Information Commissioner’s Office

Sandbox beta phase discussion paper

ico.
Information Commissioner’s Office

Sandbox beta phase discussion paper

What is the purpose of the sandbox?

The ICO Sandbox is a key commitment in our Technology strategy 2018-21 and supports the dual aims of privacy and innovation.

The purpose of the sandbox is:

1) to support the use of personal data in innovative products and services that can be shown to be in the public interest;

2) to help develop a shared understanding of what compliance in particular innovative areas looks like; and

3) to support the UK in its ambition to be an innovative economy.

We have reflected these purposes in the criteria, mechanisms and operational approach we have taken to the design of the sandbox.

What is the ICO sandbox beta phase?

The ICO sandbox beta phase is a fully functioning test of the ICO's sandbox over a defined period. If the beta phase is successful, the sandbox will then form a part of our regulatory toolkit.

In this beta phase, we will aim to involve around 10 organisations of different types and sizes ideally from across from the private, public and third sectors. We will particularly welcome applications for products or services that address specific data protection challenges central to innovation.

These challenges are:

- use of personal data in emerging or developing technology such as biometrics, internet of things, wearable tech, cloud-based products;
- complex data sharing at any and all levels;
- building good user experience and public trust by ensuring transparency and clarity of data use;
- perceived limitations, or lack of understanding of the General Data Protection Regulation and Data Protection Act 2018 provisions on automated decision making, machine learning or AI; and
- utilising existing data (often at scale and in linking data) for new purposes.

Whilst we will welcome applications that address these issues these are not exclusive and we are open to other innovative ideas that are in the public interest.

Discussion Question: Do our data protection challenge areas seem appropriate? Are there other specific challenges we should consider? Are there any that should be removed?

Successful applicants will sign up to a bespoke plan that will define how the sandbox will work for them and what support the ICO will provide. We will work in partnership with organisations to define and agree, execute and monitor this plan and manage exit from the sandbox.

Each sandbox plan will contain a number of mechanisms depending on the product or service. The mechanisms available to organisations in the sandbox have their origins in the NESTA paper, “Regulation Renewed”, which identifies three techniques that regulators can use to deal with innovation. These are:

- **Advisory regulation**: ensuring innovative products and services meet existing regulatory requirements, and support innovators in bringing compliant products to market.
- **Adaptive regulation**: adapting regulatory frameworks, and removing potentially unnecessary regulatory barriers to innovation.
- **Anticipatory regulation**: identifying and enabling monitoring of emerging but uncertain opportunities or risks, and supporting timely responses.

Our sandbox seeks to provide mechanisms in all three areas. We provide a suggested list below but we will welcome suggestions from applicants as to how this may work in practice and ideas we may not have considered. Organisations will be able to request a mixture of mechanisms across all three areas, as appropriate to their product or service, and these will be agreed as part of their sandbox plan.

Advisory Mechanisms

As supported by the outcome of our call for views, one of the main offers in the sandbox would be the provision of informal advisory mechanisms. These could include activity such as:

- phased or iterative ‘informal steers’ – from idea and concept to prototyping;
- informal supervision of product or service testing;
- processing ‘walkthroughs’ – step by step analysis of proposed processing activity, leading to informal advice;

- workshops with design and development teams at an early stage in order to inform very early thinking; or
- informal steers on risk mitigation and privacy by design/default.

This is an indicative, suggested list. How these advisory mechanisms work in practice would need to be shaped around the product or service being tested and will be planned for each organisation when their sandbox plan is developed.

Discussion Question: What other mechanisms could we use to provide informal steers? How can we ensure that these are beneficial?

Adaptive Mechanisms

The legal requirements contained within GDPR and the Data Protection Act 2018 (DPA18) cannot be changed through the sandbox and are in no way relaxed for participating.

We will always reserve the right to take whatever action we consider appropriate in respect of any breach, whether suspected or actual. However, we do have some discretion in our approach to regulating data protection law.

