# Regulatory Sandbox beta review

Date: November 2021

Information Commissioner's Office

# Contents

1. Introduction ..... 3
2. Overview of participants ..... 5
3. Key lessons learned ..... 8
4. Feedback from beta phase participants ..... 18
5. Impact of the Sandbox ..... 20
6. What's next? ..... 21

# 1. Introduction

## What is the Regulatory Sandbox?

1.1 The Regulatory Sandbox is a service developed by the ICO, to support organisations who are creating products and services which utilise personal data in innovative and safe ways.

1.2 Participants have the opportunity to engage with our Sandbox team, to draw upon our wider ICO expertise and advice on mitigating risks and embedding 'data protection by design'.

1.3 The Sandbox provides a free, professional, fully functioning service for organisations, of varying types and sizes, across a number of sectors.

## What are benefits of the Sandbox?

1.4 The benefits of the Sandbox include the following:

- access to ICO expertise and support;
- increased confidence in the compliance of the participants' finished product or service;
- participants have a better understanding of data protection frameworks and how these affect businesses;
- increased consumer trust in the participant's organisation as they are seen as accountable and proactive in their approach to data protection;
- the opportunity to inform future ICO guidance;
- the ability to support the UK in its ambition to be an innovative economy; and

- contribute to the development of products and services that can be shown to be of value to the public.

## What was the beta phase?

1.5 In autumn 2018, the ICO launched a call for views on a potential data protection Sandbox. This consultation concluded with a face-to-face workshop with organisations interested in the Sandbox in London in early 2019. The Sandbox team used the feedback to create the beta phase Sandbox procedures and we opened for applications in March 2019. By September 2019, following 65 applications and a rigorous selection criteria, we accepted a sample of organisations to try out the service.

1.6 Organisations had to meet core criteria. They had to show that their product or service was:

- innovative in its use of personal data,
- of demonstrable public benefit, and
- operating in a genuinely challenging or 'grey area' of data protection law.

1.7 We established the high-level general areas of innovation that we were interested in, but these were intentionally very broad as we did not want to unnecessarily limit demand in the beta phase.

1.8 Each organisation signed terms and conditions and entered the Sandbox project. We then conducted a scoping visit, from which we developed and agreed a bespoke sandbox plan setting out what we would do with the organisation.

1.9 We initially planned for the participants to remain in the Sandbox for no more than 12 months. However six months into the project, the COVID-19 pandemic hit which naturally caused delays both for the ICO and the

participants. Despite the challenges, we were able to successfully exit nine of the original ten participants between June 2020 and March 2021.

# 2. Overview of participants

2.1 The ten participants that were chosen to participate were as follows:

- **FutureFlow:**
  FutureFlow is a RegTech start-up designing a Forensic Analytics platform that monitors the flow of funds in the financial system. Its platform enables multiple financial institutions, regulators and agencies to leverage each other's intelligence on Electronic Financial Crime without heavy reliance on personal data. This collaborative approach to tackling financial crime opens the prospect of higher detection rates with lower false positives, while reducing the burden of scrutiny on each individual and business consumer.

- **Greater London Authority (GLA):**
  In order to reduce levels of violence in London, the Mayor has set up a Violence Reduction Unit (VRU) which is taking a public health approach to this issue. As part of this work, the VRU needs to better understand how public health and social services can be managed to prevent and reduce crime, with a focus on early intervention. There is increasing interest from the VRU, the Mayor's Office of Policing and Crime (MOPAC) and the Greater London Authority (GLA), for health, social and crime data to be looked at in an integrated and collaborative way.

- **Heathrow Airport Ltd:**
  Heathrow Airport's Automation of the Passenger Journey programme aims to streamline the passenger

journey by using biometrics. Facial recognition technology would be used at check-in, self-service bag drops and boarding gates to create a seamless experience for passengers travelling through the airport. Current processes require passengers to present different forms of documentation, such as boarding cards and passports, at different points in their journey to prove their identity and show that they are authorised to travel. By offering passengers the option of using facial recognition technology they would have the choice to enjoy a frictionless journey through the airport.

