Children’s data in financial services

Executive Summary

Introduction

In 2022 the Information Commissioner set out his vision for the regulator we want to be in his ICO25 strategic plan. This plan will empower organisations to use information responsibly and confidently, to invest and innovate and empower people to confidently share their information to use the products and services that drive our economy and our society.

The pace of technological change and innovation means the landscape we regulate is constantly transforming. To empower and support organisations we need to maintain our understanding of how these transformations are being implemented. As part of the ICO25 strategic plan, the ICO's Assurance department approached organisations within the financial services sector to review their processing of information.

The review looked at two main areas:

1. The use of children's data
2. The use of AI and automated decision making.

We were also keen to collect the views of organisations within the sector about their experiences of implementing good data protection practice, compliance challenges, competing regulatory or legislative priorities and any general data protection concerns.

Recital 38 of the UK GDPR says that

> "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data."

For these reasons children are identified as a vulnerable group within the ICO25 strategic plan and protecting them through the responsible use of their information is a current priority. The ICO has already published a guide to using children's information however, this report contains themes and findings drawn from the information provided by a range of organisations within the financial services sector, who offer products and services to children. It does not name or otherwise identify any individual participant. The report highlights good practice as well as areas of risk, or where improvements may be needed.

The findings of the review of the use of AI and automated decision making in the financial services sector are contained in a separate report.

Methodology

From March to September 2024, we gathered information about the processing of children's data from participants and in particular those who supply current accounts, savings accounts, trust accounts, ISAs and prepaid cards to children or that use children's data for their administration. This was done using a mix of questionnaires and direct engagement which provided the views of over 40 organisations (participants).

Several participants provided access to their key documents to support the review process. Where participants engaged directly, we held interviews with key staff who have responsibility or involvement in processing children's data.

The review of children's data processing focussed on the following areas:

1. Governance
   The measures in place to control the processing of children's data.
2. Transparency
   The information given to children which tells them what their data will be used for.
3. Use of information
   What information is processed, for what purpose and which lawful basis is used.
4. Individual Rights
   How individual rights relating to children's data are handled, whether received from children, parents 1 or other third parties.
5. Age Verification
   The methods used to identify, and verify the age of, children.
6. Further contact and marketing
   How children are contacted about their accounts and information provided to them about other products and services.

The review focussed on these areas with all participants so that common themes could be identified and included in this report for the benefit of other organisations who carry out similar processing.

This report summarises:

- evidence of good practice;
- evidence of risks to data protection compliance; and
- instances where we found that improvements may be necessary to data practices.

Key Findings

Children are important customers for many financial services. Several participants highlighted children's products as a key area of focus for development as they represent the future customer base for the wider range of products and services offered. The review

of processing of children's data provided the following key findings.

Governance

Most organisations had policies in place to control the use of children's information. However, there was limited monitoring of compliance with these policies. Nearly all organisations provided data protection training to staff however, less than a fifth included specific training about the use of children's information.

Transparency

Only half of organisations reported having age appropriate privacy information. However, following our review the number that we considered to have effective age appropriate privacy information was lower. The examples of privacy information that were suitable for children included age appropriate language and engaging descriptions of how organisations use their information.

The approach taken by several organisations appears to have passed their own transparency responsibilities onto parents. As a result, there was a significant risk that children are recorded as agreeing to terms and conditions or privacy information that they do not actually understand. Providing privacy information was also often a onetime only exercise and is not revisited as children age and their understanding increases.

Use of information

Most organisations regularly reviewed the categories of children's data collected to ensure it was limited to what is necessary, particularly for special categories of data. There were effective controls in place to prevent excessive data collection or purpose creep across all organisations observed.

Consent was used for some purposes for processing however, some organisations asked for parents to provide the consent on behalf of their child in the first instance but failed to keep this consent under review. This means as the child gets older and their ability to understand the processing for themselves increases, the original consent is likely to become invalid until it is refreshed and obtained from the child.

Individual rights

Respondents reported that requests to exercise the individual rights set out in UK GDPR by, or on behalf of, children are infrequent and low in volume. However, as a result of the issues found with explaining privacy information and their rights to children, parents wishes often, unfairly, supersede those of children. In several cases the decision whether to accept requests for children's information from the child or their parent is made using a predetermined age limit rather than an assessment of the child's competence.

