Centre for Information Policy Leadership
HUNTON

Learning from Practice: Designing Effective Regulatory Sandboxes

October 2025

Contents

Introduction

In an era where technological development continues to outpace regulatory frameworks, responsive and forward-looking regulatory approaches are essential to maintaining the agility necessary to protect fundamental rights without impeding the development of new technologies. Innovation is a key driver of economic progress, but it requires legal and regulatory certainty if organisations are to bring new and disruptive technologies to market responsibly.

CIPL[i] has long promoted proportionate and outcomes-based regulation, supported by progressive regulatory tools. Effective regulation of emerging technologies, such as AI, cannot rely on traditional, static approaches alone. It must instead be adaptive, agile, and collaborative. Within this context, the regulatory sandbox has increasingly emerged as a recognised oversight mechanism to enable responsible innovation.

A regulatory sandbox,[ii] as it is now commonly called, is a 'safe space' to pilot and test innovative products, services, business models, or delivery mechanisms in real-world conditions under a formal, structured programme in partnership with a regulator. Properly designed, a regulatory sandbox is a process of collaborative compliance, in which regulators and participants co-design practical approaches to meeting legal requirements in the context of new products or services. When implemented effectively, sandboxes facilitate innovation while safeguarding a high standard of fundamental rights protection.

Originating from earlier forms of regulatory experimentation, the sandbox model was given a distinct identity by the UK Financial Conduct Authority (FCA)[iii] in 2016 and has since matured into common regulatory practice. Today sandboxes can be found to operate in multiple sectors and jurisdictions – including data protection, health technology, and mobility services – as regulators have sought flexible tools to keep pace with rapid technological change.[iv]

In the European Union (EU) the Artificial Intelligence Act (AI Act)[v] embeds sandboxes in law, requiring that each Member State has one. These sandboxes are intended to provide a structured environment in which organisations can test and validate their Artificial Intelligence (AI) systems under regulatory supervision. The vision is to unlock the potential of AI while ensuring compliance with the AI Act and other EU laws preserving fundamental rights.

While the AI Act has mainstreamed the sandbox model, its relevance extends far beyond AI. As digital regulation expands, sandboxes offer a practical way to test new approaches without stifling innovation. CIPL first proposed data protection sandboxes in 2019[vi] under the General Data Protection Regulation (GDPR)[vii], and the case for their adoption continues to grow – with opportunities for sandboxes in domains such as online safety, cybersecurity and data governance.

The purpose of this paper is three-fold:

1. **Identify the key success factors for regulatory sandboxes**

   Building on CIPL's earlier work and new comparative research into existing sandboxes, this paper identifies the key success factors that underpin sandbox models.

2. **Based on these insights, provide tailored recommendations for implementing effective sandboxes under the AI Act**

Drawing on these key success factors, the paper sets out practical recommendations to guide Member States in designing and operating regulatory sandboxes under the AI Act.

3. **Position sandboxes as a cornerstone of smart, pro-innovation regulation**

   Looking more broadly, the paper examines how sandboxes can drive responsible innovation not only in the data and AI context but also across the wider digital governance landscape.

Building on our previous research, CIPL has found the following success factors for regulatory sandboxes:

Recommendations for effective sandbox design and participation

For regulators

1. Clearly define and communicate the sandbox's objectives, proposed outputs, expected outcomes, and benefits (e.g. regulatory certainty, accelerated market entry).
2. Establish transparent entry and exit criteria, defined timelines, structured feedback loops, and clear roles for all participants.
3. Allocate adequate financial, human, and technical resources to manage and support sandbox operations effectively.
4. Select projects strategically to maximise public benefit, considering their potential to generate learning and influence market practice.
5. Provide regulatory forbearance where appropriate through structured supervisory dialogue and proportionate enforcement discretion.
6. Ensure confidentiality and robust protection of commercially sensitive information to maintain trust.
7. Promote a regulatory culture that prioritises engagement with organisations and collaborative problem-solving.
8. Coordinate with other regulators across sectors and jurisdictions to promote interoperability and reduce duplication.
9. Publish exit reports or summaries to share lessons and promote wider understanding.
10. Use insights gained through sandboxes to inform policy development, refine regulatory guidance and target future regulatory interventions.

For organisations

11. Allocate adequate financial, human, and technical resources to support sustained sandbox participation.
12. Designate staff with appropriate legal, technical, and operational expertise to engage meaningfully.
13. Build a shared internal understanding of the sandbox's purpose, structure, and governance prior to participating.
14. Define the intended benefits and risks of participation, set measurable success criteria, and identify how technical, legal, and operational risks will be mitigated.
15. Evaluate whether a sandbox is the most suitable mechanism for achieving the desired objectives, considering alternative experimentation tools where appropriate.

We also make the following additional recommendations to guide Member States in designing and operating regulatory sandboxes under the AI Act:

Recommendations for AI Act regulators

16. Define the respective roles and responsibilities of competent authorities and other stakeholders involved in AI Act sandboxes to ensure clear accountability and coherent decision-making.
17. Promote interoperability and mutual recognition among AI Act sandboxes across Member States by aligning evaluation criteria, procedural frameworks, and outcome standards to support regulatory convergence and cross-border innovation and trust.
18. Promote national specialisation within AI Act sandboxes by building centres of excellence around specific sectors or national strengths, while enabling cross-border collaboration to share expertise and ensure coherence across jurisdictions.
19. Establish pathways for cross-regulatory cooperation with other relevant competent authorities, including those responsible for data protection, online safety and financial services.
20. Integrate AI Act sandboxes with the wider EU AI innovation ecosystem, including Test and Experimentation Facilities (TEFs), European Digital Innovation Hubs (EDIHs), Data Spaces, and AI Factories, to expand access to expertise, infrastructure, and funding.
21. Use insights generated through AI Act sandboxes (e.g. exit reports, aggregate findings) to strengthen EU-wide regulatory learning, with the European Commission's AI Office coordinating a central resource hub to consolidate lessons, themes, and emerging best practices.

Beyond the AI Act, there are opportunities to embed sandboxes in a wider set of digital rulebooks:

Recommendations for other digital regulators

22. Adopt regulatory sandboxes in digital regulatory regimes such as data protection, online safety, data interoperability or cybersecurity to unlock responsible innovation, coordinating across regulatory domains where necessary.

