Regulatory Sandbox Final Report: FlyingBinary

A summary of FlyingBinary's participation in the ICO's Regulatory Sandbox

Date: August 2022

ico.
Information Commissioner's Office

Contents

1. Introduction

1.1 The Regulatory Sandbox ('the Sandbox') is a service provided by the ICO to support organisations that are developing products or services which use personal data in innovative and safe ways, and deliver a potential public benefit.

1.2 The Sandbox is a free, professional and fully functioning service that is available to organisations of all sizes who meet our entry criteria and specified areas of focus. The ICO assesses these criteria via our application processes.

1.3 In August 2020, the Sandbox opened for applications for organisations developing products or services in two key areas of focus:

- projects that fall within the scope of the ICO's Children's code[1] and are seeking to ensure the privacy of children online.
- projects involving complex personal data sharing, ideally within the health, finance, education or central government sectors.

1.4 The ICO specifically wanted innovative projects operating within challenging areas of data protection.

1.5 Sandbox participants have had the opportunity to engage with us; draw upon our expertise and receive our advice on mitigating risks and implementing 'data protection by design' into their product or service, whilst ensuring that appropriate protections and safeguards are in place.

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services

1.6 The ICO selected FlyingBinary Limited ('FlyingBinary') to participate in the Sandbox. FlyingBinary is a 'deep tech' company which provides innovative products and services in the information technology and online sector, including artificial intelligence (AI).

1.7 FlyingBinary is developing an online service which seeks to assist with the traditional mental healthcare of patients with pathologies such as eating disorders. The current planned approach is that clinicians will recommend this online service to their patients as part of their existing care. During Sandbox participation this project was known as 'Social Guardian'. However, FlyingBinary has indicated that the final product is likely to be named 'lookafterme'. That name will be used for the purposes of this report.

1.8 In its current format lookafterme is designed to assist with conditions such as anorexia and bulimia. The service aims to improve and maintain the mental health of the patients. lookafterme operates as an advisory 'web-intervention system'. When logged into the service, the system provides its user with a warning if they request to view online content which is deemed to be risky or content which could potentially aggravate their mental health condition. It uses a pre-trained AI engine which scans the requested content in real-time. FlyingBinary has identified that the youngest likely user of lookafterme will be eight years old.

1.9 FlyingBinary applied to enter the Sandbox to maintain children's privacy and to ensure it appropriately considered data protection requirements and themes during the development of lookafterme. FlyingBinary has worked to operationalise the requirements of the Children's code and to seek to comply with the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). The ICO accepted FlyingBinary into the Sandbox on 12 November 2020 and appointed a Senior Case Officer to the project. The Senior Case Officer conducted an online scoping meeting with FlyingBinary on 19 January 2021 in order to understand more about their organisation, lookafterme and to begin developing the objectives of the Sandbox plan.

1.10 FlyingBinary and the ICO agreed the content of FlyingBinary's bespoke Sandbox plan on 18 March 2021. Work commenced on the first objective in April 2021.

1.11 The agreed objectives of FlyingBinary's bespoke Sandbox plan 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:** FlyingBinary will 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.

1.12 The ICO provided FlyingBinary with steers on topics such as:

- data minimisation;
- age appropriate application;
- parental controls and user authentication;
- controller and processor relationships for processing activities expected to be carried out in relation to lookafterme's use; and
- appropriate lawful bases for processing and special category data conditions for processing.

The ICO also reviewed FlyingBinary's DPIA.

1.13 The final objective of FlyingBinary's plan was completed on 14 April 2022. This report summarises the work that the Sandbox team supported FlyingBinary with during its time in the Sandbox.

2. Product description

2.1 Prior to entering the Sandbox, FlyingBinary identified a need to support the traditional mental healthcare pathways provided to patients in clinical settings, such as within the NHS. Current research has indicated that online content can be a risk or aggravating factor to a patient's condition. FlyingBinary intend that the use of lookafterme will help to address this existing clinical need. FlyingBinary note that the pandemic has accentuated the need for support in this area, as some mental health patients are waiting longer for clinical support. As a result, FlyingBinary intend lookafterme to supplement existing treatments. Initially, lookafterme will focus on eating disorders such as anorexia or bulimia. However, in the future FlyingBinary hope that lookafterme will also support additional pathologies.