- **Jisc:**
  Jisc is developing a Code of Practice with universities and colleges wishing to investigate the use of student activity data to improve their provision of student support services. This will help them protect both privacy and wellbeing.

- **The Ministry of Housing Communities and Local Government (MHCLG):**
  The Ministry of Housing, Communities and Local Government's project partners with Blackpool Council and the Department of Work and Pensions and seeks to match personal information controlled by multiple parties to create a dataset that will allow MHCLG to understand more about the private rented sector in Blackpool, who lives there, and how they can help improve the quality of properties.

- **NHS Digital:**
  NHS Digital is working on the design and development of a central mechanism for collecting and managing patient consents for the sharing of their healthcare data for secondary use purposes, including medical research and regulated clinical trials.

- **Novartis Pharmaceuticals UK Limited:**

Novartis is exploring the use of voice technology within healthcare. Through its Voice Enabled Solutions project, Novartis is working with healthcare professionals to design solutions to make patient care easier and addressing the data privacy challenges posed by this emerging technology.

- **Onfido:**
  Onfido will research how to identify and mitigate algorithmic bias in machine learning models used for remote biometric-based identity verification.

- **Tonic Analytics:**
  The Galileo Programme was launched in 2017 and is jointly sponsored by the National Police Chiefs' Council and Highways England. Galileo's primary focus is on the ethical use of innovative data analytics technology to improve road safety while also preventing and detecting crime.

- **TrustElevate:**
  TrustElevate provides secure authentication and authorisation for under- 16s. TrustElevate is the first company globally to provide verified parental consent and age checking of a child. It is working to enable companies to comply with regulatory requirements, and to make the Internet a safer environment for children, facilitating a more robust digital ecosystem and economy.

2.2 The exit reports for the beta phase participants can be found on our website.

# 3. Key lessons learned

3.1 As result of the feedback provided during the beta phase, we developed our processes prior to moving onto the next stage of the Sandbox. We decided to:

- Narrow **our focus in line with the ICO's strategic aims**, and revise these on a periodic basis.
- Move away from the 'cohort' model of the beta phase that works with a set number of organisations over a set period to **a 'roll on roll off model',** where we accept organisations as and when they meet our commissioning briefs and resource permits.
    - **Increase upfront engagement** with potential participants by introducing an 'expression of interest' stage. This allowed us to identify the organisation's basic objectives, timescales and enabled us to triage the applications. Following the triage process, we would then engage the organisation in dialogue and scoping activities and if both parties still felt the project was worthwhile, we would then invite the organisation to apply formally.
    - Include **key activities and subject areas** within new Sandbox plans that worked well within the beta phase, such as workshops involving participants and ICO staff, examination of lawful basis and development of more bespoke DPIA templates where appropriate. This allowed our newer participants to benefit from tried and tested methods, streamlined progress and meant we were able to work more efficiently.

3.2 We are thankful that our participants demonstrated a real commitment to transparency during the beta Sandbox. We noted those who demonstrated the most candour about their difficulties in applying UK data protection legislation appeared to gain the most useful insights from their Sandbox participation. This gave the ICO an invaluable opportunity to gain an industry eye view of the sectors which we regulate and has already informed on some aspects of our approach as a regulator.

3.3 The Sandbox team noted that there were some common misconceptions about the UK data protection legislation which we had to work through. These included a lack of understanding about:

- **Roles and responsibilities such as controller/processor, lawful basis**
  Some of our beta phase participants struggled to understand how to apply ICO guidance on controllers and processors to their innovations. This was often in cases with novel technologies where the distinctions between controllers and processors were not clear and in cases with complex data supply chains involving numerous partners. The Sandbox team worked with participants and analysed data maps and granular descriptions of their processing activities in order to advise participants how to apply the definitions of key roles and responsibilities to their innovations.

