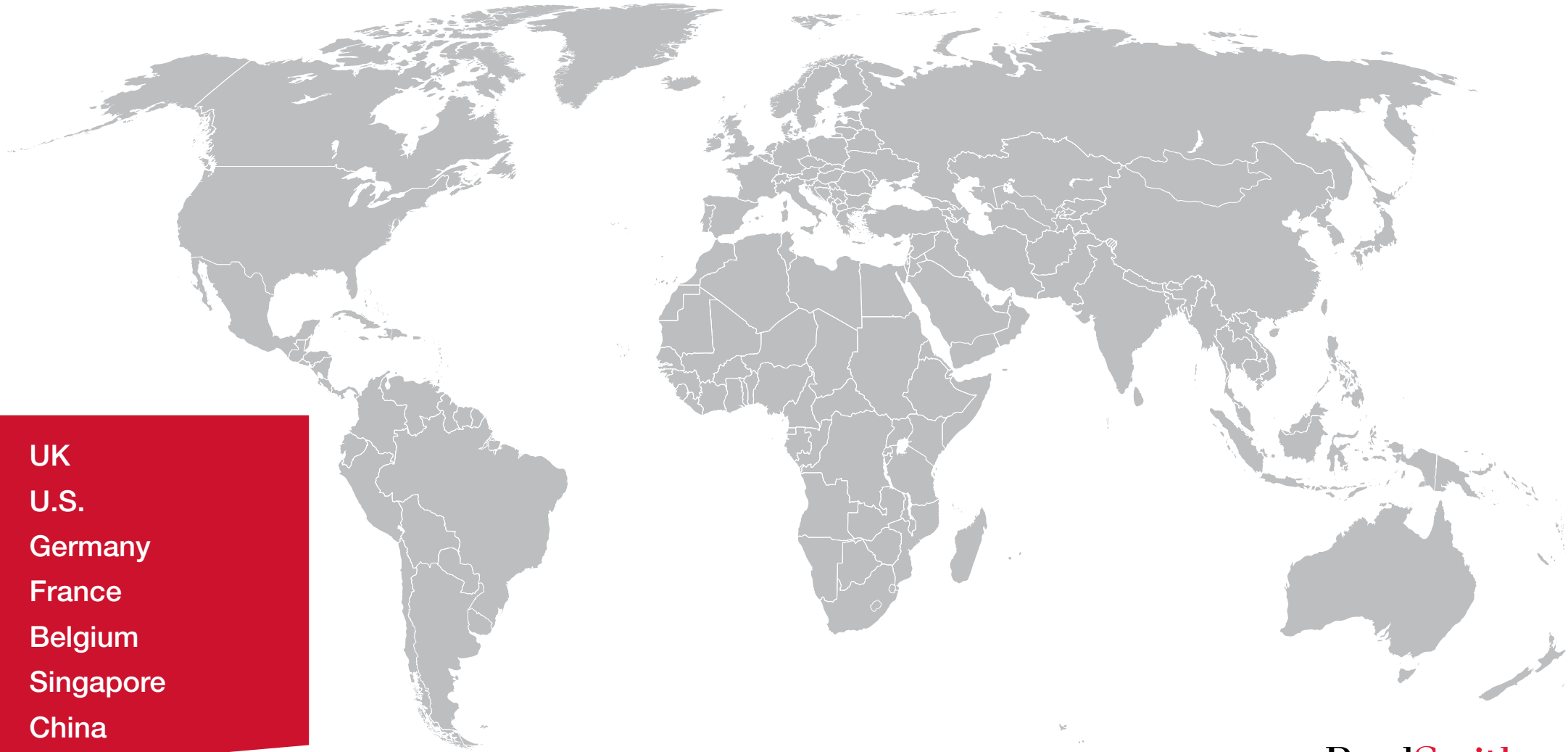
Adtech regulatory round-up December 2021

In this third international adtech round-up of the year, it is very clear that the number of stories we need to cover in our updates is increasing as the pace of regulation and industry initiatives accelerates. In this update, those following such developments will also note the need to look across multiple different legal disciplines to get a firm picture of what is happening. Whilst privacy and competition laws and regulators have been obvious areas of focus to date, as we move into 2022, the inclusion of adtech in the UK's Online Safety Bill recommendations and EU's digital safety proposals show a move into wider content and platform regulatory domains. Unsurprisingly, we also see discussions in respect of the so-called "cookie-less" future begin to take better shape with regulators finally beginning to make their concerns known even if we are yet to see any final decisions or enforcement action. This, combined with the awaited response of EU data protection authorities to the Belgian preliminary report on the Interactive Advertising Bureau's Transparency and Consent Framework (IAB TCF) in January, shows that another busy, yet uncertain, year is ahead of us.