2.2 lookafterme is an online 'web-intervention system', and clinicians will offer this service to patients in support of their existing care. It is an internet based system, which the patient will log into, to support the management of their consumption of online content. The system will scan online content, in real time, when it is requested by the user. If the content is not considered 'risky' to the patient's pathology then it will be displayed as normal. If the content is considered 'risky' then it will be obscured with a warning, which the patient has the option to accept and skip the content, or refuse and consume it normally.

2.3 FlyingBinary has identified three primary age groups of patients who are likely to use the service. They are the:

- child cohort (8-12 years);
- teen cohort (13-17 years); and

- adult cohort (18+ years).

As the youngest users of lookafterme are likely to be under the biological age of 18, FlyingBinary has determined that lookafterme falls within the scope of the Children's code.

2.4 During its Sandbox participation, FlyingBinary has indicated that lookafterme makes use of a number of different user journeys, aligned to the cohorts identified above. Initially, personal data relating to the patient is inputted into lookafterme by the clinician when use of the service is agreed to. For example, the clinician will input the assessed developmental age of the patient and the patient threshold. The patient threshold is described by FlyingBinary as a set of numbers, related to human emotions, which are determined by the patient's pathology group and is used by lookafterme's AI function to assess the suitability of online content requested by the patient. When the patient commences using lookafterme, they are then placed into the relevant cohort based on their assessed developmental age, and this impacts the user journey that follows. The user journeys differ in areas such as the level and complexity of transparency information that is presented and the degree of control that parents or guardians have to monitor their children's online activity or to make decisions related to data sharing permissions.

2.5 In order to assess whether online content is deemed 'risky' to the patient's condition, lookafterme uses an AI system which is pre-trained to assess the emotional impact of online content. The AI engine scans each item of web content and then assesses the emotional impact against the patient threshold. FlyingBinary define the patient threshold as a set of numbers, related to human emotions, which are determined by the patient's pathology group only, and start the same for each patient within a pathology group. The clinician can adjust the threshold as needed based on the patient's clinical progress. FlyingBinary has also indicated that the AI system does not continue to learn or adapt with the user. It is only used to make deductions about the perceived emotional impact of the requested online content which is then assessed against the patient threshold.

2.6 Outside of the personal data that lookafterme directly collects, it also processes additional personal data derived from the way the patient uses the service. For example, FlyingBinary advised the ICO that the system collates 'detailed event' personal data. This is a file which details each of the patient's requests for online content, and includes information such as

the patient user ID, the URL of the web content, the time and date of the request, the AI assessment and, where applicable, the patient's course of action. In addition, the system collects 'summary event' personal data. This grouping provides a more high-level overview of the patient's online behaviour such as the amount of times they viewed 'safe' online content and the amount of times they accepted or skipped the warning for 'risky' content. FlyingBinary stated that lookafterme uses both groupings to support the patient's mental health. Both the situational context and the user journey determine how lookafterme processes this data.

2.7 In addition, lookafterme uses data sharing functions for different purposes. For example, in order to support their mental health treatment, lookafterme may share personal data relating to the patient's usage of the service with their parent or guardian, their clinician or both. In addition, lookafterme may share the summary event data, relating to patient usage of lookafterme, with clinical researchers so that they can further develop lookafterme for additional pathologies. In this case, FlyingBinary will seek to deidentify that personal data before it shares it with clinical researchers. Only the deidentified data will be used for research purposes. These data sharing functions are agreed to at different times and in different ways depending upon the patient's user journey.

3. Key data protection considerations

3.1 FlyingBinary and the ICO considered a number of key data protection themes in relation to the development of lookafterme. Some of those key areas of consideration are outlined below.