Age verification

Processes to verify the age of children were robust across all organisations.

Contact (including marketing)

Many organisations provided administrative communications. Nearly all had a policy that prevents marketing to children. There is limited distinction between parents and children when communications were provided, which was sometimes based simply on whose contact information is available. This creates a high risk of non-compliance with communications and marketing requirements.

---

1 Parent refers to the individual(s) who has parental responsibility for a child as defined by s 3(1) Children Act 1989.

Detailed Findings

Governance

69% of participants had policies and procedures in place to control the use of children's data; however, only 67% of those organisations proactively monitored compliance with their policies and procedures. This means that 45% of participants had limited assurance that staff are processing children's information in line with internal or even legislative requirements. For example, in one case an organisation would not know what to do if they received a subject access request from a child.

The risk of non-compliance was increased because only 14% of participants had assigned responsibility for children's data in policy or relevant job descriptions. This means that children's data will often be subject to the same rules that apply to adults' information.

97% of participants provided staff with general data protection training however, only 18% of participants included content about the use of children's personal information.

Accountability is one of the principles of the UK GDPR which means organisations are responsible for demonstrating compliance with its requirements. This must include appropriate technical and organisational measures such as, adopting and implementing data protection policies, providing staff with appropriate training as well as monitoring the effectiveness of these measures.

Considerations

If staff are not aware of their internal and legislative responsibilities then there is a higher risk to compliant processing of personal data. In order to reduce this risk organisations should consider:

1. Defining their approach to processing children's personal information in policies and procedures.
2. Documenting specific responsibilities for processing children's personal information in job descriptions.
3. Provide data protection training to all staff that is refreshed at regular intervals. This should include additional information about the processing of children's personal information where this would be different to processing the data of adults.
4. Provide specialist data protection training to staff with specific responsibilities for processing children's personal information.

> These can help demonstrate compliance with Article 24 of the UK GDPR which requires organisations to implement appropriate technical and organisational measures to ensure, and to be able to demonstrate, compliance.

Transparency

49% of participants say they provided children with age appropriate privacy information. The review identified several good examples of privacy information designed to provide children with the information they need to understand what will happen with their information in age appropriate language. Some of these included illustrations or cartoons to bring the content to life. However, less than a quarter of all participants have carried out any testing to check how easily children would understand their privacy information.

Where some form of testing has been adopted it is usually an assessment using Flesch–Kincaid [2] readability tests. Whilst this provided some assurance that children are able to read privacy information comfortably, some examples that have been subject to this testing still contained terminology or industry jargon which are unlikely to be meaningful to children at the lower age range for available products.

In addition, some 'child friendly' privacy notices contained all the information that is provided in adult notices, although using more accessible language. However, we questioned if all of this information is necessarily relevant or meaningful to children. For example, some privacy information provided for accounts available to children aged 11 and over included examples of data sharing to HMRC or the Financial Services Compensation Scheme (FSCS).

Article 12 of the UK GDPR requires that

> "information relating to processing is provided to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."

Furthermore, Recital 58 provides further explanation, adding

> "Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand."

Therefore, information must be provided in a way that will appeal to the age of the children it is intended for so they will understand all the terminology that is used. For example, 'so we can make sure you are the right person' could be used instead of 'ID verification'.

Also, we advised organisations to limit information to what is relevant at the point in time it is provided and layer or introduce new privacy information as it becomes relevant, whether this be a particular point in time or even a specific event. This may mean that different versions of privacy information needs to be produced, particularly where new processing is introduced. However, this will actually reduce the amount of information presented at any one time and help increase the ability of children to understand it, particularly those at a younger age. So, in the example above, privacy notices do not need to inform that information is shared with HMRC when a child under 16 opens an account. Whilst this can happen [3], in the vast majority of cases this sharing will only become systematic as the child reaches the age of 16. Therefore, it would be more transparent to provide this information at the point the sharing starts. This would prevent younger children from having to understand information that is not relevant to them. Equally, when they reach 16, they are not expected to retain, recall or understand something that was provided to them a number of years earlier.

