Yubo

Age Appropriate Design Code Audit Report

November 2022

Executive summary

Background & Scope

Under section 123(1) of the Data Protection Act 2018 (DPA18), the Information Commissioner produced a code of practice on standards of age appropriate design ("the Code"). The Code applies to "relevant information society services which are likely to be accessed by children" in the UK. This includes many 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. It is not restricted to services specifically directed at children.

The Code sets out 15 headline standards of age appropriate design that companies need to implement to ensure their services appropriately safeguard children's personal data and process children's personal data fairly. The Code came into force on 2 September 2021.

More widely, the Information Commissioner is also responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UKGDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

Yubo agreed to a consensual audit of the measures, processes, and policies they have in place to demonstrate conformance with the Code and data protection legislation.

The purpose of the audit is to provide the ICO and Yubo with an independent assurance of the extent to which Yubo, within the scope of this agreed audit, is complying with the Code and data protection legislation.

The scope areas covered by this audit are determined following a risk based analysis of Yubo's processing of UK children's personal data. The scope may take into account any data protection issues or risks which are specific to Yubo, identified from ICO intelligence or Yubo's own concerns, and/or any data protection issues or risks which affect their specific sector or

organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of Yubo, the nature and extent of Yubo's processing of children's personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to Yubo.

It was agreed that the audit would focus on the following areas:

- *A: Governance, Transparency and Rights*
- *B: Due Diligence and Data Protection Impact Assessments (DPIAs)*
- *C: Data Minimisation and Sharing*
- *D: Age Assurance*
- *E: Detrimental Use*
- *F: Privacy Settings and Parental Controls*
- *G: Geolocation*
- *H: Profiling and Cookies*
- *I: Nudge Techniques*
- *J: Artificial Intelligence (AI)*

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and a virtual review of evidential documentation.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate conformance with the Code and data protection legislation. In order to assist Yubo in implementing the recommendations each has been assigned a priority rating based upon the risks to children that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. Yubo priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Overview of Service and Processing

Twelve App SAS – trading as Yubo – is a French app developer that is headquartered in Paris with a UK office in London. Twelve App was founded in 2015 when the Yubo social discovery app (formerly known as Yellow) was first launched.

Yubo's ethos is to have safety at the core of every decision made; Yubo has adopted a safety-by-design approach across the organisation which is guided by its '4 pillars of safety': risk prevention for all users, detection and real-time intervention, team expertise, and user education. All new Yubo staff spend one week observing the AI and human moderation in place as part of their induction programme, in order to better understand and appreciate the potential risks to real child users on their app.

Yubo is constantly evolving and upgrading the Yubo app in order to protect, support, and educate young people and build positive connections in a safe digital space. App development is subject to oversight by the independent Yubo Safety Board, which comprises industry experts on digital safety and children's privacy.

The Yubo app is currently available on iOS and Android. Yubo believes that the Age-Appropriate Design Code (AADC) applies as the Yubo app is accessed by UK children under 18 years.

The Yubo app facilitates online social connections using features such as Lives with video and audio interaction between users, direct online messaging between users, and the Swipes feature to find new social connections based on mutual interests and subject to mutual acceptance.

To enforce a minimum user age of 13 years, Yubo has deployed a combination of age assurance measures to new and existing users on the app, including a third-party age estimation AI tool, in-house age verification from ID documents, and in-house automated age detection/ moderation tools.

A range of protective measures are applied to all users, including UK child users, including: age gates to separate users into different communities based on their age range, enforced community standards, high privacy default settings, minimal use of profiling, no targeted advertising or marketing, and an aversion to using nudge techniques to influence child users negatively.

Yubo has also deployed a range of AI and human detection and moderation tools in order to ensure user content is age appropriate, including text moderation of user profiles and messages, video moderation of Live streams, and audio moderation which is currently being implemented in selected regions. Content is moderated based on a wide range of triggers relating to grooming patterns, child sexual abuse material, child pornography material, bullying, nudity, sexual content, requests and offers of sex, sexual exploitation, harassment, sextortion, explicit/ graphic material eg blood and gore, drugs, firearms, hate symbols, pornography, spam messages, promotion of products/ services, requesting payment details, and users sharing personal data specific to child safety. Yubo has partnerships with industry-leading child safety organisations such as NCMEC, IWF and Thorn and uses their databases to detect threats.

