RECENT DEVELOPMENTS ON COOKIES:

What You Need To Know

Research by OneTrust DataGuidance™

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

OneTrust DataGuidance provides a suite of privacy solutions designed to help you monitor regulatory developments, mitigate risk, and achieve global compliance. With focused guidance around core topics, comparative Cross-Border Charts, a daily customised news service, and expert analysis, OneTrust DataGuidance provides industry leading solutions to design and support your entire privacy programme.

These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy programme.

Website **www.dataguidance.com**

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

HOW ONETRUST HELPS

The changing global privacy landscape, like the CCPA and the GDPR, have put a spotlight on how companies collect cookie consent and preferences and how that data is shared with third-parties. Businesses are seeking to build intelligent, data- driven websites that respect user's privacy and build trust and brand loyalty. By leveraging OneTrust, organisations can operationalise compliance and integrate a privacy strategy into their websites and marketing activities.

OneTrust PreferenceChoice™

Creating personalised user experiences while respecting customer data is a growing challenge for marketing teams in the age of data privacy regulations. As consumers become more privacy-conscious, businesses must be transparent with their data collection and usage to build trust and maintain relationships with their end users.

PreferenceChoice allows organisations to centrally manage consent and preferences while giving consumers control and visibility into how their data is used. By syncing consent and preference settings throughout marketing applications, businesses can create consistency across marketing activities and deliver positive user experiences that respect customer preferences.

Preference Choice is a customer-centric consent and management platform:

Consent Management Sync Valid Consent
Marketing Preferences End User Preference Center
Cookie Compliance Website Scanning & Consent
Consumer Rights Requests Automate Intake & Fulfillment
Policies, Notices & Disclosures Centrally Host, Track & Update
Mobile App Compliance App Scanning & Consent

OneTrust DataGuidance™

Use OneTrust DataGuidance to access a centralised resource aggregator that includes cookie summaries, comprehensive guides, and regulatory guidance. OneTrust DataGuidance is continually updated by the OneTrust global research team and includes latest amendments, news, and guidance.

Recent Developments on Cookies: What You Need to Know

What has happened?

The topic of cookies has become a major focal point of this year's privacy landscape. Currently, cookies are regulated in the European Union under Article 5(3) of the Directive on Privacy and Electronic Communications (2002/58/EC) (as amended) ('the ePrivacy Directive'). Recently, the implementation measures of cookies and similar technologies have been addressed by the Court of Justice of the European Union (CJEU') and national supervisory authorities. The following report breaks down the findings of the CJEU and further details respective relevant requirements provided by the French, German, Spanish, and British supervisory authorities.

CJEU ruling on Planet49

The CJEU issued, on 1 October 2019, its judgment on Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v. Planet49 GmbH (C-673/17) ('the Planet49 Judgment'). In particular, the Planet49 Judgment addressed the following questions, as referred to the CJEU by the German Federal Court of Justice:

Does it constitute a valid consent if the storage of information, or access to information already stored in the user's terminal equipment, is permitted by way of a pre-checked checkbox which the user must deselect to refuse their consent?

The Planet49 Judgment highlights that it would appear impossible in practice to ascertain objectively whether a website user had actually given their consent to the processing of their personal data by not deselecting a pre-ticked checkbox nor, in any event, whether that consent had been informed. At the same time, the Planet49 Judgment notes that it is conceivable that a user would not have read the information accompanying the pre-checked checkbox, or even would not have noticed that checkbox, before continuing with their activity on the visited website.

Moreover, the Planet49 Judgment states that valid consent requires an active and specific indication of the data subjects' wishes. As a result, a pre-checked checkbox which the user must deselect to refuse their consent cannot be considered a lawful way to obtain consent for the storage or access of cookies.

For the purposes of the application of Article 5(3) and Article 2(f) of the ePrivacy Directive, read in conjunction with Article 2(h) of the Data Protection Directive (Directive 95/46/EC) ('the Data Protection Directive'), does it make a difference whether the information stored or accessed constitutes personal data?

