Graduating from the Sandbox — a look at the first four exit reports

Ali Vaziri, Managing Associate with Lewis Silkin LLP, mines the first four exit reports from the ICO's regulatory Sandbox for actionable insights

Since first taking office four years ago, the UK Information Commissioner has repeatedly affirmed that "privacy and innovation are not mutually exclusive" in what has become something of a mantra. Her message has become more vociferous over the course of 2020 in the face of the new National Data Strategy and pro-growth data regime it will seek to foster. Indeed, a trade-off for the flexibility offered by a principles-based law like the GDPR, which can accommodate advances in the state of the art, is an inherent lack of certainty. The UK government sees that uncertainty as being bad for innovation and, therefore, bad for business. At the same time, it is no secret that regulators have struggled to cope with the pace of change in technology. The adoption of new regulatory approaches — be they advisory, adaptive or anticipatory — is, however, starting to reshape how regulation supports innovation. Those approaches have in common a more proactive and engaged role for regulators in the innovation process, and sandboxes are a key tool being deployed by them to help identify, build and test solutions to emerging challenges.

The Information Commissioner's Office ('ICO's') Sandbox was inspired by the Financial Conduct Authority which has been running its own since 2015, and aims to provide specialist support to participants using personal data to develop innovative products or services with a demonstrable public benefit — a safe space to test new concepts and technologies. When launched in beta back in September 2019, the ICO anticipated that projects accepted would be at the cutting edge of innovation and operating in challenging areas of data protection where there is genuine uncertainty about what compliance looks like.

10 participants were selected from 64 applicants. Although during the Summer, the ICO had re-opened the Sandbox to new projects focused on children's privacy or data sharing, by the close of 2020, only four had graduated from the beta phase. This article looks at the key data protection issues identified from the exit reports published so far, in the hope that others might benefit from shared insights.

JISC

JISC is the UK-based, higher education, further education and skills sectors' not-for-profit organisation for digital services and solutions. Its participation in the Sandbox related to a data analytics project for universities and colleges wishing to analyse student data to improve their support services, particularly in relation to wellbeing and mental health. This was data processing identified as intrusive and potentially high risk.

Use of data — Since institutions may use data from different sources for varying purposes, rather than be prescriptive, JISC developed a 'purpose/notice matrix tool' in collaboration with the ICO through a series of questions which could be used to guide and record institutions' assessments of purpose compatibility, and the best way to achieve the required level of privacy notification. Both the matrix tool and further guidance on how to provide privacy notices to students were documented in JISC's Wellbeing Code of Practice.

Evidencing necessity — JISC had commissioned a separate report from a higher education think tank on the necessity of making better use of data in supporting students with wellbeing and mental health issues. JISC's discussions with partners in a project with the independent regulator of higher education in England and a professional association for leaders of student services in higher education also supported that need.

Meeting key data protection challenges — JISC's Wellbeing Code of Practice included information about how universities can demonstrate compliance with the GDPR's accountability principle, including the requirement to perform a Data Protection Impact Assessment ('DPIA'). This in turn would help them to identify appropriate lawful bases and conditions for processing, guidance on privacy notices and how to provide for under-18s. The ICO supported JISC in its development of a DPIA tool having agreed the most suitable basis — either 'public task' or 'legitimate interests', as universities uniquely carry out some tasks as a public authority, and others as a private institution. JISC and the ICO also agreed on the condition for receiving/inferring Special Cate-

(Continued on page 10)

(Continued from page 9)

gory personal data in the form of information about an individual's mental health — Article 9(2)(g) GDPR, on the basis of the substantial public interest condition for safeguarding children and individuals at risk at Schedule 1, Part 1, Paragraph 18 of the Data Protection Act 2018 ('DPA 2018').

Heathrow Airport Limited ('Heathrow')

Heathrow provides airport services to airlines flying passengers around the world. Heathrow's participation related to its automated passenger journey ('APJ') project, where facial recognition technology ('FRT') is used to automate passenger identification at touchpoints such as automated baggage drops and self-boarding gates. An 'on the day image' taken of the passenger at the bag drop is matched to the image recorded on their passport chip to confirm their identify. To expedite the passenger journey, at subsequent touchpoints, scans of the passenger's facial biometrics are matched to those extracted from the first 'on the day image' to prove that it is still the same passenger, without having to provide documentation again. Heathrow also wanted to explore allowing airlines flying passengers to the US to verify their identities against the US Customs and Border Protection's ('CBP') Traveller Verification Service ('TVS'), by matching the 'on the day image' against the TVS database of individuals who have entered the US previously.