Data protection roles and responsibilities

3.2 A crucial first step for any organisation seeking to comply with the requirements of the UK GDPR is to appropriately establish and understand its data protection role or roles in relation to the personal data being processed. Understanding whether an

organisation is acting as a controller, joint controller or a processor[2] for each processing activity means that all parties can take appropriate steps to adhere to the various responsibilities established by data protection law. Where more than one party is involved in the processing of personal data, particular care should be given to the appropriate assignment of data protection roles and responsibilities.

3.3 The appropriate assignment of these data protection roles and responsibilities was not a key focus within the scope of FlyingBinary's originally agreed Sandbox plan. However, both the ICO and FlyingBinary found that the consideration of these roles and responsibilities continued to permeate through FlyingBinary's Sandbox participation. Following the review of FlyingBinary's DPIA, the ICO and FlyingBinary agreed that there could be risks if it did not consider data protection roles and responsibilities in more detail. The ICO and FlyingBinary felt that these risks warranted a further and specific examination of these themes during Sandbox participation. As a result the ICO and FlyingBinary agreed that as part of objective five, it would consider data protection roles and responsibilities with a specific focus on the clinician's role in the onboarding of the patient to lookafterme.

3.4 Following its initial assessment of roles and responsibilities FlyingBinary stated that it would act as the controller of any personal data processed by lookafterme. This assessment applied to the personal data processed for patient health and pathology research purposes. FlyingBinary has identified both of these as lookafterme's overarching purposes. These two purposes involve a number of different processing activities. The ICO acknowledged that whilst it would be likely that FlyingBinary would exercise a significant amount of influence over the processing of personal data, the ICO highlighted that an organisation can take on different data protection roles for different processing activities. Therefore, FlyingBinary would need to further consider its purposes and means of processing personal data for different processing activities, in a granular way, as its Sandbox participation progressed.

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors

3.5 Upon reaching objective five, FlyingBinary had revised its assessment. FlyingBinary indicated that a clinician, who is employed by a clinical entity, would recommend that a patient uses lookafterme as a suitable supplement to their established mental healthcare. The clinician would onboard the patient and provide their personal data directly to lookafterme. This personal data could include their name, pathology and assessed developmental age, as well as the personal data of their parent or guardian (where appropriate). Although the clinical entity is not itself continuing to process personal data within the context of lookafterme, the clinical entity 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, FlyingBinary concluded that, for the processing of the personal data during the onboarding process, FlyingBinary and the clinical entity would act as joint controllers[3].

3.6 Based on the information available, the ICO determined that this joint controllership assessment seems correct. We noted that within this specific context more than one party is expected to participate in determining how and why the same personal data would be processed. Joint controllership may still be established even when controllers do not have exactly the same purpose, but have purposes which are linked or are complementary, and independent converging decisions, which are both necessary for the processing activity, are being made about the purposes and means of processing personal data.

3.7 Although FlyingBinary had already indicated that it planned to take primary responsibility for complying with the wider requirements of the UK GDPR, this closer assessment of data protection roles assisted it in identifying additional compliance obligations which could be applicable. For example, where a joint controller relationship is established, a transparent arrangement between the parties will need to be put in place. Although this does not have to be a specific contract, it must be a transparent arrangement that sets out the agreed roles and responsibilities for complying with the UK GDPR. Additional requirements related to what it means if you are a joint controller[4] are set out in more detail in the ICO's published

[3] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/#3
[4] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers

guidance. This has also proven to be a useful exercise for FlyingBinary in continuing to review data protection relationships in a granular way, against the current, and potentially future iterations of lookafterme.

3.8 For the purposes of this report, it should be noted that data protection roles and responsibilities were only considered in greater depth in relation to the processing expected to be carried out when patients are onboarded to lookafterme. However, the ICO also advised that detailed and ongoing assessments of controllership should be carried out by FlyingBinary in relation to the breadth of processing activities that will occur during the use of lookafterme. For example, we advised FlyingBinary to consider whether it is solely determining the purposes and means of processing for other processing activities and, as a result, would be acting as an independent controller for those activities.