The Planet49 Judgment highlights that the interpretation of the ePrivacy Directive should not differ according to whether or not the information stored or accessed on a website user's terminal equipment constitutes personal data. In particular, the Planet49 Judgment states that, according to Recital 24 of the ePrivacy Directive, any information stored on the user's terminal equipment is part of their own private sphere and requires protection under Article 8 of the European Convention on Human Rights. As a consequence, information stored in the terminal equipment of users of electronic communications networks must be protected, regardless of whether it is personal data within the meaning of the Data Protection Directive and the GDPR.

What information does the service provider have to give within the scope of the provision of clear and comprehensive information to the user that has to be undertaken in accordance with Article 5(3) of the ePrivacy Directive? Does this include the duration of the operation of the cookies and the question of whether third parties are given access to the cookies?

The Planet49 Judgment outlines that a cookie policy must detail the lifespan of any cookies and whether third parties are given access to cookies. In particular, it outlines that for information to be clear and comprehensive, the user's consent must be well informed in order for the same user to be able to easily determine the consequences of the consent they might provide. In addition, the Planet49 Judgment finds that information regarding the duration of cookies' operation and whether or not third parties may have access to those cookies shall be included in the clear and comprehensive information presented to the user.

CJEU ruling on Fashion ID

The CJEU issued, on 29 July 2019, its judgment on Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV (C-40/17) ('the Fashion ID Judgment'), addressing a dispute concerning the insertion by Fashion ID of Facebook Ireland Ltd.'s 'Like' button on its website through a plug-in, allowing users' personal data, such as IP addresses and browser history, to be transferred to Facebook regardless of whether the user clicked on the 'Like' button.

In particular, the Fashion ID Judgment responds to the Düsseldorf Higher Regional Court's ('the 'Referring Court') request for a preliminary ruling in relation to the interpretation of certain provisions of the Data Protection Directive. The Fashion ID Judgment states, among other things, that Fashion ID can be considered to be a joint controller with Facebook, in respect of the collection and disclosure by transmission of data to the latter, because Fashion ID and Facebook jointly determine the means and purposes of those operations.

Furthermore, the Fashion ID Judgment outlines that Fashion ID could not be considered to be a controller in respect of the operations involving the processing of data carried out by Facebook after such data had been transmitted to it.

Moreover, the Fashion ID Judgment highlights that it is for the Referring Court to assess whether the provider of a social plug-in gains access from the operator of the website to information stored in the terminal equipment of a visitor to that website, within the meaning of Article 5(3) of the ePrivacy Directive.

France: Updated CNIL guidance

The French data protection authority ('CNIL') issued, on 4 July 2019, new guidelines on cookies and other online trackers ('the Guidelines'). In particular, the Guidelines outline methods of obtaining consent when using an online tracker, the use of audience measurement trackers, and the configuration of terminal settings. In addition, CNIL highlighted that the Guidelines will be followed by a new recommendation ('the Draft Recommendation'), which will specify the practical arrangements for obtaining consent.

The Draft Recommendation will be created after consultation with professionals and civil society and will then be subject to public consultation. After the Draft Recommendation is published, operators will have six months to adapt to the same.

Key takeaways

1. Consent given for the installation of cookies and similar technologies must be freely given, specific, informed, and affirmatively expressed, as well as independently and specifically provided for each distinct purpose of the processing activity. The user shall always be able to validly exercise their choice and must not suffer any inconvenience in the event of absence or withdrawal of consent.
2. Service providers should establish mechanisms in order to enable users to consent to the placing of cookies at a **granular level**, for each purpose, and for each controller.
3. Neither the fact that a user **continues to browse** a website, using a mobile application, or scrolling through the page of a website or mobile application, nor the use of a **pre-ticked banner**, nor the general acceptance of **terms of use**, can be considered a valid way of obtaining consent.
4. **Refusing and withdrawing** consent must be as easy as it is to provide the same. Service providers must implement user-friendly solutions in order to allow users who have given their consent to the placement of cookies to withdraw the same at any time.
5. Service providers operating cookies and similar technologies shall implement mechanisms to **demonstrate** that they have validly obtained the consent of users, even in the cases when consent is not directly collected by the service provider. In particular, the mere presence of a contractual clause committing one of the organisations to obtain valid consent on behalf of the other party is not enough to demonstrate the presence of valid consent.
6. The practice of blocking access to a website or mobile application for a user who does not agree to be tracked ('**cookie walls**') is to be deemed incompatible with the GDPR.
7. **Analytic cookies and audience measurement technologies** may be regarded as necessary for the provision of the service explicitly requested by the user, and thus can be exempted from the collection of consent. In particular, the exemption applies when, among other things, analytic cookies are implemented by the web publisher by their processor, the user is informed prior to their implementation and is able to object to the same, data collected by tracking technologies are not cross-checked with other processing activities nor transmitted to third parties.

