The Pokémon Company International, Inc. response to the Irish Data Protection Commission, request for Public Consultation on Processing of Children's Personal Data and Rights of Children as Data Subjects under the GDPR

28 February 2019

For more information please contact:

[redacted]

Seattle Office

10400 NE 4th Street, Suite 2800
Bellevue, WA 98004
United States

T (425) 229 6000

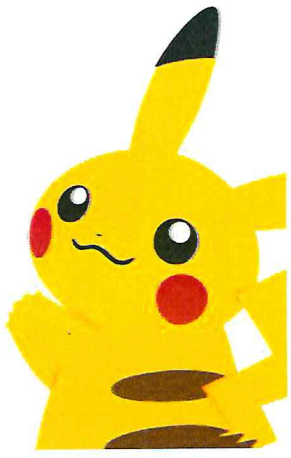
London Office

3rd Floor Building 10
Chiswick Park
566 Chiswick High Road
London, W4 5XS
United Kingdom

T +44 (0)20 7381 7000

www.pokemon.com

The Pokémon Company INTERNATIONAL



Introduction

The Pokémon Company International, Inc. (TPCi), a subsidiary of The Pokémon Company in Japan, manages the Pokémon children's entertainment properties outside of Asia, and is responsible among other things for brand management, licensing, marketing, the Pokémon Trading Card Game, the Pokémon animated TV series, home entertainment, and the official Pokémon website with its associated Pokémon Trainer Club program. For example, in the United States through partnerships with the Children's Advertising Review Unit's ("CARU") COPPA Safe Harbor Program[1], as well as support of CARU's Self-Regulatory Program for Children's Advertising[2] of the Better Business Bureau, TPCi is a strong proponent of children's privacy and child safety. TPCi has established itself at the forefront in children's privacy and child safety using methods and technologies that provide robust consent methods and controls for parents and, in many cases, do so without involving processes that would create barriers to access for children in economically disadvantaged circumstances such as using credit card verification methods. For example, TPCi has implemented an industry-leading age verification system in the United States, developed by Veratad Technologies, LLC, to help parents feel confident that they, and only they, are the ones who have authorized their children to access products distributed and supported by TPCi, including the 2016 phenomenon "Pokémon GO". Using Veratad's solution costs TPCi hundreds of thousands of dollars every year but TPCi believes this is a small price to pay to help parents have the confidence they deserve while helping them to retain control over their child's Internet experience, and to provide the world of entertainment to children who might otherwise encounter barriers resulting from their parents' lack of access to the banking system.

TPCi appreciates this opportunity to submit comments to the Irish Data Protection Commission (DPC), request for Public Consultation on Processing of Children's Personal Data and Rights of Children as Data Subjects under the GDPR[3]. We also support the periodic review of any best practices to ensure that consideration is being given to advancements in technology assisting with children's consent and verifying holder of parental responsibility (HPR).

TPCi looks to help best practices become industry norms, and some of our suggestions in this document will be targeted at helping to suggest ways to approach such norms rather than describing current practices adopted by any specific company today (including TPCi). The company is supportive of standardising methods to assist children in understanding their fundamental rights, and HPR verification through a code of conduct. Standardisation would assist TPCi and other companies who process the personal data of children in continuing to respect an individual's fundamental right to ownership and protection of their personal data. Additionally, such effort will provide more legal certainty and consistency across organisations furthering respecting of those rights. In this respect we also acknowledge that standardisation is by no means a substitute for parental responsibility, but aids organisations in providing continued transparency and information on the processing of personal data so parents can make informed decisions.

---

[1] In January 2001, CARU's self-regulatory program became the first FTC-approved Safe Harbor under the Children's Online Privacy Protection Act of 1998 (COPPA). Participants who adhere to CARU's Guidelines are deemed in compliance with COPPA and essentially insulated from FTC enforcement action as long as they comply with program requirements.

