Date: March 26th, 2021

RE: Comments on the Irish Data Protection Commission's consultation: Fundamentals For A Child-Oriented Approach to Data Processing.

Dear Commissioner,

Privacy Vaults Online, Inc., d/b/a PRIVO is pleased to have an opportunity to share our comments on the Irish Data Protection Commission's consultation: Fundamentals For A Child-Oriented Approach to Data Processing (the "Fundamentals"). We very much welcome the robust and comprehensive nature of the consultation on what is such an important area of privacy protections. The US Federal Children's Online Privacy Protection Act (COPPA) has long been the gold standard in child privacy protection. However, the privacy landscape is evolving and with the advent of the General Data Protection Regulation (GDPR)[1], the ICO's Children's Code and the Irish Data Protection Commission's consultation firmly shines the spotlight on child privacy. Further afield there are more regulations for online service providers to navigate in relation to children, including Brazil's LGPD and China's version of COPPA. PRIVO hopes that data protection authorities will work together to ensure there is a consistent approach to children's data protections within the European Union. Lack of harmonisation can prove challenging and costly for companies trying to comply with requirements when it comes to the practical implementation in apps, websites and other online services.

Our comments are based on our experience working at the coalface with regulators and Information Society Services (ISS). PRIVO has served as a Federal Trade Commission (FTC)-

[1] The General Data Protection Regulation is a European Union law that was implemented May 25, 2018, and requires organizations to safeguard personal data and uphold the privacy rights of anyone in EU territory. The regulation includes seven principles of data protection that must be implemented and eight privacy rights that must be facilitated. It also empowers member state-level data protection authorities to enforce the GDPR with sanctions and fines. The GDPR replaced the 1995 Data Protection Directive, which created a country-by-country patchwork of data protection laws. The GDPR, passed in European Parliament by overwhelming majority, unifies the EU under a single data protection regime. https://gdpr.eu/

approved COPPA Safe Harbor since 2004. It has participated extensively in all FTC proceedings, including responses to all request for comment since the law was enacted in 2000. We have both participated in and organized Safe Harbor roundtables, lending our extensive experience to help inform the FTC and industry on issues of children's privacy and developments in the marketplace. PRIVO strives to fulfil the FTC's expectation that Safe Harbors move quickly to address new practices and changes in the marketplace as well as to innovate and, where possible, approve new solutions for processing verifiable parental consent. PRIVO was the first to use government issued data via a combination of last name, date of birth and the last for digits of social security number in securing meaningful parental consent to child participation online, which the FTC later codified as an enumerated method in the COPPA Rule. PRIVO was the first to deliver a **GDPR***kids*™ Privacy Assured Program and a secure privacy enhanced and interoperable family friendly identity and consent management platform compliant with both regulations. PRIVO also, via its work with the National Institute of Standards and Technology (NIST), under the National Strategy for Trusted Identities in Cyberspace (NSTIC - Obama Whitehouse Initiative), co-authored the Minor's Trust Framework. This is available on the OIX Registry which facilitates ecosystem-wide compliance solutions for those participants adopting its principles for protection of child privacy online.

PRIVO is providing comments on the following three areas:

1. Chapter 6: Direct Marketing, Profiling & Advertising - IBA
2. Chapter 6: Chapter 6: Direct Marketing, Profiling & Advertising -cookie conundrum
3. Chapter 5: Age of Digital Consent and Age Verification

Chapter 6: Direct Marketing, Profiling & Advertising -IBA

The GDPR requires high standards of protection when processing children's data. While the GDPR does not define the term child, the United Nations Convention on the Rights of a child defines anyone under the age of 18 as a child. The UK's Information Commissioner's Office (ICO) defines a child as anyone under the age of 18. Recital 38 to the GDPR[2] states 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. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child."