Cookie policy and information

A cookie policy must include information regarding the **identity of the data controller**, the **purpose** of the placing or tracking operations, and the r**ight to withdraw** consent.

A cookie policy shall be drafted in simple and comprehensible terms, since overly complex legal or technical terminology would not satisfy the requirements of clear and comprehensive information.

A cookie policy must be visible and evident at the time of the collection of consent, and a simple reference to general terms and conditions cannot be considered sufficient.

Roles and responsibilities

In the case that several actors participate simultaneously in the placing and tracking of cookies, they may be considered, depending on the specific case, 'single' controllers, joint controllers, or data processors.

In the case of joint controllership, the operators will have to transparently define their respective obligations, in accordance with Article 26 of the GDPR, with specific reference to the demonstration of valid consent.

In the case one of the involved actors act as a data processor, accessing or placing trackers on behalf of the controller, a contractual relationship under Article 28 of the GDPR must be established.

Germany: DSK Guidance

The German Data Protection Conference ('DSK') issued, in March 2019, its Guidance from the Supervisory Authorities for Providers of Telemedia ('the Guidance') which addresses, among other things, consent requirements for cookies and the interplay between the Telemedia Act ('TMG'), the ePrivacy Directive, and the GDPR. In particular, the DSK concludes that Article 5(3) of the ePrivacy Directive has not been implemented in Germany, and that the GDPR has precedence over the TMG and is directly applicable. Furthermore, the Guidance clarifies that its application would not have precedence over possible divergent interpretations, as provided by the European Data Protection Board or through the adoption of the Proposed Regulation on Privacy and Electronic Communications ('the Draft ePrivacy Regulation').

The Guidance states that Article 6 of the GDPR provides for the legal bases for the processing of personal data. In particular, the data subject's consent (Article 6(1)(a) of the GDPR) is of importance with regards to cookies. However, performance of a contract (Article 6(1)(b) of the GDPR) and a successful balance of interests test which proves the legitimate interest of the service provider (Article 6(1)(f) of the GDPR) are further possible legal bases for data processing that apply to cookie practices, in addition to consent.

Key takeaways

1. In accordance with Article 4(11) and Article 7 of the GDPR, consent must be **informed, specific, freely given** and **affirmatively expressed**. It must be an authentic and unambiguous indication of the individual's wishes. The user shall always be able to validly exercise their choice and shall not suffer any disadvantage in the event of absence or withdrawal of consent.
2. **Suitable options to ensure valid consent to data processing** include the ticking of boxes on a website, the selection of technical features, or other forms of declaration of will or active behaviour.
3. In accordance with the principles of Data Protection by Design and by Default (Article 25(2) of the GDPR), different categories of cookies, as well as the cookie provider need to be **confirmed separately**.
4. A prerequisite for consent is that any form of data processing is **transparent and understandable to the user**. Therefore, a data subject needs to receive detailed information about the scope and the consequences of their consent and must also have the option to specifically consent to certain forms of data processing but not to others.
5. **Opt-out processes are insufficient** as they do not respect the requirement of active consent. In accordance with Recital 32 of the GDPR, implied conduct such as silence, inaction, or pre-checked boxes cannot be considered consent.
6. **Cookie banners** providing information about cookies and an 'OK' button, but no option to refuse to the setting of cookies are not considered to be sufficient as consent is not freely given as required under Article 7 of the GDPR.
7. The **lifespan of cookies is not specified** under German law. However, shorter lifespans are more likely to meet the requirements of the balance of interests test between service providers and users under Article 6(1)(f) of the GDPR.
8. An **option to withdraw consent** must be provided and the procedure to withdraw must be as easy as the procedure to consent (Article 7(3) of the GDPR).

