WHITEPAPER

EU Cookie Audits
Are you Compliant?

TRUSTe Inc.

EU: +44 (0) 203 078 6495

www.truste.eu

US: 1-888-878-7830

www.truste.com

Fieldfisher

Riverbank House

2 Swan Lane

London, EC4R 3TT

+44 (0)20 7861 4000

www.fieldfisher.com

In 2014, European Data Protection Authorities conducted a series of audits to assess current levels of compliance with the EU Cookie Directive.

This joint TRUSTe–Fieldfisher Whitepaper will help you to:

- understand the requirements of the EU Cookie Directive and how these have been implemented across different Member States
- know what consumers think about cookies and tracking and what they expect from businesses
- understand how the different regulators expect you to obtain consent
- gain an overview of latest enforcement actions
- see examples of best practice solutions
- put in place a plan to ensure compliance, avoid costly warnings and fines and win the trust of European customers.

1. EUROPEAN COOKIE CRACKDOWN HAS STARTED

Since the introduction of the so-called "EU Cookie Directive"[1] and the EU's proposals for a new EU General Data Protection Regulation there have been concerted efforts by regulators to set common standards for data privacy across the EU. But as anyone doing business in the EU knows there are still markedly different approaches to compliance and consumer attitudes across key EU markets. These differences have often made compliance seem onerous and complex but this is an issue that businesses can no longer afford to ignore as the drumbeat of European enforcement has started.

At a European level, the Article 29 Working Party ("WP 29") released on February 3rd, 2015 its report[2] analyzing the results of a EU cookies sweep that was conducted from September 15th to 19th 2014 by the Data Protection Authorities ("DPAs") of eight EU Member States, namely: Czech Republic, Denmark, France, Greece, the Netherlands, Slovenia, Spain and the United Kingdom. The cookies sweep focused on three "privacy-risk" sectors, namely media, e-commerce and the public sector, and targeted 250 of the most frequently visited sites by individuals within each Member State. The goal of this sweep was to inform the WP 29 on the current usage of cookies and likely state of compliance with the EU Cookie Directive by providing a statistical and manual review of cookie compliance in those three sectors. The purpose was not to assess individually for each website the level of compliance with cookie rules, but rather to gather information about the extent of the cookies used, the level of information provided and the types of control mechanisms in place on the websites that were visited. The report found that he average website placed 34 cookies on a device during a person's first visit, 70% of these were third party cookies and 86% of them were persistent. Only 74% of the websites surveyed across Europe provided any information about cookies.[3]

In parallel, 2014 has also seen a significant increase in enforcements by EU data protection authorities in several Member States. This cookie crackdown began in Spain where Regulators obtained the first European cookie fines from two companies that used cookies without obtaining informed consent and providing adequate control. The momentum continued with two enforcement actions in the Netherlands against ad network YD Benelux in May and the Dutch Foundation for Public Broadcasting in August 2014. The recent European Court of Justice ruling against Google on the 'Right to be Forgotten' was also a prominent reminder that US companies can be subject to EU requirements when processing data about EU citizens.

In France, the French data protection authority (the "CNIL") audited approximately 100 companies as part of the EU cookies sweep and conducted additional remote and on-site cookie audits under national law in October 2014 by using the new inspection powers that were introduced in France last year (27 online audits, 24 on-site inspections and 2 auditions[4]).

In the Netherlands, a new law came into force on March 11, 2015, which amends Article 11.7a of the Telecommunications Act (implementing the EU Cookie Directive). Without explicitly referring to the term "implied consent", the amended article 11.7a allows the possibility of implied consent of the user as a lawful form of consent according to the Explanatory Memorandum to the amendment. Also, the most significant change under this new law is the introduction of a lighter regime for cookies that are (i) used to gather information on the quality and effectiveness of a requested service; and (ii) have little or no effect on the privacy of the user of the service. For these cookies, obtaining prior consent is no longer required. The Dutch Consumer and Markets Authority has also replaced the former Telecommunications Authority as the regulator that is competent for enforcing cookie rules in the Netherlands.

1 Although commonly referred to as the Cookie Directive, this name is misleading for two reasons. First, the actual name of the legislation is Privacy and Electronic Communications Directive 2002/58/EC (as amended by the Citizens' Rights Directive 2009/136/EC). Second, the consent requirements of the Cookie Directive apply to any collection or storage of information on an individual's device, whether or not using cookies, and so apply equally to, for example, web beacons and Local Shared Objects.

