23 January 2018

TIE COMMENTS ON THE GUIDELINES ON CONSENT (WP259) UNDER REGULATION 2016/679

Toy Industries of Europe (TIE) welcomes the opportunity to provide feedback on the Draft Guidelines on Consent under Regulation 2016/679 (GDPR). Overall, TIE supports the principle based direction WP29 has taken in developing the Guidelines. We especially welcome the recognition of a proportionate approach to parental verification that differentiates between low-risk and high-risk processing in relation to children's consent; this approach is essential to implement the Regulation in the real world. Nevertheless, the Guidelines also raise a number of questions on the implementation of the rules on children and consent that we would urge for clarification on. In light of the relationship between transparency and consent, we have also provided our comments on the parallel WP260 consultation at the end of this document.

Ensure a harmonised approach across the DSM to children and the GDPR

The section on Children's Consent provides much needed guidance in this area, especially with regard to sites and services that are aimed at children.

We welcome the WP29 call for harmonised solutions with regard to age thresholds. We suggest that this call should go further: it should be applied to Article 8 as a whole, in order to ensure the rules on children are interpreted consistently across the Digital Single Market.

To provide additional certainty for business operating in multiple markets, we would also suggest that additional EU level Guidelines on the application of the GDPR in the context of children (as per the recently published draft UK Guidance) are needed to increase harmonised application of the rules. This would be especially helpful for those topics which the Guidelines leave to the discretion of the controller such as 'reasonable effort' and low vs. high risk processing.

Illustrate additional examples of a proportionate, risk based approach to children's consent

We see a proportionate and risk based approach as essential to achieving a workable implementation of parental verification under Article 8. It would, however, be useful to have further examples of:

- What is considered to be low- and high-risk processing;
- The balance test between legitimate interest and children's rights (see section on lawful grounds below)
- What would be considered an "appropriate check" in relation to age verification methods and the eventuality that a child lies about its age?
- What might be considered as reasonable age verification methods on those sites that are not offered directly to children (for example in the comment on e-commerce provided later in this document)
- What might be considered as appropriate methods for obtaining parental authorisation in high-risk data processing. At present, several methods are accepted under US children's privacy framework COPPA. We would suggest that these could be looked to as examples to start with, but that this list should be expanded to reflect the realities of the EU market, for example, mobile verification methods should also be accepted.
    - COPPA states that parents can verify consent by: signing a consent form and returning to company via fax, mail, or electronic scan; using a credit card, debit card, or other online payment system that provides notification of each separate transaction to the account holder; calling a toll-free number staffed by trained personnel; connecting to trained personnel via a video conference; providing a copy of a form of government issued ID that companies check against a database; answering a series of knowledge-based challenge questions that would be difficult for someone other than the parent to answer; or verifying a picture of a driver's license of other photo ID submitted by the parent and then comparing that photo to a second photo submitted by the parent, using facial recognition technology.

Give further insight into the lawful grounds for processing children's data

As per Article 6 of the GDPR, the Guidelines note that consent is not the only lawful grounds for processing personal data. In many cases, legitimate interest or legal obligations will be the correct basis for processing children's data. An incorrect judgement on the part of the controller, no matter how well intentioned, would render the processing unlawful and the controller would be liable. As such it would be helpful for WP29 to incorporate additional examples under which the other lawful grounds would be valid in order to increase certainty for business. This is especially true in the cases of legitimate interest and legal obligation.

Suggested examples:

- *Legal obligation: of the collection of parent's contact information (i.e. email address or phone number) in order to verify consent.*
- *Legal obligation: Processing an IP address if a user signals that they are under the digital age of consent on a site not directed towards children.*
- *Legal obligation: Age verification and geo-screening to ensure that correct age of Digital majority is applied.*
- *Legitimate interest: Processing of an IP address specifically for the purpose of remember a game scores and/or site set-up preferences when a child returns to the site.*
- *Legitimate interest: Processing of an anonymous username and password to create a user account for a child to access the child targeted area of a site that hosts games and activities for children. The processing of the data would enable previous game scores and/or site set-up preferences to be remembered each time a child logs in, but there would be no additional processing of personal data*
- *Legitimate interest: Processing device ID or other persistent identifiers to enable in-game activities that do not include behavioural advertising. For example, tracking session length and OS type on an aggregated basis to understand whether an app is performing or crashing on certain OS.*
- *Contract: Processing of information needed to activate parental verification methods (for example a credit card payment)*

Give more guidance on how to strike a balance between expiration of parental consent and data minimisation

On one hand the Guidelines call for the minimisation of data, whilst on the other hand they note that parental consent expires when the subject reaches the age of digital consent, which would need to be given by the subject themselves. This appears to contradict the principle of data minimisation as well as the guidance on data retention.

Toy companies who offer ISS to children generally aim to minimise the amount of data they process to provide these services. In the scenario above, even for the most low-risk consent based processing, the controller would have to process the date of birth and contact information for the child. This increases the amount of personal data that is processed about the child, and so potentially increases the processing risk.

In addition, it is not clear what would happen if consent has not been successfully requested from the child once it reaches the age of digital consent. For example, if a child has a user profile on a toy website, would the controller automatically have to delete the account and all linked information (for example stored game scores, virtual worlds that have been built, tokens that have been collected, etc.) the moment the child reaches the age of digital consent?

Finally, if a child can only give consent once they reach the age of digital consent, but the moment a child reaches the age of digital consent parental consent expires, at what point should a company

receive consent from the child themselves? Is the child expected to give consent for any of their data that has been processed on their birthday?