Methodology

For this paper, CIPL analysed regulatory sandboxes across multiple jurisdictions in data protection, AI, and financial services, drawing on publicly-available documentation, regulatory guidance, and previous research into sandboxes conducted by CIPL. This was complemented by a series of interviews and a roundtable discussion with regulators and other stakeholders who have designed, overseen, or participated in some of the most well-known sandbox initiatives to date.[viii] These conversations provided valuable insights into how sandboxes operate on the ground, the conditions under which they succeed, and the challenges they face. We surfaced practical perspectives on the conditions under which sandboxes can support innovation while ensuring legal compliance and public trust.[ix]

Comparative insights into regulatory sandboxes

This section reviews a selection of sandbox models and distils key themes from existing practices that CIPL considers especially relevant to the design and implementation of future sandboxes.

Sandbox design

A sandbox can deliver significant benefits for organisations, regulators, and society, but realising these and mitigating the associated risks depends on careful design. The process, potential benefits and regulatory expectations should be clearly communicated to participating organisations to encourage engagement and build trust.

Benefits of regulatory sandboxes, for organisations, regulators, and society:	**Challenges that regulatory sandboxes need to consider and mitigate:**
• **Regulatory clarity**. Sandboxes provide clarity on regulatory expectations, helping organisations design products and services with compliance in mind. • **Constructive engagement**. They create opportunities for structured and open engagement between regulators and innovators, fostering mutual understanding and proactive regulatory engagement. • **Cost savings and return on investment.** Participants benefit from reduced compliance costs by getting things right first time, offsetting participation costs.[x] • **Accelerated market access.** Regulatory clarity and certainty can help organisations bring innovative products and services to market faster. • **Raising investor funding**. Regulatory involvement can enhance investor and consumer confidence in products and services.[xi] • **Regulatory learning**. Sandboxes allow regulators to deepen their understanding of emerging technologies, generating insights that inform regulatory guidance and policy. • **Public interest**. By encouraging responsible innovation and protecting individual rights, sandboxes can support broader social benefits alongside economic growth, contributing to the development of a trustworthy digital society.	• **Costs**. Sandboxes require a significant investment of resources from organisations and regulators. • **Limited market impact**. Poorly designed or implemented sandboxes may fail to generate benefits beyond a small group of participants. • **Perceptions of inequity**. Sandboxes may be seen as granting special advantages or privileges to a select group of organisations, raising concerns about fairness, neutrality, and a level playing field.[xii] • **Participant hesitations**. Organisations may be reluctant to participate due to fears of losing a 'first mover advantage', enforcement exposure, risks to commercial confidentiality, and the possibility of adverse publicity. • **Unrealised learning**. Transparency through exit reports alone may not deliver value if the lessons are not effectively shared or integrated into broader regulatory practice. • **Fragmentation across jurisdictions**. A lack of harmonisation and interoperability across jurisdictions can create barriers for cross-border innovation and complicate compliance for multinational organisations. • **Unsettled legal interpretation.** Sandboxes often involve testing regulatory boundaries in areas of legal uncertainty. While this can generate valuable insights, it also risks complicating downstream guidance or enforcement if not carefully managed.

These benefits point to the broader potential of sandboxes if re-imagined beyond their current applications. By extending the model across digital domains, such as online safety, data governance, or cybersecurity, regulators could proactively address novel risks and generate solutions that serve both innovation and public trust.

When is a regulatory sandbox the most appropriate instrument?

Although regulatory sandboxes are increasingly recognised as a valuable mechanism in both the public and private sectors, they may not always be the most suitable tool. Its applicability often depends on specific conditions, the developmental stage of the initiative, and the intended objectives. CIPL has identified several key considerations:

1. **Novel or innovative products**. Sandboxes are often considered a key tool for novel or innovative products and services with, as yet, undefined risk profiles that may nevertheless have a positive impact on society but potentially present challenges to existing regulatory frameworks. There is limited regulatory benefit to engaging via a sandbox on products that are already widely available; other regulatory tools are available.

2. **Sufficient project maturity**. The level of maturity of a given project is also a key consideration when determining whether sandboxes are appropriate. Sandboxes are generally longer-term engagements with participants who are at the pre-deployment phase. There is a 'sweet spot' in the development cycle at which a product is sufficiently mature for real-market testing. At this stage, organisations and regulators have the most room to collaborate and create meaningful change to the process.

3. **Regulatory intelligence gathering**. Sandboxes provide a mechanism for regulators to understand novel and complex emerging technologies in a controlled environment. Sandboxes serve as a capacity builder within the regulatory body through hands-on experience and direct interaction with innovators. Regulators may therefore actively seek out cutting-edge technologies or projects for sandboxes that also provide the possibility for strategic insights into complex and innovative technology trends.

4. **Informing policy and regulatory development**. The interaction with innovators and new technologies in the sandbox space also provides an opportunity to identify emerging trends and potential gaps in existing regulatory policy or guidance. Regulators may use insights gained in a sandbox to review and update existing guidance, ensure consistency across regulatory mandates where multiple regulators are involved, and, in some cases, to inform potential reforms to existing law or the introduction of new law.

5. **Strategic value for society**. Sandbox projects are selected not just for technical novelty, but also for their capacity to generate real-world value that ultimately benefits individuals, organisations, and society at large. For instance, privacy-tech sandboxes are typically chosen for the public good they promise.[xiii] Importantly these benefits need not be limited to privacy or AI. Applied across other areas of the digital framework, the sandbox model could help deliver solutions with far-reaching impact.

When are other tools more appropriate?

While regulatory sandboxes are a powerful way to enable responsible innovation, they are not always the most appropriate or efficient instrument.

Sandboxes should be used selectively for novel and strategically important issues where live experimentation will generate learning that benefits both regulators and participants. In other cases, lighter-touch tools can often achieve similar outcomes with lower resource demands.

Key factors to consider include:

- **Project readiness**. Projects that have not yet reached a sufficient level of technical or organisational readiness, or that lack a clear understanding of their regulatory obligations, are unlikely to benefit from the intensive engagement in a sandbox.

- **Regulatory uncertainty**. Where the regulatory questions are highly specific, straightforward, or clearly addressed by existing guidance or tools, a sandbox may be an unnecessarily complex and resource-intensive solution. In such cases advice services, published guidance or third-party support may be more appropriate.

