ICO - Age-appropriate design code consultation response

About us

A provider of ISS likely to be accessed by children.

Yoti provides a consumer-focused digital identity platform and related services to a general audience. Our main product is an app through which individuals can prove identity and age. Our other products include a password manager, a way to establish and prove relationships between people, and B2B products such as age estimation technology, document e-sign and an ID document checking service.

Yoti has deliberately chosen to include privacy, security, transparency, data minimisation and accountability as part of its business principles. One aspect of this is that we have architected our digital identity app so we have no access to user data. Yoti's focus is to provide individuals with a secure and privacy-friendly way to prove their identity and age by only sharing the minimum details necessary.

General comments

Yoti is a company which focuses keenly on privacy and ethics; as such we very much laud the intent behind the code. We would like to take this opportunity however to outline some of the practical implications we foresee in implementing the code.

We would also welcome a session with the ICO to set out the complexities for implementing age verification - even for an organisation who is specialised in this area.

We would also welcome open discussion on how age estimation could support the code's requirements. At present this technology is only available for young people over 13, due to the lack of consented, ethically-sourced image and age datasets of under 13s required to train and develop the technology.

It is useful to see examples in the code of good and poor practice. However, it is worth bearing in mind that the technical solutions required to make the good practice examples work are not necessarily straightforward.

To help put our comments into context, here is a non-exhaustive set of requirements that any product development aimed at a general audience has to consider if it is operating globally.

- Recognition of territory where an individual is located - is a country code deemed sufficient?
- Approach to age verification.
- Approach to spot where a child lies about a self-asserted age or provides false information.
- Ability to send parent / guardian privacy information and consent requests where needed that is streamlined and that parents will engage with.
- Providing country- or region-specific consent options, for example, EU parental consent to specific processing; US parental consent to all personal data processing.
- A record of the consent for both child and parent / guardian.
- Ability for parent to revoke consent easily at any time.
- Separate revoke consent options for EU and non-EU, and possibly several opt-outs of several activities.
- Ability to prompt child for their own consent when they get to the relevant age and remove the ability for the parent / guardian to revoke consent.

- Allowing for a two-tier approach for countries like France where consent-based data processing of under 13s requires parental consent; whereas for 13-14s requires dual parent and child consent.
- Allowing parents to have the requisite degree of control, for example, in the US that may include getting additional consents for specific actions or other products available.

These issues are even more acute for apps where you have a small screen and devices tend to be personal to each individual rather than shared, as a household laptop may be.

This then poses a further set of challenges.

- How to provide the privacy information that meets legal requirements on a small phone screen.
- How to mitigate the risk that the person giving consent isn't the real parent / guardian, for example, by asking for a self-declaration of age, using technology to estimate that a parent or guardian is an adult over 18 or over 25, or requiring other hard proof?
- What will be a parent's tolerance for volume of consents per day or week for them to respond? Does this otherwise lead to the unintended consequence of only the most dedicated parents complying and the rest zoning out...or suppliers redesigning services to avoid the need to keep getting consents from parents for product activity by limiting what under 13s can do?
- How to manage multiple consents and revocation of some or all consents.
- How to manage parental consent when parents or guardians of a child disagree.
- How to support young people in care or without an active parent or guardian.

Organisations which provide safety-enhancing services, such as password managers or identity services which are privacy-preserving are providing a useful tool to people of all ages. This type of service will be severely impacted by a blanket approach which requires a default of treating all UK users as under 18 initially until age verification is put in place.

This is complex, given that any company operating globally will be faced with multiple different thresholds of ages and the different requirements of COPPA and GDPR which currently conflict. It would be useful to convene a working group with wider industry to review how this will be achieved as this is currently the missing link and the elephant in the room.

'About this code' section

On the face of it the section is clear. However, the code does not necessarily contain all the elements that this section of the code says it does. The focus of the code is on children's privacy, not the other Convention rights listed.

