PRIVACY PARTNERSHIP

AGE Appropriate Design Action Plan

SEPTEMBER 2020

Age Appropriate Design Code.

Checklist and Action Plan

At a glance

- **The Code introduces new rules for processing children's personal data in relation to online services**
- **It requires organizations to create transparent and protected environments for children online, follow 15 standards for protecting children's data online, to always consider the best interests of the child when providing online services and to implement the highest level of privacy settings by default for child users.**
- **Organisations who are covered by the Code must comply by 2nd September 2021**
- **Children up to the age of 18 are protected under the Code**
- **The Code covers overs all online services accessible to children not just those aimed at them (it will be exceptional that an organization offering services online is not covered by the Code)**
- **The Code may require significant (and potentially costly) technical changes, for example, in relation to new in-app prompts and notices, age gates and age verification, removal of nudge techniques and new settings for geo-location data**
- **The ICO has said that if an organization is subject to an investigation and cannot show that they took steps to comply with the Code they are more likely to be subject to regulatory action including fines under the GDPR.**

Our Action Plan summarises the Code and highlights key areas businesses caught by the Code need to focus on. Please get in touch if you need further advice or support by contacting admin@privacypartnership.com

Overview

The UK Information Commissioner has introduced a new Code of Practice for processing Children's personal data in the context of online services. **The Age Appropriate Design Code** ("the Code") https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf

has been passed by Parliament but there is a 1-year transition period until 2nd September 2021 allowing organizations time to take the steps necessary to bring themselves into compliance with the Code.

The Code is a Statutory Code of Practice under the Data Protection Act 2018 and sets out 15 standards explaining how GDPR applies to children using online services.

Who does it apply to?

The scope of the Code is exceptionally wide. The UK Information Commissioner (ICO) has said that, as "a starting point, you should note that we expect most online services used by children to be covered, and those that aren't covered to be exceptional".

The Code applies to organizations with establishments, branches or offices in the UK and to providers based outside of the EEA if their services are provided to or monitor users based in the UK. It does not currently apply to an organisation established in the EEA with no UK establishment (even if it is offering services to UK users or monitoring the behaviour of users in the UK).

What services does the Code cover?

The Code applies to 'information society services' likely to be accessed by children in the UK. This includes, apps, online games, connected toys and devices, search engines, social media platforms and websites that offer goods, news or education services. It does not cover online broadcasts such as radio or TV provided online. It would be likely to cover online competitions, research or other content provided online. It is unlikely to cover simple website providing information or public authorities' services unless there is a commercial element. Child counselling services and helplines are also likely to fall outside the Code.

Who is a child?

Children are defined in the Code as under 18 (based on United Nations Definitions rather than GDPR). Although you can tailor your approach depending on the age group most likely to access your online services.

When is a service "likely" to be accessed by a child?

The services you offer do not have to be aimed at children to be covered by the Code. Services which are 'likely to be accessed' by them need to comply. Restricting access to attempt to exclude children via appropriate controls is probably the only way most online services can prove that the services are not accessible to children. If you can't be certain that you have restricted access the ICO suggests that your service should be designed as though a child would have access. The Code therefore also has significant implications for adult only sites such as gambling sites and adult entertainment

portals. It may also have significant implications for search engines who provide access to content and services which may be accessible to children and which are not appropriate for them.

If you consider that your services are not likely to be accessed by children then you should nevertheless document why you think this is the case, in case you need to justify this to the ICO at a later date.

The 15 Standards of Age Appropriate Design

1. The best interests of the child

This should be a primary consideration when designing and developing online services likely to be accessed by a child. This means the design of the service should take account of the child's privacy needs and how they can be best supported by the design of the service.

What this means for you: Your Privacy By Design approach must take into account the fact that an application or product is accessible by children. Your organizations' Privacy by Design approach should now reflect the requirements of the Code of Practice not just the GDPR.

You may also want to review and update your accountability framework to ensure that it includes senior individuals who can advise upon and take responsibility for ethical decision making surrounding young people's data.

Suggested Actions:

- *Update your Privacy By Design documentation to include references to the requirements of the Code. Train project managers, architects and technologists in the requirements.*
- *Consider who will be responsible for ensuring the organization complies with the Code and who can advise on what the best interests of children may be in relation to product development.*

2. Data Protection Impact Assessment

You should undertake a DPIA before launch to assess and mitigate the rights and freedoms of children likely to use your product or service. You should also undertake a DPIA of your existing services to understand what changes may be required.

What this means for you: You may now need to conduct a different type of DPIA for children's data processed online in the UK. There is an ICO template which can be used for this. It contains additional sections which need to be completed to allow you to evaluate and mitigate the risks for children. The template can be found here: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/annex-d-dpia-template/

If you don't use this template, you can update your existing Data Privacy Impact Assessment template to reflect how the requirements of the Code have been met.

Suggested Actions:

- *Update your DPIA template to reflect the requirements of the Code (or adopt the ICO one). This should be used for all new projects and systems changes where you identify that children's data may be processed and is subject to the Code.*
- *Consider whether your DPIA consultation process needs to be widened to include consultation with child behavioural experts, panels of parents or even sample groups of the children themselves. If you believe you do need widen the groups with whom you consult, establish a*

mechanism for achieving this, for example, by working with specialist market research companies.