- **Underlying goal**. If the regulator's principal aim is to deepen understanding of a market or technology, without the need for live experimentation, lighter-touch tools such as innovation hubs, thematic reviews, or stakeholder roundtables may provide similar benefits with lower resource demands.

Choosing the right approach is critical. As sandboxes are resource intensive, both regulators and participants must be highly selective. Ultimately, the value of a sandbox can also lie in recognising when lighter-touch tools are more suitable.

Positioning sandboxes within the wider regulatory toolkit

Sandboxes are a powerful way to gain understanding through controlled experimentation and play a crucial role in enabling responsible innovation. Yet they are only one tool in the broader regulatory oversight toolkit, and because they are resource intensive, they should be reserved for the most novel and strategically important issues.

To be effective, sandboxes must sit within a wider ecosystem of legal and policy experimentation and support services. One-to-one innovation advice and one-to-many innovation hubs can provide quicker, less resource-heavy pathways for addressing emerging issues. The UK FCA's service offer[xiv] illustrates this evolution from a single sandbox to a full suite of innovation services that support firms from idea generation through to final authorisation. Similarly, the Dutch AI Act sandbox proposal allows issues not suited for a sandbox to be raised in writing, ensuring valuable questions are still addressed outside the formal sandbox process.[xv]

Other experimentation services such as living labs and testbeds also provide regulators the opportunity to explore emerging technology and market trends, while addressing discrete legal issues posed by organisations. What distinguishes sandboxes and innovation hubs from testbeds and living labs is their focus on regulatory oversight and compliance, rather than purely technical or user-centred testing. These techniques are now being fused in some offerings: for example, the Canton of Zurich's AI hub now offers strong regulator involvement plus unique access to data.[xvi]

Table: Differentiating innovation services

Innovation advice services and hubs: Their primary goal is to enhance an organisation's understanding of regulatory expectations regarding innovative products or services by providing direct contact with the regulator for discrete and small-scale guidance.	**Testbeds:** Technical programs that allow participants to test, develop, and introduce new products and services, and can also allow for controlled experimentation, similar to sandboxes, but they are often used earlier in the technology development cycle.[xvii]	**Living Labs:** An experimentation tool used to co-create, test, and upscale innovative solutions to real-life settings.[xviii]

CASE STUDY: The ICO's Innovation Services
The UK's Information Commission Office (ICO) has grown its service offering beyond its Regulatory Sandbox to include Innovation Advice, which gives bespoke responses to novel data protection questions from innovators within 15 working days, and an Innovation Hub which provides mentoring and advice to cohorts of innovators. These offerings enable the regulator to provide legal clarity more quickly and at lower cost than more resource-intensive sandbox projects.

The wider conversation on what constitutes effective regulation and regulatory oversight is moving decisively toward more agile and adaptive approaches. Sandboxes are an important element of this evolution, offering regulators and organisations a structured space to experiment responsibly. Yet they are not a standalone solution. To achieve truly effective oversight, sandboxes must be embedded within a wider framework that also includes constructive engagement[xix] with stakeholders, cross-regulatory collaboration, and forward-looking tools such as legal or policy prototyping. Only by combining these approaches can regulators ensure that oversight keeps pace with innovation while safeguarding fundamental rights and public trust.

Comparing selection criteria

Regulatory sandboxes usually have defined objectives that determine which organisations and what types of projects qualify to participate. A carefully defined focus and careful selection process ensures that sandboxes can generate insights that extend beyond individual participants and contribute to wider regulatory certainty. An overview of alternative sandbox designs is provided in the Annex.

Some differences in sandbox design are intentional and reflect distinct regulatory objectives. For example, a sandbox aimed at developing market intelligence and building internal technical capacity may adopt a rolling application model and allow for broad sectoral participation. By contrast, a sandbox designed to test and refine specific regulatory positions is more likely to apply a narrow thematic focus and operate through time-limited cohorts, thereby enabling structured comparison and more robust policy learning.

Being clear about these strategic choices supports transparency and helps other authorities design sandboxes aligned with their specific goals.

The shared aim of promoting innovation has led to a degree of consistency in entry requirements, including the following:

- **Genuine innovation**: The product or service must represent an emerging technology or novel application of a technology, novel business model, or a significant change in scale.
- **Societally or individually beneficial project**: Products or services that are likely to serve a common or individual benefit are more likely to be selected. This is to ensure that the products selected don't pose a risk to society or individuals, as well as prioritising the products that may bring some benefit too.
- **Regulatory need**: There must be sufficient complexity, overlap, or ambiguity to justify testing as part of a sandbox.
- **Readiness for testing**: The service must be ready for testing in a controlled but real-world environment, with well-defined objectives, plans, controls, and safeguards.

Some notable variances between the selection criteria for a sandbox include:

- **Eligibility of applicants**: Sandboxes can target participants by sector, technologies used, regulatory issues faced, and size and location of the organisations. Many are national in focus, and some specifically target start-ups and small-to-medium enterprises (SMEs). For example, Singapore's Infocomm Media Development Authority's (IMDA) first sandbox on generative AI was aimed at helping SMEs harness the benefits of the new technology, under regulator supervision.[xx]
- **Funding and resources**: Participants are generally required to have the knowledge and resources to participate effectively and complete the sandbox. However, we also found that some of the sandboxes offered additional funding or support to participants. Examples include the UK FCA's Supercharged Sandbox, which gives access to NVIDIA's AI Enterprise Software[xxi] , and the Singapore IMDA's GenAI Sandbox, which offers financial assistance to participants.[xxii]
- **Potential for learning**: Regulators actively prioritised projects where the outcomes could be leveraged for learning across their jurisdictions. Considering the investment for both regulator and participant during a sandbox, the goal is often to choose a sandbox project which has a 'multiplier effect' in the market through updated policy, guidance, or enforcement.
- **Aligning with own strategic priorities**: Similarly, some regulators also actively prioritised projects that have an explicit connection with their own stated regulatory priorities, which complements their use of the sandbox for broader goals than just early compliance feedback for one organisation.

It is not just sufficient to select the right projects, but also to ensure that the sandbox is well designed and implemented to ensure maximum impact beyond individual participating organisations.

Flexibility and transparency

Regulatory sandboxes differ widely in their design; there is no single universal model that governs how they operate. Their value lies in being agile and responsive, while also providing legal certainty to participants. Flexibility and transparency are central features of most sandbox models, though the way they are applied varies significantly across jurisdictions.