Yubo's general approach to data is to collect only the minimal data absolutely necessary and ensure use of personal data does not have a detrimental impact on any user, whether the user is a child or not. Users are required to create an account and provide some personal data to access the app, and after this the majority of personal data processed is user messages and content generated during app use. Data processing activities are scrutinised by the Legal team and DPO, and new or proposed changes to data processing or functionality are assessed in a DPIA and approved before implementation.

Users are informed about data processing taking place through the Privacy Policy and Terms of Use, which are available on Yubo's website and signposted to the user during account creation. Yubo has also produced a suite of videos and graphics providing specific privacy information in a more age-appropriate format such as a 'Your Privacy at a Glance' and 'Security tips' pages, and plans to integrate these into a new Privacy Centre for launch in 2023.

Audit Summary

Overall Assurance Rating	Overall Opinion
Reasonable	There is a reasonable level of assurance that processes and procedures are in place, that the organisation is in conformance with the AADC and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-conformance with both the AADC and data protection legislation.

Scope area	Assurance Rating
Governance, Transparency & Rights	Reasonable
Due Diligence & DPIAs	Reasonable
Minimisation & Sharing	Reasonable
Age Assurance	High
Detrimental Use	Reasonable
Privacy Settings & Parental Controls	Reasonable
Geolocation	High
Profiling & Cookies	Reasonable
Nudge Techniques	Reasonable
Artificial Intelligence (AI)	Limited

*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

Areas for Improvement

The privacy management framework should be embedded further, by documenting the approach to data protection and children's privacy in sufficiently comprehensive policy documents, documenting role-based training needs and required knowledge of data protection and children's privacy for all relevant personnel, and formalising the DPIA and risk management processes.

High-level information and privacy risks, including those related to the processing of children's data, should be recorded in a centralised risk register, which should be used to track and monitor the status, severity and ownership of such risks, as well as to monitor the effectiveness of ongoing mitigating controls.

Privacy information and user documents presented to child users should be in an age-appropriate format and clearly understandable so child users are fully informed how their personal data is processed. Age-appropriate informative messages or bite-sized privacy information should be provided at the point that processing takes place or is activated, and child users should be nudged to speak to parents or trusted adults if they do not understand.

When designing and developing online services with the best interests of children as a primary consideration, all material risks and potential online harms to child users should be assessed and documented, for example the risks of commercial exploitation and excessive engagement. Safeguards and protective measures should be implemented to mitigate these risks, and should be reviewed regularly to monitor their effectiveness.

AI systems that are processing children's data should be closely monitored, and statistical accuracy/ discriminative bias assessed regularly. Gaps in protective measures and safeguards in place should be identified – such as content areas where AI detection/ moderation systems are not fully deployed – and mitigations implemented. Planned improvement actions for AI systems should be documented and a prioritised based on risk.

Best Practice

Yubo appointed an independent Safety Board in 2018 to provide advice, guidance and scrutiny to Yubo around its approach to user safety. The Safety Board is made up of experts in child protection, online safety and other related fields, and can be contacted at any time about specific safety matters, such as when new product features are being developed.

All new Yubo staff are required to receive basic data protection training and spend one week working alongside human moderators in the safety team during the onboarding process. Yubo believes it is important that new staff can understand the need for user safety on the platform and can experience first-hand what inappropriate content and behaviours look like, and how these are moderated by Yubo.

Yubo has produced a number of short age appropriate videos and content that child users can access via the Support Centre on Yubo.live or Yubo's YouTube channel that cover a range of topics including privacy and online safety. The videos use animations, graphics, text and audio which are likely to appeal to younger users. Yubo intends to continue to build this library by adding additional relevant videos for children, which will further strengthen existing resources and educate and inform users about important privacy and safety issues, as well as to explain the features of the Yubo app that can support these matters.

Yubo uses the swipe feature feed to promote wellbeing campaigns and provide wellbeing-enhancing resources and support to all users including child users, including previous campaigns around sexual harassment, the in-app muted words feature, anti-bullying, young mental health, and safer internet use.

Yubo has introduced the 'muted words' feature which allows child users to pre-set words that they do not want to see and automatically filter messages containing these. This helps to ensure that child users are not subject to content that might be specifically harmful or a trigger to them.

Yubo uses moderation warning messages and real-time alerts to educate users by explaining the community rules in place, informing them exactly how they violated these, and nudging them towards more positive behaviours.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the engagement and are not necessarily a comprehensive statement of all the areas requiring improvement. The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Yubo.

We take all reasonable care to ensure that our report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is solely for the use of Yubo. The scope areas and controls covered have been tailored to this engagement and, as a result, the report is not intended to be used in comparison with other ICO report.