3. Age appropriate application

Take a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this Code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or if that is not possible, or you do not wish to do this, you should apply the standards in the Code to all your users instead.

What this means for you: The code makes clear that formal age verification will not always be needed to establish age and self-declaration can be used where appropriate to the level of risk.

Organizations can either:

• establish age with a level of certainty that is appropriate to the risks to children that arise from their use of personal data, or

• ensure that they follow the Code and protect the personal data of all users by default instead (so that they don't have to establish age as above).

Where you choose to employ an appropriate mechanism for age verification before allowing access to your services the level of verification needs to be proportionate to the risk. If there is a significant risk of harm or distress being caused to younger users, you may need to employ the strictest age verification standards.

Stating that a website is not aimed at a certain age group is unlikely to be a sufficient safeguard unless the risk is extremely low/negligible or other means are used to mitigate the risk.

Self-certification will be allowable but probably only where the content or service being access is lower risk.

The Code gives examples of ways of checking age, including AI and use of third-party vendors. The age verification method selected must also be proportionate and not require an excessive amount of additional information from younger users which could be seen to breach data minimization principles. In particular, be very careful in deploying biometrics as a means of age verification and this involves special category data and may need parental consent and/or regulatory consultation. Care should also be taken where collecting national identifiers or using techniques based on Artificial intelligence (AI).

Suggested Actions:

- *Review your existing age-verification mechanisms and consider whether any new mechanisms need to be adopted.*
- *Where appropriate deploy appropriate age checks or age gates for those accessing your services.*

- *Conduct a DPIA for the Age verification to ensure that it is proportionate. Complete a LIA for the verification is based on legitimate interest grounds to demonstrate that any verification or age checks are balanced and proportionate.*

- *If using a vendor to deploy age verification, ensure appropriate due diligence is completed and ask the vendor to provide any relevant DPIAS or risk assessments.*

- *If you intend to use biometric checks or AI based on biometrics consult your Data Protection Officer and consider seeking the input of the ICO or other stakeholder groups, such as parents, before deploying them as part of your age verification process.*

4. Transparency

The privacy information you provide must be concise, prominent and in clear language suited to the age of the child. Provide additional specific "bite-sized" child-accessible explanations about how you use personal data at the point that use is activated.

What it means for you: The language you use in your privacy policies and 'just in time' privacy notices should be appropriate to the level of understanding your users have. Difficult concepts may need to be explained in simpler terms and delivered by shorter notices. The Code contains details suggestions on what type of notice is appropriate for which age group and on how to present information.

Suggested Actions:

- *Review all your privacy and consent notices and privacy policies to ensure they are drafted in an appropriate language and are of a length that is appropriate to the child user*
- *Implement a child friendly summary privacy policy aimed at under 18s to supplement your full privacy policy.*
- *Design and implement age appropriate ways (as suggested in the Code) for Children to access information about how their data may be used, for example via social media videos, pictures etc*

5. Detrimental use of data

Do not use children's personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice (such as the CAP code for marketing and advertising).

What this means for you: You need to be able to identify where data processing or the presentation of certain content may have a harmful effect on a child user and restrict the use of that child's data to avoid causing harm or detriment. You need to understand how any codes of practice you follow deal with children's information and implement their recommendations.

You also need to ensure that you do not encourage over-use of your service, for example, by using personal data to incentivise the child user to remain engaged or to penalise them for logging off early.

Suggested actions:

- *Consider whether you need help with making these assessments and if so, find appropriate resource with the relevant expertise, such as a child behavioural expert or child psychologist, to add to your Data Protection Accountability Framework*
- *Review the Codes of Practice for your data processing activities and identify and implement any recommendations relating to children and their information*
- *Review incentives and penalties which form part of the service and which may encourage child users to increase their screen time.*
- *Implement pause buttons which allow children to take a break at any time without losing their progress in a game or provide age appropriate content to support the child's choice about taking a break, advice on this has been provided by the UK Chief Medical Officers.*

6. Policies and community standards

Uphold your own published terms, policies and community standards including privacy policies, age restriction, behaviour rules and content policies.

What this means for you: You must be able to demonstrate that you actively apply any policies or standards aimed at protecting children.

Suggested actions:

- *Review and audit the effectiveness of child protection policies or procedures, such as content moderation, on a regular basis*
- *Ensure any content moderation is effective and have a mechanism to keep this under review*

7. Default settings

Settings must be "high privacy" by default unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child.

This is likely to mean that where a service is accessible to a child you may need to implement high privacy settings by default. You will particularly need to address risks related the automated profiling of children and the use of geolocation data, and novel marketing techniques which must be made transparent in a way a child can understand.

What this means for you: You should have standards and processes in place to ensure your privacy by design strategy reflects the privacy settings required for processing children's data

Suggested Actions:

- *Update your privacy by design documentation to reflect the Code, in particular in relation to profiling, geo-location data and any novel or complex marketing or advertising techniques*

8. Data minimisation

Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate.