[2] CARU's Self-Regulatory Program for Children's Advertising, voluntary industry guidelines, enforced by CARU, which set out how to ensure that advertising to children is accurate, appropriate and not misleading and that website practices conform to CARU's guidelines on Online Privacy Protection.

[3] Adult Consultation Stream 1 open for response from 19 December 2018 until 1 March 2019 inclusive. https://www.dataprotection.ie/en/news-media/latest-news/public-consultation-processing-childrens-personal-data-and-rights-children.

We hope that our responses to the first stream of the consultation will be helpful, and we remain at your disposal and look forward to further engage with the DPC to discuss our responses should such opportunity arise.

TPCi's Responses to the Data Protection Commission, request for Public Consultation on Processing of Children's Personal Data and Rights of Children as Data Subjects under the GDPR

I. Children as data subjects and the exercise of their data protection rights

(A) Transparency and the right to be informed about use of personal data (Art 12 -14)

I (A) 1: What methods could organisations who collect and use children's personal data employ to easily convey this transparency information to children?

The use of simple language and graphics combined with robust parental notice is in line with the principle of transparency of Recitals 39, and 58 of the GDPR[4].

For a child directed notice, "packaging" the words would assist in encouraging the child to read about personal data processing and data protection. Employing graphics (standardized icons), cartoon format, video or even "gamification" of the information contributes to the use of clear and plain language for easy understanding. An example of this gamification concept would be limiting one or two sentences on a screen, providing a click function on screen to advance to the next set of information, or having the child provide an answer to an easy question advancing to the next screen, where the child earns a token on screen reward for completing the screens.

Given the current trend of privacy notices being very long documents that primarily the privacy lawyers, regulators, and consumer protection organizations read and understand, many parents may instead be looking to the child formatted privacy notices in order to gain a better sense of what personal data is, how it is being processed, and explaining to their child reasons for allowing or denying the child's use of the service.

It would be difficult for any company, even with the best intentions, to establish such a policy as is described above today due to absence of standardisation of iconography and information. Without such standardisation, each company would develop its own system of symbols, which would most likely increase and not decrease complexity for exactly those readers for whom simplicity is at a premium. DPC could provide a meaningful service to the community by helping to develop such iconography. That would provide a common "language" for such documents so that children and parents throughout

---

[4] Recital 39 of the GDPR "[...] The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language is used. [...]".
Recital 58 of the GDPR, "The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualization be used. ... 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."

Ireland, and Europe, could come to understand these issues. TPCi would happily work with DPC to provide such input as may be desirable in that process.

I (A) 2: What approach should be used by organisations whose products or services are aimed at both adults and children? For example, should two separate sets of transparency information be provided that are each tailored according to the relevant audience?

The optimal initial position for all organisations to which the GDPR applies should be content parity, and that whatever you do for children you do for adults and vice versa as this would avoid issues as the child reaches the age of digital consent. If there is a reason to provide dual transparency information in the form of privacy notices each with differing content (such as a site's providing certain services for adults that would be inappropriate for children such as the ability to post photographs or other personal information, processing medical information, or the like) then the notices must be clear and concise. As children customers age up to adults, these new adults should be entitled to exercise their own control and protections over their personal data, including the right to revoke consent that was previously granted by a HPR. Children should be able to revoke at any time, without the revocation process being cumbersome. Once a child reaches the age of digital consent, the organisation should provide the new adult information that they no longer have their HPR to control the processing of their personal data. It now becomes the new adult's responsibility to understand what data is being processed, how it is being used, and he or she can exercise any of their rights surrounding their personal data. The new adult is directed to privacy notices for the services they have been/are using. Having differing content between the notices would likely confuse the consumer as to which privacy notice applies, and is the child data of the individual processed differently than his or her adult data? To further the support of a consistent privacy notice, some customer facing websites provide a "for children" and "for grown-ups" split of their site where the website services and experiences may differ, however, the Privacy Policy and Cookie Notice are the same for both versions of the site. As stated in I (A) 1, having a different format to serve the varying age and comprehension levels supports understanding.