UK
U.S.
Germany
France
Belgium
Singapore
China

reedsmith.com

ReedSmith
Driving progress
through partnership

United Kingdom

Back to map

Online Safety Bill

The Government's ambition to make the UK the safest place in the world online has most recently taken the form of the draft Online Safety Bill, which was published in May 2021. The draft Bill, which follows the publication of the Online Harms White Paper in 2019, aims to establish a new regulatory regime to address illegal and harmful content online, with new requirements for user-to-user and search services. A Joint Parliamentary Committee Report, published on 14 December 2021, contains various recommendations for changes, and the UK government must now respond within two months with a view to final legislation being prepared in the spring of 2022. Advertising and related technologies feature heavily in the Report's recommendations. In particular, the Report recommends that: (i) service providers should be accountable for paid advertising carried on their services and, therefore, the exemption in the draft Bill for paid advertising should be removed; (ii) the risks of micro-targeting of adverts based on data collection should be a specific foreseeable risk of harm that service providers should be required to consider and; mitigate against, including in respect of algorithms used for this purpose; and (iii) Ofcom should draw up risk profiles that should include the "risks caused by surveillance advertising."

Cookie-less but not less privacy: ICO issues new Opinion on adtech

In a new 48-page Opinion issued on 25 November 2021, the UK Information Commissioner set out its expectations (and a warning) around privacy standards for new advertising technologies. Although the Opinion is not binding, it still helpfully covers a lot of ground, including the evolution of cookie browser mobile software technology, standards body initiatives, the IAB's TCF, and other specifications such as Global Privacy Control and Advanced Data Protection Control. Please see our full article on the ICO's new adtech Opinion.

The Children's Code is finally here

The ICO's Age Appropriate Design Code (AADC), along with its 15 standards for the design of online services processing children's personal data, finally came into force on 2 September 2021. Personalisation of online advertising is covered by the scope of the Code, which prohibits profiling by default, and requires that only the minimum amount of a child's personal data should be processed in order to provide them with an online service. In short, this means that ads that are personalised based on profiling or some other data processing should be switched off by default for children. In practice, many services using cookies for such purposes already operate a consent model, so the impact largely forms on other non-cookie-based data usage for targeted advertising and ensuring that privacy settings and information are suitable for children.

Since the Code came into force, the ICO has released an Opinion on age assurance that explains how the regulator expects those who fall within the scope of the AADC to comply with its standard age-appropriate application.

Further proposed reforms: Digital markets, regulation, and strategy

As expected, there have been a huge number of developments to tackle the unique challenges of globally fast-moving digital markets in 2021.

Sitting alongside the Digital Regulation Cooperation Forum (DRCF) Work Plan for 2021 to 2022 (mentioned in our previous round-up), the DRCF has since submitted its response to the Department of Digital, Culture, Media, and Sport (DCMS) on the future of the digital regulatory landscape and how to achieve coherence in regulatory approaches across digital services. Whilst the response suggests that the DRCF views regulatory cooperation as essential, it also acknowledges that there are barriers to joint working that need to be addressed, which may even mean there is a need to develop a further legislative framework to support cooperation.

The Communications and Digital Select Committee also launched a new inquiry into the work of digital regulators in the UK. The inquiry follows the Committee's Report from March 2019 that found regulators "had failed to keep pace with advances in digital technologies," the publication of the draft Online Safety Bill, and the launch of the new Digital Markets Unit. With the deadline for responses having passed on 22 October 2021, we will have to wait to see how effective digital regulation really is and what steps (if any) will be taken to reduce the gaps and overlaps in the current regulation.

Earlier this year, the government consulted on a new pro-competition regime for digital markets, which essentially plans to give powers to the Digital Markets Unit (DMU), including creating enforceable codes of conduct for the biggest tech firms that could result in major fines if broken. The proposals would also give the DMU powers to intervene to boost market competition, as well as powers to scrutinise and potentially block mergers involving the most powerful digital firms. The Competition Markets Authority (CMA) has just issued its response, which positively welcomes the proposals.

It doesn't stop there – in terms of next steps and proposed digital regulation, later this year the UK government plans to publish its Digital Strategy and National Cyber Strategy, and to consult on its Online Advertising Programme.

ICO publishes guidance on the use of live facial recognition technology

In June 2021, the ICO published an Opinion on live facial recognition (LFR) technology. The Opinion addresses the processing of personal data, biometric data, and special category data when using LFR and touches on the use of LFR for the purposes of identification and categorisation when marketing and advertising.

The key requirement here is that, since the personal data may be particularly sensitive and some processing is automatic, there must be stronger protections in place and there is a higher bar for its processing to be considered lawful. The ICO expects to see high standards of governance, including clearly defined procedures and review processes.