- **Risk to data subjects and organisational risk and how this should be communicated in a data protection impact assessment (DPIA)**
  Article 35(1) of the UK GDPR suggests that a DPIA should be completed whenever the use of new technologies is likely to result in a high risk to the rights and freedoms of individuals. As many of our beta phase participants' innovations involved the use of new technologies or innovative uses of existing technologies, the Sandbox team often advised our participants to consider, evaluate and mitigate data protection based risks through the use of DPIA. The Sandbox team offered support to participants when

creating these documents, helping them to iterate on their thoughts to ensure they had given fair consideration to all the risks associated with their innovations and offer advice on ways to mitigate these risks.

For example, the ICO supported Jisc in its development of the DPIA. In doing so, the ICO ensured that Jisc had considered and documented the relevant data protection risks that the universities would generally need to consider, whilst acknowledging that the precise risks that each university would encounter, would need to be considered on a case-by-case basis.

- **What is personal data within the scope of the UK GDPR**
  Our participants sometimes were unclear as to what constituted personal data, particularly when discussing personal data which could indirectly identify individuals. This was further compounded by misunderstandings surrounding anonymisation and pseudonymisation. Some participants assumed that as they had secured personal data using encryption and hashing techniques, the data was rendered anonymous. The Sandbox team were able to explain and show organisations which data would be considered personal data within their projects. The team also explained to organisations that the UK GDPR sets a high bar for anonymisation, which means that if an organisation keeps the means to reidentify data subjects (eg by retaining the encryption or hashing key used to secure the data) or the data could reidentified by combining it with other datasets, the data would not be considered anonymous and thus the processing activity would remain under the jurisdiction of the UK GDPR.

  The Sandbox team reported these common misunderstandings internally so that they can be clarified in the ICO's upcoming guidance on anonymisation and pseudonymisation.

- **Ways to scale up big data processing from research to operationalisation**
  **S**ome of our participants wanted to understand how best to apply data minimisation principles to big data processing. This applied particularly when they considered how best to include data sets, which may have complex relationships to their processing that they had not yet fully explored. The Sandbox team explained the importance of using unidentifiable information in these instances where possible, providing evidence based rational reasons as a basis for the inclusion of personal data in a given data set and looking at possible other ways to scale the data, particularly when looking at operational uses of big data analytics. These methods of scaling could include, but are not limited to, limited scope trial exercises where the scope is limited by geographical area, number of data subjects' data collected, fields of data collected and the timescale of the exercise.

3.4 Moving forward, we now anticipate that the above issues will need to be considered and make sure that actions relating to them are included in future Sandbox plans. This has already been useful as it has allowed us to clarify these issues either pre-participation or very early on in our engagements which has made it easier to tackle the more novel aspects of our projects.

## Key overarching trends

3.5 Following the exit of our participant organisations from the Sandbox, we have identified several key overarching trends from the work conducted which are outlined below alongside some examples[1].

- **The ICO has gained valuable insights into a specific sector, topic or issue**

  FutureFlow's participation in the Sandbox gave the ICO a valuable insight into the financial sector and how banks and other financial institutions might choose to leverage and share the data they already collect to detect and tackle instances of financial crime.

  Tonic Analytics participation in the Sandbox gave the ICO insight into the transportation and law enforcement sectors and how the innovative application of technology underpinned by effective data sharing can effectively help to tackle the challenges of reducing crime and increasing safety on the roads.

  Heathrow Airport Ltd's participation in the Sandbox gave the ICO insight into the airport sector and how organisations may seek to utilise Facial Recognition Technology (FRT) in new and innovate ways, and from working with Onfido the ICO gained insight into the practical issues relating to a supply chain involved with the provision of Artificial Intelligence (AI) services, particularly where the application of the data protection legislation and guidance to such an environment is not always clear, this work fed into the ICO's guidance on AI. MHCLG's participation in the Sandbox allowed the ICO to consider how organisations, specifically public authorities carrying out complex data sharing activities, can comply with data protection law.