Similarly, sharing information to the FSCS is not a systematic process and is only likely to happen should a covered financial service organisation fail. Furthermore, this sharing would take place when a person raises a claim for compensation through the FSCS, who provide this information in their own privacy notice. This means it is unnecessary to provide this information to children when they are opening an account and could be reserved for any communications sent in the event of an organisation failing.

Survey results showed that only 36% of children's savings account products which are opened by parents but transferred to the child at 16 provided the child with privacy information during the transfer process. Not only is this denying the child their right to be informed under Articles 13 and 14 of the UK GDPR, but any new processing that will take place from this point is unlikely to be considered as fair or transparent.

The survey also showed that there are a range of ages that children are able to take charge of their own account. This can be as young as seven years old; however, a parent must be present when these accounts are opened, particularly for children aged under 13 years old [4]. When opening a child owned savings account, 83% of participants provided children with privacy information [5]. 75% of participants also required children to acknowledge that they have read the privacy information, usually recorded by signing the application form. However, only 11% of these participants actually carried out any assessment as to whether children are competent enough to understand their notice. This includes cases where the child is presented with the same notice that would be provided to an adult. In one example where an adult notice is used, it was assumed that the child

understands it unless they express their lack of understanding and proactively seek further assistance.

For current accounts, 66% of participants indicated it would be the parent's (where they are present) responsibility to ensure the child understood privacy information and no attempt would be made to confirm the child understood the privacy information. In some cases the parent is required to acknowledge privacy information on the child's behalf so the child would not be provided with any privacy information. However, in all of these examples the child is considered to be the owner of, and therefore responsible for, the account; so, once the account is opened, parents have no rights or influence over it or the use of information.

Children have a right to be informed about what will happen with their information. This means organisations have the obligation to ensure they are aware of, and understand, the processing of their information that will take place. It can be helpful to involve parents with developing the child's understanding, or asking them to accept terms when the child is not competent to do it themselves as long as this is acting in the child's best interest (see page 18). However, responsibility cannot be passed over to parents because it may be easier.

Consideration

Organisations who process children's data should have child-friendly versions of their privacy information. Repeating privacy information in simpler or more descriptive language does not necessarily make it easier to understand so the information should be suitable and engaging for the audience it is intended for. Even when relying on parental consent children do not lose their rights to transparency. Organisations must ensure their privacy information can be understood by children as they will likely be competent enough to make their own decisions long before the lifecycle of the product expires. This can be achieved by:

1. Using clear and plain language avoiding industry jargon and terminology that may be meaningless to children.
2. Limiting the content to only what is relevant and necessary at the time they will receive the information.
3. Providing different versions of privacy information for different ages. If choosing to only have one version then it must be accessible to all and understood by the youngest age range.
4. Being transparent on an ongoing basis rather than a onetime only activity. Where necessary, provide supplementary privacy information at the point additional processing will take place. This will make understanding of notices easier for children and sure they are provided with the right information at

the right time. This can also be revisited as their capacity for understanding their rights evolves.
5. Considering different methods of conveying key information that is more engaging to the intended audience, such as cartoons, pictures, diagrams or videos.
6. Producing something designed to be used by children and parents together when relying on parental consent. This will provide parents with a tool to help with the education of the child.
7. Testing privacy information on actual children to see if they can understand it.

Having child friendly privacy information reduces reliance on parents to acknowledge privacy information and will help demonstrate compliance with Articles 5(1), 12, 13 and 14 of the UK GDPR.

Further information about children's right to be informed is available on the ICO website.

Use of information

66% of participants reviewed the categories of information they collect on a regular basis to make sure it is limited to what is necessary. Information collected related to parents and children, and was found to include:

Child	Parent
• title, • gender, • name, • data of birth (DOB), • country and place of birth, • nationality, • address, • country of residence, • contact details incl email (not compulsory), • NI number (where applicable).	• title, • gender, • name, • DOB, • country and place of birth, • nationality, • address, • country of residence, • contact details incl email, • marital status, • NI number, • occupation, • ID verification data.

40% of participants collected special category data [6]. Where this related to children it is limited to health data and will only be processed having obtained explicit consent. Health

data was also collected about parents, again using consent as an additional condition for processing. For both children and parents, health information was processed to provide better service based on particular needs or vulnerabilities.

Some participants indicated that they may process criminal offence information (parents only), but this would be for accounts held in a parent's name such as Junior ISAs or savings accounts.