2 The Article 29 Working Party's "Cookie Sweep Combined Analysis – Report" adopted on 3 February 2015 (WP 229) is available here: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

3 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/02/a-cookie-can-last-7984-years-according-to-new-study/

4 These figures are provided in the CNIL's Annual Activity Report for 2014.

While the implementation of the Directive into national laws is complex, there are many simple solutions now available to help companies comply with the different implementations across Europe. Given the renewed focus on this issue by European regulators, companies should not wait until they are being investigated to put their house in order.

In this Whitepaper we look in more detail at the requirements of the Directive, consumer attitudes to compliance, recent regulatory activity and outline some basic steps companies can take to address these issues and comply with the EU Cookie Directive.

2. THE EU COOKIE DIRECTIVE

The so-called EU Cookie Directive has been around for a long time — since 2002, in fact. At that time, it required only that businesses make very basic cookie disclosures in their privacy policies and inform users how they could refuse cookies by changing their browser settings. Over time, this became the market standard approach to disclosing cookie use.

Then, in 2009, an amendment to the Cookie Directive was passed that introduced for the first time a requirement that companies provide "clear and comprehensive information" to users about the use of cookies, including a way for users to "consent" to any cookies which are not "strictly necessary" for the delivery of an online service.

In response to reports that companies were exploring device fingerprinting in an attempt to avoid the consent requirements under the EU Cookie Directive the Article 29 WP confirmed[5] last November in Opinion 9/2014 that the Directive also applies to all methods of tracking including device fingerprinting.

After an initial period of uncertainty, the majority of EU Member States have now adopted their own Cookie Laws implementing the requirements of the Cookie Directive. However the approaches taken by each of the Member States are not uniform, and vary in the standard of consent required. This in turn has resulted in a confusing patchwork of compliance obligations for companies doing business in the EU when it comes to cookies and similar tracking technologies.

In very broad terms, EU Member States broadly fall into two categories: those that require strict "opt-in" consent, meaning that individuals must expressly consent to cookies before cookies are served to their device; and those that tolerate the use of cookies on an "implied" consent basis.

At a market level, implied consent is the more popular of the two consent models. This consent model entails the website operator serving a prominent notice to visitors to its website (typically in the form of a cookie banner):

a. explaining at a high level that it uses cookies and what those cookies do (E.g. "This website uses cookies for advertising, analytics and functionality purposes");

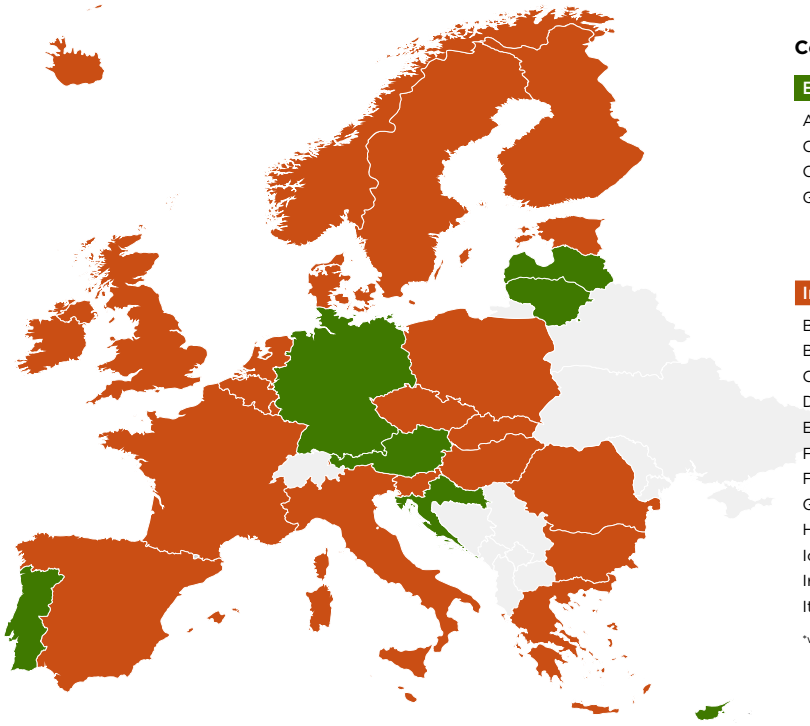
b. linking to more detailed cookie disclosures in its privacy policy or standalone cookie policy;

c. also linking to granular controls that enable the individual to accept or refuse the use of cookies (such as the TRUSTe Cookie Consent Manager); and

d. informing visitors that if they continue to browse the website without changing their cookie settings, they will be consenting to the use of cookies. Under this model, cookies are often served at the same time as delivery of the notice itself, although some website operators may choose not to serve cookies until they are confident that the visitor has indicated its implied consent.