- **The Sandbox participant demonstrated commitment to using innovative technology in compliance**

[1] The full learnings from each organisations participation in the Sandbox can be found in their exit report published on the ICO's website, accessible via: https://ico.org.uk/for-organisations/regulatory-sandbox/previous-participants/

**with the data protection legislation**

When working with Novartis, who sought to use digital technologies to help transform patient care, the ICO determined that they followed the principles of accountability and data protection by design, to ensure requirements were identified and met. Novartis achieved this even though it was deemed that they would not have an established data protection role in relation to personal data processed via their digital solution in subsequent deployments within the NHS. Their work in the Sandbox helped them to produce a preliminary DPIA and privacy notice. Novartis intended to supply these to the NHS to help them consider the wider risks of the deployment of the digital solution and reduce their burden in ensuring appropriate documentation would be in place. As a result, the NHS could then tailor or individualise documentation that related to their specific circumstances in support of a solution that had already 'baked in' certain data protection principles.

The ICO was of the view that other Sandbox participants similarly demonstrated a commitment to using innovative technology compliantly.

- **The Sandbox participant demonstrated awareness of potential risks for their innovation, have developed measures to mitigate these risks, and/or the ICO has highlighted risks for the participant to consider**

GLA demonstrated awareness of the full array of potential risks to their data processing activities which they continued to monitor as they developed the innovation. As a result of GLA's diligence they were able to ensure that they had sound procedures in place to mitigate these and other potential risks.

Through constructive and collaborative engagement with the ICO, Novartis gained new perspectives and insights into complex third-party ecosystems, technological innovation, and emerging privacy challenges. In

this context, Novartis was able to assess and manage third party risk, establish roles and responsibilities, and implement appropriate safeguards. For example, due to a change in their priorities as a result of the COVID-19 pandemic, Novartis elected to offer its Digital Solution to the NHS without voice functionality enabled. Despite this, the data protection implications of processing voice data were still explored within the Sandbox. This included elements such as how the voice solution would be activated, the different methods used for improving speech recognition and ensuring due diligence on system accuracy levels is carried out. This consideration of potential risks allowed Novartis to engage with a number of technology providers and carefully consider the future enabling of the voice element of their Digital Solution. This is an approach that may continue to help future Sandbox participants to conceptualise non-mandatory or optional elements of products or services.

- **The ICO was able to provide a view or recommendation on further measures which may improve compliance in a particular industry or for a particular type of processing**

  The ICO's work with Jisc has provided insight on how to break down the research and operational stages of data analytics as two sets of data processing and so assessing the risks and requirements for compliance for each separately. It is hoped that Jisc's resulting Wellbeing Code of Practice will, as it is increasingly put to live use, provide universities with sector tailored guidance.

  In respect of MHCLG's participation in the Sandbox, the team hoped that upon their exit the considerations document, that was provided in lieu of informal steers, would be helpful for similar pilots involving data sharing with other organisations. This document provides a checklist of key data protection considerations MCHLG should take to identify and mitigate data protection risks associated with their pilot which should be scalable to other projects.

- **The ICO was able to provide a view on whether it was likely the data processing subject to Sandbox participation was compliant with the UK data protection legislation, either before or after mitigations where applicable**

  Based on the information seen in the Sandbox and solely in respect of the FutureFlow platform considered in the Sandbox, the ICO explained it appeared likely that the financial transactional data processed by FutureFlow's platform was processed securely and not in a way which breaches the UK data protection legislation. This view has helped FutureFlow to proceed with developing partnerships with other organisations beyond the scope of their Sandbox work. Prospective partners can proceed with projects with the confidence that FutureFlow's operating model is compliant with UK data protection legislation.

  Similarly, the ICO concluded that it appeared likely the data processed by Tonic Analytics' technology for the purposes of law enforcement research, as conducted within the Sandbox, was processed securely and not in a way which breaches the UK data protection legislation, which again led to their operating partners' increased confidence in the project.