> ***"The Information Commissioner has long presented the GDPR as being an advantage in the marketplace… the reality on the ground, however, is that its subjective terms and nebulous concepts often inhibit the development of new products and services. That is why the Sandbox is so important to Ms Denham in demonstrating that privacy and innovation can be a 'win-win' rather than a zero-sum game."***

Complex data controllership issues — Heathrow would likely be a joint controller with each of its partner airlines for processing of personal data associated with the APJ. That is because Heathrow appears jointly, with airline partners, to be making the decision to introduce FRT in the terminals; determines the means and manner of FRT verifications; has its own business interest in introducing FRT; and determines the lawful basis and condition for processing biometric data. In relation to the TVS processing, Heathrow would likely be a processor on behalf of each partner airline because, in the context of that processing, it is providing a service to, and acting on, the instructions of those partner airlines (who are assumed to be the controllers). The ICO advised that those roles be formalised in a contract or an instrument such as its Conditions of Use.

Use of biometric data — A 2009 amendment to the Immigration Act 1971 stated that Heathrow must use a biometric system to secure and prevent international transitioning passengers from breaking the UK border security controls in common departure lounges, by exchanging boarding passes with a passenger on a domestic flight. The ICO's view was that the 2009 amendment could not be relied upon for processing all passengers' biometric data for APJ purposes, because APJ processing goes further than the processing specifically mandated by the amendment. Consent and explicit consent would therefore likely be the most appropriate legal basis and condition. Whilst a future legislative amendment might provide a sufficient lawful basis (e.g. compliance with a legal obligation), a suitable condition would still need to be found.

Collecting explicit consent — The ICO facilitated a design workshop on how Heathrow might collect valid consent. The proposed method relied on passengers clicking 'yes' to full consent statements. Heathrow was concerned that this might impact negatively on their experience (e.g. in terms of time taken). An alternative method was therefore explored. It involved layering communications and an affirmative action as an express statement of consent (e.g. joining a clearly signed queue for APJ processing, with screen signage indicating that scanning a boarding pass will be taken as an express statement of explicit consent to biometric processing). The ICO's feedback was that this alternative method would not meet the threshold for explicit consent.

TVS processing — It was determined that Heathrow would likely be a processor, and that the controllers (i.e. partner airlines) could reasonably argue that the international transfer and subsequent processing was in their legitimate interests (subject to undertaking a Legitimate Interests Assessment ('LIA')). It was unclear whether Article 9 GDPR was triggered by the transfer, given complicated questions about the point at which a digital image could become biometric data. Heathrow would need to consider discussing such matters with the controllers. The ICO also advised that provided passengers could opt out whilst in the UK, reliance on the explicit consent derogation under Article 49(1)(a) GDPR would likely be valid.

The ICO was keen for Heathrow to collaborate with other airports, ports, airlines and further relevant stakeholders to establish sectoral standards for the APJ processing and suggested creating an Article 40 Code of Conduct.

FutureFlow Research Inc. ('FF')

FF is a regtech start-up which provides a platform that monitors the flow of funds in the financial system to detect, identify and ultimately tackle instances of financial crime, including money laundering. The platform does this by scrutinising transactional data provided by financial institutions in pseudonymised form to identify potentially suspicious behaviours. In 'indirect mode' a trusted third party ('TTP') facilitates the exchange of data between each financial institution client and FF, and provides deduplication with optional further obfuscation. In 'direct mode', FF completes the role of the TTP as well as its own analytics role. Whilst 'direct mode' reduces the complexity in terms of coordination and data exchanges between FF and its clients, it offers a lower degree of obfuscation.

Complex data controllership issues — FF was asked by the ICO to create visual diagrams of dataflows to understand which party ultimately had decision making power over contributed data. FF was likely a processor both in 'indirect' and 'direct' modes, because it was not deciding the means or purpose of the processing activity, nor was it pursuing its own interests (it was acting in accordance with the instructions of its financial institutions). FF's clients were likely individual controllers for the data contributed to the pooled dataset, given that they are determining the means and purposes of the processing and obtained the data from data subjects in the first place. Any TTPs were considered processors, as they were simply acting under the instruction of financial institutions and not exercising any real discretion.

Anonymisation v pseudonymisation —The obfuscation techniques used would not, in the ICO's view, render the data anonymous within the meaning of Recital 26 GDPR and, as such, the data should be regarded as having undergone pseudonymisation only. That is because even though the data, once obfuscated and submitted to FF, could not be identified by FF, there was a chance that a motivated intruder could theoretically re-identify the information were they to gain access to it. The ICO helped FF to create a suitable model DPIA to manage the risk of re-identification. It included a risk register which documented the risk of re-identification and measures implemented by FF to mitigate that risk. Although it was not strictly necessary for FF — as a processor — to complete a DPIA, the document was intended to function as an expanded guide to the platform and a model document for FF's clients to use when completing their own DPIAs.

GDPR compliance — The ICO assisted FF in developing its collateral documentation. FF created its own Record of Processing Activities ('ROPA'), adopting the processor version of the ICO's template. The ICO also worked with FF to develop a data protection policy (along with some suitable template wording for inclusion in its clients' privacy notices) and a DPIA. Whilst recognising that the selection of a lawful basis was FF's clients' decision, the ICO advised that Article 6(1)(f) GDPR was likely to be most appropriate in order to share, collate and commission the analysis of transactional data using the platform. The ICO also made a number of observations were FF's clients to rely on Article 6(1)(c) GDPR.

