Freshfields Bruckhaus Deringer

The European 'Cookie Monster' – Digital services and cookies under scrutiny

Michael Schwaab, Christoph Werkmeister
Co-authors: Satya Staes Polet,
+3 more...

August 12, 2022

Co-authors

European lawmakers and data protection authorities have been very active recently regarding the lawful use of cookies and other digital services. Whilst new laws and guidelines are helpful, complaints by data subjects and non-profit organisations have given cause to some interesting decisions so far.

In particular, the European Center for Digital Rights (NOYB), co-founded by Austrian privacy activist Max Schrems, issued over 500 complaints in 2021, and already another 270 complaints in 2022 to companies, concerning the alleged use of deceptive cookie banners and the use of US-based service providers for their websites. Following these complaints, some companies adapted their settings, whilst most companies did not change their cookie banners. Hence, NOYB has lodged 226 complaints with 18 authorities against these allegedly non-compliant companies. It is also rumoured that NOYB even developed a software solution to screen websites for the (un)lawful use of cookie banners.

As further decisions of authorities are inevitable, we recap the guidelines and decisions already issued to offer some idea of what to expect.

Stricter guidelines increase pressure for compliant implementation

Directive 2009 / 136 / EC (Directive on Privacy an Electronic Communications also known as the ePrivacy Directive) was intended to fully harmonise the requirements

of processing of personal data and the protection of privacy in the electronic communications sector.

The ePrivacy Directive was transposed into national law by means of various implementation laws, most recently in Germany within the framework of the Telecommunications and Telemedia Data Protection Act (Telekommunikation-Telemedien-Datenschutz-Gesetz or TTDSG), which came into force on 1 December 2021.

Germany was one of the last EU countries to implement the requirements of the ePrivacy Directive (see our blog post on the TTDSG). Rumours about this regime being replaced by an ePrivacy Regulation circulated again last April after a tweet from the Parliament's Rapporteur, Birgit Sippel. However, taking into account a potential two-year transitional period, we do not expect any ePrivacy Regulation coming into force before 2025.

Considering that the ePrivacy Directive was in force almost a decade before the General Data Protection Regulation (GDPR), there have been few guidelines and little enforcement of cookie use. However, European and national data protection authorities are now issuing guidelines and are ready to enforce. Most recently, German data protection authorities issued guidelines on the TTDSG such as the Data Protection Conference (DSK) and the Bavarian Data Protection Commissioner (BayLfD) which, among other things, address three key aspects:

- **High granularity of processing purposes**. Cookie use generally requires the prior consent of the user, unless legal exemptions apply, whereby blanket consent, for example for 'advertising purposes', is generally not sufficient.
- **No nudging**. The user must not be subliminally induced to consent to cookie use and this must not be easier than refusing it.
- **Information obligations**. The information obligations pursuant to Articles 13 and 14 of the GDPR shall apply accordingly for the use of cookies. In particular, the user must be informed about who is accessing his device, in what form and for what purpose, what the functional duration of the cookies is and whether third parties can gain access to them.

In addition, some countries have issued cookie guidelines, which can be found under the following links:

- Austria (available in German)
- Belgium (available in French and Dutch)
- Denmark (available in Danish)
- Finland (available in Finnish)
- France guidelines, recommendations and Q&A (available in French)
- Ireland (available in English)
- Italy (available in Italian and English)
- Netherlands (available in Dutch)
- Spain (available in Spanish)
- United Kingdom (available in English)

Increased regulatory scrutiny

Whilst enforcement from European authorities has increased significantly, France's Commission Nationale de l'Informatique et des Libertés (CNIL) has made some noteworthy recent decisions, including a three-digit million euro fine against a big tech corporation. In this fine the CNIL criticised refusal mechanisms for cookie use and required that refusal options must provide a similar degree of simplicity as the options for providing consent. DPAs such as the CNIL argue that refusal mechanisms must not be designed as a user 'consent out of convenience', which would be distorting and interfering with the user's freedom of choice (see in this context our recent blog post on the EDPB's publication on 'dark patterns').

The CNIL also emphasised the importance of creating a simple alternative to consent. This must be easy to understand and not require the user to concentrate on or even interpret it. In this matter, the CNIL published on 28 July 2022 that it accepted a refusal button entitled 'Only allow essential cookies' above the acceptance button entitled 'Allow essential and optional cookies'.

In addition to the CNIL, other data protection authorities in Belgium, Spain (as evidenced by the very high number of decisions since 2019), and the US are also known for being extremely tough on perceived 'cookie-violations' (you can find a more detailed analysis on data privacy fines in our Global data risk study).

Mitigating enforcement risk

Due to the stricter guidelines of European authorities and the increasing enforcement, corporations should be analysing their cookie use policy to mitigate

enforcement risk. Especially the CNIL decisions described above clarify the recommendation that the BayLfD also explicitly expressed in its statement:

All websites should be checked for correct cookie use and, if necessary, adapted accordingly. All responsible companies must be aware of the many different requirements and closely monitor developments. It is no longer advisable to refer to a 'market standard' if it deviates from the official recommendations because of the risk that existing data processing – especially Google Analytics – becomes illegal overnight.