The Children's code

3.9 A key focus of FlyingBinary's Sandbox participation was on how it would adhere to, and operationalise, the requirements of the Children's code. The Children's code contains 15 standards of age appropriate design which seek to appropriately safeguard the privacy of children online. This code applies to "information society services likely to be accessed by children" in the UK. This includes but is not limited to apps, programs, connected toys and devices, search engines, social media platforms, streaming services, online games, news or educational websites and websites offering other goods or services to users over the internet. The code came into force on 2 September 2020, and adhering to its standards will help organisations to design online products or services which comply with the requirements of the UK GDPR and the DPA 2018. FlyingBinary has determined that lookafterme will fall within the scope of the Children's code. It should be noted at this stage that not all 15 standards of the Children's code have been considered during FlyingBinary's Sandbox participation. The below sections highlight the work that has been carried out during Sandbox participation in relation to certain individual standards of the Children's code.

3.10 The third standard of the Children's code is 'age appropriate application'[5]. In order to comply with this standard organisations must consider the age range of the audience, they must place the different needs of children at different ages and stages of development at the heart of their service design and ensure they apply the code. In relation to this standard, FlyingBinary sought to ascertain the age of the youngest likely user of lookafterme, and designed different user journeys for each cohort of patient outlined earlier in this report. In order to place them into their corresponding user journey, FlyingBinary intends to use the patient's assessed developmental age as opposed to their biological age. The patient's clinician determines the patient's assessed developmental age. It is the ICO's view that these approaches should provide FlyingBinary with a foundation to appropriately design their service when considering the different capacities, skills and behaviours different children display at different ages. It is also the ICO's view that the use of the assessed developmental age of the patient provides an opportunity to tailor transparency messages and pitch them at an appropriate level for the user. The ICO highlighted that there are certain potential risks in processing this personal data, such as the possibility that the clinician may provide an incorrect assessed developmental age. FlyingBinary should mitigate these risks.

3.11 FlyingBinary has also 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[6] 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.

---

[5] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/3-age-appropriate-application

[6] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

3.12 The transparency[7] standard of the Children's code states that organisations must provide privacy information and other published terms, policies and community standards in a way that is "concise, prominent, and in clear language suited to the age of the child". It also states that additional specific 'bite-sized' explanations about how personal data is processed should be provided when different uses of personal data are activated. This standard links in with the transparency requirements outlined in Articles 5(1)(a), 12, 13 and 14 of the UK GDPR. During Sandbox participation, FlyingBinary indicated that it is committed to ensuring all of its processing of personal data would be transparent, including any optional elements of lookafterme that the user can activate. FlyingBinary's use of the patient's assessed developmental age as opposed to their biological age has presented the Sandbox with an opportunity to explore the concept of transparency further. The Sandbox work has looked at how to ensure patients are presented with transparency information that is suitable to their individual capacity depending upon their different user journeys. FlyingBinary and the ICO also worked together to consider how all versions of transparency information could be made available to all users should they wish to view a version more appropriate to their individual capacity. The ICO and FlyingBinary looked at how arrangements could be made with the clinical entities to ensure transparency information is provided to data subjects at the first opportunity.

3.13 Standard nine of the Children's code relates to data sharing[8]. It states organisations must not disclose children's data unless they can demonstrate a compelling reason to do so, taking into account the best interests of the child. As mentioned in section 2.7 of this report, lookafterme is expected to contain data sharing functions. In the earlier stages of its Sandbox participation, FlyingBinary intended that all of these functions would be 'off by default' with granular activation controls provided. However, in the case of 'acute' patient cases FlyingBinary determined that it would be required to share data with the clinician, for patient health purposes. Although the ICO are not experts in the health sector, we engaged constructively to help FlyingBinary consider whether a case being deemed 'acute' is a compelling reason and so would require mandatory

[7] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/4-transparency/
[8] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/9-data-sharing/

data sharing. FlyingBinary has since determined that all data sharing options being off by default is more likely to demonstrate a 'high privacy by default' approach. Data sharing in relation to 'acute' cases will not be mandatory.