We plan, therefore, to operate with two flexible mechanisms:

1) comfort from enforcement for participants on entry; and

2) letters of negative assurance on exit.

It is also possible that products/services that come into the sandbox cause us to think about what adaptations to our regulatory approach may be needed, or what advice we may want to give to Government or others on adaptations they should consider.

Comfort from enforcement

We will be clear when accepting organisations into the sandbox that, provided they are taking appropriate steps to try to comply, any accidental breach of data protection legislation during the sandbox process will not lead immediately to enforcement action.

As set out in our Data Protection Regulatory Action Policy, before any enforcement action is taken, there will be a period of interaction between our officers and the organisation to establish the facts. We will then decide whether to take any action and, if so, what that should be.

We expect there would be ongoing discussions between ourselves and sandbox participants to ensure that any concerns we raised were addressed.

If the organisation in the sandbox reports breaches to us immediately, the relevant processing ceases, and concerns are then addressed in a timely and satisfactory manner, then we would be very unlikely to take any action. This comfort from enforcement would be subject to organisations maintaining a productive dialogue with the ICO throughout the sandbox process.

Letters of negative assurance

One of the mechanisms that can be requested by participants as part of their sandbox plan will be a letter of negative assurance. This is designed to provide information about the product or service in respect of its compliance with data protection legislation.

Assuming all conditions set out within the sandbox plan have been met, these letters would be issued to participants on exiting the sandbox and would confirm that at the point the relevant product or service transitioned out of the sandbox, we saw nothing to indicate its operation would breach data protection legislation and that any potential areas of concern or potential breaches were resolved.

This confirmation would be provided on the basis of the information provided to us during an organisation's participation in the sandbox and would only apply to the product or service tested in the sandbox. We would retain the right to change our view and to revoke this confirmation based on future legal or market developments, or if we were made aware of information we have not previously seen.

If the product breaches data protection laws in the future, then all liability would sit with the organisation and not the ICO.

Discussion Question: Will these mechanisms be of benefit to potential participants? Are there any other areas of ICO's approach that could be adapted to support innovators in achieving compliance?

Anticipatory Mechanisms

Products and services that come into the sandbox may be at the cutting edge of what is possible within their field. They may be operating in some particularly challenging areas of data protection or areas where there is genuine uncertainty about what compliance looks like.

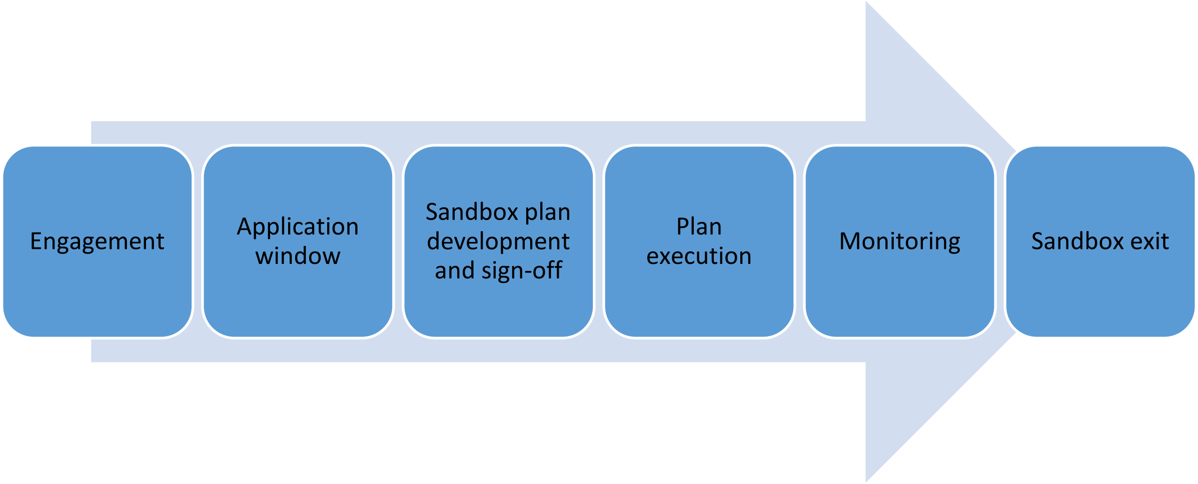
We want to be open to these products and services coming into the sandbox. In these cases, more fundamental questions may be identified, with broader implications for data protection. We may then treat these products or services as a 'use case' to develop specific public information or guidance on compliance or to consider what future regulatory provision may be desirable.