Flexibility

In certain instances, sandboxes permit participants to test products or services under a defined set of special conditions. This may include the temporary suspension or relaxation of particular regulatory requirements, though full derogations from the law remain rare.

CASE STUDY: Financial sector sandboxes in the UK
The UK FCA sandbox allows participants to test innovative financial products and services with individuals under their oversight. They may receive modifications or waivers to certain regulatory requirements on a case-by-case basis, but they are not able to waive national laws.

CASE STUDY: Data protection sandboxes in Singapore
The Singapore Personal Data Protection Commission (PDPC) has used "regulatory sandbox" mechanisms in AI governance and data innovation. While they do not offer blanket immunity, they do provide regulatory guidance and exemptions under controlled circumstances (e.g. limited waivers under the Personal Data Protection Act if projects meet sandbox conditions).

To support experimentation regulators may provide a form of regulatory forbearance, commit to delayed enforcement actions, or offer comfort letters signalling that participants acting in good faith will not face immediate penalties (as used by the UK ICO).[xxiii] These measures can reduce enforcement risk and strengthen participants' confidence to experiment.

Importantly, the use of flexibility and regulatory discretion in sandboxes requires a broader cultural and philosophical shift within regulatory authorities. Regulators must be prepared to act as collaborative partners, working with participants to provide guidance and reassurance and ultimately building trust.

Few jurisdictions offer a full legal safe harbour, and the AI Act does not permit formal derogations from EU law either. However, the UK is currently considering introducing a time-limited derogation from certain requirements of data protection law ,[xxiv] signalling a move towards greater flexibility in certain contexts.

Transparency

Transparency is another essential element. Many sandbox frameworks conclude with a post-sandbox exit report or formal decisions, documenting the regulator's assessment of the project. These not only provide participants with a clearer understanding of their compliance position, but when shared more broadly, also extend the learning to the wider market and inform regulatory guidance or policy development.

For instance, Norway's Datatilsynet publishes detailed exit reports from each individual sandbox project, which aims to benefit all stakeholders, including other innovators designing new products or services, or other regulators.[xxv] While care is needed in the drafting of exit reports to avoid revealing commercial secrets, the publication of such reports can provide participants with legal certainty.

For legal certainty to be meaningful, participants need confidence that such conclusions will remain valid unless there are material changes or unforeseen harms. A key feature of good design is the structured use of sandbox outcomes to inform guidance, policy, and enforcement practices, thereby creating a multiplier effect that strengthens compliance and innovation across the market as a whole.

What does good look like? Key success factors for regulatory sandboxes

Taken together, these themes highlight that the effectiveness of a sandbox depends not only on its structure but on how it balances openness with focus, flexibility with accountability, and collaboration with transparency. By distilling these lessons from practice, we can identify a set of success factors that provide regulators and organisations with practical guidance for designing sandboxes that deliver value beyond individual projects.

Recommendations for effective sandbox design and participation

For regulators

1. Clearly define and communicate the sandbox's objectives, proposed outputs, expected outcomes, and benefits.

For organisations to be incentivised to participate, the benefits must be clear and easy to communicate in order to get buy-in. Objectives, outputs and outcomes should be stated plainly so that participants understand what the sandbox seeks to achieve and how success will be measured. This enables focus, supports accountability, and ensures each project contributes to wider regulatory and market learning.

2. Establish transparent entry and exit criteria, defined timelines, structured feedback loops, and clear roles for all participants.

Effective implementation relies on structured processes. Entry and exit requirements, timeframes and feedback mechanisms should be transparent and predictable. Each participant's role and responsibility should be formally agreed, reducing uncertainty throughout the project.

3. Allocate adequate financial, human, and technical resources to manage and support sandbox operations effectively.

Sandboxes are resource-intensive, requiring dedicated personnel, technical expertise and infrastructure over an extended period. Regulators must ensure sufficient staffing and analytical capability to manage cohorts, engage with participants and capture lessons without delay or resource strain.

4. Select projects strategically to maximise public benefit, considering their potential to generate learning and influence market practice.

Projects should be chosen for their capacity to advance the public interest and deliver insights with wider policy or market value. Selecting strategically ensures that sandbox outcomes extend beyond individual participants and help shape future guidance and regulatory practice.

5. Provide regulatory forbearance where appropriate through structured supervisory dialogue and proportionate enforcement discretion.

While formal legal exemptions are rare, flexibility can be achieved through dialogue, derogations from guidance or comfort letters. Where participants act in good faith, regulators may exercise proportionate discretion to encourage experimentation while managing risk responsibly.

6. Ensure confidentiality and robust protection of commercially sensitive information to maintain trust.
Trust between regulators and participants depends on secure handling of information. Formal confidentiality agreements and clear designation of sensitive material help participants share data openly and confidently, enabling the sandbox to deliver genuine innovation and learning.

7. Promote a regulatory culture that prioritises engagement with organisations and collaborative problem-solving.
Running a sandbox requires a cultural shift from enforcement to collaboration. Regulators should act as partners in co-designing compliance solutions, investing in dialogue and joint problem-solving that strengthens mutual understanding and builds confidence. Sandboxes require clear leadership from the top of the regulator. This includes setting and communicating a defined risk appetite that clarifies the level of legal and reputational risk the regulator is prepared to accept.

8. Coordinate with other regulators across sectors and jurisdictions to promote interoperability and reduce duplication.
While challenging due to differing regulations, mandates, enforcement cultures, and variances in resources, regulatory collaboration is important to ensure harmonisation and interoperability. Exchanging research, insights, and experiences, as well as developing common criteria or interoperable standards, creates legal certainty across overlapping regulatory competences.

9. Publish exit reports or summaries to share lessons and promote wider understanding.
Publishing findings allows the benefits of sandbox participation to reach beyond the immediate cohort. Exit reports or aggregate summaries provide transparency, demonstrate accountability and feed directly into policy development and guidance.

10. Use insights gained through sandboxes to inform policy development, refine regulatory guidance and target future regulatory interventions.
Sandboxes should be recognised as tools for institutional learning and capacity-building, especially in areas of rapid technological or market development. Insights from participation and outcomes should inform regulatory priorities, stress-test existing policies and highlight areas for future reform.