3.14 An important aspect for an organisation seeking to comply with the Children's code is a full understanding of the personal data they process about children. This understanding should help to develop a firm grasp of the potential impacts upon a child's rights from the use of the product or service. Those impacts may also constitute risks which must be assessed within a DPIA. To help organisations consider those impacts, the ICO has developed the best interests framework[9] which draws on the rights set out in the United Nations Convention on the Rights of the Child (UNCRC).

3.15 During work on objective three of the Sandbox plan, the ICO and FlyingBinary considered the best interests framework within the context of lookafterme's envisaged processing of personal data. This was an earlier iteration of the best interests framework and not the version currently published on the ICO website. Initially, the ICO helped FlyingBinary assess how lookafterme's processing of personal data may result in risks to the child's rights under the UNCRC. For example, FlyingBinary considered whether its approaches to complying with the data minimisation principle would contribute to the protection of the child's right to privacy by limiting the processing of personal data to what is necessary. FlyingBinary's approach to the provision of transparency information, which is tailored to the differing capacities of its users, was also considered under the lens of the right to parental guardianship and the evolving capacities of the child. For example, the provision of different versions of privacy information that allow children to seek more or less detail depending on their capabilities may help mitigate risks in relation to this right. Where this work identified potential risks, alongside those identified in its DPIA, FlyingBinary was able to consider their severity and identify any necessary mitigations. Following this initial phase of work in relation to the best interests framework, FlyingBinary provided feedback to the ICO on the framework's use as a tool for controllers whose processing of personal data falls within the scope of the Children's code. That feedback was particularly valuable for the ICO in areas such as, but not limited to, the most appropriate way to present the framework to external audiences, the identification of risks in a novel context and the processing of personal data that

[9] https://ico.org.uk/for-organisations/childrens-code-hub/how-to-use-our-guidance-for-standard-one-best-interests-of-the-child/children-s-code-best-interests-framework

inhabits cross-regulatory environments. The feedback was also useful in assisting with the ICO's development of the framework during its early phases.

Data minimisation

3.16 During the second objective of its Sandbox plan, FlyingBinary and the ICO worked together to consider the application of data minimisation in relation to the personal data that is expected to be processed by lookafterme. The data minimisation principle[10] of the UK GDPR, under Article 5(1)(c), requires that "Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)". In order to comply with these requirements, FlyingBinary must ensure that the personal data lookafterme processes is:

- adequate – sufficient to properly fulfil FlyingBinary's stated purpose or purposes;
- relevant – it should have a rational link to that purpose or purposes; and
- limited to what is necessary – FlyingBinary should not process more personal data than it needs for such purpose or purposes.

In addition to the UK GDPR's requirements on data minimisation, standard eight of the Children's code also relates to data minimisation[11]. It requires that organisations only collect and retain the minimum amount of personal data they need to provide elements of the service in which a child is actively and knowingly engaged. It also requires that children are given separate choices over what elements of the service they wish to activate.

[10] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/
[11] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/8-data-minimisation/

3.17 By working together, within the context of lookafterme's proposed processing of personal data, the ICO and FlyingBinary have sought to ensure that these data minimisation requirements will be adhered to. Initially, both parties sought to develop a firm understanding of FlyingBinary's purposes for processing personal data when data subjects use lookafterme. Sandbox work in this area helped to highlight the importance of defining these purposes in a detailed and granular way. That approach resulted in FlyingBinary subsequently being able to consider the personal data it plans to process in detail, and whether it would meet data minimisation requirements when considered against their purposes for processing it.

3.18 This Sandbox objective assisted FlyingBinary in identifying 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, thereby providing a solid foundation on which it could assess data minimisation requirements.

3.19 This objective also provided the ICO with the opportunity to help FlyingBinary 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. This helped FlyingBinary to identify and consider items of personal data that may not have originally been identified.