The Fundamentals puts the child at the heart and centre of privacy protections. This approach is particularly pertinent when it comes to profiling and automated decision making. Profiling in the form of interest-based advertising (IBA) is vital to the operation and success of many ISS which rely heavily on it for revenue. Recital 71 to the GDPR[3] states that such automated decisions 'should not concern a child'. The EDPB guidelines on automated individual decision making and profiling states that organisations should, in general, avoid profiling children for marketing purposes, due to their particular vulnerability and susceptibility to behavioural advertising and the ICO's Children's Code speaks to the risks of profiling in relation to children but states it should be off by default implying it could take place. Article 22 (2) of the GDPR[4]

[2] 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. 2Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. 3The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child. https://gdpr.eu/recital-38-special-protection-of-childrens-personal-data/

[3] In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child. https://gdpr.eu/recital-71-profiling/

[4] Paragraph 1 shall not apply if the decision:

allows profiling with explicit consent however the EDPB guidelines state that, as a rule, controllers should not rely upon the exceptions in Article 22(2) to justify it. There appears to be some inconsistency to the approach to profiling in relation to children. Furthermore, although children are technically under the age of 18, the GDPR Article 8[5] allows countries to set an age (16 for example) where children can provide consent for themselves. Therefore, many ISS will serve IBA to users at or above the age of consent when consent is obtained. The lack of harmonisation with regard to the age of consent across the EU results in children being treated differently and lack of a level playing field. A child can opt into this form of profiling anywhere from 13 years old and up to 17 years old depending on their country of residence. However, there is a fundamental difference between the understanding of a 13 or 14 year old and a 16 and 17 year old in relation to the inherent risks of profiling and IBA, which many ISSs may not take into account when serving IBA to children at or above the age of consent. This is a cause for concern in an online world where algorithms can build a profile of sexual orientation, eating habits and health and beliefs and influence behaviour long term. Industry also faces difficulty in aligning PECR in the UK[6] , ePrivacy Directive and the GDPR in terms of profiling and understanding when it is and isn't in the best interests of the child.

---

is necessary for entering into, or performance of, a contract between the data subject and a data controller;
is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
is based on the data subject's explicit consent. https://gdpr.eu/article-22-automated-individual-decision-making/

[5] Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.
Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.
The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.
Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child. https://gdpr.eu/article-8-childs-consent/

[6] The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications.
There are specific rules on:
marketing calls, emails, texts and faxes;
cookies (and similar technologies);
keeping communications services secure; and customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

If the interpretation of the GDPR allows for profiling of children at or above the age of consent the question remains is a child 13, 14 or even 15 years old truly able to provide informed consent? Should an ISS be relied upon to weigh the risks and choose not to serve IBA to its younger users?

Chapter 6: Direct Marketing, Profiling & Advertising – cookie conundrum

The challenge for ISS directed to or attracting children is in aligning the GDPR and ePrivacy requirements. The ePrivacy Directive requires consent from the user for cookies other than those strictly necessary for the operation of the site[7] and does not leave scope for the consideration of the other appropriate legal basis that are applicable under the GDPR.

PRIVO continually comes up against the issue of cookie consent on a child directed or mixed audience service. When a child lands on the home page of an ISS directed to them and perhaps older users (and therefore what we might determine to be mixed audience under the definitions for COPPA) they cannot consent for themselves to the use of cookies. Simply adding, ask your parent to consent, is not meaningful in our opinion as a child will simply accept.

We aim to help organisations comply with PECR and promote good practice by offering advice and guidance. We will take enforcement action against organisations that persistently ignore their obligations, starting with those that generate the most complaints. https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/

[7] (25) However, such devices, for instance so-called "cookies", can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in on-line transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.

Therefore in consideration of the above perhaps consent is not the only appropriate legal basis and the instance where risk of harm to the child is low, legitimate interest maybe more appropriate. The Presidency of the Council of the European Union suggested changes to Articles 6 & 8 that would see legitimate interest as a legal basis to process metadata and collect information from devices as an alternative to consent in its first draft proposal for the ePrivacy Regulation in February 2020. According to the presidency, "This legal ground is accompanied, in line with the GDPR, by a number of conditions and safeguards provided in a new Article 6b(2)."