5 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf

Included below is a map of EU member countries showing the consent standards currently applicable throughout the EU as of May 2015:



Countries That Have Passed a Cookie Law

Express Consent

Austria	Latvia
Croatia	Lithuania
Cyprus	Portugal
Germany	

Implied Consent

Belgium	Liechtenstein
Bulgaria	Luxembourg
Czech Republic	Malta
Denmark	Netherlands*
Estonia	Norway
Finland	Poland
France	Romania
Greece	Slovakia
Hungary	Slovenia
Iceland	Spain
Ireland	Sweden
Italy	United Kingdom

*where cookies fall under list of defined exceptions

Source: TRUSTe

3. EUROPEAN CONSUMER ATTITUDES TO COOKIES AND TRACKING

The TRUSTe EU Consumer Privacy Index was the first study to provide a comprehensive analysis of consumer attitudes to data privacy and company practices across the EU. The extensive study included an analysis of the tracking on the top 50 websites as ranked by Alexa.com in France, Germany, Great Britain and the Netherlands and responses from a representative sample of over 4,000 consumers in those four countries.[6]

Cookie Use by top EU websites

TRUSTe's Website Monitoring Service was used to provide a snapshot of cookie usage across the homepages of the top 50 websites as ranked by alexa.com in the four countries surveyed. The results showed that French websites were dropping nearly twice as many third-party cookies (434) as websites in the Netherlands (237). There were an average of 9 third-party cookies per homepage in France compared with 5 third-party cookies on Dutch websites.

3rd Party Cookie Averages

France: 9 per homepage

Germany: 6 per homepage

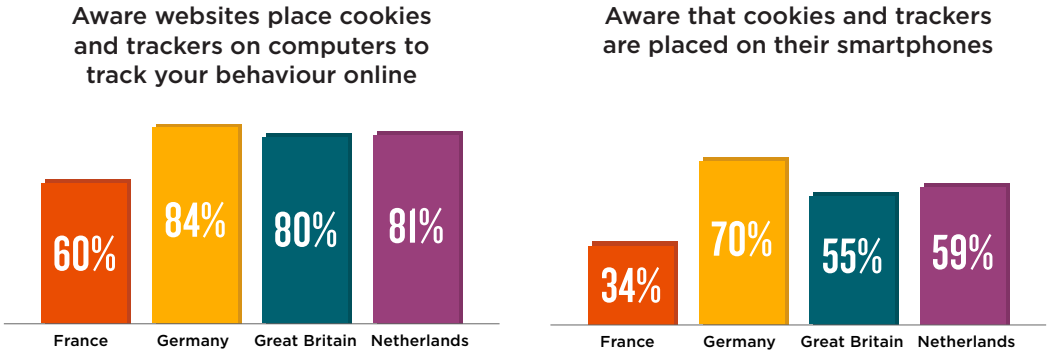
Great Britain: 8 per homepage

Netherlands: 5 per homepage

What do EU consumers understand about cookies and tracking?

The study found that the majority of EU consumers were highly knowledgeable about internet cookies and trackers on both computers and mobile devices. Although they were aware of the pay-off between online targeting from advertisers and receiving free online services, content and games, few were willing to accept tracking in exchange for free services.

There was high consumer awareness that websites place cookies and trackers on computers to track online behavior, and slightly lower levels of awareness that this also takes place on smartphones. Awareness that tracking takes place on mobile devices was twice as high in Germany (70%) as it was in France (34%).



75% of EU consumers were aware that tracking enabled companies to provide more relevant content and ads. 67% were aware that this was used to fund free online services, content and games by selling ads based on the tracking information. But EU consumers were not prepared to trade their privacy for free online services.