Discussion Question: We want the sandbox to genuinely push our understanding of what compliance looks like so we can anticipate what changes to regulatory approaches may be needed in future. What areas might this be most useful in? What kind of outputs might be produced as a result?

What is the beta phase operating model?

The sandbox will be a structured journey through a number of defined stages over a defined period from July 2019 to September 2020. Individual organisations may exit well before September 2020, however, depending on their specific journey. The length of time spent in the sandbox will be flexible and agreed on a case-by-case basis – we are just as open to short focussed engagements on specific issues as to larger complex challenges that take the full year.

We aim to publish full details of our sandbox beta phase online by the end of March, and to open applications near the end of April.



Engagement

Our sandbox team is available now to discuss how it might assist an organisation's development of innovative products and services. They can also provide information and guidance on the application process. All queries should be sent to sandbox@ico.org.uk.

Informal engagement will be available throughout the sandbox application window. Staff will not invite draft submissions or provide drafting assistance but will be available to explain the criteria and what is required. They can also provide informal advice on what the organisation might need to consider when completing the application.

Application window

The application window should be open at the end of April. Applicants will need to provide information regarding how they meet our threshold eligibility criteria, along with a number of other factors we will need to consider. They will also need to set out what sandbox mechanisms they wish to make use of and a plan for how they would like to work with the sandbox.

We will be open and transparent in the approach we take to applications, and have created some draft indicators (See Annex A) that we plan to use to help assess applications and to guide applicants.

Our three key threshold eligibility criteria for entry into the sandbox are:

- Innovation
- Public interest
- Data protection maturity and accountability.

Innovation

We want to welcome products and services into the sandbox that are genuinely innovative. We will use the definition of innovation set out by the Department for Business, Energy and Industrial Strategy (BEIS):

Innovation is the application of new knowledge to the production of goods and services; it means improved product quality and enhanced process effectiveness.[1]

Applicants will need to demonstrate how new knowledge is being applied to improve product quality or enhance process effectiveness.

Public interest

We want to accept products and services into the sandbox that deliver demonstrable public benefit. This will be interpreted broadly to include any positive benefit to the public, and will be assessed on breadth, eg how many people benefit, or depth, eg how much benefit, or a combination of both. The assessment will be based on quantitative and qualitative evidence provided by the applicant.

Organisational data protection maturity and accountability

We want organisations to demonstrate a mature and accountable approach to data protection. We will require applicants to complete our data controller self-assessment checklist and submit the results with their

[1] BEIS Economics Review 'Innovation and Research Strategy for Growth' 2011

application. We would also reserve the right to request any information referred to in that assessment, should we feel it necessary to assess the organisation's maturity.

Other factors

In addition to these criteria, we will consider a number of other factors in selecting sandbox participants for the beta phase. These are laid out below and will be reflected where appropriate in the application form.

a. Getting a balance of size, sector and type of organisation. This will be dependent on the applications we receive but ensuring a broad mix of organisations will be important in testing our approaches.
b. Any recent data protection incidents or ICO enforcement action. We do not consider that previous enforcement action or reported incidents should be a clear-cut bar to entry to the sandbox. However, we would need to consider their severity and relevance to the application when making our decision on entry to the sandbox.
c. Whether and what data innovation challenge they are planning to address.
d. Our own resources and capabilities. We will not commit ourselves to working with a product or service that is beyond our resource capacity or our knowledge and expertise. We will use the application and assessment process to identify what these are likely to be, and whether we can meet them, want to meet them, or need to obtain additional resources to do so
e. Other regulatory remits. We will need to be conscious of other regulatory remits and where products and services are in any associated processes.
f. The viability of proposed sandbox plans. While we expect to develop an agreed plan with each organisation in the sandbox, we need to take a view on whether the proposal is viable. This would include issues such as what risk assessment they would undertake and what controls they would have in place, what their exit strategy will be, and how they would protect data subjects' rights.

