https://cnpd.public.lu/content/dam/cnpd/fr/professionnels/sandbox/sandbox-charte-de-participation-2024.pdf

5. The Netherlands

Context

In May 2024, the Dutch data protection authority and the Dutch authority for digital infrastructure published an advice letter to the Minister of Economic Affairs and Climate Policy, the Minister for Digitalisation, the Minister for Legal Protection on the **Dutch supervisory structure for the AI Act**.[169] The document describes how the supervision of the AI Act could be organised at the national level and notably addresses the issue of AI regulatory sandboxes. This document is advisory only, but it is likely to be endorsed at least in part. The Netherlands has also launched a pilot project on AI regulatory sandboxes, about which there is no published document yet.

Key actors

- The Dutch **data protection authority**
- The Dutch **authority for digital infrastructure**
- Other supervising authorities may be involved such as the Netherlands Institute for Human Rights, the Netherlands authority for consumers and markets and the Inspectorate of justice and security.

Legal framework

According to the advice letter, the Dutch data protection authority and the Dutch authority for digital infrastructure should become **coordinating market surveillance authorities** regarding the enforcement of the AI Act**.** Other authorities could play the role of market surveillance authority for a specific domain. For example, the Dutch authority for the financial markets and Dutch central bank should be the market surveillance authority regarding the high-risk AI systems developed for creditworthiness assessments.

The letter states that these two authorities "*should be involved in **facilitating sandbox trajectories**, supporting and involving the relevant supervisors, monitoring a consistent application of the AI Act by market surveillance authorities and, where relevant, notified bodies, aspects related to communication to providers, and reporting to and interaction with or within the AI Office and the AI Board, as far as general matters are concerned*".

The letter considers that "*for each situation (sandbox), it should be considered which competent authorities, including market surveillance authorities and notified bodies, are most involved in relation to a specific AI system being tested*." (2024, p. 12). Other supervisors such as the Netherlands institute for human rights, the Netherlands authority for consumers and markets or the Inspectorate of justice and security should also be involved when relevant.

[169] This document was preceded by a first advice delivered in November 2023.

Reference

- Dutch Data Protection Authority and Dutch Authority for Digital Infrastructure, Second (interim) advice on supervisory structure AI Act, 12 June 2024.
- Dutch Data Protection Authority, Department for the Coordination of Algorithmic Oversight (DCA), AI & Algorithmic Risk Report Netherlands, winter 2023-2024.

6. Norway[170]

Context

As part of the Norwegian '*National Strategy for Artificial Intelligence*', a '*regulatory privacy sandbox'* has been established within Datatilsynet (the data protection authority) in 2020 for a period of two years. The regulatory sandbox initially aimed to "*promote the development and implementation of ethical and responsible artificial intelligence from a privacy perspective*". In the future, the sandbox will not be only focused on AI but more broadly on innovation and digitalisation.

An evaluation of the sandbox was published in a report in 2023.

Key actors

- **Datatilsynet**, the Norwegian data protection authority

Legal framework

The **Norwegian personal Data Act** and the **GDPR** constitute the legal basis for the creation of the sandbox. The Norwegian authority can collaborate with other national authorities if relevant. **No legal exemption** can be granted in the sandbox.

Funding

The setting up of the sandbox in 2021 and for a period of two years has been made possible thanks to a **national funding**. In 2022, the National Budget proposed to allocate a funding for a permanent sandbox. According to the Evaluation report, the sandbox received a budget of 3 million NOK in 2020, 9 million NOK in 2021, and 9.2 million NOK in 2022.[171]

It is jointly funded by the Ministry of Local Government and Regional Development, Ministry of Labour and Social Affairs, the Ministry of Health and Care Services, the Ministry of Education and Research, the Ministry of Trade, Industry and Fisheries, and the Ministry of Transport.

Participation in the sandbox is **free**.

Sandbox Framework

The sandbox framework is described on Datatilsynet's website.