Cookie policy and information

The principles of Data Protection by Design and by Default require a cookie policy to be user-friendly.

A cookie policy shall be drafted in simple and comprehensible terms, since overly complex legal or technical terminology would not satisfy the requirements to provide clear and comprehensive information.

Cookie walls are deemed to be incompatible with the GDPR.

Roles and responsibilities

In the case that joint controllers wish to rely on user consent, or when data is transferred to or processed by further controllers, these organisations must be identified and the processing activities of each organisation sufficiently described. In such cases, all actors involved must check whether there is effective consent for their activities and whether this can be demonstrated, in accordance with Article 5(2) of the GDPR.

Germany: DPAs issue statements on consent to cookies and Google Analytics

More recently, seven German data protection authorities ('DPAs') issued, on 14 November 2019, statements ('the Statements') on the use of cookies, consent requirements, and Google Analytics, based on the Guidance to telemedia providers, issued by the DSK.

In particular, the DPAs called upon website operators that utilise services of third parties to assess whether they comply with consent obligations, and highlighted that website operators require explicit consent of the visitor of a website if operators want to utilise the services of third parties, which in turn use the acquired personal data for their own purposes. Specifically, the DPAs stressed that the requirement for consent would also apply to analytical tools if the third party uses the data, as in the case of Google Analytics, as well as more detailed information about the behaviour of website visitors such as keyboard entries, mouse clicks, or swiping movements. In addition, the DPAs stated that it can be considered permissible for website operators to calculate the reach of their website through the number of visitors per page, the devices used and language settings, if this is conducted by a data processor and in accordance with Article 28 of the GDPR. However, the DPAs noted that the data processor may not use the data for its own purposes and highlighted in this regard, that Google Analytics has been developed in recent years in such a way that it no longer constitutes an order processing tool in its current design.

Moreover, the DPAs outlined that website operators must assess their websites promptly with regards to third party content and tracking mechanisms and delete services that require unambiguous consent if they have no valid mechanism in place to obtain it. The DPAs also stated that data processing for which consent is required may only start after consent was given, and emphasised that continued navigation in the framework of a simple cookie banner does not constitute consent, nor does the pre-selection of checkboxes. Finally, the DPAs advised that non-compliance may lead to fines, and that investigations have commenced.

Spain: Updated AEPD guidance

The Spanish data protection authority ('AEPD') released, on 8 November 2019, its Guide on the Use of Cookies ('the Guide'). In particular, the Guide highlights the best practices for providing the information required by Article 22(2) of Law No. 34/2002, of 11 July 2002, on Information Society Services and Electronic Commerce, for the purpose of obtaining lawful consent from the data subject under the GDPR. Moreover, the Guide outlines, among other things, the definition of cookies and similar technologies, transparency obligations, and consent requirements.

Key takeaways

1. Users' consent may be obtained through explicit expression or in other similar terms. In addition, it may also be inferred from an unequivocal action carried out by the user, when the same has been provided with clear and accessible information. However, users' mere inactivity cannot constitute valid consent.
2. Consent must be **freely given, informed, unambiguous**, and **actively provided**. A user must also always be able to withdraw consent.
3. A user navigating a website in order to manage their cookie preferences is not providing valid consent.
4. When a cookie policy is presented through layers, consultation of the second layer cannot be deemed as a valid way to obtain consent.
5. When a cookie policy is presented through layers, consent can be deemed to have been given in a valid manner when the user **continues browsing the website,** an activity which includes:
    - **using a scroll bar**, when information on cookies is visible without the use of a cookie banner;
    - **clicking on certain content links** within the website; and
    - swiping the screen to provide access to website content in devices such as mobile phones and tablets.