'Services covered by this code' section

Although the ICO's starting point for the code is the wording in the DPA 2018, the code fails to take or promote the risk-based approach from the GDPR. The code will disproportionately affect small businesses, start-ups, charities and non-profits who do not have the resources to carry out extensive market research or be able to apply in full all the requirements of the code. The code is not scalable; it takes an 'all or nothing' approach for every organisation.

The main intent behind the code is to limit or avoid negative impacts on under 18s from online products and services not designed with them in mind. However, there are significant differences between products and services with addictive qualities, or that could provide inappropriate content or experiences, and those that are safety-enhancing or educational. The code makes no such distinction and a risk-based approach would allow organisations to focus efforts on where there is risk of harm or detriment. One example is a password manager. A tiny percent of the UK market uses one and an even smaller percentage of these users are under 18. The entire aim of this product is to keep people safer online by generating and storing secure passwords and avoiding the risks that come with individuals choosing weak passwords and reusing passwords across products because they have to remember so many. It would be disproportionate to require a global password manager product to implement the entire code for a tiny percentage of the UK market when there is no child-specific risk with this type of product.

Standards

Best interests of the child

It is important the ICO does not underestimate the time, effort and resources required to consider the best interests of every single under-18 age group, their developmental differences, and the associated standards in this code, and incorporate these into every product or service that is aimed at a general audience. There is a risk that smaller companies simply cannot compete with the larger tech organisations.

It would be helpful to have clarity from the ICO about its expectations for scale and how it intends to support smaller organisations.

Age-appropriate application

The code has purposefully avoided how age verification will be implemented. Even organisations who have taken part in the development of age verification for over 18s are just starting to address how to age verify or age estimate younger users.

It is worth the ICO being aware that these requirements will impact products and services that protect children online but that are general audience products and have no specific risks for under 18s, such as password managers. It would seem a disproportionate requirement for these providers to develop or maintain, for example, different versions of T&C and privacy notices, or to not collect any anonymous statistics on how their product is used, unless they age verify users upfront.

With regard to robust age verification checks an organisation will need to collect certain information that they can rely on to provide age. If they choose to use a third-party provider, that provider will also need reliable age information. It is worth noting that under 18s have fewer identity or other documents available that would contain reliable age information, such as a date of birth. According to HMPO statistics approximately 34% of young people under 18 do not have a passport. (Freedom of information request from HMPO data, mapped against UK population stats per age band.)

Given the time, resource and cost implications of applying the code’s requirements, organisations with products / services aimed at a general audience should be able to take a risk-based approach to determine whether designing for each specific age-band listed is appropriate. In some circumstances it may be appropriate to categorise users as 0-12, 13-17 and 18+ where designing for these age bands instead does not present significant risks.

Transparency

There is a practical challenge for organisations with app-based products to provide alternative or multiple versions of privacy information / T&C, including videos. These can significantly increase the size of the app. This requirement could lead industry players towards choosing embedded web solutions instead to achieve compliance, but ultimately this degrades the final UX for users, and can lead to performance issues with websites if they have more data, images and videos to load.

App store rules require apps to provide the privacy notice and T&C within the app. It is not allowed to link out to web-based content. The in-app version is very limited as regards formatting and layout and has to be text-only. Therefore, the reality will be that the full, written privacy information will have to continue to be the only one available in an app, with other versions linked to and hosted elsewhere.

When a product or service asks for an access permission (such as location, contacts, camera, storage files and so on) it is the operating system that provides the pop-up mechanism and copy it contains. For apps: organisations cannot edit the copy on Android. It uses the name of the app and decides the rest of the permission phrasing. Organisations have limited ability to edit the copy on iOS with one line for a 'usage description' string. This means that organisations are prevented from being as transparent as they would like to be or as precise as they would like to be. Organisations can of course provide their own information before the user sees the pop-up permission screen, but the user can be confused by what appears to be different information. The same is true for web-based products.