Adtech investigations and enforcement

In July 2021, the ICO released its annual report for 2020/21, which provided an update on its ongoing investigation into real-time bidding in the adtech industry. The Report states that the ICO issued the first of a series of assessment notices to those it considered were not complying with their legal obligations, with the remaining audits and corresponding notices being conducted and issued in the months following the publication of the Report.

United States

Back to map

CPRA opt-in/opt-out

California's newest data privacy law, the replacement for the CCPA, is the California Consumer Privacy Rights Act of 2020, California Assembly Bill No. 1490 (2021-22) (CPRA). The CPRA requires that consumers have the ability to opt-out of sharing when a company shares personal information with a third party for cross-context behavioral advertising. This requirement takes the form of a "Do Not Sell or Share My Personal Information" link on the homepage, or ensuring the option exists for companies to recognize opt-out signals. The technical specifications for these op-out signals are still to be set by the recently established California Privacy Protection Agency.

However, there is an exception to this requirement. If the consumer has given opt-in consent in the first instance, subsequent disclosures do not constitute "sharing." The CPRA states that if a consumer "uses or directs" a business to "intentionally disclose personal information or intentionally interact with one or more third parties" then such disclosures do not constitute "sharing" for the purposes of the CPRA [CPRA section 14(ah)(3)(A)]. One possible outcome of this exception is that obtaining opt-in consent in the first instance alleviates the need to post a Do Not Sell or Share button or comply with opt-out.

Data minimization

The adtech community and brands should be aware that the new state laws have provisions that contain requirements similar to the "data minimization" concept first introduced in Europe under the GDPR.

In California, the CPRA provides that personal information should be collected "only to the extent that it is relevant and limited to what is necessary in relation to the purposes for which it is being collected, used and shared." [CPRA section 3B(3)] Further, the collection, use, and sharing of personal information must be "reasonably necessary and proportionate" for a company to achieve the business purpose for which it was collected. Such data may only be retained for as long as it is necessary to achieve that purpose. Finally, the CPRA provides that personal information must not be processed in a manner that is "incompatible" with the original purpose. Similar to the CPRA, Virginia's Consumer Data Protection Act (CDPA) contains requirements in respect of data minimization. Virginia appears to be taking data minimization seriously. The very first line of the law's text under "Data Controller Responsibilities" reads, "A controller shall: Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer."

These data minimization requirements will directly impact advertisers that may, for example, collect information to sell a pair of shoes, but later use it to advertise another service. This places a huge emphasis on the disclosed purposes for collection, as improper disclosure can effectively limit both the collection and subsequent use of consumer data, as well as potentially necessitating secondary disclosures and recollection of that data. Proper disclosure should also be accompanied by data classification, data mapping, and a thorough understanding of what is collected and how it is used. This will help ensure data is collected appropriately and used in an adequate, relevant, and reasonably necessary way.

Virginia and Colorado DPA requirement

Virginia's CDPA requires controllers to conduct Data Protection Assessments (DPAs). According to the CDPA "a controller shall conduct and document a data protection assessment" in each of the following situations: Processing for targeted advertising; Sale; Processing for profiling, if profiling presents a risk of unfair/deceptive, financial, physical, or reputational injury, intrusion, or other substantial injury; Processing of sensitive data; and Processing that presents a heightened risk of harm."

These DPAs are also required to identify and weigh the benefits of processing. The benefits shall be identified and weighed for the following parties: controller, consumer, other stakeholders, and the public. Additionally, the Virginia Attorney General may request DPAs relevant to an investigation be produced.

There are a few ways that DPAs can be leveraged for multiple purposes. For example, one DPA may address similar processing activities, and DPAs conducted for other compliance or regulatory purposes may satisfy the requirement if they have a "reasonably comparable scope and effect." Finally, the DPA requirements set forth in Virginia's CDPA are not retroactive and only apply beginning on 1 January 2023.

Colorado has become the latest state to pass a comprehensive data protection law, the Colorado Privacy Act (CPA). The CPA has many similarities to the Virginia CDPA, including data minimization, secondary purpose, and the requirement to conduct DPAs.

Platform targeted advertising changes

Platforms continue to undergo a fundamental shift away from third-party cookies and tracking in light of regulatory developments. Certain browsers have changed default settings while mobile platforms have implemented opt-in consent to device tracking, forcing advertisers and publishers to look at alternative advertising methods to reach consumers.

Advertisers are moving to explore alternatives to third-party cookies, including the development of more robust first-party data, email-based universal identifiers such as UID 2.0 (linked from users' logged-in states on publishers' properties), and a move back to contextual marketing.

