

Client Alert: Cookie Enforcement on the Rise & Mass NOYB Complaints

Date : June 1, 2021

Introduction

Yesterday's announcement from Max Schrems' pressure group NOYB has put the spotlight back on cookies enforcement across Europe. It comes at a time when many more DPAs are concentrating on cookies enforcement with fines on the rise. In the NOYB action alone more than 10,000 complaints to DPAs are threatened.

There are some abbreviations and privacy terms in this note which are explained at www.bit.ly/gdprwords

What is this all about?

Cookies are regulated in the EU not only by GDPR but also by the so-called Cookies Directive (properly called Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector). Since the Cookies Directive requires each member state to introduce its own law, each country's implementation of the Cookies Directive varies. Post-Brexit, UK law still includes GDPR (see <http://bit.ly/brexitdp>) and the UK's implementation of the Cookie Directive known as PECR (full name The Privacy and Electronic Communications (EC Directive) Regulations 2003).

Recently we have reviewed a large number of websites for cookies compliance. From our experience, most organisations have now procured software to enable them to comply with cookies law, but it often is not configured correctly. Common errors which we have seen include:

1. Not giving sufficient prominence to a reject all button.
2. Not being transparent about the cookies on a website. For example, we have frequently seen cookies relating to security applications missed off. This is likely to be particularly problematical given recent developments including the Portuguese DPA's enforcement action over the use of Cloudflare (see <https://bit.ly/schremsport>).
3. Not having an adequate cookies policy and/or privacy policy. In some cases we have seen cookies banners with links to these policies which do not work.
4. Underestimating the number of cookies involved – for example in one case, the marketing department disclosed around 20 cookies where the true number was more than 200. Sometimes this lack of clarity can be because a vendor uses more than one cookie. Even something as simple as having location maps on your website or links to videos can lead to a fairly large number of cookies.
5. Having unjustifiably long retention periods for cookies. For example how can a 999 year term for a cookie be justified?

Enforcement Action

We have seen a real rise in enforcement activity from DPAs across Europe.

The highest fines have been in France with fines of €100m for Google, €35m for Amazon and €2.25m for Carrefour. The current status of the Google and Amazon enforcement actions seems unclear however after a recent CNIL announcement. We've written about the French enforcement action here <https://bit.ly/32YICDM>. There are some previous French cases here <https://www.corderycompliance.com/cnil-cookies-investigation/> and here <https://www.corderycompliance.com/french-dpr-fine-for-dtt-non-compliance/>.

Last week CNIL announced further enforcement action against around 20 organisations who it said are "mainly important companies in the digital economy". They have until 18 June 2021 to comply with CNIL's requests after which CNIL says it will take enforcement action.

France is not the only DPA to get involved however. We have seen fines in Belgium, Czech Republic, Norway and

Spain. We have also seen official reprimands in Denmark and Finland and sweep activity in The Netherlands and France. The UK has had a long-running investigation into Adtech which stalled during the pandemic but has been up and running again since January.

Today German regulators also announced a data protection sweep exercise which will also include questions on cookie compliance as well as wide-ranging questions on related topics such as data transfer. 5 common questionnaires have been agreed by German DPAs although enforcement will still be down to each individual DPA within Germany. You can find out more about this exercise in our note here <https://bit.ly/gerenforce>.

At the EU level the EDPS has also been active finding that the ECJ's own website was non-compliant.

What are the NOYB complaints about?

NOYB feels that the majority of the websites which are popular in the EU simply don't meet current legal requirements.

NOYB seems to have built a tool to investigate cookie compliance. It said that of the 560 websites in 33 different countries it looked at in its first batch of complaints, 81% had no "reject all" option on the first page. It said that 90% provided no easy way to withdraw consent. NOYB is using its tool to issue draft complaints to 10,000 of the most visited websites across Europe. It says that if the recipients do not comply with cookies law within a month it will file a formal complaint with the relevant DPA or DPAs.

NOYB also seem to be concerned about some vendors of cookie management tools – a video on their website is said to feature an internal video from one vendor about the sales tactics they use. Whilst some data from the video has been redacted, it seems possible to identify who the vendor is.

What about civil action?

We have also handled some threatened litigation recently. This seems to be an area where there are some "get rich quick" litigants around who are asking for a payment to avoid litigation. The claims that we have seen have looked good on paper but the claimants seem unwilling from our experience to put in the effort needed to substantiate their claim. It is important to act promptly if you are threatened with litigation and to take proper advice on your immediate response.

Most of the litigation which we have seen follows on from an ECJ case in 2019, Planet49, which we wrote about here <https://www.corderycompliance.com/ecj-cookies-consent-ruling/>. It is relevant to note that this case was brought by another active consumer group, the Verbraucherzentrale Bundesverband (also known as the vzbv or in English the(Federation of German Consumer Organizations)).