- **Eligibility criteria**
  - It is open to both private and public organisations.
  - Projects must make use of AI or otherwise involve AI.
  - Projects must benefit individuals or society in general.

[170] Norway is part of the European Economic Area.
[171] In August 2024, 1 NOK = 0,085 €.

- Projects must clearly benefit from participation in the sandbox.
- Participants must be subject to the Norwegian data protection authority.

The selection committee is composed of members of the Norwegian data protection authority assisted by an external reference group.

- **Testing Process**
  - The time limit is 3 to 6 months, depending on specific cases.
  - Each participant establishes an individual **plan with the data protection authority**.
  - The services offered include: assisting in carrying out a data protection impact assessment; providing feedback on relevant technical and legal solutions to data protection challenges; implementing privacy by design; etc.
  - At the end of the project supervision, the data protection authority publishes an **exit report**. The reports are available online (and in English).

- **Sectors concerned**

The sandbox is intended for projects which raise legal uncertainties and might be of interest for others. This includes "*innovative use of personal data with the help of technology that combines artificial intelligence with other technology, such as biometrics, the Internet of Things, portable technology or cloud-based products*"; "*complex data-sharing*"; "*building a good user experience and trust by providing transparency and explainability*"; avoiding bias or discrimination, etc.

In 2024, for the 5th round of the sandbox, the selection committee selected three projects which involve generative AI, and more specifically large language models.

- **Nature of the support**

The team in charge of the sandbox within the data protection authority is said to be composed of lawyers, but also technologists, social scientists and communication consultants. However, the support is of **legal** nature and mainly focused on data protection legislation. The sandbox offers **no testing platform** or any other technical infrastructure.

- **Results**

There have been four application rounds so far with 13 participants in total (Evaluation, 2023, p. 17). Most of the participants come from the healthcare sector. Others are active in the financial sector or are public services. Projects are detailed on the data protection authority's website.

References

- Datatilsynet, Regulatory privacy sandbox, accessed 15 August 2024.
- Evaluation of the Norwegian Data Protection Authority's Regulatory Sandbox for Artificial Intelligence, published by Datatilsynet, 2023, report number R1022215.
- Datatilsynet, Time for Generative AI in the Sandbox', Datatilsynet (website), 9 January 2024.

7. Spain

Context

In 2022, the Spanish Government launched an AI sandbox pilot funded by the National Recovery, Transformation and Resilience Plan for an amount of 4.3 million euros. The pilot was expected to run for three years, until 2025. This is the first sandbox directly aimed at implementing the AI Act. The project started while the AI Act was still being negotiated. However, there is little information on this pilot, and it doesn't seem to have been very conclusive.

Key actors

- The Spanish Agency for the Supervision of Artificial Intelligence (AESIA) has been created in 2023. The agency will be responsible for the supervision of the AI Act, including the implementation of regulatory sandboxes.
- The Spanish data protection authority should also play a role when personal data is processed in the sandbox, as it is required by the AI Act.

Legal framework

A Royal Decree has been adopted which establishes a framework for AI regulatory sandboxes. The concepts and rules contained in the Royal Decree are based on the Council's version of the AI Act (the final text had not yet been adopted at the time). While some rules have evolved since then, the general approach of the legislation remains the same.[172]

Funding

The pilot received funding of 4.3 million euros. Participation in the sandbox is free but does not involve the granting of a financial contribution.

Sandbox framework

- **Eligibility criteria**
  - It is open to both public and private actors established in Spain.
  - Applications can be submitted by providers of AI systems or jointly by providers and users (*usuario* in Spanish) of AI systems (the definition of "*user*" in the Royal Decree corresponds to "*deployer*" in the AI Act).
  - AI systems which fall out of the scope of the AI Act (such as AI systems used solely for military purposes) and those that are prohibited under the AI Act cannot participate in the sandbox.
  - The other criteria taken into account include (see Article 8(2) of the Royal Decree): the degree of innovation or technological complexity, the degree of social, business

[172] For example, the Royal Decree refers to the notion "*foundation model*", which is not present in the final text.

or public interest, the degree of explainability and transparency of the AI system, its maturity, the type of high-risk AI system (to include over different types of high-risk AI systems in the sandbox), the quality of the technical report, the characteristics of the AI provider (with a view to having different types and sizes of AI providers in the sandbox), compliance with data protection legislation and with the Spanish Government's Charter of Digital Rights.