Meta recently announced that it will no longer let advertisers buy targeted ads for users on its major platforms (Facebook, Instagram, and WhatsApp) or across its network of sites based on sensitive information such as race, political affiliation, sexual orientation, religion, or health. For example, advertisers will no longer have options to target ads around categories such as "Lung Cancer Awareness Day," religious holidays, or certain political causes or organizations.

Section 230 of the Communications Decency Act

Section 230 of the Communications Decency Act (CDA) continues to be under fire and the focus of legislative activity, with many of the concerns focused on the amount of power given to platforms under the CDA to decide what content and information we see. At its heart, section 230 protects Internet service providers from liability for content provided by third parties. Thus, platforms aren't held liable for harmful content a user posts on their platform. Section 230 also allows platforms to remove without liability any posted content they deem objectionable, provided they acted in good faith. There are a host of legislative proposals (at least 17 in 2021) that vary from the complete repeal of section 230 to significant amendments that would eliminate protections for certain types of actions. This will continue to be an area of great debate and legislative activity in 2022.

Association of National Advertisers' Programmatic RFP

The Association of National Advertisers (ANA) issued a Programmatic RFP in May to conduct a comprehensive study of the programmatic media buying ecosystem. The aims were to help demystify the programmatic media buying ecosystem and the associated monetary waste and to develop solutions and tools for the industry to better protect the billions of dollars spent by advertisers each year in programmatic media. The outcome of this study is important because the industry is at a critical inflection point to rectify the issues of fraud and advertising dollar waste uncovered in previous studies by the ANA and other industry trade associations.

Germany

Back to map

AC Wiesbaden injunction on cookie consents and international transfers

On 1 December 2021, in a much-noted decision, the Administrative Court of Wiesbaden (AC Wiesbaden) handed down a preliminary injunction dealing with international data transfers (case 6 L 738/21.WI, available in German here). The court ruled there was no data transfer mechanism in place (specifically there were no standard contractual clauses) and thus the defendant was ordered to stop using a cookie consent management platform. Contrary to some reports, the court did not rule that U.S.-based consent management solutions or cookies cannot be used anymore. The injunction can still be appealed and could also be lifted in the main proceedings. Please see our full article for details of what the court did and did not rule on and what this means in practice for companies.

New German cookie law

On 1 December 2021, the Telecommunication Telemedia Data Protection Act (the so-called TTDSG) entered into force. The TTDSG includes new regulations on the use of technologies that store information in the end user's terminal equipment and on access to information already stored in the terminal equipment, such as cookies, pixels, beacons, fingerprinting, and similar technologies (cookies) for companies operating in the German market.

The TTDSG must be considered in addition to the GDPR when using cookies:

- The TTDSG applies to the setting and reading of information in cookies. The TTDSG only provides for two categories of cookies: (i) cookies that require consent, and (ii) cookies that are strictly necessary for the provision of the telemedia service requested by the user. The TTDSG does not establish the legal basis of legitimate interests (as was previously the case, for example, for "light" reach measurement).
- The GDPR applies to the further processing of personal data obtained by the cookies.

There is already a lot of discussion on the TTDSG, in particular, on the scope of strictly necessary cookies. For example, the German supervisory authorities (German DPAs) stated in numerous webinars that they are currently discussing whether and in which cases reach measurement cookies can be considered as "strictly necessary cookies," taking into consideration that the CNIL has published guidance earlier this year stating that certain reach measurement cookies can be classified as absolutely necessary (read more on our blog). The German DPAs announced that they intend to publish TTDSG guidelines in early 2022.

Companies that fall within the scope of the TTDSG must review their entire cookie setup (in particular, legal bases and cookie banner and cookie descriptions). We have also seen that companies are starting to look for cookie-less technologies as alternatives. The TTDSG will not apply to such cookie-less technologies if no information is stored in or accessed in the terminal equipment of the end user, and in such case, only the legal basis of the GDPR (including legitimate interests) will apply.

German DPAs audited the use of cookies by media companies

German DPAs have audited the websites of 49 organizations in 11 states regarding the use of cookies – in particular, regarding the use of tracking cookies for ad purposes – since mid-2020. The German DPAs have now released the findings of their audits. They found that most media companies' use of cookies is not compliant with the legal requirements. The main violations included:

- Obtaining consent for the use of cookies that require such consent, but doing so rather directly when the user visits the website.
- Provision of insufficient or false information in the first layer of the cookie consent solution.
- Use of cookies that require consent even after the user has declined the use of cookies.
- Missing options to decline cookies in the first layer of the cookie consent solution.
- Use of unlawful nudging techniques.

The EDPB launches a cookie banner task force

The European Data Protection Board (EDPB) announced after its September 2021 plenary meeting that it has established a cookie banner taskforce to cooperate on complaints concerning cookie banners. The EDPB stated that the task force will, in particular, "exchange views on legal analysis and possible infringements, provide support to activities on the national level, [and] streamline communication." There have not yet been any publications on activities by the task force.