Cookie policy and information

A cookie policy shall include, among other things, definitions and generic functions of cookies, the type and the purpose of cookies used, the identification of the operator installing and using cookies, information on how to manage consent, information on data transfers to third countries made by the service provider, and the retention period of the data.

A cookie policy shall indicate if consent is given only for the web page on which it is being requested or if it is also provided for other web pages of the same service provider, or of associated third parties.

The information provided in the cookie policy must be **concise, transparent, intelligible**, and **easily accessible**. The language must also be **clear and simple**, in order to avoid expressions that may confuse or distort the message.

The Guide suggests the provision of the requested information through **layers**, where the first layer contains essential information, while the second presents more detailed indications on the use of cookies.

UK: Updated ICO guidance

The Information Commissioner's Office ('ICO') issued, on 3 July 2019, its updated Guidance on the Use of Cookies and Similar Technologies ('the Guidance'). In particular, the Guidance addresses the requirements for valid consent to cookies, the relationship between the Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PECR') and the GDPR, as well as how to comply with cookie rules.

Key takeaways

1. Consent for non-essential cookies, as required by Section 6(2) of PECR, implies a clear and affirmative action taken by the user, since a failure 'to engage with the consent box cannot be said to consent to the setting of these cookies.'
2. The fact that the user **continues to use the website** cannot be considered a valid way of expressing consent. If users do not click on any of the options available in the cookie banner and go straight through to another part of the website, the placement of non-essential cookies on the users' terminal equipment would not constitute valid consent.
3. Service providers must ensure that any established consent mechanism allows users to have **control over all the cookies** the website places, since the implementation of a consent mechanism that works only for some of the cookies would not be compliant with PECR.

4. The service provider may not need to ask for new consent each time a user visits the website. However, different factors need to be taken into account, such as the frequency of visits, as well as updates of content or functionality. As a result, in some cases the user may need to '**reconsent**' to cookie settings, such as in the case that the service provider is setting non-essential cookies from a new third party.
5. **Analytics cookies** are not exempt from PECR requirements, since they are not part of the functionality that users request when they use online services. As a result, they are not strictly necessary and require consent.
6. **Cookie walls** which attempt to require or influence users to agree to the processing of their personal data by the service provider or any third parties as a condition for accessing the service must not be considered a valid way of obtaining consent. Individuals shall be provided with a genuine free choice, and consent should not be bundled up as a condition of the service, unless it is necessary for that service.

Cookie policy and information

1. The information to be provided to users in accordance with Section 6(2) of PECR shall cover the kinds of cookies the service provider intends to use, the purposes for which they will be placed, and the duration of the same.
2. Information requirements also apply to cookies set by any **third parties**. A proper way of displaying cookies could be a long table or detailed list of all the cookies operating on the site.
3. A cookie policy and information must be provided in such a way that users will see it when they first visit a service. In this regard, the service provider should consider the design the online service in order to ensure the visibility of the link to the policy.
4. The service provider shall take into account different levels of users' understanding, making a particular effort in order to explain the use of cookie activities in a **clear and comprehensive** way.

Roles and responsibilities

1. Where the website sets third-party cookies, both the service provider and the third party have a responsibility for providing users with clear information about cookies in order to obtain consent.
2. Service providers using third party cookies must **clearly** and **specifically** name who the third parties are and explain what they will do with the received information.
3. Third parties willing to set cookies, or to provide a product that requires the placing of cookies, should include a **contractual obligation** into the agreements with web publishers and ensure that user consent was validly obtained.

Future harmonisation

The European Commission adopted, on 11 January 2017, the Draft ePrivacy Regulation, which would replace the ePrivacy Directive and is currently under consideration.