  Whilst working with MHCLG, the ICO became aware of the challenges faced by organisations in establishing the correct roles and responsibilities in a multi-agency approach. In this example, participants in a new data sharing initiative took a more granular approach in understanding new personal data processing activities and the different stages of the user journey. This subsequently allowed each participant to understand whether they would be a controller, joint controller or processor, and carry out the responsibilities appropriate to their respective roles. This has been an important theme for the ICO to engage with as data sharing continues to be an area of focus for the Sandbox team in 2021 – 2022.

- **The work in the ICO Sandbox will influence the ICO's views and future work on a specific sector, topic, or issue**

  The ICO's work with FutureFlow will help to influence our views and any future work on how large organisations can anonymise, pseudonymise and share data for the purposes of tackling financial crime in a compliant and secure manner while maintaining individuals' rights to privacy. The ICO's work with Heathrow will impact our guidance on the collection and recording of explicit consent, as well as the use and deployment of FRT systems generally and in the context of ports.

  NHS Digital's participation has allowed the ICO to gain additional insight and build on our existing understanding of the sharing of patient data for secondary uses such as research in the health sector and the interplay between the data protection legislation and other laws such as the common law duty of confidence. This understanding will be shared internally within the ICO and will support colleagues engaging with stakeholders in the health sector. This work fed into our guidance on special category data and will influence any future work on the research exemption.

- **Participating in the ICO's Sandbox has placed the participant in the position to be able to develop their data protection compliance for their innovation to address future developments**

  The Sandbox has placed GLA in a strong position to iteratively develop both their data-sharing and their SafeStats policies and procedures to address future developments. Participating in the Sandbox gave NHS Digital and National Institute for Health Research confidence that they had achieved the key aims of their vision, comprised of respecting privacy, upholding data subject rights and maintaining public trust, at the point of launching their service and has enabled NHS Digital to consider future developments to the service

in line with these principles. The ICO understands that upon their exit of the Sandbox, Novartis would use their deepened understanding of voice technology, the evolving risks in this area and the Sandbox steers when continuing its journey to design and deploy privacy-focussed voice solutions that can be used to support the NHS and improve patient care.

- **The ICO has become aware of certain difficulties and challenges with the implementation of technologies or the application of the data protection legislation**

  Jisc's participation in the Sandbox gave the ICO a greater understanding of the challenges that organisations can face when trying to identify a suitable lawful basis. This project highlighted that some organisations, such as universities, are deemed to be public authorities, but do not always have the clear basis in law that is needed for them to use public task as a lawful basis for processing. Jisc produced guidance which provided steers on the steps universities could take to decide on the most appropriate lawful basis if processing personal data for use in data analytics. This included a DPIA template which provided examples of data protection risks as a starting point for universities considering using this type of data processing.

  Through working with Heathrow Airport Ltd, the ICO recognised there are likely to be several challenges faced by any airport as they seek to implement technologies like facial recognition scanners. This includes achieving clarity between all parties as to who is the processor and who is the controller in any given circumstance; particularly given the many different parties involved in handling passenger data.

# 4. Feedback from beta phase participants

4.1 Before we began accepting applications to enter the Sandbox, the Sandbox team decided to seek feedback from participants, and to a lesser extent unsuccessful applicants, at three key points during the Sandbox beta, which are as follows:

- Phase 1: post application
- Phase 2: post Sandbox plan sign-off
- Phase 3: pre-Sandbox exit

4.2 At each phase we asked our participants key questions to help gauge the effectiveness of the service we provided and the impact that Sandbox participation was having on their organisation.