France

Back to map

CNIL's recommendations on the protection of minors online

On 9 June 2021, the CNIL published eight recommendations that provide practical guidance to enhance the protection of minors online and clarify the applicable legal framework. Similar to the UK's AADC (discussed above), the CNIL seeks to strike a balance between the need to protect children and the requirement to respect their desire for autonomy. The recommendations lay down the conditions under which children can consent to the processing of their data and exercise their own personal data rights, notably on social networks and gaming and video sharing platforms, without prejudice to the parents' rights. The CNIL recommends setting up stricter default privacy settings, deactivating by default any profiling systems for children (especially for the purposes of targeted advertising), and refraining from re-using or passing onto third parties the data of children for commercial or advertising purposes, unless companies can demonstrate that they are acting for overriding reasons in the best interests of the child. The CNIL has also worked on the design of new prototype interfaces that will be published on the CNIL's Data and Design platform.

Clarifications on third-party cookies and alternative technologies

The CNIL has recently confirmed that website publishers can be held liable for cookies placed by third parties on their websites. The CNIL stressed that the fact that cookies come from third parties does not absolve website publishers of liability. Website publishers must ensure that third parties obtain users' prior consent to place cookies on their devices, in cases where such consent is required, and that they respect the users' choices. The CNIL considers that, while this is an obligation of means, website publishers should implement sufficient measures to ensure compliance and to end potential infringements.

On 13 October 2021, the CNIL also published a fact sheet on technologies used as alternatives to third-party cookies. These include first-party cookies returning data via URL calls on the advertiser's domain, fingerprinting, single sign-on, unique identifiers, and cohort-based targeted advertising. The CNIL considers that such alternative technologies must comply with the rules laid down in the GDPR and the e-Privacy Directive, as implemented by the French Data Protection Act. In particular, the CNIL emphasized that the monitoring for advertising purposes, when based on information from the users' browsers or devices, is subject to the users' consent regardless of the type of technology used. Users must be able to consent to (or reject) monitoring that is not strictly necessary for the provision of the requested service.

Approved audience measurement solutions

Earlier this year, the CNIL launched an evaluation programme aimed at identifying audience measurement solutions that do not require consent. Companies offering audience measurement solutions for websites hosted in France or having users residing in France were invited to send their submissions. On 24 September 2021, the CNIL published a fact sheet containing an updated list of solutions meeting the conditions for consent exemption.

CNIL's enforcement actions

This year, the CNIL has again shown its willingness to use the full range of its enforcement powers to ensure compliance with the GDPR and the French Data Protection Act. Between May and July 2021, the CNIL sent formal notices to 60 companies and organisations, requiring them to amend their cookie consent solutions to ensure that users are able to reject cookies as easily as they can accept them. The amendment typically entails having both "accept" and "reject" buttons on the cookie banner or enabling users to reject cookies by closing the banner. The CNIL also issued injunctions and imposed financial sanctions, including daily fines, on companies that failed to obtain the users' consent before placing cookies. In exercising its enforcement powers, the CNIL considers that, regarding cookies, the GDPR's one-stop-shop mechanism does not apply and that the CNIL has jurisdiction over foreign companies to the extent that the companies are placing and reading cookies on terminals of users residing in France, in the context of activities carried out by an establishment in France. In its annual report published in May 2021, the CNIL noted that in 2020, it conducted almost 250 investigations and imposed 11 fines totaling more than €138 million.

Increased cooperation between EU data protection authorities

In its annual report, the CNIL emphasized the intensified cooperation between EU authorities, referring to more than a thousand European cooperation cases initiated as a result of complaints or investigations. In November 2021, the French, Lithuanian, and Polish authorities announced the launch of a working group to investigate practices implemented by a marketplace available to users in various EU countries. The data privacy and protection authorities of the G7 countries also organized their first roundtable meeting on 7 and 8 September 2021 to discuss emerging data protection challenges. Regarding cookies and online tracking, the authorities raised the issue of consent fatigue, noting that most users reflexively select "I agree" on cookie banners, as well as concerns regarding cookie walls and dark patterns. They stressed that further action was needed to ensure that web users can meaningfully control the processing of their personal data.

Continued scrutiny of adtech practices under competition law

European competition authorities have been increasingly active in the adtech sector. The French Competition Authority (FCA) recently issued its first decisions on practices relating to advertising technologies, and the European Commission opened a new antitrust probe into a global player providing online display advertising technology services. Discriminatory and self-preferencing practices, whereby dominant companies favour their own services over those provided by third parties using their platform or services, are particularly under the radar.