3.20 As mentioned in section 2.6 of this report, lookafterme derives additional personal data as the patient uses lookafterme. The 'detailed event' personal data and 'summary event' personal data will be shared with third parties, such as parents, guardians or clinicians, based upon different user journeys. This is summarised in more detail in sections 2.7 and 3.13. In seeking to comply with data minimisation requirements, FlyingBinary has determined that the less detailed, yet adequate, 'summary event' personal data would be shared for pathology research purposes, which seek to consider how lookafterme may be used to support additional mental health conditions. FlyingBinary intends to deidentify that personal data before sharing it As a result, FlyingBinary has sought to identify what personal data is required for different elements of the service.

Furthermore, the ICO helped FlyingBinary to consider whether particular items of personal data would need to be processed as part of the processing activities intended to help maintain the patient's mental health. For example, following discussions in the Sandbox, FlyingBinary determined that certain demographic personal data, some of which would likely constitute special category data, that it intends to collect for the research function of lookafterme would not be required for the processing activities which seek to help maintain the patient's mental health.

Lawful basis for processing

3.21 In order to process personal data lawfully under Article 6 of the UK GDPR, FlyingBinary needs to ensure that it can establish an appropriate lawful basis for processing[12] for its various processing activities. Where special category data[13] is processed, a separate condition for processing under Article 9 of the UK GDPR, will also be required.

3.22 Following the ICO's review of FlyingBinary's DPIA, during objective four of their Sandbox plan, it was agreed that objective five would include an additional assessment of this topic. FlyingBinary produced written documentation detailing its up to date assessments of appropriate lawful bases and special category conditions for processing and, in a written steer, the ICO provided their response to these assessments.

3.23 In those assessments, FlyingBinary identified that it intended to rely upon legitimate interests under Article 6(1)(f), and explicit consent under Article 9(2)(a) for its core processing activities. FlyingBinary defined its core processing activities as those which seek to support the patient's mental health, such as the onboarding of the patient, the processing of their contact details and lookafterme's online scanning functions. For their non-core processing activities, FlyingBinary determined that consent, under Article 6(1)(a), and explicit consent were appropriate to rely on. It defined its non-core processing

[12] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/
[13] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

activities as those which are aligned with lookafterme's pathology research purposes, such as FlyingBinary aggregating and seeking to deidentify personal data related to the patient's usage of lookafterme, before sharing it with clinical researchers who will carry out research as described earlier in this report.

3.24 Whilst the identification of appropriate lawful bases and special category conditions for processing ultimately remains the responsibility of the relevant controller, this work allowed the ICO to consider FlyingBinary's rationale for relying on the above mentioned lawful bases, and to provide guidance in relation to those assessments.

3.25 The ICO agreed that based upon the information provided by FlyingBinary in relation to its core processing activities, legitimate interests is likely to be the most appropriate lawful basis for it to rely on. In support of that assessment, FlyingBinary provided a legitimate interests assessment (LIA). Whilst a full review of that LIA was not within the scope of the Sandbox work, it presented the ICO with the opportunity to provide initial feedback to FlyingBinary as it continues to develop its LIA. The ICO clarified that FlyingBinary could consider its commercial interests and the potential expansion of the lookafterme service as part of its legitimate interests. Those aspects could also be considered within the context of potential wider societal benefits should lookafterme's scope be extended to additional pathologies in the future. In each case, these additional legitimate interests would need to be balanced against the rights and freedoms of the individuals whose personal data is processed. In addition, we were able to advise FlyingBinary on the importance of ensuring the specific interests of children, which have been considered during Sandbox participation in specific reference to the requirements of the Children's code, are included within its LIA.