(B) Right of Access (Art 15)

I (B) 3: At what age or in what circumstances should a child be able to make an access request to an organisation and receive a copy of their personal data? Is age the only relevant factor and if not, what other factors should be taken into consideration?

From TPCi's perspective, it is difficult to see why the criteria would be different as between children and adults for any of the data subject rights under Articles 15 – 22. Setting different criteria for the data subject rights would cause further confusion for not only the data subject, but the organisations as well. TPCi shares the same challenges as other organisations and are seeking guidance on any requirements as to if the organisation is required to communicate also with parents. If so, what the right balance should be in terms of how much and the details parents should know, in addition to the balance between the child's rights, and parental rights and responsibilities. Parental consent would be a consideration before a company/organisation converses with a child about his or her data access request, as most parents would want to know that such conversation is happening. Should consent be granted by the parent, then both parent and child would receive communications so long as the child is under the established age of digital consent. Consideration should also be made as to the differing maturity levels spanning an age

range of 13 – 15 years old. Younger children may be more accepting and comfortable with parental supervision than older children. TPCi is aware of DPC's consultation process with experts in child development and looks forward to the results of that process to help develop rules and policies around this.

On the other hand, if age should not be the only relevant factor for a child to make an access request and receive a copy of their personal data without parental consent, then additional factors should be objective. It would be difficult for organisations to make a capacity determination if not based on age and additional objective or established[5] criteria. For example, 13-year-old in Ireland, plus completion of a certain level in school, and membership to established organizations could be an indication that a child under 16 years old can request their personal data without parental consent. However it would be very difficult for a company acting on a pan-European basis to apply such a standard were it to come into existence EU-wide due to the multiplicity of applicable organizations in every EU territory. Also, aside from societal expectations of suitable qualifying criteria which will vary on a country-by-country basis, verifying additional criteria would result in collecting more personal data from a child and companies must continue to apply data minimisation principles. Put simply: adding relevant factors seems like it would cause more problems than it solves. For edge cases such as emancipated minors or issues of personal or public safety, the relevant rules should provide for companies making a good faith determination based on reasonable evidence (*e.g.* a judgment of emancipation) without being needlessly prescriptive. DPC will no doubt make itself available for assistance under such circumstances, so rulemaking can provide for approaches to DPC by companies as appropriate.

I (B) 4: In what circumstances should a parent be able to make an access request and receive a copy of their child's personal data? Is there an upper age limit after which a parent should not be able to make an access request for their child's personal data? Are there circumstances where both the parent and child should have to jointly make an access request for the child's personal data?

Below the age of data subject's digital consent should be the circumstance where the parent is able to make such a request and for an organisation to consider that access request. TPCi contemplates a situation where joint requests would make sense when the child is below the age of digital consent. If the upper age limit for organisations to decline a parent's access request is set at 18 as the United Nations Convention on the Rights of the Child (UNCRC) has done, companies would be ignoring the technical savvy of those under 18 years old and legislative process. The GDPR has established an upper age threshold of 16 years old as to where an organisation is not required to obtain consent from the child's HPR. A code of conduct addressing children's consent and verification of an HPR should not be able to change established law and extend the age of digital consent to 18 years old (for example). If the age limit is higher than the age established for digital consent, to no longer require parental consent or their parent can access their data, the alternative for a child who is at least 16 years old would have in order to

[5] It can be envisioned that through approved organisations that teach children life skills, such organisations could also offer a personal data and security course where the child would receive a certification or achievement badge for completing that lesson. The results from Children and Teacher's participation in the second stream consultation could shape the content or a course of classroom curriculum for children to learn about their data privacy rights and how technology is involved in the processing of their data.

prevent his or her parent from accessing their data is then to exercise his or her data subject right and request the organisation to delete their data.

I (B) 5: How should the balance be struck between a parent's right to protect the best interests of their child and the child's right to privacy when organisations are dealing with access requests for the child's personal data?