4.3 For feedback phases 1 and 2 applicants were asked several Net Promotor Score (NPS)[2] based questions but were also provided with a free text field to clarify their reasoning for their scores. In phase 1 these comments were well balanced and constructive. For example, most applicants noted that the staff they interacted with while completing their application or seeking further information about the Sandbox were helpful, but that the beta

[2] NPS is used as an alternative to traditional customer satisfaction research, it aims to measure the loyalty which exists between the customer (ie the participant/applicant) and the service provider (ie the ICO). For our statements we have asked respondents to provide a score between 1, signifying least agreement with the statements, and 10, signifying the strongest agreement with the statements. A score between 1-6 makes an individual a detractor, scores between 7-8 identify customers as being passive toward the statement and a score between 9-10 indicates an individual is a promoter of the service.

phase application form was not specific enough in terms of expected word count and content for applicants to give adequate answers. Some applicants felt that the ICO would have benefited from introducing a web-based form with these restrictions already embedded, others suggested that the Sandbox team should screen all potential applicants prior to the completion of an application form to ensure that organisations do not commit a large amount of resource to an application that may ultimately be unsuccessful.

4.4 In phase 2 participants appeared to be largely pleased with the structure of their engagement which led to the formation of their respective Sandbox plans, however one participant specified that they would have found it useful to have key policy questions and objectives identified earlier on and suggested that this could be included as its own section in the Sandbox plan. All participants noted that they were satisfied that their Senior Case Officers were taking the time to learn about their organisation and their Sandbox product and were enthusiastic about the assistance they received.

4.5 The Sandbox team are working to identify key policy questions and objectives at the outset of Sandbox participations to ensure that they are actively answered as part of organisations' engagement with the Sandbox feedback.

4.6 The Sandbox sought quantitative feedback from the beta phase participants as part of the exit process and the themes that emerged were as follows:

- The Sandbox process enabled them to understand the importance of privacy by design and feel they can use the knowledge gained and apply it to future projects.
- The relationship was open, integrated and constructive and the ICO provided honest advice and support in a timely way.

- They are now able to articulate the data protection risks and mitigations of the product or service to other organisations when working with them and will be able to use lessons learnt in future work.

# 5. Impact of the Sandbox

5.1 ICO's Sandbox was the world's first GDPR-territory data protection Sandbox. Since its inception, the Sandbox has worked effectively in collaboration with industry to help them create innovative products and services in the public interest in a way that is compliant with UK data protection legislation.

5.2 ICO's Sandbox takes an innovative approach to governance and management of risk providing 'regulatory comfort' from enforcement to participants and clear and transparent exit reports from which wider learnings are distilled.

5.3 ICO worked transparently and collaboratively with industry to design the Sandbox, inviting them to provide feedback through consultations and workshops. We continue to seek feedback about the Sandbox and have consistently recorded satisfaction levels of 90% from participants. Our willingness to manage the risks that come with working in challenging areas has allowed us to deliver great public interest outcomes and demonstrated the value of upstream compliance work to industry.

5.4 Since inception the ICO sandbox has assisted with key public interest projects such as the successful COVID-19 vaccine trial registry, supporting young people's mental health, combating violent crime, helping remove algorithmic bias, enhancing safety transport network, and the use of voice recognition in healthcare settings.

5.5 The Sandbox has helped to inspire adoption elsewhere (eg Sandboxes in France and Norway) and acted as a model of good practice, demonstrating how regulators can work flexibly and proactively while navigating complexity and innovation.[3]

# 6. What's next?

6.1 In November 2020, the Sandbox re-opened to receive expressions of interest from organisations with the following two key areas of focus:

- **Innovations related to the Age Appropriate Design Code (AADC)**

  With the AADC coming into force on 2 September 2020, the ICO was keen to work directly with innovators through the Sandbox, ahead of the 12-month transition period. We wanted to work with organisations in the Sandbox to explore the specific issues innovators face and to help inform further guidance and practical tools. We were particularly interested in hearing from innovators who wanted to work with us to ensure the best possible standards in age-appropriate design, and who were focusing on issues posed by implementation of the Code. We welcomed any applications in this area but were particularly interested in the following areas of age-appropriate design:

  - Age-appropriate privacy information, including tailoring the right to be informed to different age

[3] Regulatory Sandboxes are Gaining Traction with European Data Protection Authorities | Privacy & Information Security Law Blog (huntonprivacyblog.com)

groups, to enable transparency and understanding whilst not undermining the user experience.

