Ubisoft

Age Appropriate Design Code Audit Report

November 2021

Information Commissioner's Office

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.

Ubisoft 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 Ubisoft with an independent assurance of the extent to which Ubisoft, within the scope of this agreed audit, is complying with data protection legislation.

The scope areas covered by this audit are determined following a risk based analysis of Ubisoft processing of children's personal data. The scope may take into account any data protection issues or risks which are specific to Ubisoft, identified from ICO intelligence or Ubisoft'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 Ubisoft, the nature and extent of Ubisoft processing of children's personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to Ubisoft.

It was agreed that the audit would focus on the following area(s):

- A: Governance and Accountability
- B: Due Diligence
- C: DPIAs
- D: Transparency
- E: Age Assurance
- F: Detrimental Use
- G: Default Privacy Settings
- H: Data Minimisation
- I: Data Sharing
- J: Geolocation
- K: Parental Controls
- L: Profiling
- M: Nudge Techniques
- N: Connected Toys and Devices
- O: Children's Rights

Audits are conducted following the Information Commissioner's audit methodology. The key elements of this are normally a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

However, due to the outbreak of Covid-19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore Ubisoft agreed to conduct the audit on both a remote and onsite basis. A desk based review of selected policies and procedures and remote telephone interviews were conducted from 3 August to 20 October. The ICO team also visited Ubisoft's Consumer Relationship Centre in Newcastle on 5 and 6 October. The ICO would like to thank Ubisoft for its flexibility and commitment to the audit during difficult and challenging circumstances.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate conformance with the Code and data protection legislation.

Overview of Service and Processing

Ubisoft are a multinational gaming company, selling console, desktop, and mobile games. Headquartered in France, they have development studios all over the world, and sell in the vast majority of countries. Ubisoft have a Consumer Relationship Centre in Newcastle, which takes the lead on

managing their consumer relationships for Europe, Middle East, and Africa (EMEA). At their head office in France, there is a well resourced Data Privacy Team headed by the Global Data Protection Officer (DPO). He has a number of Deputy DPOs who function as DPO for specified regions (for example DPO for UK and Europe).

Ubisoft gather a limited amount of personal data, having consciously made efforts to minimise the amount of personal data they process.

Players of console and desktop games are required to create an account with Ubisoft, which requires some personal data. Players have to indicate their age at the creation of the Ubisoft account. On PC, in the context of free to play games, if they are between 13 years old and the age of consent subject to applicable local law, the account creation process switch to Young Player accounts with specific functionalities to protect minors and give visibility to parents on their spending, friends added, and playtime.

Mobile games do not require an account to be created. Small amounts of data is gathered by Ubisoft during gameplay to track performance issues, however consent based processing activities including the sharing of data with 3rd party can be turned off and is automatically turned off for mobile's players who self-identify as under 16.

Areas for Improvement

Ubisoft have only recently begun their Age Appropriate Design Code (AADC) journey, and so have work to do in terms of factoring in specific consideration of risks to children and their privacy. Their broader privacy environment is well developed, and so the requirement is to adjust the existing controls rather than build new controls from scratch in order to bring them into compliance with the AADC.

Good Practice

Ubisoft have utilised their user research and testing lab to trial their privacy information and ensure it is effective with different age groups and target audiences. Utilising their already existing user research methods and resources has ensured that Ubisoft have high confidence in their findings regarding privacy information, and can implement improvements or changes effectively.

Ubisoft have a strong privacy infrastructure across the organisation, including a well resourced Data Privacy Team and a network of privacy champions embedded across all business units. There is clear and

effective senior governance in place, with Executive level steering committees overseeing a range of privacy and AADC related projects, and the tone from the top on privacy appears to be unambiguous and positive.

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 Ubisoft.

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 Ubisoft. 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