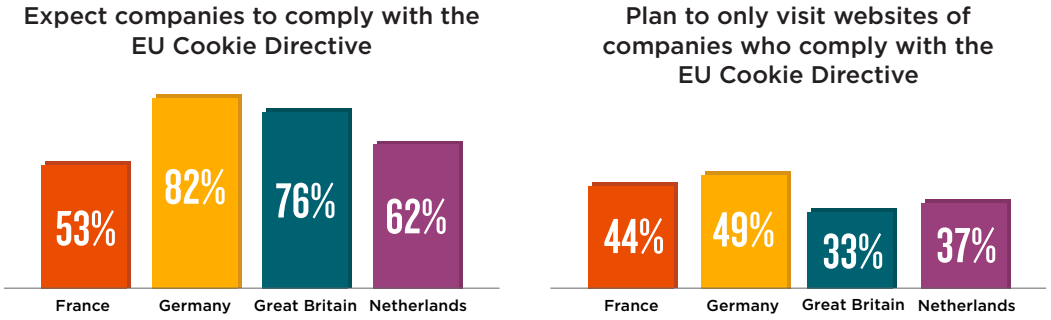
6 Ipsos MORI's i:Omnibus interviewed a representative sample of 4,041 adults aged 16 to 75 across Great Britain, the Netherlands, France and Germany. Those interviewed in the Netherlands and Germany were aged 16 to 70. Interviews were conducted online during the 19th to 26th October 2012. Data has been weighted to match the profile of each country's population.

Only 16% of French consumers, 18% of Dutch consumers and 21% of German consumers were happy for companies to track them online in exchange for free services and content such as social networks, news and games. The highest levels of acceptance were in Great Britain where less than 1 in 4 people (23%) were happy to be tracked, despite extensive use and availability of free online services.

Consumer privacy concerns and expectations of compliance with the EU Cookie Directive

The study found high levels of privacy concerns across all four countries.

85% of EU consumers felt that companies should get their permission before tracking them online. 68% of EU consumers expected companies to comply with the EU Cookie Directive and 41% planned to only visit websites that do.



With nearly half of German consumers (49%) planning to only visit websites of companies that comply with the Directive there are clearly significant potential consequences for businesses of ignoring the Directive.

In France, where there was the highest level of privacy concern 1 in 2 consumers (53%) expected companies to comply and 44% planned to only visit the websites of those that did.

4. SUMMARY OF RECENT ENFORCEMENT ACTIONS AND PLANNED INSPECTIONS

Between 2009 and 2014, there was no meaningful enforcement of the EU's new cookie consent law. This served as a grave disappointment both to those legislators, regulators and advocacy groups who had pushed hard for the introduction of greater cookie transparency and consent requirements, and also for businesses that had taken significant compliance efforts to meet the EU's new cookie consent standard.

Over time, this lack of enforcement resulted in some businesses scaling back their cookie compliance programs while others that had been planning to introduce cookie compliance programs decided to put these on hold in order to prioritize more pressing compliance risks. However, after several years of apparent enforcement silence, it now seems that the data protection authorities around the EU have decided to turn their attention to cookies once again. Since 2014, several notable regulatory actions have taken place:

- **Spain**: The Spanish data protection authority issued fines against two jewellery companies, Navas Joyeros S.L. and Luxury Experience S.L., each operating a variety of promotional websites, for not providing clear and comprehensive transparency about their use of cookies. The fines in total amounted to EUR3,500. For technical legal reasons, the Spanish data protection authority was not able to issue fines against these companies for failure to obtain sufficient consent, although new legislation has since been introduced to rectify this. While the aggregate value of the fines is relatively modest, the symbolic importance of this first ever cookie enforcement is significant — indicating that EU data protection authorities now feel bold enough to pursue formal enforcement against businesses that are not cookie compliant. In recent months, the Spanish authority has issued several resolutions against companies with respect to their use of cookies, although in all these cases, the Spanish DPA either did not pronounce a sanction where the company had complied during the inspection procedure, or pronounced a simple warning against the non-compliant company. The Spanish DPA is rumoured to be pursuing potential enforcement actions against other companies, although this cannot be verified as at the date of this whitepaper.
- **Netherlands**: The Netherlands has seen two separate cookie enforcement actions last year: the first against targeted advertising network YD Display Advertising Benelux and the second against the Dutch Public Broadcasting Service (NPO) — the Dutch enforcement activity therefore spanning both a website publisher and, separately, a third party vendor providing services to a publisher. For non-compliant businesses, the Dutch market was already high risk — with cookies regulated both under Dutch telecoms law (which sets out the consent requirement) and also under Dutch data protection law (which regulates the collection of personal data by cookies). In the case of YD Display Advertising Benelux, the Dutch Data Protection Authority found that it had failed to obtain prior consent from website visitors to the use of its cookies, and had failed to inform them about the purposes for which its cookies were used — simply providing an opt-out from its tracking cookies was found not to be sufficient. In the case of NPO, it found itself at the mercy of jointly-led enforcement by the Dutch Data Protection Authority and the Dutch Authority for Consumers and Markets, who found that it had failed to obtain proper prior opt-in consent (the legal standard in the Netherlands). Following the amendment of the cookie regime in the Netherlands, the Dutch Consumer and Markets Authority is said to be conducting investigations into several websites with a particular focus on cookie compliance, which could potentially lead to enforcement procedures in the near future.