Onfido Limited ('Onfido')

Onfido provides remote biometric identity verification technology. Its clients' customers provide a photo of an ID document and a selfie which Onfido analyses to determine the likelihood that: (i) the document is genuine; and (ii) using its FRT, that the face in the selfie matches the face in the ID document, and that the selfie image does not show evidence of spoofing or fraud. Clients review Onfido's recommendations and make their own decisions on whether to provide customers with access to their platform or services. Onfido trains its FRT models using images collected during the provision of its services to clients, and its Sandbox participation focused on its activities in a research project to improve those models by measuring and mitigating any bias.

Article 6 considerations — Having observed that Onfido is a controller when processing to improve its FRT, the ICO advised that Article 6(1)(f) GDPR would be the most appropriate lawful basis for that processing. Onfido's DPIA factored in the requirements of a LIA and, in particular, the impact on relevant data subjects from using large datasets to develop the FRT.

Special Categories of data — Two key findings were communicated by the ICO:

- biometric data processed by Onfido for developing its FRT was unlikely to be Special Category personal data because although they might allow for the unique identification of individuals, they are not being used for that purpose; and
- to the extent that labels used for training and testing related to the race or ethnicity of an individual, those labels were a Special Category of personal data as they revealed or inferred the racial/ethnic origins of data subjects.

Article 9 considerations — The substantial public interest condition at Article 9(2)(g) GDPR could be used by Onfido in order to process Special Category information on the perceived racial/ethnic origin of individual data subjects as part of its research project. In the case of Onfido's research, the substantial public interest condition identified was the condition for equality of opportunity set out in Schedule 1, Part 2, Paragraph 8 of the DPA 2018.

Providing privacy information – Onfido is often not visible to the end customer, and has limited ability to provide a fair notice of processing. The ICO, whilst developing its thinking on providing privacy notices in complex AI supply chains, could not identify any steps further to those Onfido was already taking. These were described by the ICO as 'a substantial effort' and involved: (i) contractually requiring its business clients to provide data subjects with privacy information and seeking warranties of the same; (ii) interspersing reminders to clients to provide that information throughout Onfido's technical documentation (available publicly and pro-

(Continued on page 12)

(Continued from page 11)

vided during on-boarding); and (iii) prominently displaying its own privacy notice on its website. Further, Onfido is also looking to expand its 'know your business' process to include due diligence checks on whether its clients are likely to fulfil the privacy obligations placed on them, including by verifying their privacy policy.

Data subject rights — As Onfido does not have a direct relationship with data subjects, facilitating data subject rights requests is challenging. The ICO's view was that Onfido's current process, described in its privacy policy, was likely to satisfy its legal obligations. This involved: (i) asking a data subject to identify themselves; (ii) identifying the relevant business client for whom Onfido was acting; and (iii) putting the data subject in contact with that client so they may handle the request.

Conclusion

Although her fines might grab headlines, the Information Commissioner has for some time now been at pains to emphasise that she does not just wield a big stick — she is also there constructively to engage with businesses and to advise and support them in their compliance efforts. The Sandbox is one of a number of initiatives aiming to provide more certainty and help operationalise the GDPR for day-to-day business. In recent months these have included the launch of the Accountability Framework (in beta) as well as a data sharing information hub to support the new Data Sharing Code of Practice which was submitted to the Secretary of State on 17th December 2020. No surprise then that data sharing is also an area where the ICO is currently accepting expressions of interest for the next phase of the Sandbox.

The Information Commissioner has long presented the GDPR as being an advantage in the marketplace which encourages trust and confidence. The reality on the ground, however, is that its subjective terms and nebulous concepts often inhibit the development of new products and services. That is why the Sandbox is so important to Ms Denham in demonstrating that privacy and innovation can be a 'win-win' rather than a zero-sum game.

The GDPR is far from perfect. But branding it 'horrific' and suggesting that "[o]ne of the many advantages of Brexit is we will soon be able to bin such idiotic laws", as one (now former) senior Downing Street advisor famously observed, is not helpful. Leaving aside the jeopardy to flows of personal data into the UK from its largest trading partner, such statements are also ignorant of the fact that the GDPR has prompted standards to be raised globally, and that, as the National Data Strategy acknowledges, "high data protection standards allow businesses and consumers to thrive".

The current uncertainty faced by the world at this time, and in our particular corner of it since 1st January 2021, means that we will need to grow our way out of economic turbulence. With use of personal data fueling much of the innovation powering growth, the Information Commissioner's pro-growth message that "the days when data protection regulation was seen as a blocker to innovative business have long passed" will be welcomed by UK plc — and she is doubtless banking on the experiences of Sandbox graduates as testament.

Ali Vaziri
Lewis Silkin LLP
Ali.Vaziri@lewissilkin.com