All participants had considered and recorded an appropriate lawful basis for their processing activities as well as a separate condition for processing special category data. However, only 94% of participants [7] recorded these in a formal record of processing activity (RoPA). 25% of these participants would be unable to identify processing related to children, as their RoPA does not distinguish between this processing and that related to adults.

24% of participants confirmed that they rely on consent obtained from the child to process their information for specific purposes. However, 42% of those participants relied on acknowledgement of information provided within privacy information or key facts documents to obtain the consent. This does not meet the requirements of the UK GDPR.

For consent to be valid, Article 7(2) of the UK GDPR says that it must be clearly distinguishable, separate and unbundled from other matters, in an intelligible and easily accessible form, using clear and plain language. We have seen from the examples in the 'Transparency' section, above, that clear and plain language requirements are not always met, therefore this is likely to undermine consent that is reliant on the acknowledgement of such notices.

Furthermore, even where privacy information is provided in clear and plain language, recital 42 of the UK GDPR says that consent must be freely given. This means that it must be a genuine choice. So, when organisations require consent to be given as part of an agreement to wide ranging privacy information and key facts documents, and this consent must be provided to set up the account, there is no free or genuine choice whether to provide consent or not.

The rules about consent requests are separate from transparency obligations under the right to be informed, which apply whether or not consent is being relied on therefore, any consent requests need to be removed from privacy notices.

Finally, obtaining consent was often treated as a onetime event and was not refreshed. This becomes problematic where consent was initially provided by the parent. When a child becomes competent enough to understand their rights, which will naturally happen as they age, they have not provided the consent for the use of their data, even though they have become capable of making their own decisions about how their data is processed. Continuing this processing would, therefore, become unlawful. Even where consent is

obtained from the child it would be good practice to refresh this at regular intervals so there is assurance that they understand exactly what it is they are consenting to.

Considerations

The UK GDPR sets a high bar for consent to be valid. As children should be provided with more protection when processing their data, it is important to make sure that methods used to obtain consent are clear, easy to understand, specific to what the consent relates to and separate from any other information being providing. When using consent (provided by either the parent or the child) to process children's information compliance can be improved by:

1. Making sure that children (or their parents) are provided with real choice about how their personal information is processed.
2. Explaining and obtaining consent separately to any other terms and conditions or acknowledgement.
3. Ensuring that any child providing their consent is competent to understand, and understands, what they are consenting to.
4. Making sure any child providing consent is aware that the refusal of any consent will not impact their ability to access the product or service they are seeking or affect the balance of power or relationship with them.
5. Refreshing consent at regular intervals particularly when it was originally granted by a parent and the child's ability to understanding their rights increases.
6. Providing the child with regular reminders about their right to withdraw any consent and how they could do this, particularly where consent was originally provided by a parent.

More information about processing children's personal information using consent and more general UK GDPR consent guidance is available on the ICO website.

Data Protection rights

The UK GDPR gives people rights over their data. This includes being able to access the data organisations process about them, correct inaccuracies and, in some circumstances, have their data erased or stop processing taking place. The approach to individual rights taken by organisations in the financial services sector was varied, and often depended on how organisations determined the competency of children to understand their data protection rights.

88% of participants had no process in place to assess a child's understanding of their data protection rights. However, for 34% of these participants this was because they had preset

age limits which determined whether a child was able to exercise their rights or not [8]. In most cases this age limit was set at 13 years old although some participants had set this age as high as 16 years old.

20% of participants who offer products which process children's information, but are controlled by parents, did not allow children to access their information or exercise this right at any age.

Organisations cannot deny children their data protection rights. Even if a child is too young to understand the implications of their rights, they are still their rights, rather than anyone else's such as a parent. Therefore, whilst setting an age limit might be useful in many circumstances it cannot be used to prevent children accessing their information rights unless there is good reason to think they are not competent. This means that organisations processing children's information should put in place processes to determine whether or not the child is competent if they try to exercise one of their rights. Where necessary, this should give some consideration to the individual nature of the request rather than relying on a fixed age limit.

If organisations allow children to acknowledge terms and conditions, privacy information or provide their consent for specific processing then this would indicate that they are considered competent, so it follows that they should not be prevented from exercising their rights. However, if a child is not considered to be competent, an adult with parental responsibility may usually exercise the child's data protection rights on their behalf.