- **France**: Following the EU-wide sweep, the CNIL carried out a more focused national review in October 2014, during which it assessed the compliance of companies doing business in France with its cookie consent guidance. According to its 2014 Annual Activity Report, the CNIL used its new online inspection powers to carry out 27 online audits. It conducted a further 24 on-site inspections and 2 auditions. The CNIL examined a number of issues, including the types of cookies used by websites, the purpose those cookies serve, whether website operators are aware of the cookies they are serving through their site, and whether obsolete cookies continue to be served. The French authority paid particular attention to processes implemented by website operators for obtaining consent to cookies, including the prominence and transparency of information, the possibility and consequences of declining consent, and the duration of cookies served. At the time this Whitepaper was re-issued, no sanction had been publicly released by the CNIL against any non-compliant company.
- **Italy**: The Italian data protection authority (Garante) published new guidance on obtaining consent. In particular, this requires businesses to notify the authority where profiling cookies (e.g. targeted advertising cookies) or similar technologies are used, meaning the authority will be put on notice as to which businesses are using profiling cookies and therefore better able to check and assess their compliance. The Garante announced a one-year grace period through to June 3 2015 before this requirement takes effect. This coincides with a recent ruling from the Dutch data protection authority that Google must obtain prior consent from individuals before collecting their data through cookies for targeting purposes. In the beginning of May 2015, the Garante publicly announced that this grace period is coming to an end and that it will soon begin to enforce cookie rules. On July 10, 2014, the Garante also issued a prescriptive rule against Google ordering it to obtain prior and express consent for online profiling and behavioral advertising activities and gave it 18 months to comply with these requirements.
- **Belgium**: On February 4, 2015, the Belgian Privacy Commission released its guidance on the use of cookies expressly confirming that implied consent is acceptable provided it is "unambiguous" and indicating that a user must give his or her specific, informed, unambiguous and freely given consent before the processing of personal data commences. Furthermore, following a report published by researchers at two Belgian universities claiming that Facebook engages in online tracking of not only its users but also people who have no Facebook account, the Belgian Privacy Commission is now leading the investigation into Facebook's tracking and data processing activities together with Dutch and German regulators.
- **United Kingdom**: The Information Commissioner's Office approach to cookie compliance is different from other EU DPAs in that it focuses on sites that are doing nothing to raise awareness of cookies, or get their users' consent. When consumers file a complaint with the ICO, it either conducts its own compliance check or writes to the organization concerned asking for an explanation about its compliance. Since October 2012, the ICO has written to 275 organizations specifically about compliance with the cookie rules and has revisited them quarterly since then. In April 2014, the ICO re-assessed this strategy and decided to pursue its efforts in this manner only whenever it receives concerns from consumers.

Overall, after several years of relative cookie enforcement activity, 2015 is shaping up to be a big year for cookie inspections and enforcement. Why it has taken this long for cookie enforcement to happen is hard to say, although many of the enforcement actions described above have in fact been several years in the making (the origins of the NPO enforcement, for example, trace back to 2012). What does seem clear though is that EU data protection authorities seem to have a renewed appetite to pursue cookie-related enforcement, likely spurred on by post-Snowden concerns about online surveillance. Taking this into account, a 'wait and see' approach to cookie compliance can only be described as the wrong strategy — businesses need to get an active grip on understanding what cookies they use and why, and implement an appropriate consent strategy to minimize their EU compliance risk.