Calls must be published, specifying the number of AI systems to be selected, the duration and the criteria that will be taken into account.

- **Testing process**

During the testing process, participants are required to implement various measures which directly relate to the AI Act, namely the establishment of a risk management system and a data governance framework, the drafting of technical documentation, recording logs, ensuring human oversight, etc. (see Article 11).

An "*implementation plan*" (which corresponds to the *sandbox plan* in the AI Act) must be agreed between the participant and the Spanish authority. This plan must detail how the participant will implement these measures. During the testing, participants must work in close collaboration with the Spanish authority to comply with the requirements. The Royal Decree does not provide much detail about the testing process compared to what is already specified in the AI Act.

At the end of this first stage, participants must complete a self-assessment aimed at showing their compliance with the various requirements. The Spanish authority will determine whether the participant meet or not the requirements.

At the end of the testing, participants must submit a report to the Spanish authority.

- **Sector concerned**

The AI system must be either a high-risk system or a general-purpose AI system.

References

- Real Decreto 568/2022, de 11 de julio, por el que se establece el marco general del banco de pruebas regulatorio para el fomento de la investigación y la innovación en el sector eléctrico.
- Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial.

8. Brazil

Context

On the 3rd of November 2023, the Brazilian data protection authority (ANPD) published a call for Contributions to collect inputs for a regulatory sandbox on AI and data protection in Brazil.

In the document describing the call, a proposal for a regulatory sandbox in Brazil is detailed. The sandbox framework described in the document is therefore not definitive. Regulatory sandboxes are defined as "*a collaborative experimentation between the regulator, the regulated entity and other stakeholders with the aim to test innovations against the regulatory framework by adopting a structured methodology*". The document precises that regulatory sandboxes can be uni-sectorial or multi-sectorial. The sandbox aims to promote algorithmic transparency, foster responsible AI innovation, establish a multi-stakeholder environment, assist in the development of parameters for human oversight of high-risk AI systems.

The text highlights that innovation can be encouraged by creating responsive AI systems. Sandbox experimentation offers a controlled setting for testing these systems, allowing various stakeholders, including researchers and regulatory bodies, to examine the effects of transparency on innovation, data protection, and individual rights. The sandbox is intended to promote innovation by giving developers a space to experiment with new AI technologies that incorporate transparency features. The sandbox should strike a balance between encouraging experimentation for participants and ensuring adherence to regulatory requirements.

Key Actor

- The Brazilian data protection authority (ANPD). The ANPD could become the central authority for AI regulation in Brazil.

Legal Framework

In Brazilian law, there is a Startups Legal Framework[173] adopted in 2021 which allows "*for Brazilian regulatory authorities to develop experimental regulation environments (regulatory sandboxes) and, if needed, to waive the applicability of some norms during the experimentation*".

Regulatory sandboxes are defined in the law as "*a set of special simplified conditions for participating legal entities to receive temporary authorisation from the bodies or entities with sector regulation powers to develop innovative business models and test experimental*

[173] LEI COMPLEMENTAR Nº 182, DE 1º DE JUNHO DE 2021 Institui o marco legal das startups e do empreendedorismo inovador; e altera a Lei nº 6.404, de 15 de dezembro de 1976, e a Lei Complementar nº 123, de 14 de dezembro de 2006.

techniques and technologies, by complying with criteria and limits previously established by the regulatory body or entity and by means of a facilitated procedure".[174]

Article 11 of this law establishes a specific legal regime for regulatory sandboxes, allowing public administration bodies and sectorial regulators to waive the application of rules within their jurisdiction for the benefit of a regulated entity. Paragraph 3 of this provision precises that the public authority in charge of the sandbox must establish eligibility criteria for selecting participants in the sandbox, determine the duration and the scope of the suspension of the application of the rules, and specify what rules are covered.