- How to provide age-appropriate privacy information via connected toys and devices (where there is no screen).
- Applications to enable increased control of personal data within connected toys.
- Exploring systems to secure in-game communications between players to protect children from unwanted intrusions or a risk of grooming.
- Exploring how to convey the best interests of the child or young person, and other AADC considerations within a DPIA.
- Use of geolocation technology involving children and young peoples' whereabouts, including in relation to COVID-19 tracking.

- **Innovations related to data sharing**

  With this area of focus the Sandbox team were particularly interested in exploring the areas of health, central government, finance, higher and further education or law enforcement. Compliant data sharing is crucial to the operation of modern economies. Our aim was to promote and enable confident, responsible and lawful data sharing in the wider public interest. In particular, the Sandbox aimed to help demonstrate that data protection legislation is not a barrier to proportionate sharing of personal data. Whilst we were open to any proposals on how to meet that wider aim, we wanted to hear from organisations who were developing products or services likely to enable substantial public benefits, but where data sharing may:

- pose the highest risk to the public and to information rights;
- involve the use of novel or innovative technologies;
- involve the use of innovative data governance frameworks or data sharing platforms; or
- involve the processing of sensitive personal data

6.2 Since we opened with these areas of focus, we have accepted the following organisations into the Sandbox[4]:

- **Yoti**, who are developing an age estimation algorithm to help 7-12 year olds access online spaces safely.
- **CDD Services** who are developing a social care passport concept called SafeGuarden which will enable ex-service people to share their data effectively when accessing social care services.
- **Seers** who are developing a cookies consent tool which provides age appropriate messaging for young people.
- **The Gambling Commission** who are developing their single customer view concept to enable gambling operators to share data to protect vulnerable adults from harms associated with gambling.
- **The Global Cyber Alliance** who are developing their Domain Trust platform to enable police forces, regulators and other organisations to work together to take down domains responsible for cybercrime.

[4] Further information on these projects is available at: https://ico.org.uk/for-organisations/regulatory-sandbox/current-projects

- **FlyingBinary** who are developing an AI enabled service to help young people understand the emotional impact of the content they see online before they see it.
- **Good With** who are developing a conversational AI-driven smartphone companion that young adults can use to seek advice, develop their financial education and demonstrate their financial readiness to gain fairer access to financial services.
- **Our Future Health** who are aiming to be the UK's largest ever health research programme. They are seeking to recruit participants from across the UK population who will provide information about their health and lifestyle, alongside samples of their saliva and/or blood. Researchers will be able to use that information to make new discoveries about human health and diseases.

6.3 In August 2021, we updated our key areas of focus for the Regulatory Sandbox for 2021-22. This includes data sharing as above and:

- **Products and services exploring the use and deployment of innovative technologies, such as privacy-enhancing technologies and distributed ledger technologies**

  The UK's digital sector contributes up to £150 billion each year to the UK economy as it works to solve problems, enhance day to day services and provide benefits for consumers across the rest of the UK's economy.

  In order to better support the UK's growing digital economy, we want to use our Regulatory Sandbox to support innovators who are designing, building and deploying innovative products and services utilising personal data to ensure that these technologies are effective and support individuals rights and freedoms.

Our aim is to promote and enable the use of secure, responsible and lawful innovations. In particular we aim to provide support to innovators working with products which:

- utilise privacy-enhancing technologies (eg homomorphic encryption, secure multi-party computation, differential privacy, privacy-preserving machine learning) to effectively anonymise data and facilitate its use and sharing; or
- utilise distributed ledger technologies (for example, in digital currencies or smart contracts) and are willing to work with us to examine the data protection challenges associated with these (eg complex data controllership issues, facilitating individual rights requests, jurisdictional issues).