What this means for you:

You need to give chid users the option to only provide their data where it is necessary for the part of the service they are using. Children should have the choice whether or not to provide their data where this is optional, and these choices need to be made clear to them.

Suggested actions:

- *Review where you collect children's data across a service and make sure it is only collected where strictly required at the time.*
- *Turn off any processes which collect data from a child in the background where this is not strictly necessary to provide the service, for example where they are not currently using it.*

9. Data sharing

Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child.

What this means for you: You may only share children's data with the third parties where there is an exceptional need for the data sharing. You will need to document this in your DPIAs and where appropriate in your LIAS.

Suggested actions:

- *Review existing sharing of children's data and stop sharing that date unless there is a compelling reason for the data sharing.*
- *Implement data sharing agreements where the sharing is justified*

10. Geolocation

Switch geo-location options off by default unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child. If geolocation services are additional to the core service, then these should be subject to separate privacy settings. Provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to "off" at the end of each session.

What this means for you: Geolocation data must be turned off for child users by default, unless this is an essential part of the service (for example, a service using maps to give direction). Remember children must always be told when their location data is being collected.

Suggested actions:

- *Review your use of geolocation to ensure that sure you provide a geolocation privacy setting wherever this is not an essential part of the service.*
- *Switch geolocation privacy settings off by default so that children have to actively agree to sharing their location*
- *Review the granularity of the location which needs to be tracked and do not collect more detail than you actually need.*
- *Review notices and settings to make sure that you are providing information privacy notices at the point of sign-up, as well as each time the service is accessed, that alerts the child the use of their location data and which advises them to discuss this with a trusted adult if they don't understand what it means.*
- *Implement symbols or notices to indicate when tracking is turned off.*
- *Make sure tracking can be turned off when it is not needed.*

11. Parental controls

If you provide parental controls, give the child age appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.

What this means for you: If you provide parental controls then you should provide a privacy notice to explain to the child that parental controls are in place. The Code provides examples of the information which should be provided for parents and children to explain the use of parental controls and their purpose.

The use of symbols and icons to indicate active tracking to the child user are recommended.

You need to also provide information to parents with separate information about the child's right to privacy under the United Nations Convention for the Rights of a Child.

Suggested actions:

- *Review and update privacy notices and other terms to ensure that they contain the information recommended in the Code (you can use the ICO's examples as a guide)*
- *Consider whether you can implement a flag or icon to indicate to children that they are being tracked*

12. Profiling

Switch options which use profiling "off" by default (unless you can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing) and separate privacy settings should be used for each different type of profiling.

What this means for you: All profiling of children must be off by default unless it is essential or there is a compelling reason to think that it would benefit the child, for example it can be used for age verification. You need to make sure you explain the use of profiling clearly to children (there are examples in the Code) and remind them of the profiling with appropriate interventions. For example, prompts that tell them they can switch profiling off or remind them that the profiling is still happening.

Note: The Code will not prevent behavioural advertising. The Government and ICO have both acknowledged the importance of this revenue stream to the media industry, however under existing legislation (the GDPR and Privacy and Electronic Communications Regulation - PECR) user consent is already needed before behavioural advertising can take place. The Code says that profiling must be switched off by default for child users, or all users if age is not established. Valid GDPR and PECR consent and transparency for cookies will allow this profiling for advertising to be 'switched on'. The ICO has recognised that the risk from behavioural advertising is also lowered when the media apply the relevant Advertising Standards Authority codes.

Suggested actions:

- *Review your profiling to ensure it is not used in a way which is detrimental to the child*
- *Review your use of cookies and the wording you use to describe profiling activities in your cookie notice*

13. Nudge techniques

Do not use nudge techniques or other tools to lead or encourage children to provide unnecessary personal data or weaken or turn off their privacy protections.

What it means for you: you will need to review your use of nudge techniques to bring them in line with the Code.

Suggested actions:

- *Review the use of nudge techniques and ensure that they are only used to help children make the right privacy choices based on proper information*

14. Connected toys and devices (IoT)

If you provide a connected toy or device, ensure you include effective tools to enable conformance to this Code.

What it means for you: You need to follow the code if you provide a toy or device which collects and personal data and transmits it via a network connection in this way. Electronic toys or devices that do not connect to the internet, and only store personal data within the device itself are not covered.

Suggested actions:

- *Find a way to provide a privacy notice explaining what personal data is collected and why (this might be aimed at children and/or parents) – ideally include this at purchase or set up*
- *Implement lights or sounds to indicate when a toy or device is collecting data or listening*
- *Turn off passive collection or listening when the device is not in use.*

15. Online tools

Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

What is means for you: you need to make it easy for children to exercise their rights under the legislation with appropriate tools and clear explanations of their rights. the Code contains relevant examples. You also need to make it easy for children to communicate with you about the progress of their request and to track their request.

Suggested actions:

- *Review your subject rights procedures to see if they can be made more child friendly*
- *Implement tools for children to use to easily exercise their rights and track their requests*

Please note this action plan is not intended as legal advice and should not be relied upon as such.