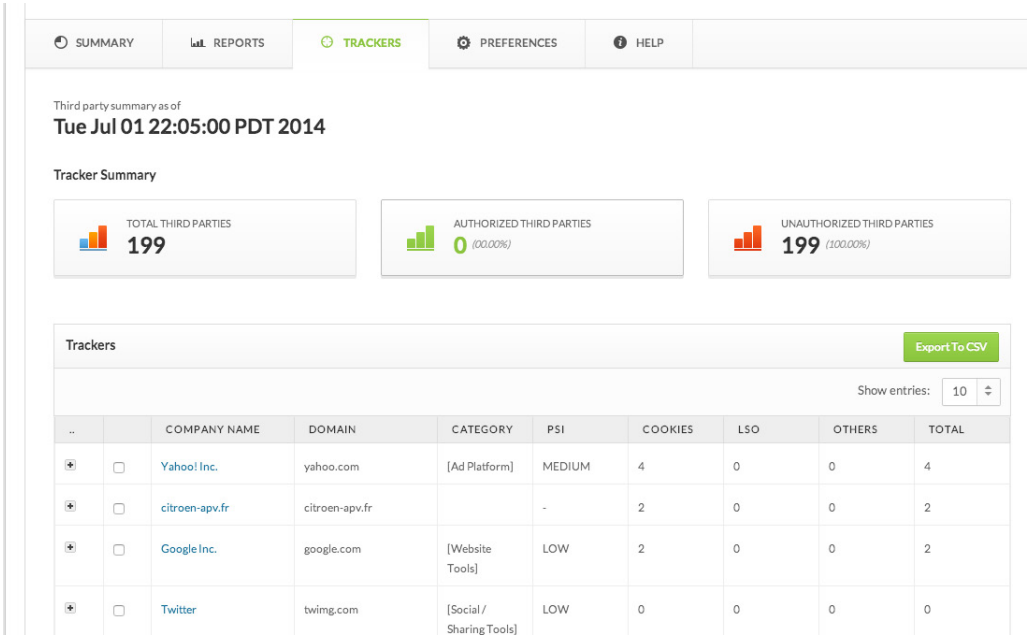
5. EXAMPLES OF BEST PRACTICE TO SOLUTIONS TO MEET DIFFERENT COMPLIANCE REQUIREMENTS ACROSS MEMBER STATES

Cookie Audits

The EU Cookie Directive makes clear that websites are accountable for all cookies and tracking mechanisms running on their site, so conducting a cookie audit of your website is an essential first step in compliance.

Tools such as TRUSTe's Website Monitoring Service can help you conduct an initial audit of what's happening on your site and then ongoing monitoring can alert you to any changes in activity so you can be confident of ongoing compliance.

Website Monitoring Service Dashboard

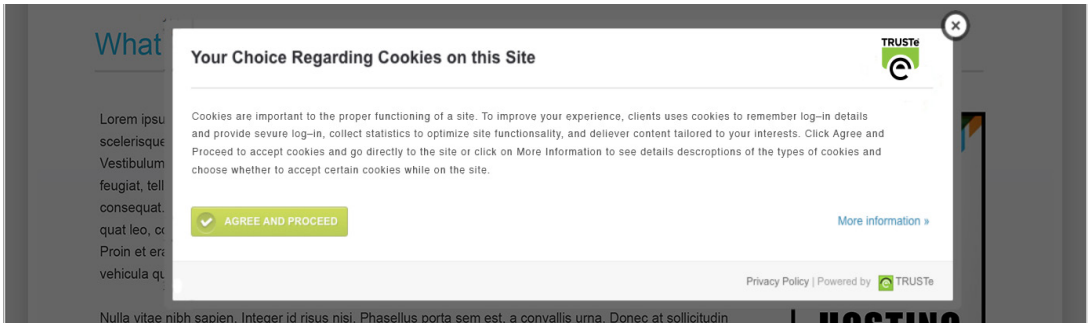


Consent Mechanisms

It is not just a legal requirement under the EU Cookie Directive, TRUSTe research has shown that EU consumers have high levels of privacy concerns and 83% thought that companies should get their permission before tracking them online.