Chapter 5: Age of Digital Consent and Age Verification

If and when consent is the lawful basis for processing a child's data, then the holder of parental consent must provide the consent for a child[8]. There is a lack of harmonisation in relation to age of consent across member states, which has proved challenging for some ISS in relation to the practical application of this requirement, particularly when it comes to the implementation of age gates to screen for a user's age. The GDPR requires that services make "reasonable efforts" to ensure it is the parent providing the consent, in light of available technology. This very much aligns with COPPA[9]. The sliding scale of consent under COPPA allows for a risk based approach to the level of assurance required for the processing of data. The more risk the data processing poses to the child the higher the level of consent required. For example, when low risk processing takes place a parent email is collected from a child to seek opt in consent for the use of the child's data. This is known as email plus[10]. Where higher risk processing takes place the holder of parental responsibility should be verified. This verification is achieved by a number of enumerated methods[11]. There are many ways to verify the age of the user without

[8] Art. 8 GDPR: Conditions applicable to child's consent in relation to information society services https://gdpr.eu/article-8-childs-consent/

[9] Obtaining verifiable consent means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child COPPA c.f.r §312.2

[10] (vi) Provided that, an operator that does not "disclose" (as defined by §312.2) children's personal information, may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent. Such additional steps include: Sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent's consent by letter or telephone call. An operator that uses this method must provide notice that the parent can revoke any consent given in response to the earlier email. COPPA c.f.r. §312.5 (b) (vi)

[11] (b) Methods for verifiable parental consent. (1) An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent

processing actual age. As an FTC approved COPPA safe harbor, PRIVO has developed several new verification methods. Age verification is a vital tool to support the protection of a child's personal data as it allows a service to provide the appropriate measures and safeguards to the child's experience. Many app developers and website providers claim obtaining parent consent is a challenge and the tools and technology are blockers to the user experience. This has led to some platforms turning a blind eye to the fact children are declaring older dates of birth in weak age gates to access services. These children must be protected and the platforms have a responsibility to acknowledge them and treat children appropriately. The DPC clearly states in the Consultation 5.5 Minimum User Age, that it does not consider that: "the setting of a minimum user age obviates the requirement on such service providers to comply with their obligations towards child users below this age, where children are likely to be using the service."[12]

It's also important to distinguish between identity verification and age verification. A child's identity must be privacy preserved. Using an age verification service that verifies age without collecting unnecessary data[13] to verify actual identity is a key to ensure that a service preserves the child's privacy protections both in terms of verifying and the service offered. The service can deliver reliable age attributes to companies engaging with children and should meet the

---

must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. (2) Existing methods to obtain verifiable parental consent that satisfy the requirements of this paragraph include:
(i) Providing a consent form to be signed by the parent and returned to the operator by postal mail, facsimile, or electronic scan;
(ii) Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;
(iii) Having a parent call a toll-free telephone number staffed by trained personnel;
(iv) Having a parent connect to trained personnel via video-conference;
(v) Verifying a parent's identity by checking a form of government-issued identification against databases of such information, where the parent's identification is deleted by the operator from its records promptly after such verification is complete COPPA c.f.r. §312.5 (a)

[12] *Fundamentals for a Child-Oriented Approach to Data Processing* – Data Protection Commission, Dec 2020

[13] Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation') https://gdpr.eu/article-5-how-to-process-personal-data/

requirements for security in relation to data collection and processing. The holder of parental responsibility should only have to verify once, associate a child by age and provide an interoperable credential for use by the child and parent, thereby reducing the need for the parent to provide verification data time and time again.

Age verification does not have to be a challenge but unless the requirement to verify is enforced the lack of protection that currently exists will continue.