ICO advises 'DeepTech' company in Sandbox about compliance with DP law and the Children's Code

Laura Linkomies reports on maximising social and economic benefits from data sharing whilst staying within data protection law and the ICO's Children's Code.

Use of AI, when delivering care to mental health patients, including children, is a potential minefield from the privacy perspective. This is exactly why FlyingBinary, a "DeepTech"[1] company applied to participate in the ICO's Sandbox prior to the coding for the development and deployment of its app.

The company entered the ICO Sandbox in November 2020 to develop an app to assist with the care of mental health patients with pathologies such as eating disorders. FlyingBinary and the ICO agreed the content of FlyingBinary's bespoke Sandbox plan in March 2021, and the company exited the Sandbox in April 2022.

Dr Jacqui Taylor, founder of FlyingBinary told *PL&B*: "This is a win-win for both organisations. The project was collaborative and we were totally transparent in the commercial approaches we are using. The Sandbox officers were very knowledgeable about the regulatory setting. We were able to inform the ICO team on the challenges we face with regulation in a complex DeepTech setting, specifically in an AI project. We were also able to explain the additional challenges we faced in implementing the ICO's Children's Code, as we move from our use of the United Nations Convention on the Rights of the Child."

What was involved?

Flying Binary was in the process of designing an app that clinicians could recommend to their patients as part of their existing care. The app, *lookafterme*, is aimed at assisting with conditions such as anorexia and bulimia, and improving and maintaining the mental health of the patients.

The idea was that patients would be able to log-in to the service which would alert them immediately if they access online content that could be potentially harmful which may aggravate their mental health condition. A pre-trained AI engine would scan the requested content in real-time.

As FlyingBinary identified that the youngest user of *lookafterme* would be only eight years old, it needed to put in place systems that would ensure compliance with the ICO's Children's' Code, the Data Protection Act and the UK GDPR. This involved considering additional risks to children with the help of a Data Privacy Impact Assessment (DPIA).

Data sharing was one of the key considerations as *lookafterme* would share personal data relating to the patient's usage of the service with their parent or guardian, doctor and clinical researchers.

Sandbox objectives and DPIA

The objectives of FlyingBinary's Sandbox participation were as follows:

- Objective 1: To review appropriate methods of user authentication and how this could be carried out in a way that is compliant with the requirements of the Children's code, as well as mapping additional requirements from relevant parts of the Children's code.
- Objective 2: To consider the application of the principle of data minimisation to the personal data that lookafterme will process. Given the sensitivity of the personal data, the project will consider ways in which FlyingBinary could mitigate risks to the data subject and how FlyingBinary can implement data protection by design and default.
- Objective 3: To explore ways in which FlyingBinary's work can be supported by the 'best interests of the child framework' to reduce the risk of harm to children, and to support the understanding of how the framework can be used as a tool for controllers whose processing falls within the scope of the Children's code.
- Objective 4: To carry out a Data Protection Impact Assessment (DPIA), which will be reviewed by the ICO.
- Objective 5: To assess any risks, identified by the DPIA, which warrant a deeper dive.

FlyingBinary's approach was "Regulation by Design" (RbyD), and it benefitted from the DPIA by being able to identify key data protection risks during the design of the product.

Taylor said: "We used a manifesto approach which means the DPIA was only one of the key regulatory deliverables. This is a radically different approach to regulation. We produced our draft DPIA and Manifesto in the Sandbox for ICO review."

"Regulation by Design has a robust approach to risk, based on the learning from our inclusion work across the world. The ICO team commented on the strength of the RbyD approach to risk from a regulatory viewpoint."

When reaching objective five, FlyingBinary had come to a conclusion that a clinician would onboard the patient and provide their personal data directly to lookafterme. It would therefore be the clinical entity that would initiate *lookafterme's* processing of personal data, and the clinician would continue to manage the direct relationship with the patient from a clinical perspective.

Therefore, during the onboarding process, FlyingBinary and the clinical entity would act as joint controllers. FlyingBinary had indicated that it planned to take primary responsibility for complying with the wider requirements of the UK GDPR. However, joint controllership

requires transparency about the roles and responsibilities of each party.