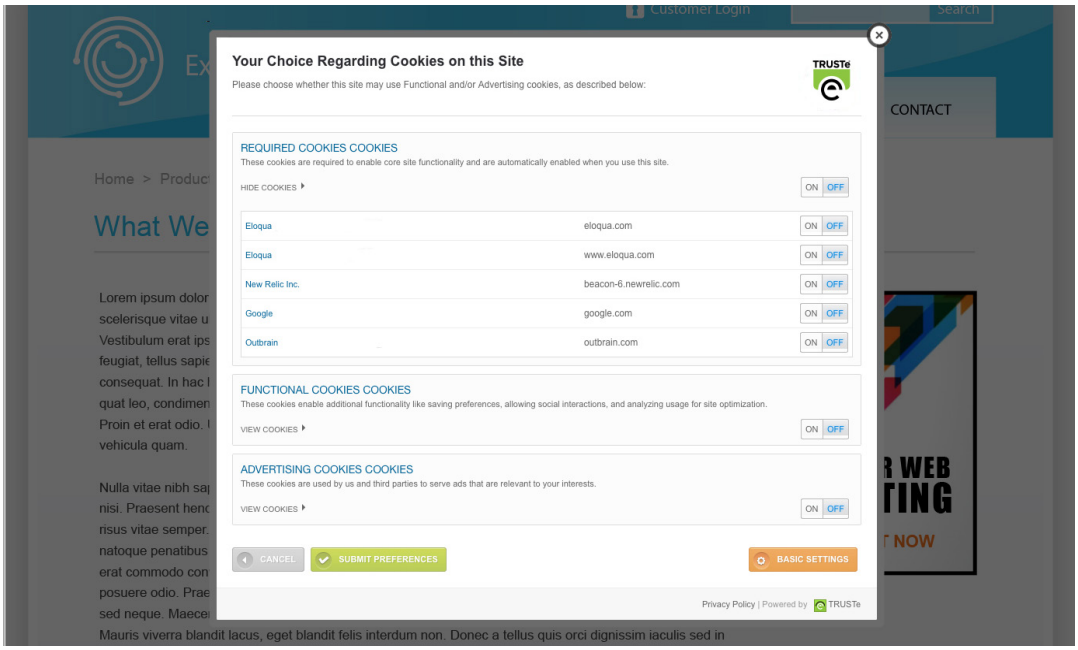
Tools such as EU Cookie Consent Manager make it simple to give notice and offer users a way to opt out of the tracking on your site.

Informed Consent

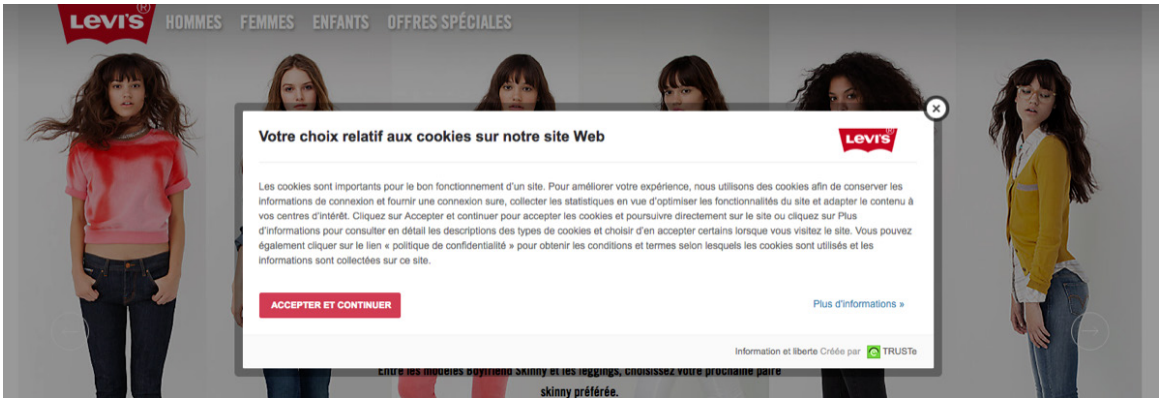


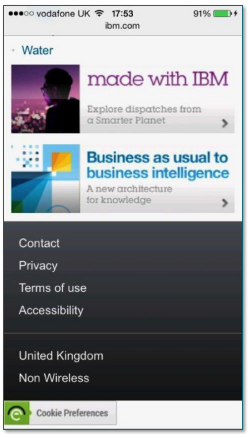
User Choice and Control

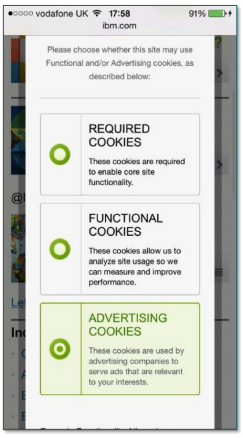
The Directive also calls for websites to provide a mechanism for the user to revoke consent and opt out of tracking.



Across Desktop and Mobile Optimized Websites







Impact of a robust compliance solution

A review of the actions taken by a sample of 3.5 million users of 29 different UK website implementations from June through September 2012 showed that the majority of users are choosing to allow the use of third party advertising cookies and only a small minority (0.05% or 5 in 10,000) are choosing to only allow "Required" or "Functional" cookies.