For organisations
11. Allocate adequate financial, human, and technical resources to support sustained sandbox participation.
Organisations must commit sufficient time, staff and funding to participate effectively. Under-resourcing, particularly among start-ups, can limit impact. Careful planning and allocation of financial and technical resources are critical to meaningful engagement.

12. Designate staff with appropriate legal, technical, and operational expertise to engage meaningfully.
Effective participation depends on having the right human resources in place. Organisations should appoint personnel with the necessary legal and technical expertise and establish a clear point of contact to ensure coherent, informed interaction with regulators.

13. Build a shared internal understanding of the sandbox's purpose, structure, and governance prior to participating.

Before entering, participants should ensure that all relevant teams understand the sandbox's aims, rules, confidentiality arrangements and expected commitments. Where key internal stakeholders do not fully understand the concept of a sandbox and its implications, sandbox projects are less likely to succeed.

14. Define the intended benefits and risks of participation, set measurable success criteria, and identify how technical, legal, and operational risks will be mitigated.

Each participant should establish a clear internal rationale for engagement, specifying expected benefits, measurable outcomes and risk-management strategies. This clarity enables both regulators and participants to focus on achievable objectives and meaningful learning.

15. Evaluate whether a sandbox is the most suitable mechanism for achieving the desired objectives, considering alternative experimentation tools where appropriate.

A sandbox should be selected only when it offers clear added value. Organisations should consider whether lighter-touch mechanisms, such as innovation advice services or testbeds, could achieve similar outcomes with fewer demands on their resources.

Sandboxes under the AI Act: A case study

Having reviewed the core design features of successful sandboxes across a range of prominent and formative examples worldwide, we now turn to the AI Act. The AI Act is rare in expressly embedding the concept of regulatory sandboxes into legislation, and in setting out a harmonised model across Member States. In this section, we use our broader research to examine the AI Act sandbox as a case study and to consider what an effective, responsible sandbox should look like in this new context.

The AI Act envisages coordinated EU regulatory sandboxes set up under a set of common rules to create a controlled testing environment in which organisations can explore new AI products or services in cooperation with competent regulators.[xxvi] By 2 August 2026, each EU Member State is required to have established at least one AI regulatory sandbox, to participate in an already existing sandbox, or establish a joint sandbox with another Member State.[xxvii] AI Act sandboxes will thus be widely available throughout the EU, open to all organisations and with a particular emphasis on including SMEs and start-ups.

Sandboxes under the AI Act are intended to support a number of goals: (a) enhance legal certainty to ensure regulatory compliance, (b) support the sharing of best practices between regulators and innovators, (c) encourage innovation, competitiveness, and the development of a robust AI ecosystem, (d) contribute to evidence-based regulatory learning to identify emerging risks, which will help shape future regulations, and (e) facilitate and accelerate market access by removing barriers for start-ups and SMEs.[xxviii]

The European Commission is charged with adopting implementing acts specifying the detailed arrangements for the establishment, development, implementation, operation, and supervision of the AI regulatory sandboxes. These rules are to include common principles on common eligibility criteria, procedures for application and participation, terms and conditions, monitoring, duration and extensions, exit and termination procedures, and the terms and conditions of participation.

Cross-regulatory collaboration in AI Act sandboxes

As Member States begin to implement the AI Act, a central question is how to ensure effective cross-regulatory collaboration, reflecting the reality that AI systems often cut across multiple sectors and oversight regimes. There are a number of prominent and mature sandbox projects already in existence across the EU and internationally and, encouragingly, the AI Act opens the door to leveraging these sandboxes whilst ensuring compliance with the obligations under the AI Act.[xxix] Furthermore, the cooperation with other relevant bodies in the operation of the sandbox, such as other sectoral regulators including data protection authorities,[xxx] is explicitly supported by the AI Act. This is currently envisaged under the proposed Dutch AI Act regulatory sandbox where all relevant sectoral regulators will be involved in one multi-sector sandbox with a single access point.[xxxi]

Cross-regulatory collaboration within a sandbox model can provide significant benefits. It enables participating organisations to receive comprehensive compliance guidance across sectors, thereby reducing fragmentation, fostering consistency, and supporting holistic solutions. At the same time, such collaboration is not without challenges. Multi-regulator sandboxes can increase complexity, extend timelines, and inadvertently create barriers to entry if not carefully designed and managed. Nevertheless, when done well, cross-regulatory collaboration has the potential to enhance legal certainty, strengthen trust, and ultimately drive responsible innovation.

Over time, these cooperation pathways could evolve into systemic models that can be replicated beyond sandboxes under the AI Act, enabling regulators in other areas such as online safety or cybersecurity to draw on solid methods of cross-regulatory collaboration.

Cross-border collaboration for AI Act sandboxes

In addition to ensuring the effective design and implementation as outlined above, the success of sandboxes under the AI Act specifically will also depend on how they support cross-border cooperation. While individual sandboxes must be robust in their own right, many of the most pressing challenges and opportunities in AI innovation are international or touch on multiple competencies by nature. Sandboxes that operate across multiple jurisdictions have the potential to present one solution to cross-border challenges by enhancing cooperation and capacity building between regulators and facilitating data sharing across borders.[xxxii] All organisations, and in particular start-ups and SMEs, can benefit from harmonised rules that support mobility between sandboxes.

Sandboxes under the AI Act are intended to increase collaboration across Member State borders. Not only will they be set up on the basis of common operating principles as previously mentioned, but the law itself requires that sandboxes be designed and implemented to facilitate cross-border cooperation.[xxxiii] To uphold the harmonisation objective of the AI Act, it is imperative that regulatory sandboxes in different Member States deliver consistent interpretations, processes, and outcomes. Divergent results from sandbox projects across jurisdictions would undermine legal certainty, fragment regulatory approaches, and contradict the Act's goal of a uniform internal market for trustworthy AI.

Sandboxes under the AI Act must be mutually recognised across Member States, including any sandboxes set up by the European Data Protection Supervisor (EDPS) for EU institutions.[xxxiv] This should mean in practice that an AI developer would not have to redo sandbox testing in every EU country, as one successful sandbox experience would ideally be recognised by all Member State authorities. The sandbox concept under the AI Act is aimed at increasing regulatory certainty for innovators by encouraging interoperability and the harmonisation of outcomes across borders.