Sandbox framework

- **Eligibility criteria**

The eligibility criteria are not described in the document.

- **Testing process**

The duration should be from 18 to 24 months, divided in the following stages:

a) Submission stage
b) Leveraging/training stage
c) Experimentation/testing stage
d) Evaluation stage

- **Technologies covered**

The call identifies different technologies that should be tested in the sandbox, namely machine learning-based systems and Generative AI used to generate content such as text, images, audio, or video.

- **Nature of the support**

The **support** provided will primarily be **legal** in nature. Participants in the sandbox will receive guidance on how to comply with Brazil's General Data Protection Law (LGPD – Lei Geral de Proteção de Dados). Specifically, the provisions covered include Article 20, which deals with the review of solely automated decisions, as well as provisions related to algorithmic transparency, interpretability, and explainability. The call also refers to the proposed Brazilian AI Bill, which closely relates to the LGPD and may also be monitored within the sandbox.

As previously mentioned, there is a legal framework that allows public authorities to create sandboxes and grant legal exemptions. However, the call also specifies that "*the*

[174] Article 2° II: "ambiente regulatório experimental (sandbox regulatório): conjunto de condições especiais simplificadas para que as pessoas jurídicas participantes possam receber autorização temporária dos órgãos ou das entidades com competência de regulamentação setorial para desenvolver modelos de negócios inovadores e testar técnicas e tecnologias experimentais, mediante o cumprimento de critérios e de limites previamente estabelecidos pelo órgão ou entidade reguladora e por meio de procedimento facilitado".

suspension of legal provisions is not always necessary". It remains therefore unclear whether the future AI regulatory sandbox will include the granting of legal exemptions.

References

- "ANPD's Call for Contributions to the regulatory sandbox for artificial intelligence and data protection in Brazil is now open", https://www.gov.br/anpd/pt-br/assuntos/noticias/anpds-call-for-contributions-to-the-regulatory-sandbox-for-artificial-intelligence-and-data-protection-in-brazil-is-now-open, 3 October 2023.

9. Colombia

Context

In 2021, the *Superintendencia de Industria y Comercio* (SIC) launched a '*Sandbox on privacy by design and by default in artificial intelligence projects*'. The sandbox focuses on privacy by design and by default solutions.

This regulatory sandbox aims to promote the development of AI products that are designed and implemented with respect for individuals' rights to personal information and in full compliance with data protection regulations. The sandbox also aims to provide lessons on how to adapt Colombian regulations to technological advances.

Key Actors

- The *Superintendencia de Industria y Comercio* (SIC): it is an agency attached to the Ministry of Trade, Industry and Tourism of Colombia. It acts among other things as the data protection authority.

Legal Framework

It is based on the Statutory Law 1581 of 2012 and Decrees 4886 of 2011 and 1377 of 2013 (incorporated in Decree 1074 of 2015). The sandbox is organised under the remit of the SIC. Under Article 21 of the Statutory Law 1581 of 201, the SIC is authorised to "*suggest or recommend adjustments, corrections or adaptations to the regulations that are consistent with technological, computer or communicational evolution*" (SIC, 2020).

Funding

Participation in the sandbox is **free**. Participants must have sufficient resources to attend meetings and carry out the work required.

Sandbox framework

- **Eligibility criteria**
  - Open to national and foreign companies, and to public entities.
  - **AI projects** in e-commerce, advertising or marketing.
  - The project involves the **processing of personal data** (but this processing must not yet have been carried out).
  - The project is in a **design stage.**

- **Testing Process**
  - The initial duration is **1 year** (but it may be extended).
  - An agreement is concluded between the participant and the SIC.
  - The SIC will notably provide reports with feedback, recommendations and observations.