These recent enforcement initiatives are a useful reminder that adtech practices can be caught by competition law, especially by the prohibition of abuses of dominant position. They sit within a wider EU debate on how competition law should be used to help tackle issues relating to the collection and use of data. While data-related issues were not traditionally seen as a matter for competition law, the development of digital markets and the assessment of data as a source of market power led to increased scrutiny from global competition regulators. The European Commission recently recalled that competition law and data protection laws must work hand in hand to ensure that advertising markets operate on a level playing field in which all market participants protect user privacy in the same manner. There has also been increased cooperation between the FCA and the CNIL, and this inter-agency cooperation should only grow in the years to come.

France

Back to map

Update on the Digital Markets Act and the Digital Services Act

As mentioned in our previous round-ups, the European Commission published two legislative proposals, the Digital Services Act (DSA) and the Digital Markets Act (DMA), as part of the EU's Digital Single Market Initiative to remake EU laws around e-commerce, copyright, and privacy.

These two draft proposals intend to fight against the disclosure of illicit or harmful content and to ensure that digital markets remain innovative and open to competition and that commercial relations between the main actors and their business partners remain balanced and fair.

- The DSA aims to hold digital platforms accountable for the risks they may expose their users to in the distribution of illegal, dangerous, or counterfeit content and products. In that context, the DSA provides for new mechanisms for an eased removal of illegal content and the effective protection of users' fundamental rights online, including freedom of expression. It also strengthens public oversight of online platforms, especially those that reach more than 10 percent of the EU population.
- The DMA introduces a new regulatory model based on a system of gradual obligations, which targets the largest market actors. It sets out criteria for delimiting the platforms "under surveillance," which, in practice, will be "gatekeepers," and impose suitable obligations/prohibitions (e.g., data sharing, interoperability, and the prohibition of favouring the platform's own services to the detriment of competitors).

As the debate around the DMA reaches new highs, the Internal Market and Consumer Protection Committee adopted its position on the DMA on 23 November 2021. Amongst the key changes, the Committee extended the scope of the DMA to include web browsers, virtual assistants and connected TV services, while it slightly increased the turnover and market capitalization thresholds for a company to fall under the DMA. The Committee added new obligations for gatekeepers, notably regarding interoperability and targeted advertising. In particular, the revised proposal provides that gatekeepers should refrain from combining data for the purposes of targeted or micro-targeted advertising – unless there is clear, explicit, informed consent in line with the GDPR – and prohibits targeted advertising for minors. Another notable change is that the Committee increased the maximum fine that the European Commission can impose on gatekeepers to 20 percent of their annual worldwide turnover.

The Committee also adopted changes on the competition side. The revised proposal enables the European Commission to temporarily restrict gatekeepers from making acquisitions in areas relevant to the DMA, to remedy or prevent further damage to the internal market. This notably covers so-called "killer acquisitions." Partly answering calls from national competition authorities (NCAs), the Committee also clarified that NCAs will be able to provide support to the European Commission in market investigations or proceedings to ensure compliance with the DMA.

The European Parliament is expected to hold a vote on the proposals this December.

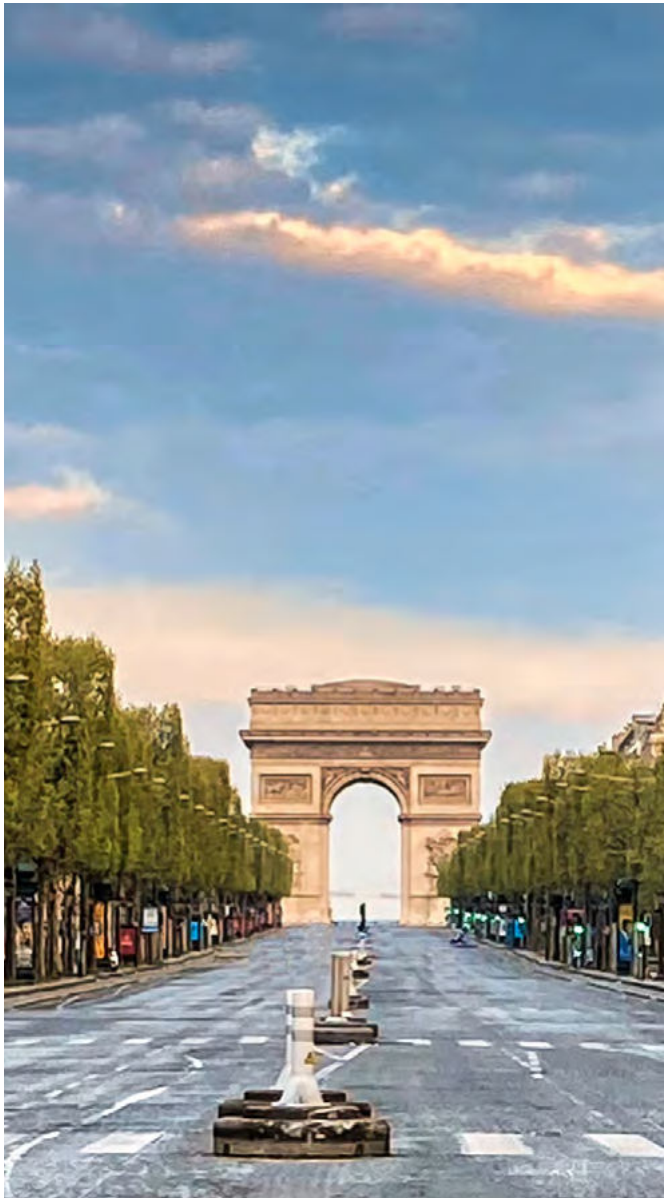
On its side, the Council of the European Union took another step forward and agreed on a general approach to the DMA proposal on 25 November 2021. The Council notably shortened the procedure for the designation of gatekeepers and provided a methodology to identify and calculate the "active end users" and "active business users" thresholds. It created a new obligation that requires gatekeepers to ensure that users can easily unsubscribe from core platform services. The Council also clarified the cooperation between the European Commission and national authorities, while confirming that the European Commission will be the sole enforcer of the regulation in order to prevent market fragmentation.