However, ensuring efficiency in the implementation of harmonised sandboxes will require more than simply aligning rules; it will also depend on how regulators organise their resources and expertise. One possible approach is the development of a 'centre of excellence strategy', whereby individual Member States focus their sandbox activities on particular sectors or aspects of AI Act compliance. By doing so, regulators could pool knowledge, avoid duplication of effort, and build deep expertise in specialised domains such as healthcare, financial services, or general-purpose AI. This model has surfaced in other jurisdictions too, such as under the United States AI Action Plan proposing domain-specific hubs where government, industry, and academia collaborate to test and refine AI applications. These centres are intended to serve as regulatory sandboxes and knowledge platforms, developing standards, sharing data openly, and generating best practices tailored to sectors such as health, energy, and agriculture.[xxxv]

Industry-specific sandbox models may also present challenges, such as the risk of added bureaucracy and uneven uptake across Member States. Without cross-border consistency in application of the law or selection of participants, it could also result in Member States effectively 'picking winners' or favouring national interests. While this model is not without practical limitations, it offers a pragmatic means of addressing disparities in regulatory capacity among Member States, reducing duplication of effort and of fostering meaningful cross-border collaboration and learning across the EU.

Interoperability should also be understood not only as an EU-wide requirement for AI Act sandboxes, but as a principle for the next generation of regulatory experimentation. By reinventing sandboxes as systemic tools across the digital framework, consistent processes and mutual recognition can extend to other regulatory domains, ensuring coherence in oversight and reducing barriers to responsible innovation across the digital economy.

Integration with the wider EU AI innovation system

Sandboxes do not exist in a vacuum. They should be viewed within the wider 'EU Innovation System',[xxxvi] which aims to promote responsible innovation across the EU and beyond. When AI Act sandboxes are effectively realised, they will play an integral role in this critical innovation space, reducing the time to market for groundbreaking technologies and applications, and ensuring that regulators can foster safety and fairness.

The European Commission has proposed components to strengthen the EU Innovation System, which include:

- *Common European Data Spaces* to ensure that data from across the EU is available in a trustworthy and secure manner, for use across the economy and society;[xxxvii]
- *AI Factories* to leverage EU supercomputing capacity and support SMEs to develop and deploy trustworthy generative AI models;[xxxviii]
- *Test and Experimentation Facilities* (TEFs) to offer large-scale specialised reference sites open to all technology providers in the EU;[xxxix]
- *European Digital Innovation Hubs* (EDIHs) to support companies and public sector organisations with expertise, testing, finance, and training;[xl]
- *Public and private sector investment* is being mobilised, including €134 billion from the Recovery and Resilience Facility.[xli]

A harmonised AI regulatory sandbox regime complements this wider innovation system by ensuring that AI systems are not only technologically functional but also fit within the wider EU legal system and infrastructure. If implemented well, the AI Act sandboxes will ultimately reduce legal uncertainty for innovators and create an environment conducive to innovating and productivity.

Recommendations for AI Act regulators

The AI Act's objective of establishing harmonised and prescriptive sandboxes across multiple Member States introduces a new dimension to the design of regulatory sandboxes. Its success will hinge on effective implementation by regulators, the European Commission's AI Office, and participating organisations. Drawing on the AI Act's structure itself and lessons from existing sandboxes, CIPL sets out the following additional recommendations for competent authorities:

16. Define the respective roles and responsibilities of competent authorities and other stakeholders involved in AI Act sandboxes to ensure clear accountability and coherent decision-making.
AI Act sandboxes will often involve multiple authorities. It is therefore essential to clarify the roles and responsibilities of competent authorities and other relevant stakeholders in sandbox governance.

Clearly defining mandates, decision-making responsibilities and coordination mechanisms will ensure accountability, avoid duplication, and enable coherent oversight across participating authorities.

17. Promote interoperability and mutual recognition among AI Act sandboxes across Member States by aligning evaluation criteria, procedural frameworks, and outcome standards to support regulatory convergence and cross-border innovation and trust.
The EU should develop formal cooperation mechanisms to facilitate the alignment of evaluation criteria, procedural frameworks and outcome standards, enabling sandbox projects to maintain legal and operational continuity when transitioning across borders or sectors. Developing interoperable and mutually recognised processes will not only support regulatory convergence but also promote cross-border innovation and trust in the AI ecosystem. [xlii]

18. Promote national specialisation within AI Act sandboxes by building centres of excellence around specific sectors or national strengths, while enabling cross-border collaboration to share expertise and ensure coherence across jurisdictions.
To increase efficiency and reduce duplication, Member States should design their AI Act sandboxes to enable collaboration across jurisdictions. Where interoperable standards exist, Member States may also develop sandbox specialisations based on national expertise or sectoral priorities. Such specialisation can lead to the emergence of EU-wide centres of excellence, fostering deep expertise, minimising redundant efforts, and enhancing the overall quality and coherence of sandbox outcomes across the EU.

19. Establish pathways for cross-regulatory cooperation with other relevant competent authorities, including those responsible for data protection, online safety and financial services.
AI Act sandboxes should create structured pathways for efficient multi-authority collaboration, where necessary, involving relevant regulators such as those for data protection, the financial sector and online safety. Such cooperation will enable coordinated supervision and more comprehensive regulatory guidance for participants.

20. Integrate AI Act sandboxes with the wider EU AI innovation ecosystem, including TEFs, EDIHs, Data Spaces, and AI Factories, to expand access to expertise, infrastructure, and funding.
AI Act sandboxes should be actively connected with existing components of the EU AI innovation system, including Testing and Experimentation Facilities (TEFs), European Digital Innovation Hubs (EDIHs), Data Spaces and AI Factories. Access to infrastructure and finance through these channels may be particularly attractive to innovators seeking to scale across the EU.

21. Use insights generated through AI Act sandboxes (e.g. exit reports, aggregate findings) to strengthen EU-wide regulatory learning, with the AI Office coordinating a central resource hub to consolidate lessons, themes, and emerging best practices.
AI Act sandboxes should be positioned as a pillar of regulatory learning and knowledge sharing. Sandbox outcomes, such as exit reports or aggregate findings, should be easily shared across the EU and contribute to regulatory guidance or policy. The AI Office could coordinate a centralised EU-level resource hub that captures key learnings, thematic focus areas and common concepts emerging from sandbox activity.