Assessing applications

Applications will be assessed against the threshold criteria, the viability of the proposed plan and considering the other factors set out above. Assessment will be made by a panel of ICO staff members.

Applications will be assessed against the threshold criteria indicators using a four-point scale (as set out in Annex A).

- If applicants receive a score of one point for innovation or public benefit they will be automatically barred from entry.
- The data protection maturity threshold will be set at three points minimum unless the organisation is a micro organisation where a score of two will be accepted on the condition that we are happy with the risk assessment and mitigation they have undertaken.

We will also undertake an initial review of the proposed sandbox plan, again on a four-point scale (as set out in Annex B). The combined total of the sandbox plan viability will be added to the eligibility scores to give an overall score.

We aim to notify organisations whether or not they have been successful in early July. Successful applicants will receive a sandbox entry letter including full terms and condition of participation.

Discussion Question: Do you have any feedback on our proposed application process? Do the indicators set out in Annex A provided a helpful guide? Are there any other factors we should be considering in assessing applications?

Sandbox plan development

We will assign a team member to work with the organisations who are accepted into the sandbox. The first step will be an introductory meeting to:

a. get a detailed understanding of the product or service;
b. get a detailed understanding of the data protection issues the organisation wishes to address;
c. answer any queries outstanding from the application process;
d. determine whether we are likely to have any additional resource requirements to support the organisation; and
e. further explore applicants’ readiness to participate.

The team member will then work with the organisation to develop a proposed sandbox plan within a maximum eight to ten-week period. Once agreed, this will form the basis of the organisation’s participation in the sandbox. We are aiming for all plans to be signed off by September. However, if a sandbox plan can be agreed earlier within this period, the organisation will be able to commence its plan.

Sandbox plan execution

Execution of sandbox plans and their start dates will differ depending on the nature of the plan agreed. Sandbox staff will work with organisations and with colleagues across the ICO to ensure the plan is delivered as agreed.

Monitoring

Monitoring will be specific to the individual sandbox plan, taking account of the risks involved in the project, with high-risk plans monitored more closely and frequently. However, in all cases we would expect there to be a minimum of three formal face to face meetings.

1. Sandbox plan launch meeting, to talk through practical arrangements, timescales of activity and mutual expectations.
2. Mid-point evaluation and stock-take, to review progress.
3. Exit meeting at end of sandbox participation.

Changes to the plan

We recognise that plans may well need to change:

a. Minor changes would be agreed by the sandbox team on an ad hoc basis
b. Material changes that stay within the original intentions and resource needs of the original sandbox plan would be agreed within the sandbox team. The plan documentation would be updated and a log kept of any changes.
c. Significant changes that either alter the intention of the plan or create additional resource needs for the ICO would need to be reconsidered.

Organisation conduct

We reserve the right to terminate sandbox participation at any time. However, this would not be undertaken unreasonably or without appropriate notice. Full details will be developed and set out within the sandbox terms and conditions. However reasons for ejection might include:

a. Repeated failure to provide documentation on request within any reasonable pre-agreed time period;
b. Failing to comply with any mandatory requirements of sandbox participation;
c. Failing to engage with us in a transparent and professional manner;
d. Enforcement action being taken against the organisation that is either sufficiently severe or relevant to the product or service that it undermines our confidence in the organisation’s ability to participate; or

e. Information coming into the public domain about the organisation that could potentially damage the reputation of the ICO through association (e.g. criminal proceedings).

Sandbox exit

At the end of the sandbox process, the team plan to hold a final meeting with the organisation to evaluate the process, seek feedback and write the sandbox exit report. The report will summarise the process and the key activity that was undertaken and whether the initial objectives have been met.