Negotiations between the European Parliament and the Council of the European Union should take place in 2022, with the DSA and the DMA coming into force on 1 January 2023.

The Cookies Factory

UNESCO has launched an international negotiation, which will soon lead to the adoption by its 193 member states of a Recommendation on the Ethics of AI that intends to provide a global normative framework on the ethics of artificial intelligence, by combining concrete actions and universal principles. The question of privacy is considered an essential objective of this framework.

In that regard, DDB Paris and the company Make Me Pulse have worked with UNESCO to develop a tool named "The Cookies Factory," which works as a Google Chrome extension and generates fake cookies. In practice, this new tool, available since 24 November 2021, allows users to erase their current cookies and to choose fictitious profiles from a large selection in order to fool tracking algorithms. This is an illustration of the many current innovations that are emerging in order to raise public awareness of the importance of cookies, but also to help individuals to make more informed decisions about their use of AI and what they can expect from it.



Belgium

Back to map

APD issues preliminary report on IAB TCF

In potentially one of the most far-reaching developments of 2021, the Belgian data protection regulator (APD) issued a preliminary report in October 2020, finding that IAB Europe's TCF, including both versions one and two, is not fit for purpose.

This follows a period of regulatory scrutiny that has prevailed for several years. A series of complaints were filed from commercial and civil society organizations across the UK and Europe in 2018 and 2019, most notably, that from Dr. Johnny Ryan of private browser Brave. These complaints focused on the TCF and, in particular, an allegation that consent requests provided under the TCF are not compliant. In parallel, there were also complaints about real-time bidding (RTB) generally, which argued that a system of high-velocity personal data trading is inherently incompatible with data security requirements imposed by EU law.

Following formal referral to, and investigation by, the APD, on 25 November 2021, the APD announced that it had finalized its draft decision regarding the compliance of the TCF with the GDPR and that it has been shared with the other European DPAs, who have 30 days (i.e., until 25 December 2021) to review it and provide potential feedback. The reason for the sharing and request for input from other data protection regulators is that the APD is the lead authority in the matter but is required under the GDPR to obtain input from other interested authorities.

The APD has said that there are two key potential outcomes from the review: (i) if the DPAs express no relevant and reasoned objection to the draft decision, the APD will adopt a final ruling; or (ii) if one or more of the DPAs express a relevant and reasoned objection to the draft decision, either the ADP will submit a revised version of its draft decision for review or the matter may be referred to the EDPB for a binding decision.

The report itself from the APD has not been published publicly, but the IAB and other sources have cited various points made in it. These include that the TCF allegedly:

- Fails to comply with the GDPR principles of transparency, fairness, and accountability; the lawfulness of processing; or free and informed consent.
- Does not provide adequate rules for the processing of special category data (e.g., health information, political affiliation, and sexual orientation, etc.).
- Involves IAB Europe itself being a data controller of personal data and specifically the personal data that exists in the "consent strings" that the TCF relies on to communicate permissions through the adtech ecosystem. IAB Europe is thereby in breach of the GDPR's Articles 24 and 32 (on the responsibility of the data controller and security of processing, respectively) because the TCF v2.0 Policies allow CMPs to continue to transact with publishers whom they suspect of engaging in behavior that breaches those policies and/or applicable EU law.
- Encourages the use of legitimate interests for data processing for profiling and personalization. The APD believes that legitimate interests is not an acceptable legal basis for the profiling involved. Moreover, even if it were, the APD notes that there is no evidence that IAB Europe (as a co-controller in the TCF context) has performed any balancing test, which it is required to do as a condition for leveraging legitimate interests.

