WERKSMANS ATTORNEYS

REGULATORY

That's the way the cookie banner crumbles: draft EU ePrivacy regulation seeks to reform the cookies recipe

3 March 2021 *9 min read*

by Ahmore Burger-Smidt, Director and Head of Data Privacy Practice and member of Competition Law Practice; and *Tristan Meyer, Candidate Attorney*

European data protection regulators kicked off the New Year with a fresh draft of ePrivacy regulations which appear to mix up the existing recipe in so far as consent to cookies is concerned. The question is whether we can gain any insight from this ahead of 1 July 2021, being the date when all entities will be expected to be compliant with the Protection of Personal information Act, 2013 ("POPIA").

More specifically, on 5 January 2021, the Council of the European Union (EU) published a new draft ePrivacy Regulation[1] ("draft Regulation") which proposes a number of noteworthy changes to the existing EU legislative infrastructure insofar as the protection of personal data in electronic communications is concerned. For the purposes of this article, our focus will be on internet cookies and the effects which this draft Regulation may have once finalised.

Internet cookies are widely prevalent, but many internet users are unaware of their presence. However, if you've ever used a virtual shopping cart to make a purchase from your favourite online store, you have undoubtedly encountered internet cookies. While cookies are frequently used for harmless website functionality, they are also used for more controversial activities such as tracking user activities.

But let's just be reminded which internet cookies we are discussing. A HTTP cookie (or cookie for short) is essentially a tiny amount of data or small text file that is automatically collected and stored on a website user's computer by the web browser he/she is using whilst browsing a website.[2] Cookies are the lifeblood of website navigation. They serve an essential function by allowing websites to identify users, remember certain information about them, and overall facilitate a far more user-friendly experience which would otherwise be lacking but for the data collected in the form of a cookie. For instance, when you shop online and add a particular an item to your online shopping cart, a cookie would help the website remember what items you had in your shopping cart, thereby preventing the cart from resetting to empty every time you were to click on a new product or be directed to a new link on the website. Without this, online shopping would prove a difficult and rather frustrating exercise. In essence then, cookies serve a vital purpose.[3] Cookies which serve such a purpose are often referred to as functional or performance cookies.

However, cookies are also used as a part of many large browser tracking schemes which create extremely detailed user profiles. Many websites use third-party ad networks – networks which span multiple sites. This allows central data aggregators to track user activity across many different domains. Cookies are not specifically used to handle this tracking, but they do play a central role in enabling the tracking of a user.

Some people consider this constant activity tracking to be a form of privacy invasion. Other people do not mind it at all.

From a data protection perspective, however, the privacy concerns associated with cookies collecting users' information without the users even being aware of it, do bring to the fore privacy concerns and have in fact led to regulatory intervention, at least in the EU. Broadly speaking, cookies are dealt with in similar fashion across legal jurisdictions in the sense that a user's consent is required prior to collecting the data (or being served cookies). Therefore, private and public entities are required to notify web users that the website serves cookies and also provide written statements as to what it intends to do with the type of data or information collected. Importantly, however, the exact type of consent required for the purposes of cookies, and exactly how that consent is obtained, tends to differ from jurisdiction to jurisdiction. For instance, the European Union's ("EU") approach to consent currently differs slightly to the SA approach. In the EU, the requirements for consent which are currently in force as per article 4(11) of the General Data Protection Regulation[4] ("GDPR") are that consent must be freely given, specific, informed, unambiguous, given by statement or an affirmative act, as well as signify agreement to the processing of personal information.

In contrast, the SA definition of consent according to section 1 of POPIA is that consent is any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

However, in contrast to the GDPR, and as it currently stands, POPIA does not actually require the consent to be unambiguous nor to be done by an affirmative act.

Insofar as consent to cookies is concerned, the current position for purposes of the GDPR is that companies must obtain "specific, revocable, and informed consent from end users, unless the cookies are strictly necessary for the website".[5] This applies irrespective of whether the information collected contains personal data.[6] Therefore, for natural persons as well as legal persons conducting business or activities in Europe, and more generally legal persons across the globe, consent is primarily obtained through cookie banners asking users to consent to cookies each time they visit a new website.