Extending the sandbox model

The case for regulatory sandboxes extends well beyond the AI Act. Around the world, governments are confronting a common problem: how to regulate fast-evolving digital systems in a way that balances trust and innovation. Sandboxes provide a proven framework for this task, offering a structured environment for collaboration between regulators and innovators. Their success in fields from finance to transport demonstrates their value as a general-purpose governance tool for complex, technology-driven markets.

Across digital rulebooks, sandboxes have been most frequently adopted in data protection. The UK ICO launched the first data protection sandbox in 2019, followed by the Norway's Datatilsynet, Singapore's PDPC and France's Commission nationale de l'informatique et des libertés (CNIL). These initiatives have enabled practical testing of age assurance technologies, data-sharing frameworks and biometric recognition systems under supervision, generating insights that have informed updated regulatory guidance and codes of practice.

However, sandboxes could have much wider application across digital regulation. For example:

- In **online safety**, sandboxes could enable supervised testing of age assurance technologies, content moderation tools or design changes to mitigate harm under frameworks such as the EU Digital Services Act, the UK Online Safety Act and Australia's Online Safety Framework.

- In **data interoperability**, sandboxes could support pilots of data-sharing frameworks envisaged under the EU Data Governance Act and the UK Data (Use and Access) Act. These initiatives involve complex questions of consent, liability and technical standards that could benefit from live, supervised experimentation.

- In **cybersecurity**, sandboxes could be used to trial novel "secure-by-design" approaches under frameworks such as the EU NIS2 Directive, the Cyber Resilience Act and comparable regimes in the United States and elsewhere.

Better coordination across regimes will be essential if sandboxes are to fulfil their potential. Emerging technologies rarely fall neatly within one regulatory domain; for example, age assurance systems may use AI technology, process personal data and underpin online safety. Without structured cooperation, innovation risks being constrained by overlapping or inconsistent oversight. Cross-regime models can provide coherence, reduce duplication and deliver holistic guidance to innovators.

CASE STUDY: The Digital Regulation Cooperation Forum AI and Digital Hub (UK)

The Digital Regulation Cooperation Forum (DRCF) launched the AI and Digital Hub in April 2024 as a one-year pilot initiative to support innovation in the UK's AI and digital sectors. This Hub provided innovators with free, informal advice on complex regulatory questions that spanned the remits of multiple regulators, including the Competition and Markets Authority (CMA), the FCA, the ICO and Ofcom. By facilitating early engagement with regulators, the Hub enabled organisations to incorporate joined-up compliance considerations into their development processes from the outset.

As the regulatory landscape becomes more complex, sandboxes offer a practical means to align diverse policy objectives around a shared commitment to responsible innovation. By embedding cross-regulatory cooperation, shared learning and international interoperability, sandboxes can evolve from isolated pilots into a connected infrastructure for adaptive governance.

CIPL makes the following recommendation for other digital regulators:

22. Adopt regulatory sandboxes in digital regulatory regimes such as data protection, online safety, data interoperability or cybersecurity to unlock responsible innovation, coordinating across regulatory domains where necessary.
Regulators should pilot sandbox approaches under other digital frameworks where technological evolution is rapid and regulatory interpretation remains uncertain, such as data protection, online safety, data interoperability and cybersecurity. To ensure coherence, regulators with overlapping mandates should coordinate sandbox activities to enable shared learning and consistent oversight.

Conclusion

The insights that can be gleaned from existing regulatory sandboxes, particularly the prominent models that we examined in this paper, reaffirm the core principles already recognised in CIPL's work: transparency, legal certainty, collaborative engagement, and proportionate, risk-based oversight. These remain the hallmarks of effective and trusted regulation.

What has changed is the regulatory context. With the AI Act mandating sandboxes across Member States, what began as experimental practice is now a formal regulatory instrument. This creates both opportunity and responsibility. Properly implemented, AI Act sandboxes can fulfil the promise of regulatory innovation by providing legal certainty for developers, enabling proactive supervision by regulators, and accelerating the responsible deployment of AI across the EU.

To achieve this, sandboxes must be more than a legal requirement. They should be interoperable across Member States, embed data protection and other competent authorities in their governance, and offer clear incentives and safeguards for participants. Integration within the wider EU AI innovation ecosystem will be essential, as will mechanisms for sharing outcomes and lessons across the regulatory community through meaningful guidance, shared learnings, and eventual contributions to the evolution of law and policy. If approached in this way, AI Act sandboxes can become a cornerstone of the EU's responsible innovation agenda.

At the same time, CIPL sees a timely opportunity to expand this approach beyond the AI Act. Sandboxes can also play a role in other fast-moving digital regulatory regimes where they can serve as testbeds for responsible innovation and foster cross-regulatory cooperation. Sandboxes may also be suited to online safety, cybersecurity, or wider data governance frameworks. A broader, systemic approach would ensure that the benefits of regulatory experimentation extend across the full digital ecosystem and not just AI.

Annex: Overview of the common criteria of five example prominent sandboxes

Criteria	FCA (UK)	ICO (UK)	IMDA GenAI (Singapore)	IMDA PETs (Singapore)	CNIL (France)
Geographic Scope	Must target the UK market and fall under the FCA's regulatory remit.	Must operate under UK data protection law; applicable to UK-based data processing.	Open to Singapore-based SMEs.	Open to companies operating in Singapore.	Projects must involve AI applications within French public services.
Innovation Focus	Requires genuine innovation that is ground-breaking or significantly different.	Focus on innovative products/services using personal data.	Emphasis on generative AI solutions for SMEs.	Focus on Privacy Enhancing Technologies (PETs) to enable data collaboration while ensuring privacy.	Projects should explore AI applications that enhance public service delivery.
Development Stage	Applicants must be ready to test in a controlled environment.	Open to various stages, from proof-of-concept to scaling, provided practical feasibility is demonstrated.	Projects should be at a stage ready for pilot testing.	Projects should be ready to pilot PETs in real-world scenarios.	Projects should be in early development stages to benefit from CNIL's guidance.
Support Provided	Regulatory oversight and guidance during testing.	Bespoke support plan, including data protection advice and compliance support.	Access to AI tools, resources, and potential funding opportunities.	Technical support, matchmaking with PET solution providers, and regulatory guidance.	Expertise from CNIL's AI department and assistance in aligning with data protection regulations.
Application Requirements	Must demonstrate in-scope activity, genuine innovation, consumer benefit, readiness for testing, and need for sandbox support.	Must show intent to develop innovative personal data applications under UK law; lead organisation required for consortium applications.	Applicants should be SMEs in Singapore with generative AI projects ready for testing.	Applicants should have use cases for PETs and be prepared to collaborate with solution providers.	Applicants must be public bodies or entities working on AI projects aimed at improving public services in France.