3.26 The ICO also accepted that it may be possible for FlyingBinary to rely upon consent and explicit consent, at least for some of its processing activities. However, the ICO advised that caution should be exercised by FlyingBinary in determining if and when consent is appropriate to rely on as we deemed there to be certain potential issues that required FlyingBinary's detailed assessment. Whilst it is not possible to summarise all of the advice provided during Sandbox participation within this report, we recommended that FlyingBinary assess in detail whether consent could be considered to be freely given and

valid, particularly within a clinical context. For example, our guidance details that consent can be inappropriate[14] if there is a clear imbalance of power between the individual and the controller, such as in circumstances when this results in consent not being freely given. It is also particularly important to assess the validity of consent provided by children, given the context within which lookafterme is expected to operate.

3.27 The ICO also recommended that FlyingBinary consider whether additional special category conditions for processing could apply to its processing activities. For example, the health or social care condition, under Article 9(2)(h) of the UK GDPR, and substantial public interest, under Article 9(2)(g), were mentioned by the ICO as possibilities. Both of these conditions require additional conditions or safeguards, as set out in the DPA 2018, to be satisfied. For example, the ICO and FlyingBinary considered whether paragraph 18 of Schedule 1 of the DPA 2018 (Safeguarding of children and at risk individuals) could be an appropriate substantial public interest that it could rely on to process special category data for certain processing activities. This might be relevant in circumstances in which the special category data of third party individuals is included within website content or social media posts, and lookafterme assesses this content for suitability on the user's request. Reliance on this public interest is subject to meeting paragraph 18's requirements in their entirety.

Data protection impact assessment

3.28 As mentioned earlier in this report, FlyingBinary produced a draft DPIA[15] which sought to outline the risks and subsequent mitigations, associated with lookafterme's processing of personal data. The ICO reviewed the content of that DPIA as part of the work carried out in the Sandbox.

---

[14] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/#when5

[15] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments

3.29 A DPIA must be carried out under the UK GDPR, where the processing of personal data is likely to result in a high risk to individuals. It is also good practice to carry out a DPIA for any other major project that requires the processing of personal data. The ICO's guidance outlines certain specific triggers which are likely to result in the processing of personal data being deemed to be high risk and what a DPIA must include. FlyingBinary determined that its processing met some of those triggers, such as the processing of sensitive data or data of a highly personal nature, and data concerning vulnerable data subjects. As a result, FlyingBinary had to produce a DPIA in order to help identify and minimise the risks of lookafterme's processing of personal data.

3.30 As part of this process, FlyingBinary has stated that it has sought to take what it terms to be a 'regulation by design' approach during the design of lookafterme. It produced a core DPIA document, as well as additional documents which sought to provide further detail, with the stated intention of ensuring strong risk management techniques were deployed during lookafterme's design phase. FlyingBinary also determined that its Sandbox participation would precede the creation of code in relation to the development and deployment of lookafterme.

3.31 Following the carrying out of a detailed DPIA, FlyingBinary identified certain key data protection risks that required further assessment. Subsequently, the ICO and FlyingBinary agreed to focus on assessing those risks in more detail at the end of its participation in the Sandbox. For example the data protection roles and responsibilities and lawful basis themes, as outlined earlier in this report, were assessed more closely. Using chapter two of the ICO's draft guidance on anonymisation, pseudonymisation and privacy enhancing technologies[16], FlyingBinary also assessed whether the data it is seeking to deidentify, in differing contexts, would constitute anonymous or pseudonymous data under the UK GDPR.

3.32 As a result of carrying out its DPIA, FlyingBinary was better able to identify potential risks. After identifying a risk in relation to the incorrect assignment of data protection roles, and consequently apportioning responsibilities under the UK GDPR incorrectly, the ICO then helped FlyingBinary to assess more closely where a joint controller relationship might be

[16] https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-anonymisation-pseudonymisation-and-privacy-enhancing-technologies-guidance

established. As a result, it understood which processing activities would require further steps, such as implementing transparent arrangements, to ensure it is adhering to the requirements of the UK GDPR. The risks identified included the potential for unlawful processing of personal data if the incorrect lawful basis or special category condition for processing was applied. This risk prompted the ICO and FlyingBinary to consider the application of alternative lawful bases in more detail, as explained earlier in this report. In seeking to mitigate that risk, the ICO were able to provide FlyingBinary with informal opinions on the appropriateness of the lawful bases and special category conditions it had identified, as well as key areas it would need to consider further such as whether consent can be valid within a clinical context. Also, FlyingBinary's DPIA assessed a number of risks that could potentially impact upon an individual's rights, such as personal data breaches or inaccurate personal data, and how those risks could be mitigated.