- **Nature of the support**

The SIC provides legal support regarding the processing of personal data.

- **Results**

A few projects that can be consulted here have been selected since 2021.

References

- SIC, "Sandbox on privacy by design and by default in Artificial Intelligence Projects" https://www.sic.gov.co/sites/default/files/files/2021/150421%20Sandbox%20on%20privacy%20by%20design%20and%20by%20default%20in%20AI%20projects.pdf, 2021.
- https://www.sic.gov.co/sandbox-microsite.

10. Singapore

Context

Singapore has been a leading actor in the development of regulatory sandboxes. The Monetary Authority of Singapore had launched a Fintech regulatory sandbox. Two sandboxes have then been set up which directly relate to data protection and new technologies: the *Data regulatory sandbox* and the *Privacy Enhancing Technologies Sandbox*.

Key actors

- The Infocomm Media Development Authority (IMDA)
- The Personal Data Protection Commission (PDPC)

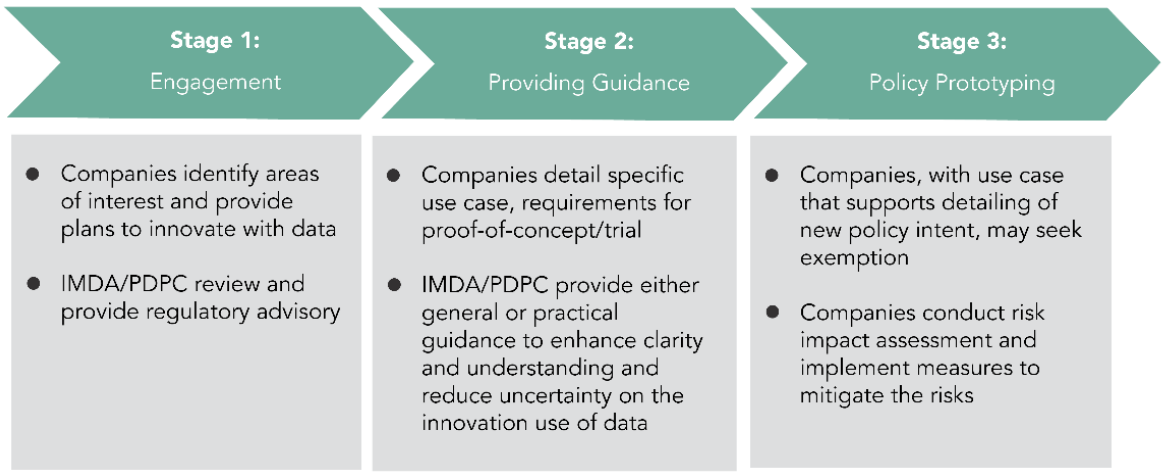
Sandbox framework

1. The Data regulatory sandbox

The Data Regulatory Sandbox "*supports businesses by clarifying regulatory boundaries when innovating with data-driven technology and providing guidance to ensure compliance with data protection policies*".

The projects entering the sandbox should be innovative, beneficial to the public, ready and concrete use cases, and the risks should be assessed and mitigated.

The testing process operates in three parts detailed in the figure below.



Source: https://www.imda.gov.sg/how-we-can-help/data-innovation/data-regulatory-sandbox

2. Privacy Enhancing Technologies Sandbox

This sandbox aims to facilitate experimentation with Privacy Enhancing Technologies (PETs). PETs are technologies designed to guarantee the protection of personal data while enabling data to be used and analysed. This includes methods such as differential privacy, federated learning, synthetic data.

The PET sandbox help matching companies with PET digital solution providers, provide grants for the implementation of pilot projects, and deliver regulatory guidance to ensure PETs are deployed compliantly.

The sandbox has recently focused on **generative AI**.

Different companies have participated in the PET sandbox, including Ant international, Mastercard and Meta.