The GDPR has started the discussion of balance and provided age thresholds, setting an upper age of digital consent as 16, which for the most part everyone will understand, and organisations can apply. The GDPR has specifically allowed Member States to derogate from 16, and TPCi looks to the DPC and society to provide standards for Ireland as to what the acceptable societal parameters are, finalising those standards into a code of conduct for organisations to honour and apply across the Member States.

(C) Right to erasure – ("Right to be forgotten" - Art 17)

I (C) 6: At what age or in what circumstances should a child be able to make an erasure request to an organisation and have their personal data erased? Is age the only relevant factor and if not, what other factors should be taken into consideration?

The age in which a child can exercise any data subject right should be the same age that the GDPR has set as the upper limit where a parent's consent is no longer required, which is 16 years old[6] (or lower as set by Member State law). As expressed previously in the response to I (B) 3 above, the criteria to exercise rights under Article 17 should be consistent with the criteria to exercise the other GDPR data subject rights. For organisations, it would be difficult to see justification for the under 16-year-old to have their data kept by the organisation against his or her will just because the parent wants it to be there. Companies would be justified in believing that such a retention is unlawful under the GDPR. If the goal is to apply a consistent standard across a wide reach of organisations, organisations would need very simple and easy to apply measures to ensure uniformity and clarity. TPCi's response to Section 1 (B) 3 addresses whether age should be the only relevant factor.

I (C) 7: In what circumstances should a parent be able to make an erasure request on behalf of their child and have their child's personal data erased? Is there an upper age limit after which a parent should not be able to make an erasure request for their child's personal data? Are there circumstances where both the parent and child should have to jointly make an erasure request?

Specific to all Member States that have set the age of digital consent at 16 years old, once the child reaches that age then parental requests should no longer be valid. Joint requests make sense for older children (13-16). We appreciate DPC's efforts to obtain information from experts in child development on this issue and we look forward to the results.

---

[6] Recital 65 of the GDPR "A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this regulation or Union or Member State law to which the controller is subject. . . . That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child [. . .]."

II. Safeguards

(A) Age Verification (Art 8)

II (A) 8: If an online service provider is relying on consent as their legal basis (justification) for processing children's personal data, what methods could/should be used to verify that a child is 16 or over in order that the child is granted access to the online service without the need for parental consent?

In an environment where privately-maintained services such as the Veratad solution which TPCi has implemented in the USA do not exist or are impractical, TPCi would welcome creation of an Application Programming Interface (API) against a government-maintained database for service providers to query and have knowledge without requesting extraneous information. More exploration would be needed in order to determine an acceptable balance between the mix of government information, the commercial activities, and societal attitudes. In support of a government-maintained database, data protection authorities could look towards other countries and how those countries verify an individual's age. South Korea verifies age using government records, and it is acceptable in Korean society to provide a Korean social security number as a way to verify age in order to enforce the Shut Down / Cinderella Law (children under 16 years old are not permitted play computer games from 12pm midnight to 6am, unless a parent consents to allow the child to play during those times).

Although this submission addresses the GDPR which applies to all forms of personal data, there is an opportunity to take small steps and address mobile applications (apps) in particular. Many apps that a child may download to their mobile device involve a 3rd party, namely a mobile carrier or the platform's app store. These apps require the customer to have an account with the mobile carrier or app store. There are opportunities for these 3rd party businesses to maintain an age authentication feature tied to the customer's account.[7] When a child wants to download an app that processes personal data, the 3rd party account can be used to verify age.