3.33 The ICO and FlyingBinary were also able to discuss the advantages and disadvantages of using additional documents to provide extra detail in support of a central DPIA document. It was determined that such an approach can be useful in providing additional context to the processing of personal data that is expected to be carried out. However, that determination is subject to certain criteria. For example the central DPIA document must sufficiently adhere to all of the requirements set out in the relevant articles of the UK GDPR and sufficiently describe the processing of personal data within the central document. It is also important that the additional supporting documents be regularly reviewed, and updated where required, to accurately reflect the processing of personal data that is to be carried out.

3.34 In reviewing its DPIA, the ICO was able to provide FlyingBinary with detailed feedback relating to how its DPIA should be further developed and kept under continuous review. For example, the ICO advised FlyingBinary that within the DPIA it should develop and expand how it specifically plans to ensure individual rights requests will be appropriately dealt with and how it will ensure compliance with the data protection principles outlined in the UK GDPR. In respect of the latter, it was discussed that the high-level outcomes of the Sandbox work on data minimisation could be used to detail what FlyingBinary's approach to complying with that principle would entail. It was also noted that FlyingBinary has sought to take a detailed and proactive approach to the mitigation of risks identified within the DPIA. FlyingBinary took a dual approach. Firstly a number of baseline mitigations were applied to all of the risks identified within the DPIA. Then, additional risk

specific mitigations were applied to those risks where it was deemed that the baseline mitigation did not sufficiently reduce the identified risk.

3.35 By carrying out this work, both the ICO and FlyingBinary were able to consider risks faced by industry parties seeking to develop novel technologies which process personal data that falls within the scope of the Children's code. Within that context, it was found to be particularly useful to make use of the best interests framework to consider additional risks to children which can then be used to supplement and further inform personal data processing risks that would be captured within the remit of a DPIA.

4. Ending statement

4.1 FlyingBinary's participation in the Sandbox has helped the ICO to continue to develop and build upon its knowledge of the challenges that technology providers can face in seeking to comply with the requirements of the UK GDPR, the DPA 2018 and the Children's code. The Sandbox gave the ICO and FlyingBinary valuable insights into how industry can implement data protection by design and default and the opportunities that this approach can bring. The ICO and FlyingBinary have learnt how industry can use new regulatory requirements as a starting point to design online services to help children within a clinical context. This also allows us to explore fundamental data protection themes. For example, how to establish appropriate roles and responsibilities when different parties exercise different levels of influence over the purposes and means of processing. This is particularly important as the ICO and industry seek to protect the rights and privacy of children online.

4.2 The ICO and FlyingBinary have also considered the risks to children from the processing of their personal data within an online service. The ICO and FlyingBinary considered these risks within the contexts of data protection legislation, the

Children's code, the best interests framework[17] and FlyingBinary's experience of their sector. This helps to demonstrate how to consider risks across multiple contexts and how organisations can then assess those risks to keep children safe online.

4.3 The Children's code came into force on 2 September 2021 and has since seen authorities from different jurisdictions considering the introduction of similar frameworks of their own. As the international discussion around children's online privacy grows, this Sandbox project shows the importance of building regulatory requirements into product and service designs. This is particularly important when developing innovative products or services which involve children. The ICO and FlyingBinary have had a constructive and positive relationship throughout the project. This demonstrates the ICO's role as a trusted information rights regulator, whilst also showing that data protection compliance is not a barrier to innovation.

[17] The best interests of the child is a foundational principle within the code. It is drawn from Article 3 of the UN Convention on the Rights of the Child (UNCRC) within which the code is grounded.