Singapore

Back to map

Guidelines are revised to include a business improvement exception to consent

On 4 October 2021, Singapore's Personal Data Protection Commission issued an updated set of advisory guidelines that differentiate analytics and research using anonymised data, and analytics and research using personal data. While organisations are generally encouraged to use anonymised data as far as possible for such activities, since such data would not be governed by Singapore's Personal Data Protection Act, an organisation that uses personal data can do away with the need for consent if its processing is for a specified business improvement, namely:

- Improving, enhancing, or developing new goods or services.
- Improving, enhancing, or developing new methods or processes for business operations in relation to the organisations' goods and services.
- Learning or understanding the behaviour and preferences of individuals (including groups of individuals segmented by profile).
- Identifying goods or services that may be suitable for individuals (including groups of individuals segmented by profile), personalising, or customising any such goods or services for individuals.

In other words, personal data collected for a particular purpose can be used or leveraged subsequently to conduct research for service or product enhancements, or to identify suitable services to be offered to relevant individuals (including prospective customers). The organisation's use of personal data must be reasonable and appropriate in the circumstances and must not be achievable without it being in an individually identifiable form. The data cannot be used to send direct marketing messages.

The use of advertising cookies is further clarified

The updated advisory guidelines also clarify that cookies used for targeted advertising (i.e., involving the processing of personal data) require consent. This may be obtained through users' browser settings, though organisations are encouraged to provide individuals with the ability to set their cookie preferences within the websites themselves.

China

Back to map

The Personal Information Protection Law requires that users be given the right to personalise their opt-out

On 1 November 2021, the Personal Information Protection Law of the People's Republic of China (PIPL) came into effect. Article 24 of the PIPL provides that:

- Where a personal information processor conducts automated decision-making by using personal information, they must ensure the transparency of the decision-making and the fairness and impartiality of the result, and must not give unreasonable differential treatment to individuals in terms of trading price or other trading conditions.
- Where information push or commercial marketing to individuals is conducted by means of automated decision-making, options not specific to individuals' characteristics must be provided simultaneously, or convenient ways to refuse must be provided to individuals.
- Where a decision that has a major impact on an individual's rights and interests is made by means of automated decision-making, the individual must have the right to request an explanation from the personal information processor and to refuse to accept that the personal information processor makes decisions solely by means of automated decision-making.

Therefore, if users do not want to see personalised content in the advertising display, they must have the right to easily turn off the personalised recommendations according to the path described in the media's privacy policy.

The Data Security Law imposes compliance requirements on data controllers and processors

On 1 September 2021, the Data Security Law of the People's Republic of China (DSL) came into effect. The DSL encourages technological promotion and commercial innovation in the fields of data development and utilization and data security, including adtech. At the same time, the DSL requires companies to establish and improve a whole-process data security management system, organise data security education and training, and take corresponding technical measures and other necessary measures to safeguard data security in conducting data processing activities.

Meet the authors

Back to map

If you have questions or would like additional information on the material covered in this Alert, please contact one of the authors – listed below – or the Reed Smith lawyer with whom you regularly work.

United Kingdom

Elle Todd
Partner, London
etodd@reedsmith.com

Tom Gates
Associate, London
tgates@reedsmith.com

Francesca Moss
Trainee Solicitor, London
fmoss@reedsmith.com

U.S.

Keri Bruce
Partner, New York
kbruce@reedsmith.com

Monique Bhargava
Partner, Chicago
mbhargava@reedsmith.com

Sarah Bruno
Partner, San Francisco
sbruno@reedsmith.com

Kile Marks
Associate, San Francisco
kmarks@reedsmith.com

Germany

Andreas Splittgerber
Partner, Munich
asplittgerber@reedsmith.com

Sven Schonhofen
Associate, Munich
sschonhofen@reedsmith.com

France

Natasha Tardif
Partner, Paris
ntardif@reedsmith.com

Daniel Kadar
Partner, Paris
dkadar@reedsmith.com

Audrey Augusto
Associate, Paris
aaugusto@reedsmith.com

Laetitia Gaillard
Associate, Paris
lgaillard@reedsmith.com

Stéphanie Abdesselam
Juriste, Paris
sabdesselam@reedsmith.com

Singapore

Charmian Aw
Counsel, Singapore
caw@reedsmith.com

China

Cindy Shen
Consultant, Shanghai
cshen@reedsmith.com

reedsmith.com

ReedSmith
Driving progress
through partnership