The draft Regulation follows the in-depth study conducted in Ireland by the Irish Data Protection Commission ("**DPC**"), which study was published on 6 April 2020.[7] In its report, the DPC made various findings, including: the finding that implied consent was the predominant basis upon which websites obtained consent for cookies; the finding that cookies were often misclassified as being necessary; the finding that various websites had pre-checked consent boxes; the finding that consent was often required in a 'take-it-or-leave-it' manner in the sense that users had no choice but to accept the cookies. As a result, the DPC implemented new rules in the form of a guidance note, which rules include that:

- Cookie notices or banners must be more specific as to what purpose the user's information will be used for;
- Users must be able to accept or reject the cookie policy in similar fashion (i.e. equal prominence must be given to both options);
- Check boxes must not be pre-checked;
- Users must be able to change their cookie preferences; and
- Clear and comprehensive information concerning the use of cookies must be given to the user[8]

The DPC report clearly states that obtaining consent to cookies by way of a pre-checked box (or an opt-out approach) is not legally valid in terms of EU ePrivacy law. In the matter of *Planet49***[9]**, the European Court of Justice found that consent requires active rather than passive conduct on the part of the user in order to be considered legally valid and to achieve the purpose of the cookie banner. For the most part though, it is clear that a clear appreciation or understanding of what exactly consent means is the driving factor behind policy change, at least insofar as cookies are concerned. Therefore, it is clear that anticipating changes to the legal landscape in relation to cookie policies requires one to appreciate the meaning of consent.

Noteworthy also is that the draft Regulation puts forward a more uniformed, simplified process in respect of consenting to data collection by way of cookies. In contrast to the contemporary position, the draft Regulation seeks to streamline the existing framework by permitting website users to give consent by way of their browser settings. In this regard, the draft states "an end-user can give consent to the use of certain types of cookies by whitelisting one or several providers for their specified purposes".[10] In doing so, users would be alleviating the need to consent to cookie banners on a whitelisted website when visiting that website, making the process of collecting data more user friendly. Users would presumably also be able to revoke their consent by amending their browser settings. In addition, the draft Regulation encourages software providers to include settings in their software "which allows end-users, in a user friendly and transparent manner, to manage consent to the storage and access to stored data."[11]

From a South African perspective; going forward, POPIA will require websites to be clear as to what personal information they collect and for what purpose, how such personal information will be used, and how a data subject can request for the personal information to be deleted or for no further personal information to be collected.

The natural place to communicate this is in a privacy policy or Terms of Service document. This ought to be – at a minimum – linked to the consent dialogue text.

Websites should reflect their actual use of cookies and it might look something like this:

This site uses cookies to help us understand user behaviour. This means that we put a small piece of text (the "cookie") in storage on your web browser. This cookie lets us know that all the different things you do on our site. We do not collect your personal information. The only information we have about your identity is the information you explicitly provide to us through submission forms on our website. We do not sell any personal information to any third parties. We do analyse user behaviour in order to better serve you and other visitors. Tracking your activity through our site (what you click on, how long you stay) helps us make better decisions about content and design.

[1] ePrivacy regulation (Council doc. 5642/21).

[2] National Compliance Regulatory Authority of South Africa ("NCRASA"), South African Website Cookie Policy, available at https://ncrasa.co.za/cookie-notice/.

[3] Irish Data Protection Commission Guidance Note: Cookies and other tracking technologies dated April 2020.

[4] General Data Protection regulation 2016/679.

[5] Morgan Lewis & Bockius LLP, "*Pending EU e-Privacy Regulation Could Bring Major Changes to Metadata Processing, Cookie Consents*" dated 11 February 2021 available at: https://www.lexology.com/library/detail.aspx?g=917faf3e-3ca9-48f7-a43f-b63528cf0e40.

[6] CaseC-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801.

[7] Irish Data Protection Commission Guidance Note op cit note 3.

[8] Hunton Andrews Kurth, "*Irish DPC Publishes New Cookie Guidance*" dated 8 April 2020 available at https://www.huntonprivacyblog.com/2020/04/08/irish-dpc-publishes-new-cookie-guidance/.

[9] CaseC-673/17, *Planet49*, 1 October 2019, ECLI:EU:C:2019:801.

[10] Regulation (20a)

[11] Ibid.

Ahmore Burger-Smidt

Head of Regulatory

View Profile