[i] The Centre for Information Policy Leadership (CIPL) is a global privacy and data policy think tank within the Hunton law firm that is financially supported by the firm, 85+ member companies that are leaders in key sectors of the global economy, and other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

[ii] This paper refers to 'sandboxes' as regulatory sandboxes, rather than sandboxes as a general term which encompasses technical sandboxes or other purely technical testing that can take place without the presence of a regulator.

[iii] The practice of controlled regulatory trials had already been used to pilot innovative solutions under regulatory supervision. For instance, before the FCA formally introduced the term 'regulatory sandbox', national authorities employed regulatory pilots or experimentation projects in sectors such as energy, e.g., the Netherlands' Crisis and Recovery Law enabling pilot exemptions for smart-grid projects and pharmaceuticals/medical, e.g., the European Medicines Agency's Adaptive Pathways pilot (2014–2016) and conditional marketing authorisations.

[iv] See Annex 1 for a broad list of regulatory sandboxes.

[v] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) 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.

[vi] CIPL Paper, 'Regulatory Sandboxes in Data Protection - Constructive Engagement and Innovative Regulation in Practice', 2019.

[vii] Regulation (EU) 2016/679 of the European Parliament and of the 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.

[viii] The outcomes of the interviews have been aggregated into one overall picture, and we have not reproduced individual details. Any reference made to examples of sandboxes is to publicly available information.

[ix] With thanks to the following organisations and institutions who provided thoughts and comments: France – Commission Nationale de l'Informatique et des Libertés (CNIL), United Kingdom – Information Commissioner's Office (ICO), United Kingdom – Digital Regulation Cooperation Forum (DRCF), United Kingdom – Financial Conduct Authority (FCA), EU Commissioner AI Office, Lithuania – Innovation Agency Lithuania, Norway – Datatilsynet (Norwegian Data Protection Authority), Singapore – Infocomm Media Development Authority (IMDA), Spain – Agency for the Supervision of Artificial Intelligence (AESIA), Ministry of Economic Affairs and Digital Transformation (development of the Spanish Strategy on Artificial Intelligence), Netherlands – Dutch Data Protection Authority (Autoriteit Persoonsgegevens, AP), Allied for Startups, CitCom, OdiseIA, Duality.

[x] For instance, the ICO's feedback from sandboxes highlighted two key areas of positive feedback from participants: They were able to better apply the data protection requirements in relation to their innovative product and they also estimated significant cost savings of up to £500,000 from overheads, including legal or consultancy services, increasing operational efficiency and better facilitating partnerships. ICO, 'Regulatory Sandbox Insights Report', 2024.

[xi] The FCA found that their sandbox firms are 50% more likely to raise funding than their peers and, on average, raise 15% more in investment. FCA, '10-year anniversary FCA innovation services', 2024.

[xii] Brian R. Knight and Trace E. Mitchell, 'The Sandbox Paradox: Balancing the Need to Facilitate Innovation with the Risk of Regulatory Privilege', 2020.

[xiii] The CNIL has launched sandboxes in digital health and EdTech, and more recently, it has been focusing on AI for public services. CNIL, 'Digital health and EdTech: the CNIL publishes the results of its first sandboxes' and 'Artificial intelligence and public services: the CNIL publishes the results of its 'sandbox', 2025.

[xiv] FCA, 'Our Innovation Services', 2022.

[xv] *Supra, n.xxxi.*

[xvi] See this report, Canton of Zurich, ‘Play & Learn: How to strengthen an AI hub with a sandbox’, 2024.
[xvii] European Commission, ‘Staff working document Regulatory learning in the EU Guidance on regulatory sandboxes, testbeds, and living labs in the EU, with a focus section on energy’, 2023.
[xviii] *Ibid*.
[xix] CIPL, supra n.**Error! Bookmark not defined.**.
[xx] IMDA, ‘Singapore’s first generative AI Sandbox to familiarise and help SMEs get a head start in capturing new AI opportunities’, 2024.
[xxi] FCA, ‘FCA allows firms to experiment with AI alongside NVIDIA’, 2025.
[xxii] Supra n.xx.
[xxiii] ICO, ‘What will happen if our application to the Sandbox is successful?’
[xxiv] As recommended in the UK Government ‘AI Opportunities Action Plan’ and further developed in the ICO’s ‘Response to Government Economic Growth’.
[xxv] Datatilsynet, ‘Sandbox Exit Reports’.
[xxvi] AI Act Article 57(5) AI Act.
[xxvii] AI Act Article 57(1) AI Act.
[xxviii] AI Act Article 57(9) AI Act.
[xxix] Recital 139 AI Act states that “where appropriate, relevant competent authorities in charge of those other regulatory sandboxes should consider the benefits of using those sandboxes also for the purpose of ensuring compliance of AI systems with this Regulation”.
[xxx] The CNIL, for instance, has stated they will require being consulted beforehand and verify compliance with a number of requirements. CNIL ‘Entry into force of the European AI Regulation: the first questions and answers from the CNIL’, 2024.
[xxxi] AP, ‘Proposal Dutch regulatory sandbox’, 2025.
[xxxii] See Datasphere, ‘Sandboxes for data: creating spaces for agile solutions across borders’, 2022; OECD ‘Regulatory Sandboxes in Artificial Intelligence’, 2023.
[xxxiii] AI Act Article 57(13).
[xxxiv] AI Act Article 58(2)(g) AI Act.
[xxxv] America’s AI Action Plan, White House, July 2025.
[xxxvi] European Commission, ‘AI innovation package to support Artificial Intelligence startups and SMEs’, 2024.
[xxxvii] European Commission, ‘Common European Data Spaces’.
[xxxviii] European Commission, ‘AI Factories‘.
[xxxix] European Commission: ‘Sectorial AI Testing and Experimentation Facilities under the Digital Europe Program‘.
[xl] European Commission: ‘European Digital Innovation Hubs‘.
[xli] European Commission: ‘European approach to artificial intelligence‘.
[xlii] While interoperability is a critical goal, it is important to acknowledge its limitations: Divergences between Member States will inevitably remain, particularly where the AI Act permits differences in national law or regulatory practice.