We would suggest a more sensible approach would be for the parent or data subject to notify the controller when the child reaches the age of digital consent. Any data that is processed on the basis of parental consent should be presumed to be legitimate until consent is withdrawn.

Better differentiate services offered directly to a child

The Guidelines state that if a ISS provider makes it clear to potential users that it is only offering its service to persons aged 18 or over then it will not be considered to be offered directly to a child, unless it is undermined by other evidence, such as the content of the site.

Given the GDPR describes an ISS as *"any services normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services",* it would be helpful if clarification was given as to whether websites that are not monetised (for example, those that do not include paid advertising) fall into this category. It would also be useful to have examples of ISS that are not covered by Article 8.

Clarity is also needed with regards to websites that are designed specifically for parents to use with their pre-literate children. What would consent look like in these cases? Would a parent be able to consent directly to the processing of data when browsing with a child that is too young to read, or would a verification method still be expected?

Additionally, with 88% of toys being purchased by adults, parents are often the focus of many toy company websites. Often, toy websites are designed purely for parents to find out more information about toys and play patterns, or else may have a designated online store area specifically intended for adult purchasers. As such, they may use behavioural tracking and retargeting.

Whilst these sites are offered to an adult audience, the content of these sites features toys and play. Would this mean that the site is assumed to be offered directly to a child? If so, what would be considered as reasonable in terms of age verification? In the case of ecommerce sites or areas, this would potentially put the sector at a competitive disadvantage to other online toy sellers, such as online platforms, who would not need to work on this assumption. We would call for a common-sense application of the Guidelines, and suggest that measures, for instance bumpers or interstitials, could be used to signal that a site, or parts of sites that are intended for adults. This option would minimise the data that would need to be collected about children.

Suggested example:

A toy company offers an online store which features examples of products, but no games or activities section, it also puts in place clear signals (such as bumpers or interstitials) specifying that this is an adult zone. In this case it is considered as being directed towards adults.

Provide examples for withdrawing (parental) consent without detriment

The Guidelines underline the need for consent to be able to be withdrawn without detriment to the user. However, in some circumstances, ending access to a service if parental consent is refused, or later withdrawn, should not be considered as a detriment to the child. For instance, a nominal credit card transaction is provided as an example of how verified parental consent can be given in high-risk processing cases. If a company uses this method to obtain parental consent to process a child's data as part of a service, then the child can only access the service when the parent pays the fee. If a parent refuses to pay the fee, or stops paying any recurrent associated fees, then not having access to a service should not be seen as a detriment to the child.

Suggested example

An app developer or website operator wishes to allow children to engage in social sharing which could involve the exchange of personal information. They elect to make this service available only for a fee

using a credit card as a method of parental consent. If a parent refuses to consent, or withdraws consent by refusing to pay the fee, the child does not suffer a detriment within the meaning of the regulation, and the controller should be able to refuse access to the service.

TIE COMMENTS ON THE GUIDELINES ON TRANSPARENCY (WP260) UNDER REGULATION 2016/679

TIE welcomes the opportunity to provide feedback on the Draft Guidelines on Transparency under Regulation 2016/679 (GDPR). Overall, TIE supports the principle based direction the WP29 has taken in developing the Guidelines. The document provides important direction on the issue of Transparency. However, there are several points that we would suggest could be usefully clarified.

Ensure a harmonised approach across the DSM to children and the GDPR

The section of the Transparency Guidelines on children provides useful guidance, in particular in relation to sites and services aimed at children. We suggest that additional EU level Guidelines on the application of the GDPR as a whole in the context of children (as per the recently published draft UK Guidance) are needed to increase harmonised application of the rules and to provide additional certainty for business operating in multiple markets.

Clarify that suggestions and recommendations are not obligations.

Throughout the Transparency Guidelines, suggestions and 'best practice' recommendations are provided. They give helpful pointers on issues such as the type of user testing, provision of information to children and information that should be included in privacy notices. However, we would call for clarity that these suggestions and recommendations are options that can be used to meet transparency obligations under the GDPR, but they are not obligatory measures that controllers must adhere to.

Give better clarity on the level of information provided to children under age of digital consent

We appreciate the intention of the Guidance in the section on provision of information to children using appropriate language. The toy industry has vast experience dealing with children of all age ranges, and supports and understands the importance of using child-appropriate language in communicating with children old enough to read.

However, we feel that the following points are worth noting. Where information society services are intended for use by pre-literate children, the primary recipient of information is always the parent. For example, apps intended for three-year olds can provide learning opportunities and fun entertainment, even simplified cartoons and icons about privacy will not be understood.

With slightly older children, for example children who can read but are still developing their literacy skills, simple language and, where appropriate, reminders to check with parents or obtain parental consent, are appropriate in the case that Article 8 is triggered. However, when children are under the age of digital consent the privacy notice must be directed to the holder of parental responsibility.

Finally, when there is potential uncertainty whether an ISS could be considered as being 'offered directly to children' we would urge for a common-sense application of the Guidelines. We would suggest that measures, for instance bumpers or interstitials, could be used to signal that a site, or a part of a site, is intended for adults. This option would minimise the data that would need to be collected about children, for example in relation to age gating or geolocation.

Provide possibility of using language qualifiers

We support the provision of information to users in clear and plain language, both to those above the age of digital consent, as well as to the holder of parental responsibility in the case that Article 8 is triggered. However, we are concerned with the inclusion of language qualifiers such as "may", "might", and "possible". The use of such qualifiers allows us to correctly describe what will happen in the real world: a company can always eventually choose not to use the data that has been processed under consent for any purpose.