Authentication

Authentication is one of the trickiest aspects in the Children's Code. In the final Sandbox report, issued in August 2022, the ICO comments on the company's take on authentication: "FlyingBinary has sought to include aspects of age-appropriate application into its user authentication processes, which seek to ensure the correct user is logging into *lookafterme*. For example, FlyingBinary intends that the security measures used for the child cohort will utilise more memorable passwords and, consequently, be more user-friendly than those used for the adult cohort. The teen cohort is generally expected to follow the same authentication process as the adult user, however, they can choose to use the processes designed for the child cohort if preferred. Sandbox work has reiterated the importance of ensuring that all user authentication processes adhere with the security requirements of the UK GDPR. The ICO have also advised FlyingBinary to ensure that all user authentication methods are appropriately secure and that it appropriately assesses their susceptibility to attacks. This work has also indicated how a proportionate user authentication system can contribute to age-appropriate application in the design of *lookafterme*," the ICO says.

Data minimisation

The Childrens' Code also emphasises data minimisation, and requires that children are given separate choices over what elements of the service they wish to activate.

The Sandbox helped FlyingBinary to identify the individual items of personal data it intends to process and the categories of data subjects the personal data will relate to. This work also further emphasised that *lookafterme* needs to process less personal data about the parents and clinicians than the patients, who are the primary focus of *lookafterme's* reasons for processing personal data. By itemising the personal data it intends to process FlyingBinary was also able to cross-reference individual items of personal data against the data subject it relates to, record the source of the personal data and the purposes for processing it. As a result, the company provides a solid foundation on which it could assess data minimisation requirements, the ICO says.

The ICO and FlyingBinary were also able to identify and consider additional items of personal data that may be processed. For example, both the URL of online content, and the content itself, scanned by *lookafterme* may in certain circumstances constitute personal data.

Consent as the legitimate basis for processing

FlyingBinary wanted to use consent and explicit consent as its legitimate basis for processing. The ICO agreed that it may be possible at least for some of its processing activities. However, the ICO said there could be instances when consent could not be considered to be freely given and valid given the clinical context, potential imbalance of power and the patient's age.

Flying Binary's experience of the sandbox

Flying Binary's experience of working with the ICO was positive – the company did not find the recommendations unworkable or too legalistic.

Collaborative working: "We all took a pragmatic approach to the Sandbox process. As part of the onboarding process, the documentation, the ICO personnel and the wider ICO team worked with us collaboratively to understand the setting, throughout the entire Sandbox process. This was key to a good outcome and in my view hugely important in DeepTech especially, as it is a very different setting to digital technology design," Taylor said.

"Many of our peers have been surprised that we were prepared to submit this pioneering DeepTech approach to the ICO. Given the pace of adoption of DeepTech, I believe that it is short sighted to ignore the key part that regulation will contribute to our Web 3.0 world."

A multi-regulator environment: "We also uncovered regulatory issues which required more than a single regulator oversight. The ICO Innovation Services team was able to help us understand a multi-regulator environment, and we have been able to create a plan to navigate this landscape."

Business secrets and confidentiality: The company had, however, concerns about business secrets and confidentiality in the Sandbox.

"We were nervous about this. As part of the onboarding process we agreed an approach. This is the first time RbyD has been shared outside of FlyingBinary. We work in the security space and created a secure approach to data and knowledge sharing using our technology which is accredited both by HM Government and the National Cyber Security Centre. The ICO Innovations team supported us throughout this process."

Conclusion

The ICO and FlyingBinary agreed to focus on assessing some of the risks in more detail at the end of the company's participation in the Sandbox. For example, the data protection roles and responsibilities and lawful basis were assessed more closely.

FlyingBinary also assessed whether the data it is seeking to deidentify, in differing contexts, would constitute anonymous or pseudonymous data under the UK GDPR.

The app is now being finalised. "The RbyD approach has been viewed as a differentiator when raising funds. To put this into context, we have an eight-digit valuation for the *lookafterme* service as a result of this work with the ICO," Taylor says.

"Regulation is an opportunity to deliver our best DeepTech innovations on behalf of society – do not wait until you are writing code."

INFORMATION

Information about the ICO's current Sandbox projects can be seen at ico.org.uk/for-organisations/regulatory-sandbox/current-projects#zamna
More information about FlyingBinary's Sandbox project is at ico.org.uk/media/about-the-ico/documents/4021302/flyingbinary-exit-report-202208.pdf

REFERENCE

1 'DeepTech' is a term applied to a start-up business that develops new offerings based on tangible engineering innovation or scientific discovery.