Detrimental use of data

It would be helpful for the ICO to acknowledge the link between different standards in the code, such as where some element of profiling will be required to comply with this standard on avoiding detrimental use of data. For example, a provider may need to deliver information on other products and services only to certain age groups, or avoid that certain age groups receive it.

Policies and community standards

No comments.

Default settings

We would appreciate clarity as to the ICO expectations for implementing this standard where an organisation has already taken privacy-protecting steps for all users to make sure that information from cookies / analytics is de-identified and reports are never run at individual user level, only at aggregate level.

Similarly, if a provider uses techniques such as notifications, but these are minimal, age appropriate, and sent at appropriate times, then risks have been mitigated and it would seem disproportionate to have to turn them off by default.

It would be helpful to have clarity from the ICO as regards an organisation’s use of data for internal R&D, where the aim of that R&D is to develop and strengthen fraud prevention and security measures or to develop identity and age-verification technology.

Data minimisation

It would be helpful to have clarity from the ICO about what kinds of activities it would consider similar enough to be categorised together as an improvement or personalisation of service. For example, data collection to identify and fix bugs, tailoring content to fit the device being used or geographical location. With regard to personalisation services, it is worth noting that the user is the recipient and beneficiary of this data processing.

There is a balance to be struck between granularity of choice and being overwhelmed with information and choices. Given the many studies showing that individuals do not read privacy notices, it would be unreasonable to expect children to navigate a long list of choices.

It is worth noting that some elements of a service involve data collection and use that the user has no choice over, but that is integral to what is being provided, such as security measures and activity for fraud prevention.

Data sharing
It would be helpful for the ICO to clarify that certain data sharing would be for a compelling reason in the best interests of the child. For example, sharing with processors to provide aspects of the product or service, or sharing with other organisations for security, fraud detection and prevention purposes

Geolocation
It is worth the ICO being aware that where websites or apps ask for permissions, such as to access location, these settings are controlled by the user. Once a permission is given, the user has to revoke that permission from their settings, the organisation that requested it cannot do so. Some operating systems, but not all, provide users with options to allow location access once or always.

With regard to the requirement to provide a clear indication of when the child's location is and isn't being tracked, it is worth noting that mobile devices do this automatically at operating-system level.

It is worth noting that some uses of geolocation data are for fraud prevention measures and so cannot be subject to user choice.

Parental controls
It is worth the ICO being aware that companies subject to US COPPA requirements may be legally required to provide full parental access and control to children's accounts / data.

Profiling
It would be helpful to get clarity from the ICO on different types of profiling that may all meet the GDPR definition, but which are very different with regards to impact, outcome and privacy intrusion. Analytics showing de-identified statistics on how individuals use a product / service are very different from a user profile containing various information linked to an identifiable individual, that is sold on to others

It is worth noting that delivering the requirements of this code will require some kind of profiling, such as age or location flags on an account to deliver appropriate content or settings.

Nudge techniques
No comments.

Connected toys and devices
No comments.
Online tools
It is worth the ICO being aware that icons and audio prompts add significantly to the size of a website or app, which impacts on the capacity of the user's device. This requirement could lead industry players towards choosing embedded web solutions to achieve compliance, but ultimately this degrades the final UX for users and can lead to performance issues with websites if they have more data, images and videos to load.

DPIAs
It is slightly concerning to see the ICO state that organisations must do a DPIA or should already have a DPIA for online services that are likely to be accessed by children. This does not align with GDPR and DPA 2018 requirements or ICO DPIA guidance. ICO guidance states that DPIAs are required where organisations are 'offering online services directly to children'. Not 'services likely to be accessed by children'. If there are no other criteria present that would make a DPIA necessary, then a DPIA is not legally required. The code would appear to be going above and beyond and contradicting the ICO's other guidance on DPIAs. This may seem like a nuance but it is an important part of the law's risk-based approach that organisations consider risk. Blanket requirements regardless of risk undermine this.

