POLICY BRIEF // DIGITALISATION

WILL THE GDPR CHANGE THE WAY CHILDREN USE AND EXPERIENCE THE INTERNET?

As the date of the effective application of the General Data Protection Regulation (GDPR) draws near, organisations big and small are examining how its various provisions will apply to them. Indeed, from the 25th of May 2018, there are a number of features and concepts in this Regulation which could potentially transform the web, including the way children experience it.

WHAT IS A CHILD?

Assessing the impact of the GDPR on children is a tricky endeavour. A 6-year-old child will certainly be affected differently to an 11-year-old or a 15-year-old. Younger children would benefit the most from higher data protection by default; older children might suffer from it since it might limit their online experience (or constantly seek parental consent). As it turns out, a data protection by design and by default is one of the new obligations of the GDPR (Article 23). As many online service providers claim to abide by such a rule already, we will have to wait to see what the end effects of this provision will be, especially on children.

But let us start with one of the most controversial provisions – article 8 of the GDPR: children below 13 (at least) or 16 (at most) will need parental consent for the processing of their personal data by a data controller (online service provider). This poses many questions in terms of children's right to privacy but also the practical implications of such a provision, forcing children to pester their parent(s) every time they install an app or subscribe to an online service. It may further limit the possibility of children from accessing a service if parental consent requirements cannot be fulfilled because of technical conditions imposed by the service (verification via e-ID, etc.).

It could also simply push services to adopt a ‘post COPPA' strategy: put a threshold of 16 for the use of their services, being fully aware that children below the age of 16 will lie about their age to subscribe, and finally resorting to a very uncomfortable ‘witch hunt' where accounts of ‘minors' are randomly deleted in order to pretend to comply with the rules. Children would end up suffering from the double blow of a lower protection (since they have to provide consent as if they were adults using a service designed for adults) and the potential loss of all their data in case their trickery is discovered by the service.

Alternatively, online service providers could decide to set up a “special” form of online account where at no time do they process personal data, which children could thereby access without having to seek parental consent. This may be the “ideal” situation, but is highly unlikely. However, children may truly benefit by enjoying a relatively unfiltered web, free from targeted advertising, but online service providers might suffer from less advertising revenue.

Users as the weakest link

User consent as such, is a very controversial issue. It glosses over the reality that users never read terms of service and tick away any box to access a service, regardless of the end effect on their privacy, leaving it up to whistle blowers, activists or civil society organisations to denounce abuses and put pressure on service providers to change their terms of service. Most importantly, users do not have a choice since ticking boxes is a precondition to using most online services, putting users in a ‘take it or leave it' situation. Sure, you can protect your privacy by not subscribing to any online service, but at the same time, you will be excluded from participating in the online world.

Thankfully, the GDPR does address some of these concerns. Firstly, it tackles the point raised above head on in Article 7 (4), where consent may not be considered as given ‘freely' if the provision of a service is made conditional on the consent to the processing of data which is not necessary for providing that service. Secondly, the Regulation clearly mentions that "children deserve specific protection of their personal data", especially when used "for the purposes of marketing or creating personality or user profiles". Thirdly, it provides any data subject the right to object to the use of his/her personal data for the purposes of "direct marketing" (Article 19 (2)).

All of these provisions can impact the experience of children online and especially their exposure to marketing and advertising. Since Article 19 (2) gives every user the right to object to the use of his/her personal data for direct marketing, online service providers may not be able to circumvent this right by simply pretending that there are no children on their service or that their service is not designed for children.

Transparency and comparability

The GDPR's third chapter dealing with transparency includes many details on the modalities for communicating to users about how their data is being processed. It includes requirements such as the use of ‘plain language' and the use of pictograms or icons to make it easier for users to understand. By ensuring a common standard for communicating about data processing, the GDPR will enable easier comparability between services in terms of their data processing activities. This could encourage the emergence of comparison websites which rate different online service providers according to their respect of privacy and data protection, including online service providers best suitable for children.

Data portability

Enabling consumers to switch between services (data portability, article 20) is essential to improve the overall quality of service providers. For instance, in the earlier days of mobile communications where operators locked consumers into contracts or made it impossible to keep your phone number, after the legislator made it easier to switch between service providers, the quality of the services improved. The same holds true for online services. At the moment, it is impossible to transfer your data from one social network to another. Part of the problem is simply the incompatibility of the data between certain online services. For instance, Tweets cannot be easily converted to Facebook posts and vice versa. Nevertheless, providing the right to export your data in an interoperable format may enable the emergence of options by service providers to import data from other service providers into their own.

It is the intention of the GDPR to ensure the right for users to get a copy of their data in a "usable" format to take it to another service, which is indeed one of the preconditions to allow for switching services. The possibilities of easily comparing between data protection policies coupled with easily switching between online service providers could put enough pressure on online service providers to behave more responsibly and thus create a better environment for all users, including children.

Objection to profiling & automated decisions

All EU citizens will have the right to object to profiling (article 21), contest automated decisions by requesting that there is some "manual" review of a decision (article 22) and ask for transparency and clarity over how algorithms arrive at certain decisions (article 15). All of these rights are extremely important, especially regarding the access to certain crucial services like healthcare insurance or mortgage loans. However, it is still unclear how these rights will work in practice. If profiling is a precondition for accessing a service, it is difficult to see how users will be able to object, save for renouncing to accessing the service. Asking for a "manual" review of an automated decision may amount to no more than a person manually approving an automated decision, which will change very little. Finally, requiring transparency over how automated decisions are taken may be impossible. Many automated decisions are now taken by algorithms generated via novel methods such as "deep learning", where computer programmes learn from a set of data without the input from humans.

Flexibility and European courts

One of the main caveats of the GDPR is all the Member States' flexibility in applying/interpreting the regulation. In order to accommodate the concerns of all stakeholders, much of the wording inside the GDPR ended up with "may" instead of "must", which may (pun intended) limit its impact to some extent. Ultimately, much of the GDPR will require clarification by European courts. Also, what an "interoperable format" is in practice for data portability or interpretation of what constitutes data "not necessary for providing a service" will most probably have to be clarified by the European Court of Justice following lawsuits. For instance, at present, Facebook provides users with all their data in HTML format, which, although it is widely used and readable, does not enable users to upload their content on another service (this would require Facebook to export data in a database readable format).

To conclude, the GDPR is a step in the right direction in terms of enhancing EU citizens 'data protection. Its implementation and the use of Member States' 'flexibility' will show whether it will have the intended effect.

November 2017

More information, contact Martin Schmalzried, Senior Policy & Advocacy Officer mschmalzried@coface-eu.org

COFACE Families Europe - Rue de Londres 17, 1050 Brussels
Tel: +32 2 511 41 79 Email: secretariat@coface-eu.org Website: www.coface-eu.org

---

COFACE is supported by the EU Programme for Employment and Social Innovation "EaSI" (2014-20). The information contained in this document does not necessarily reflect the official position of the European Commission