This is distinguishable from a traditional credit card verification process in two major ways: it leverages an account that already exists rather than requiring the creation of a new one, and it does not result in a charge against a credit card to conduct account verification. Many parents no doubt find it difficult to understand why they should pay €1 to create an account for their child. Credit card verifications therefore can result in exactly the opposite result to the one good policy would suggest: parents might request that their child provide inaccurate personal information to data processors, which would allow those processors to collect further information about those children, all so the child's parents can avoid paying money to have the ability to exercise their legal right to supervise their child's online activity and privacy. Bad though this is as a matter of policy, it also risks creating a situation where children whose parents do not have access to the formal banking system become functionally blocked from accessing these services entirely. Parents might have bought prepaid mobile phones or otherwise obtained access

[7] See Section (20a) of the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). https://www.parlament.gv.at/PAKT/EU/XXVI/EU/05/43/EU_54357/imfname_10879938.pdf. The proposed language suggests opportunities for consent to apply across services by and end-user giving consent to use of certain types of cookies by whitelisting one or several providers.

to the mobile Internet without needing to hold a credit card and wish to provide the same to their children. It is difficult to understand why their lack of access to formal banking should be an impediment to their child's development. TPCi endeavours to use non-credit-based age and consent verifications in its own authentication protocols for these reasons.

II (A) 9 (a): What methods could/should online service providers use to ensure that the person providing consent in these circumstances is actually the HPR over the child?

It should be understood that the verification methods given the current technology available such as credit card verifications do not actually verify the parent/child relationship but verify that the individual the child provided as his or her parent is over 18 years of age and has a credit history. In order to actually verify that the adult is the HPR would require the collection of additional highly intrusive personal information that an organization has no real interest in having; it would arguably violate the GDPR for organizations to ask for sufficient information to know this answer with certainty. Then should compliance become a question, the provider would retain such information in order to demonstrate later that valid consent was given[8]. This additional information would go beyond the standard credit and national identification number, but possibly birth certificates, court documents in circumstances of determining divorced, non-custodial parents, and legal permanent or temporary guardianships.

As noted above in section II (A) 8 TPCi does not recommend the use of credit cards for verification purposes. An additional method TPCi would not recommend is that of video chatting with parents to verify HPR. This would be an incredibly expensive method for companies, as it could not be implemented at scale (a chat system presupposes a live human at each end) and would have to be available on a 24/7 basis to accommodate such things as parents who do shift work and may not be available during a company's regular business hours. Nationwide standardised training for organisations' video chat representatives would need to be established as to the criteria the video chat would need to meet in order to determine that the individual on the other end is the HPR. This could inadvertently complicate things should the organization be required to retain the video footage to prove compliance that reasonable efforts were made to verify HPR. A video may also reveal special categories of personal data[9] such as racial or ethnic origin, biometric data, sexual orientation, etc.

II (A) 9 (b): What constitutes a "reasonable effort" made by organisations to verify such consent is being given by a person who is actually the holder of parental responsibility over the child? How should "reasonable efforts" be measured in this regard?

TPCi would appreciate guidance from DPC as to the standard of "reasonable efforts" and imagines that other companies would be equally appreciative.

---

[8] Additional guidance is necessary for Article 11 of the GDPR. Article 11 provides situations where the "controller shall not be obligated to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation". However, in the event of a challenge from a data subject claiming that organisations did not take reasonable steps to verify a HPR, will DPAs dismiss such complaints outright?

[9] See Article 9.1 GDPR.

II (A) 10: Prior to 25 May 2018, there was no law setting the age of digital consent in Ireland, but many online service providers required users to be at least 13. If an online service provider now is aware that an existing user of their 14 service is under 16, should the user be locked out of the service until they reach 16?

It is difficult to see why a pre-25 May 2018 user should be locked out of a service to which they previously had access prior to the GDPR unless there is a very strong public policy reason to do so such as an organisation's having implemented no form of age verification whatsoever. From a legal perspective, "grandparenting" is permissible in other contexts and should be applied in this context also. And pragmatically, as noted in the question, responsible companies will have implemented some form of parental verification process on a worldwide basis. It would be a different conversation for organisations that did not have any verification process at all and it would be understandable for DPC to create some form of *de minimis* criteria to allow for "grandparenting" to occur. But for organisations that had acted diligently and conducted age verifications prior to the coming into force of the GDPR, those organisations may not have obtained or retained information sufficient to accommodate a change at this point. They would therefore be at risk of a requirement to cancel accounts and delete information. Cancellation of accounts and deletion of information would often result in the loss for the data subject of things such as online item purchases in video games, access to apps and digital content, and other items of value. Those consumers would not have had any reasonable ability to foresee this consequence and would therefore experience a significant prejudice resulting from such a change.