Full DPIAs are also not always necessary where an organisation is adopting a privacy-by-design approach, and where it adopts this for all users, regardless of age. It would be helpful to have clarity on whether an organisation being able to demonstrate this approach, risks identified and mitigating solutions through the design and development process would be considered valid compliance with this standard.

It would be helpful to get clarity as regards DPIAs for products / services that have already been developed. Organisations, particularly those who are start-ups, SMEs, charities and non-profits will be unlikely to have the resources to carry out retrospective full DPIAs. It would be helpful to understand whether a review to determine if there are any child-specific issues and an action plan to address any found would be considered an appropriate risk assessment.

Governance and accountability
Many organisations will have the elements of accountability already set up and it is unlikely that they will have the resources to create a parallel structure just for children. It would be disproportionate for the ICO to require this. If organisations can incorporate risks to children into existing governance and accountability structures, this should be considered a valid approach.

Organisations may in practice not differentiate under 18 users or customers where privacy-protecting measures are in place for all users equally, and there are no residual child-specific risks.

Annex B: Lawful basis for processing

As regards the section on the 'contract' lawful basis on page 105, is this intended to mean that in the event that a contract is considered void, at that point in time you no longer have a lawful basis to process the data of those affected?

Or do you mean that an organisation can never use the contract lawful basis for data processing for children who are too young to legally enter into a contract?

If the latter this would be a remarkable statement to make and leave organisations unable to offer online services to children under a certain age as they would not have any lawful basis. For example, to use a password manager the provider needs to collect and store the website URLs and login details for all the sites a user enters and wants to use the product for. This is clearly processing necessary to provide the product the user has signed up for and there is no other suitable lawful basis.

As regards the section on parental consent and third-party mechanisms on page 109, a 'yes / no' response to whether you have parental responsibility is too weak if the organisation getting the consent is required to have evidence or an audit trail. An organisation would have to rely on the third-party provider collecting and retaining evidence and this is an issue that no organisation has managed to resolve yet, given the limited types of evidence such as birth certificates or adoption certificates that prove an individual is a parent / guardian. A proxy may be all that is possible; such as an assertion or evidence that the person is over 18 or 25.

The organisation trying to get parental consent may need different evidence depending on what they are getting consent for, meaning the third-party provider would need to collect all possible types of evidence, which is excessive and disproportionate. Many current methods for parental consent do not prevent older siblings or strangers from asserting they have parental responsibility.

As a minimum the third-party provider or the organisation getting consent directly does need to collect information about the identity of the person claiming parental consent. It would be helpful to have clarity from the ICO about how to verify parental responsibility and what methods are considered robust enough to be relied on.

Transition period

The ICO should not underestimate the time and resources required to implement the code's requirements, especially if there is no accommodation for a risk-based approach. We estimate organisations will need 6-9 months on average to build and test the required changes to products and services. The more products and services that are affected, the longer an organisation will need.

Organisations need to build this time into their development roadmaps, but will need the final approved version of the code to begin planning and estimating time and resources required for all the elements involved.

Therefore, we think a longer transition period will be needed, even more so if time is short between Parliamentary approval and entry into force of the code.

Further work, research or innovation – and collaboration

We think the issues raised by the code should be looked into before publication, as well as there being workshops and research after publication to look at examples of practical implementation, unintended consequences, and the extent to which online service providers have changed their services to be 18+ and why.

For pre-publication work we would also welcome a session with the ICO to outline the complexities for implementing age verification, and investigate possible solutions.

We are considering how Yoti Sign could be used to gather parental consent in certain circumstances, for instance where an audit trail or formal documentation is required and where there is no current platform or website. We have out in a Sandbox application on this topic.

Yoti is also keen to work with regulators to develop a robust parental consent mechanism both for our products and for other companies. We are keen to be able to offer AV solutions, but need ICO support in developing options, given the challenges set out, and the lack of data with which or against which organisations can age verify under 13s.