There are some larger, well-resourced claims involving cookies and other technologies going through the courts, and it seems that this litigation is attractive to litigation funders currently. We have written previously about the Safari Work Around case where a decision is currently awaited from the UK Supreme Court (see the background here

[h
tps://www.corderycompliance.com/doors-open-for-class-action-appeal-as-court-allows-google-claim-to-proceed/](https://www.corderycompliance.com/doors-open-for-class-action-appeal-as-court-allows-google-claim-to-proceed/)).

We are also following an action against TikTok brought in part by the former Children's Commissioner for England and Wales. There's also a long-running civil action brought by Mr Schrems against Facebook (see here for background <https://www.corderycompliance.com/schrems-class-action-to-continue/>).

The rise in cookie litigation is one of the trends we spoke about in our recent film looking at five trends from the first 3 years of GDPR here <https://bit.ly/GDPR5film>.

Other Pressure Group Activity

NOYB is not the only pressure group involved – for example in addition to vzbv a Spanish pressure group is

focussed on the “*refuse all cookies*” requirement and is pressing the Spanish DPA to investigate all complaints. In 2018 Privacy International also started a campaign against cookie banners and so-called nudging (using strategies to steer a user to consent). Privacy International has made complaints to DPAs in France, Ireland and the UK against 7 different companies.

What about the future?

It is important to remember that the Cookies Directive is in the process of being updated. That has been a somewhat long and tortuous process at an EU level and has undergone many proposed attempted changes. We've written on the original proposed changes here <https://www.corderycompliance.com/proposed-eu-e-privacy-regulation/> and more recently here <https://www.corderycompliance.com/client-alert-eu-privacy-reg-proposed-amends-metadata-cookies-legitimate-interests-consent/>. The proposal is to replace the Directive with a new Regulation which should mean that the legal position is more consistent across the EU, although enforcement will still be up to each EU Member State. There had been some positive announcements earlier in the year on progress on updating the EU cookies rules but there still seems to be much divergence on the way forward, including in particular about users' consent for tracking cookies and other non-cookies issues such as companies' use of metadata and data retention.

Today a group of 32 human and digital rights organisations also wrote to EU institutions asking them to look at cookie banners. They said “*consent is being exploited, and deceptive interfaces nudge users to accept and surrender their privacy.*” They would like the ePrivacy Regulation “*to create legally binding privacy controls that would allow users to communicate their preferences automatically and repeatedly to the sites they visit through their browsers. The European Data Protection Board should be given the task of defining the requirements and technical specifications for signals to communicate and withdraw consent, and to object to processing based on legitimate interest.*” The campaign also asks MEPs to ‘ban cookie walls’. Whether or not this campaign succeeds it is also likely to add to the pressure on DPAs to enforce the current rules.

What should I do?

Cookie compliance should be high on the list of any business – these concerns are not just limited to ‘big tech’ or those selling online. Amongst the steps you will want to consider are:

1. A thorough review of your website to make sure that your site complies.
2. Looking critically at the cookies which are used on your website. Are they all needed? Can alternative technology do the same job? Have you agreed to all of the third party cookies which are there? Reducing the number of cookies displayed on the site will make your transparency obligations easier too. It may also make your website more secure.
3. Checking your existing cookies policy, especially from the perspective of transparency (types of cookies, cookie duration and third party cookie access, amongst other issues), and amend it as appropriate.
4. Address retention specifically. As we have said long retention periods will be very hard to justify and this was a key feature in Carrefour's fine.
5. Check your consent mechanisms (including the technology used) and revise them as necessary. Buying software won't be enough – it will need to be properly configured and sufficiently prominent. Timing is important too.
6. Put in place a mechanism to record any consent given. The burden of proving consent is likely to be on your in any investigation or litigation.
7. Have a plan in place to deal with any threatened litigation.
8. If your vendor is based outside the EEA/UK you'll need to look at data transfer too. This was a feature in the recent Portuguese case which we've mentioned above as the Portuguese DPA said that the required data transfer mechanisms were not in place. Data transfer was also a feature in the Carrefour case too.
9. Make sure that any cookies processing is included in subject access request responses. Some litigants are making SARs to find out what you're doing with cookies and you'll need to make sure that you look in the right places and that your response is consistent with the disclosures you make.
10. Look at any official social media channels too. A case in 2018 (see <https://www.corderycompliance.com/client-alert-european-court-facebook-fan-page-ruling/>) suggests you're

also likely to be responsible for the way in which the social media site processes data too.

For more information

There is more information about this and other data protection topics in Cordery's GDPR Navigator subscription service. GDPR Navigator includes short films, straightforward guidance, checklists and regular conference calls to help you comply. More details are at www.bit.ly/gdprnav.

You can find more details of the NOYB campaign at www.bit.ly/noybcook

The text of PECR is here <https://www.legislation.gov.uk/ukxi/2003/2426/contents/made>.

Details of the new German DPA activity is here <https://datenschutz-hamburg.de/assets/pdf/2021-06-01-press-release-questionnaires.pdf>.

For more information please contact Jonathan Armstrong or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.

[Jonathan Armstrong](#), Cordery, Lexis House, 30
Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com



[André Bywater](#), Cordery, Lexis House, 30
Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com



Farringd