If pre-agreed as part of the sandbox plan, and all relevant conditions of that plan have been met, we will issue a letter of negative assurance following the final meeting.

Will the ICO keep information about products and services in the sandbox confidential?

The ICO sandbox team is bound by strict obligations of confidentiality by Section 132 of the DPA 2018. This includes confidential information that relates to an identified or identifiable individual or business provided as part of the sandbox process.

Staff working on the sandbox team will only share information about a product or service with other ICO staff as is necessary to undertake sandbox work or if it is not in breach of our confidentiality obligations.

As a public authority we are subject to the Freedom of Information Act 2000 (FOIA) and so are legally required to respond to any FOIA requests we receive, which may include requests for information provided to us in relation to the sandbox.

We will treat any FOIA request made to us on a case-by-case basis and organisations should therefore make it clear to us which information they provide to us they consider confidential or commercially sensitive and why. Should we then receive a request for information, we would consider what, if any exemption applies, bearing in mind the exemptions in Section 41 (information provided in confidence) Section 36 (conduct of public affairs) and Section 43 (commercial interests) of the FOIA, as well as any other relevant exemptions.

This approach to confidentiality will not preclude us mutually agreeing with participants public information about their involvement, such that it can be shared with third parties.

How does the sandbox relate to DPIAs?

Requirements under the GDPR to undertake a Data Protection Impact Assessment (DPIA) in respect of high-risk processing activities, and our processes for DPIA consideration as set out on our website, will continue to apply.

At the sandbox application stage, we will require applicants to identify if their product or service presents such a high risk, based on the current DPIA guidance on our website, and remind them of their responsibilities in this area. We will also ask for information about how they intend to mitigate that risk and consider it as part of the application process, and if they are then successful as a key element of agreeing that organisation's sandbox plan.

The sandbox team will then be able, if agreed within that organisations sandbox plan, to provide informal advice on risk mitigation that might need to be considered in completing a DPIA. However, there is no formal requirement for DPIAs to be submitted to ICO unless the DPIA indicates risk has not been mitigated and an organisation wishes to commence processing.

If undertaking new processing (e.g. through live testing) is part of the agreed sandbox plan then we will need to be assured that risks have been appropriately mitigated before that processing can start.

If in the course of working with an organisation it becomes clear that the residual risks are still high**,** and the organisation wishes to start the relevant processing, the sandbox team will remind the organisation that it needs to submit a DPIA for prior consultation before any new methods of processing are used.

If an organisation then decides not to submit its DPIA, sandbox participation will end immediately. If we then become aware that the processing in question has started, enforcement action could be taken within the usual parameters of our regulatory action policy. We may also consider the refusal to consult or engage with the ICO as a factor in any subsequent action.

Prior consultation with the ICO regarding a sandbox participant's DPIA

If prior consultation regarding a DPIA relating to a sandbox participant is undertaken with the DPIA team, participation in the sandbox will be paused, contact with the sandbox team will cease and new processing must not start until we have delivered the outcome of that DPIA process. We will review ongoing sandbox participation at that point on a case by case basis, and depending on the outcome of that process.

Discussion Question: Does our approach to handling the interface between DPIAS and sandbox participation appear effective?

Annex A: Indicators – Threshold Criteria

Indicators	1	2	3	4
Innovation	*Product or service is clearly a reworking of an existing approach.* *Limited or no comparison with other approaches to show how they are innovative.*	*Information provided shows that there is likely to be some form of innovation being undertaken* *Some form of comparison with existing approaches is made that shows the difference and innovation.*	*The innovation present is clear to the reader with use of effective qualitative and quantitative evidence.* *Comparisons with existing approaches are specific, relevant, and well-evidenced.*	*The innovation present is likely to be transformative as shown through effective qualitative and quantitative evidence.* *Comparisons with existing approaches are specific, relevant, and well-evidenced.*
Public Benefit	*Product or service does not clearly benefit the public beyond the organisational benefit of the submitting organisation.* *Limited or no attempt to quantify the breadth or depth of benefit to the*	*Product or service is likely to bring some benefit to the public beyond the benefit of the submitting organisation.* *A reasonable attempt is made to quantify that public benefit in terms of breadth and depth and supported with*	*The breadth and depth of public benefit created by the product or service is clear and substantive.* *Effective qualitative and quantitative evidence is provided to support the application.*	*The breadth and/or depth of public present is likely to be significant and transformative.* *Compelling qualitative and quantitative evidence is provided.*