References

- https://www.pdpc.gov.sg/news-and-events/announcements/2022/07/launch-of-privacy-enhancing-technologies-sandbox
- Privacy Enhancing Technology Sandboxes, https://www.imda.gov.sg/how-we-can-help/data-innovation/privacy-enhancing-technology-sandboxes,

11. United Kingdom

Context

In 2019, the Information Commissioner's Office (ICO) sandbox initiated a regulatory sandbox. It aims "*to support organisations who are creating products and services which utilise personal data in innovative and safe ways*" (ICO, 2021). A wealth of information is available on ICO website and in ICO reports.

Key Actors

- The UK Data protection authority: the Information Commissioner's Office (ICO)

Legal Framework

The sandbox is organised as part of the ICO's mission. **No legal exemption** is granted. UK data protection law fully applies in the sandbox. Terms and conditions must signed by participants.

Funding

The participation is **free** and the ICO does not provide financial support to participants.

Sandbox framework

- **Eligibility criteria**
  - The sandbox is open to any kind of organisation as far as the data processing falls within the scope of the UK data protection law.
  - It is only open to products that are under development. This means that no personal data may have been processed.
  - 3 main indicators are taken into account:
    1) Innovation defined as "*the application of new knowledge to the production of goods and services; it means improved product quality and enhanced process effectiveness*".
    2) Public benefit, assessed "*in terms of both breadth (the amount of people benefiting) and/or depth (the extent to which they benefit)*".
    3) Sandbox plan viability: the support requested from the ICO appears to be commensurate with the ICO's resources. Risk mitigation measures need to be considered.

- **Testing process**
  - *Sandbox plan*: The participant and the ICO agree on a sandbox plan which may "*specify testing parameters, measures for outcomes, reporting requirements, safeguards, timescales, milestones and term of the sandbox*" (see Terms and conditions).
  - Participation in the sandbox lasts no longer than **12 months**.

- *Exit plan*: the exit plan aims to "*to ensure the sandbox can be closed down at any point whilst minimising the potential detriment to data subjects*".
- At the exit stage, the ICO may issue a statement of regulatory comfort (see below).
- Under certain conditions, the ICO or the participant may terminate the participation in the sandbox earlier than initially planned.
- The ICO publishes a report at the end of the participation in the sandbox which is available online.

- **Sectors concerned**

Open to any sector as long as there is processing of personal data. However, the ICO lists current **key areas of focus**, which include Central bank digital currencies, Commercial use of drones, Consumer healthtech, Decentralised finance, Genomics, Immersive technology and virtual worlds, Neurotechnologies, Next-generation Internet of Things (IoT), Next-generation search, Personalised AI, Quantum computing.

- **Nature of the support**

The support is mainly **legal**. The feedback and guidance given by the ICO are not compulsory and do not constitute full examination or audit. It does not prevent the ICO from taking other decisions or regulatory measures. However, the ICO may issue a statement of regulatory comfort setting out "*that, on the basis of the information provided whilst in the Sandbox, the ICO did not encounter any indication that the organisation's operation of its developed product or service would infringe upon data protection legislation*". The ICO offers no infrastructure, testing environment, or data; participants must use their own.

- **Results**

Since 2020, over twenty projects have passed through the sandbox. Exit reports are available on the ICO website. Several projects were involving AI, such as:

- Good With Limited: a fintech and edtech company which is intended to "*develop mobile applications which help educate young adults on personal finance*". The mobile application will produce a "*financial readiness score*" which can then be used by financial institutions to assess the creditworthiness of app users. This app would probably qualify as a 'high-risk AI system' within the meaning of the AI Act if it were marketed within the EU.
- Yoti: a company developing an age estimation system based on the analysis of images of human faces using machine learning methods. This could also qualify as a 'high-risk AI system' as Annex III.1(c) lists biometric AI systems "*intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics*" (age being a protected characteristic).

References

- ICO, Regulatory Sandbox Insights Report 2024, July 2024.
- ICO, Regulatory Sandbox beta review, November 2021.
- ICO, Guide to the sandbox, ICO website.