Therefore sites with a robust compliance solution are not experiencing significant opt-out rates and at the same time are further building trust with their customers by giving them both notice of the tracking activity and the ability to easily make an informed choice about their tracking preferences

All the companies included in the analysis used TRUSTe's EU Cookie Consent Manager[7] solution to comply with the Directive. TRUSTe has been working with clients ranging from Oracle and IBM to publishers such as Forbes and the Economist, and consumer brands such as Levi's and Kelloggs who have all chosen the TRUSTe EU Cookie Consent Manager solution to ensure compliance and manage cookie preferences on their websites.

6. RECOMMENDED NEXT STEPS

1. Conduct an audit of all the cookie and similar tracking technologies deployed across your online properties.
2. Understand the consent compliance requirements of each of the European countries in which you operate
3. Categorize the cookies and tracking technologies on your site and put in place ongoing monitoring solution so that this information is updated on a regular basis
4. Implement a consent strategy for the cookies and tracking technologies deployed through your online properties, either on a "full compliance" or "risk management" basis. However, as a minimum, your strategy must:
    a. Provide users with prominent notice of the cookies served through your site (both first and third party cookies);
    b. Inform them about the purposes for which those cookies are used;
    c. Inform them where they can find more detailed cookies information (for example, in a cookie policy or privacy policy); and
    d. Provide a way to accept or decline those trackers
5. Use a consent management solution to implement your chosen consent strategy.
6. Ensure the information in your privacy policies is complete, accurate and understandable to non-specialists.
7. Make sure you are also current on satisfying "adequacy" for commercial data transfers from the EU to the US (for example, through the use of US-EU Safe Harbor, BCR, or model contractual clauses data export solutions).

7 Find out more about TRUSTe's Website Monitoring & Cookie Consent Manager Solutions http://www.truste.com/products-and-services/enterprise-privacy/eu-consent-manager

7. ADDITIONAL INFORMATION

Article 29WP Cookie Sweep Combined Analysis — Report: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

Article 29WP Opinion 2/2013 providing guidance on obtaining consent for cookies: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

Article 29WP Opinion 4/2012 on cookie consent exemption: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf

CNIL, Recommandation sur les cookies: quelles obligations pour les responsables de sites, quels conseils pour le internautes? http://www.cnil.fr/linstitution/actualite/article/article/recommandation-sur-les-cookies-quelles-obligations-pour-les-responsables-de-sites-quels-conseils/

CNIL, Cookies : des contrôles à partir d'octobre http://www.cnil.fr/linstitution/actualite/article/article/cookies-des-controles-a-partir-doctobre/

ICO, Guidance on the rules on use of cookies and similar technologies: http://ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide/~/media/documents/library/Privacy_and_electronic/Practical_application/cookies_guidance_v3.ashx

ICO, Cookies enforcement: http://ico.org.uk/enforcement/action/cookies

ACM, Frequently asked questions about the Dutch cookie act: https://www.acm.nl/en/publications/publication/11917/Frequently-asked-questions-about-the-Dutch-cookie-act/

ACM, Netherlands Public Broadcasting violates cookie rules: https://www.acm.nl/en/publications/publication/13171/Netherlands-Public-Broadcasting-violates-cookie-rules/

Belgian Privacy Commission, Guidance on the use of cookies: http://www.privacycommission.be/fr/recommandations-cpvp

TRUSTe

TRUSTe is the leading global Data Privacy Management (DPM) company and powers privacy compliance and trust by enabling businesses to safely collect and use customer data across web, mobile, cloud and advertising channels. Our cloud-based Data Privacy Management Platform delivers innovative technology products, including website monitoring and advertising compliance controls — along with privacy assessments and certifications. More than 5,000 companies worldwide rely on our DPM platform and globally recognized Certified Privacy Seal to protect/enhance their brand, drive user engagement and minimize compliance risk. For more information, please see www.truste.com.

FIELDFISHER

Fieldfisher is a European law firm with market leading practices in many of the world's most dynamic sectors including Real Estate, Energy, Financial Services, Government & Public Services, Hotels & Leisure, Life Sciences, Media, Telecoms and Technology. Clients choose to work with us because we deliver commercial, pragmatic and innovative solutions through our exceptional legal expertise and experience, on time and on budget.

We have more than 400 lawyers working with large businesses like the BBC, Pearson, Karen Millen, Citigroup and Accenture but also with private wealth and social enterprises as trusted advisers, providing highly commercial advice based on an in-depth understanding of their needs.

We operate across our international offices in Brussels, Düsseldorf, Hamburg, Paris, London, Munich, Manchester, Palo Alto and Shanghai. Fieldfisher is the trading name of Field Fisher Waterhouse LLP. For more information please see www.fieldfisher.com.