Indicators	1	2	3	4
	public of the product or service.	*some quantitative or qualitative evidence*		
DP Maturity	*DP checklist is RED – There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. Immediate action is required to improve the control environment.*	*DP checklist is AMBER – There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. There is considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.*	*DP checklist is YELLOW – There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. There is some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.*	*DP checklist is GREEN – There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. There is only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.*
Sandbox plan viability	*Plan objectives are clearly not Specific Measurable Achievable Realistic and Timely (SMART)*	*A clear effort has been made to make objectives SMART* *Mechanisms proposed related to the*	*Plan objectives are SMART and clearly relate to the intended purpose*	*Plan objectives are SMART and clearly relate to the intended purpose with potential for further stretch in ambition beyond them.*

Indicators	1	2	3	4
	Mechanisms proposed do not clearly look like they will deliver the objectives and/or fall within the scope of our suggested approach *The organisation does not appear to have sufficiently mitigated any of the risks they raise.* *Exit plan has clear deficiencies and/or does not adequately mitigate risks or provide redress.*	*objectives they wish to achieve.* *There are clear risk mitigations and control mechanisms in place that appear efficient and effective.* *There is a clear exit plan in place that clearly attempts to mitigate risk to participants and provide redress where needed.*	*Mechanisms have been well thought through, clearly relate to the objectives with clear relation to timescales and resources likely to be needed.* *There are risk mitigations and control mechanisms in place that appear efficient and effective.* *There is a clear exit plan that clearly evidences how risks will be mitigated and any redress needed will be provided.*	*Mechanisms have been well thought through, clearly relate to the objectives with clear relation to timescales and resources likely to be needed.* *There are sophisticated risk mitigations and control mechanisms in place that have been shown to be efficient and effective through the provision of evidence.* *There is a clear exit plan that clearly evidences how risks will be mitigated, how any redress needed will be provided, and in effect ensure a 'failsafe' approach.*

Annex B: Indicators – Sandbox Plan Viability

Indicators	1	2	3	4
Sandbox plan viability	*Plan objectives are clearly not Specific Measurable Achievable Realistic and Timely (SMART)* *Mechanisms proposed do not clearly look like they will deliver the objectives and/or fall within the scope of our suggested approach* *The organisation does not appear to have sufficiently mitigated any of the risks they raise.* *Exit plan has clear deficiencies and/or does not adequately mitigate risks or provide redress.*	*A clear effort has been made to make objectives SMART* *Mechanisms proposed related to the objectives they wish to achieve.* *There are clear risk mitigations and control mechanisms in place that appear efficient and effective.* *There is a clear exit plan in place that clearly attempts to mitigate risk to participants and provide redress where needed.*	*Plan objectives are SMART and clearly relate to the intended purpose* *Mechanisms have been well thought through, clearly relate to the objectives with clear relation to timescales and resources likely to be needed.* *There are risk mitigations and control mechanisms in place that appear efficient and effective.* *There is a clear exit plan that clearly evidences how risks will be mitigated and any redress needed will be provided.*	*Plan objectives are SMART and clearly relate to the intended purpose with potential for further stretch in ambition beyond them.* *Mechanisms have been well thought through, clearly relate to the objectives with clear relation to timescales and resources likely to be needed.* *There are sophisticated risk mitigations and control mechanisms in place that have been shown to be efficient and effective through the provision of evidence.* *There is a clear exit plan that clearly evidences how risks will*

Indicators	1	2	3	4
				be mitigated, how any redress needed will be provided, and in effect ensure a ‘failsafe’ approach.