However, children's information still belongs to the child. So, where a parent makes a request on a child's behalf, it would not always be appropriate to fulfil that request as the child may not want certain information being provided to the parent. Parents should only be allowed to exercise these rights on behalf of a child if the child authorises them to do so or when it is evident that this is in the best interests of the child (see page 18).

Examples

a) An account is owned by a 14 year old who is responsible for their own spending. The parents are concerned that the child is spending money on things they disapprove of, so submit a request for bank statements to see where the child is spending money. The providers policy allows parents of children under 16 to make such requests and provides the parents with this information. The child is capable of understanding their data protection rights and would rather the parents were not provided with this information as it does not relate to them.

By providing the parents with this information they are unlawfully sharing the child's information, and are in breach of data protection legislation. Parents should only be allowed to exercise these rights on behalf of a child if the child authorises them to do so, when the child does not have sufficient understanding to exercise the rights him or herself, or when it is evident that this is in the best interests of the child.

b) A parent opens an account for a child when the child is 8 years old, and shares the child's information with the provider in order to administer the account. Although the parent assisted in the opening of the account, the account belongs to the child. When the child is 12 years old they inform the provider of their new address following a move, however their statements continue to be delivered to their old address. Having tried to update the address again, the child then requests a copy of their information, from the provider, to see if the requested changes have been made. However, the policy of the provider will only allow children over the age of 13 to exercise these rights so they refuse the request, even though the child has demonstrated they are competent enough to do this.

The policy of the provider means that they are preventing the child's access to their information, and are in breach of data protection legislation.

c) A 16 year old's account is frozen following some unusual activity. A notification is sent but the child is not mentally competent enough to understand or act upon it or understand their data protection rights. The child tries to make a purchase which is declined, so the parent contacts the provider requesting information related to the child and their account to try and resolve the issues. As the child is over the age of 16 the provider refuses the request as their policy states that at this age only the account holder can make requests to access information.

The provider should have procedures in place to seek the child's authorisation or assess the understanding or best interest of the child rather than relying on a predetermined age limit. Where the child is not competent, refusal of the request made by the parent is not acting within the child's best interest and is not complying with data protection requirements.

Considerations

It is worth emphasising again that children have the same data protection rights as adults. Depending on the circumstances it can be more complicated to

respond to requests as these could come from children or their parents. To ensure that requests are handled effectively:

1. Develop and document policies and procedures for dealing with requests involving children's data to supplement any other procedures already in place.
2. Assess each request on its own merits and acting in the child's best interest to understand the nature of the request and impact of providing the response to the child, or parent.
3. Recognise that where a child has been able to provide consent or acknowledge privacy information this demonstrates competence that should allow them to exercise their own rights.
4. Provide regular reminders to children about their rights and how to exercise them.
5. Seek authorisation from a child when a request is received by a parent.

More information about children and their rights can be found on the ICO website.

Age verification

96% of participants had an embedded process for verifying the age of children when an account is opened. This was done with one or two validating documents which were the birth certificate and, where available, a passport.

The remaining 4% are accounts that are held in trust for children such as ISAs or savings accounts. In these circumstances ID and age verification took place when the child becomes active on the account. This was usually at age 16 or above where other validating documents may be available to assist in the verification process.

Contact (including marketing)

63% of participants had a policy in place to govern communications provided to children, including marketing material. For 83% of participants the policy prohibited the provision of marketing material to children.

75% of participants provided communications which included general information about the service provider and also administrative account information. 29% of participants provided communications containing general organisational administrative information. 8% of participants provided marketing communications to children.

Communications were provided using a range of channels where 38% used phone, 17% used SMS, 33% used email and 92% used post.

33% of participants had a process in place to regularly update the contact information they hold. This usually took place when any contact is made. Where no regular contact takes place then updates were requested at various intervals from six months to three years of no contact, depending on the participant.

Only 8% of participants required children to have access to their own email and/or phone to enable them to open an account, however if children did have these, then this information was recorded in the majority of cases where the child has some control over the account (current or savings accounts). 76% of participants used parents contact information such as email or phone to provide communications.