(B) Online service providers and different national ages of digital consent in the EU (Art 8)

II (B) 11: How should such online service providers ensure they comply with different ages of digital consent in different Member States?

The age of digital consent derogations permitted by the GDPR results in requiring online service providers to keep a piece of personal data that they otherwise would not need to keep (i.e. country of residence). It also could create issues when each parent lives cross-border and online service providers would need to know multiple data points depending on to what extent the online service providers are to verify HPR. Given the different ages, what would greatly assist online service providers /controllers would be for a relevant organization, the European Data Protection Board for example, to be the official source for providing a centralised and maintained publicly available resource listing the ages per Member State in an easy to read format and explaining the derogation of "age of digital consent" made by the EU Member States. This source should also be easily accessible by data subjects.

III. Profiling and marketing activities concerning children (Art 21-22)

III.12: In the case of marketing to a child, what factors should be taken into consideration when balancing an organisation's own legitimate interests in conducting direct marketing and the interests and rights of a child who is being marketed to?

Compliance with law, marketing and advertising regulations, and best practices on advertising to children should address this.

III.13: Should organisations be prohibited from profiling children for marketing purposes? If so, should this be age-dependent or dependent on other factors? If so, what are these other factors?

Parents should be allowed to decide whether they want their children to receive marketing communications or not.

In order for organisations to know if the HPR has consented and allows profiling children for marketing purposes, we would seek guidance on solutions to be in place in order to address the operational challenges in obtaining a child's consent and verifying the HPR in the context of the ePrivacy Regulation. The Council of Europe's recent publication (15 February 2019), under the Romanian Presidency[10], includes proposed language, reinforcing that consent should be required where personal data is collected for purposes other than for what is necessary to carrying out the transmission of an electronic communication over an electronic communications network or for the provision of the information society service requested.

IV. Data protection by design and by default (Art 25)

IV.14: What measures should organisations take to incorporate the principles of data protection by design and by default into the services and products that they offer to children?

Organisations that are committed to practicing data privacy and security frameworks should be conducting initial and recurring data protection training for employees whose roles involve the design/development of applications and systems that process personal data. This is would support an organisation's ability to incorporate the principles of data protection by design and by default. These principles organically become part of the DNA of the organisation and its employees that produce these products or services.

In addition to role-based training, use of data protection impact assessments (DPIA) would also support incorporation of the principles of data protection by design and default for services and products offered to children and processing personal data. Guidelines recommend that when processing children's data, Data Protection Impact Assessments should be conducted.[11]

IV.15: Do you think products/services that are used by or offered to children should have built-in default privacy settings that vary according to the age and evolving capacities of a child? For example, should there be stricter privacy settings for younger children? How should these variations in the privacy settings be given effect?

---

[10] Section 21 of the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). See https://www.parlament.gv.at/PAKT/EU/XXVI/EU/05/43/EU_54357/imfname_10879938.pdf

[11] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Section III B (a) 7, "Vulnerable data subjects may include children (they can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data) [. . .]. "

It is difficult to know how best to answer this question without substantial expertise in child development, which is beyond the ability of many organisations reasonably to procure. This is an area in which DPC's expertise and ability to obtain academic and other experts will be very welcome to help organisations determine the best outcomes for them.

V. General

V.16: Are there any other particular issues you would like to raise with the DPC in connection with the subject matter of this consultation?

TPCi thanks DPC for the opportunity to provide a submission in this consultation and hopes to have the opportunity to work with DPC to develop solutions that address the needs of the children and parents of Ireland and all of Europe.