Of the participants who do allow marketing to children, 75% of them included opt in and opt out options on the account application form. Completion of the application form and understanding of terms and conditions, including privacy information and consent, could be provided by either the parent or the child. The remaining 25% of participants sought consent from the parent only. This approach, similar to those discussed already, requires a careful balance of responsibility and control between the parent and the child over the life cycle of the account. For example, the review found children's transactional information being profiled to provide personalised marketing. This happened on accounts that were available to children from an age where they are unlikely to understand and consent to this type of processing, so this consent was obtained from parents. However, consent shouldn't be used as a way of avoiding responsibility for assessing the risks inherent in the processing. Although consent is a lawful basis for processing children's personal data, using it does not necessarily guarantee that the processing is fair. Particularly as these accounts are available to children until they reach 18. If no attempt is made to refresh this consent, from the child, throughout the product lifecycle continuing to process the data would likely be in breach of the UK GDPR. As a child's competence increases and they have a better understanding of their rights, they also have the ability to make their own decisions, including whether or not to consent to certain processing.

There is nothing in the UK GDPR the prohibits profiling or providing marketing to children however, the UK GDPR states that children's information merits specific protection. This in particular applies to the use of their information for marketing or profiling. As with the above topics processing must be fair and comply with all data protection requirements. This means children must be informed about what will happen with their information in a way that they can understand. This is particularly important as, like before, children have the same right as adults to object to the processing of their information for direct marketing or profiling, so any lack of understanding or vulnerability cannot be exploited to continue these activities. Doing so would not provide the required special protection.

Considerations

There is nothing in the UK GDPR that prohibits providing communications, including marketing, to children. However, it must include special protections for children when they are provided with marketing. The approach to providing marketing to children should:

1. Ensure a DPIA is carried out to adequately assess whether processing will result in any high risks to the rights and freedoms of children as a result of this type of processing. This would be required when providing marketing to children as targeting marketing at children is one of the circumstances which the ICO considers is likely to result in such a risk.
2. Make sure that children are aware of, and understand, their information being used for marketing purposes or other related processing such as profiling.
3. Make sure that children are aware of their right to object to profiling and marketing and how they can exercise this right.
4. Ensure that any marketing communications that are provided by electronic means (eg phone calls, SMS, emails) are compliant with the Privacy and Electronic Communications Regulations (PECR).

Additionally, consideration must be given to what information is provided in communications, to prevent the disclosure of information a child might not expect to be, when communication via their parents. This should include:

1. Whether the information provided, when using parent contact information, discloses any personal information, that the parent may not be already be aware of, be against the child's wishes or not be in the best interest of the child.

Further information about:

1. marketing to children,
2. profiling using children's information,
3. children's consent,
4. PECR and
5. DPIAs can be found on the ICO website.

Best interest of the child

The concept of the best interests of the child comes from Article 3 of the United Nations Convention on the Rights of the Child (UNCRC):

> "In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration."

It is not specifically referenced in the UK GDPR however, it is still something that should be at the forefront of considerations when making decisions about processing children's information.

Further information about what the general approach to processing children's information should be, including the best interest of the child can be found on the ICO website. In addition, the ICO's Children's Code [9] Guidance contains other resources explaining the best interest of the child including a self-assessment in relation to information society services (ISS).

Acknowledgements

The ICO would like to thank all participants for their positive and open contribution to this review and the resources they provided to: complete questionnaires; meet face to face, both virtually and in person; respond to additional questions; and provide documentation, presentations and demonstrations.

---

2 The Flesch–Kincaid readability tests are readability tests designed to indicate how difficult a passage in English is to understand. They use the word length and sentence length of a passage to calculate a score.

3 For example, where children earn high levels of interest that exceed personal tax allowances.

4 The highest age recorded where a parent must be present at the opening of an account is 15.

5 This is any privacy information, not necessarily age appropriate information.

6 Special categories data is set out in Article 9 of the UK GDPR. Due to their more sensitive nature they require a higher level of protection, including a separate condition for processing in addition to a lawful basis.

7 The remaining 6% do not meet the thresholds in the UK GDPR which require them to compile a RoPA.

8 This does not mean that there is no access to rights below these age limits, but that requests must be made by parents.

9 Whilst this information may be helpful, the Children's Code applies to "information society services (ISS) likely to be accessed by children". The definition of an ISS is "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."