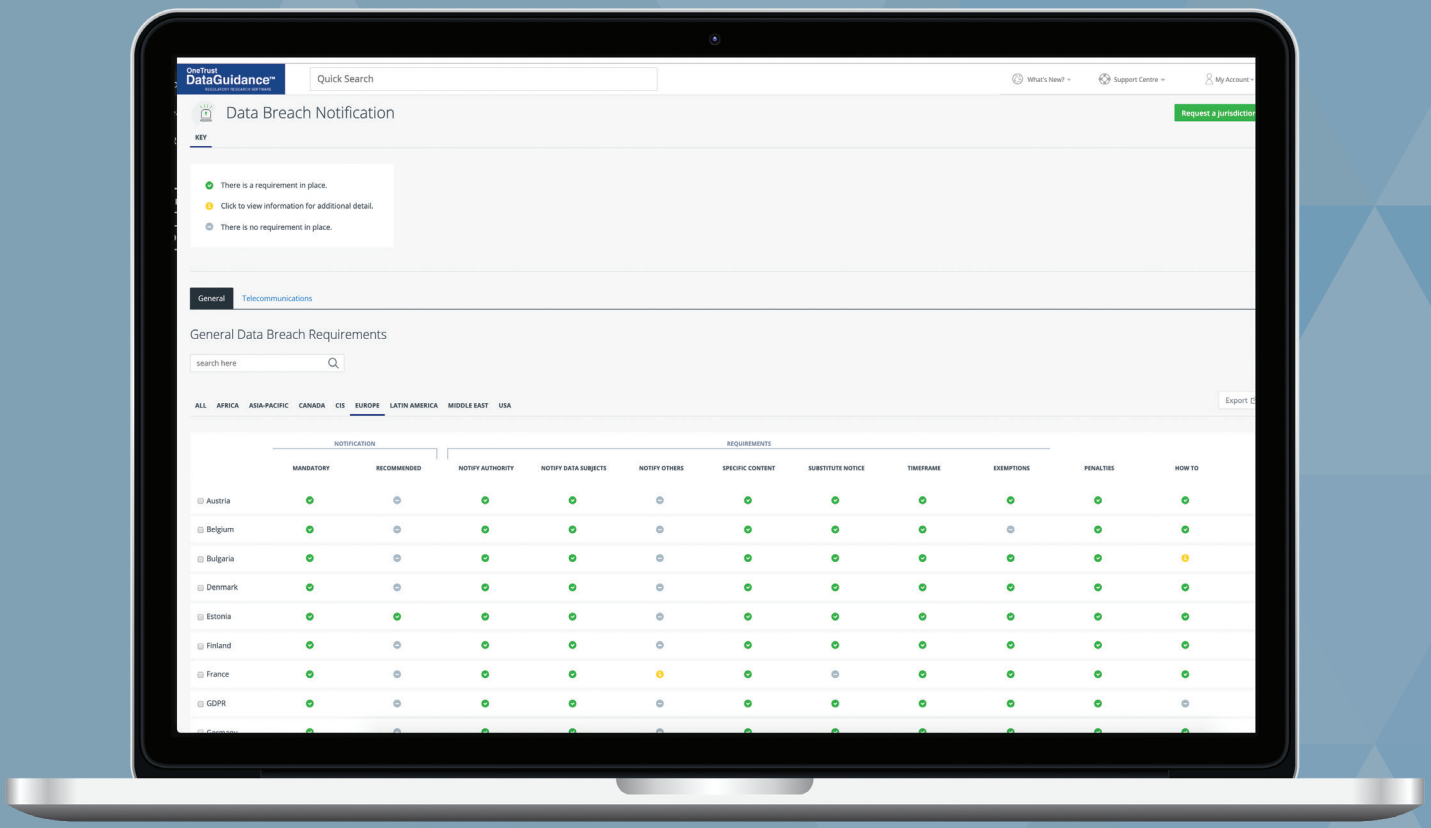
The adoption of the Draft ePrivacy Regulation would harmonise the applicable European legislation among Member States. In particular, the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment would be regulated under Article 8 of the Draft ePrivacy Regulation, while consent requirements would be regulated under Article 9 of the Draft ePrivacy Regulation.

Global Regulatory Research Software

40 In-House Legal Researchers
500 Lawyers Across 300 Jurisdictions

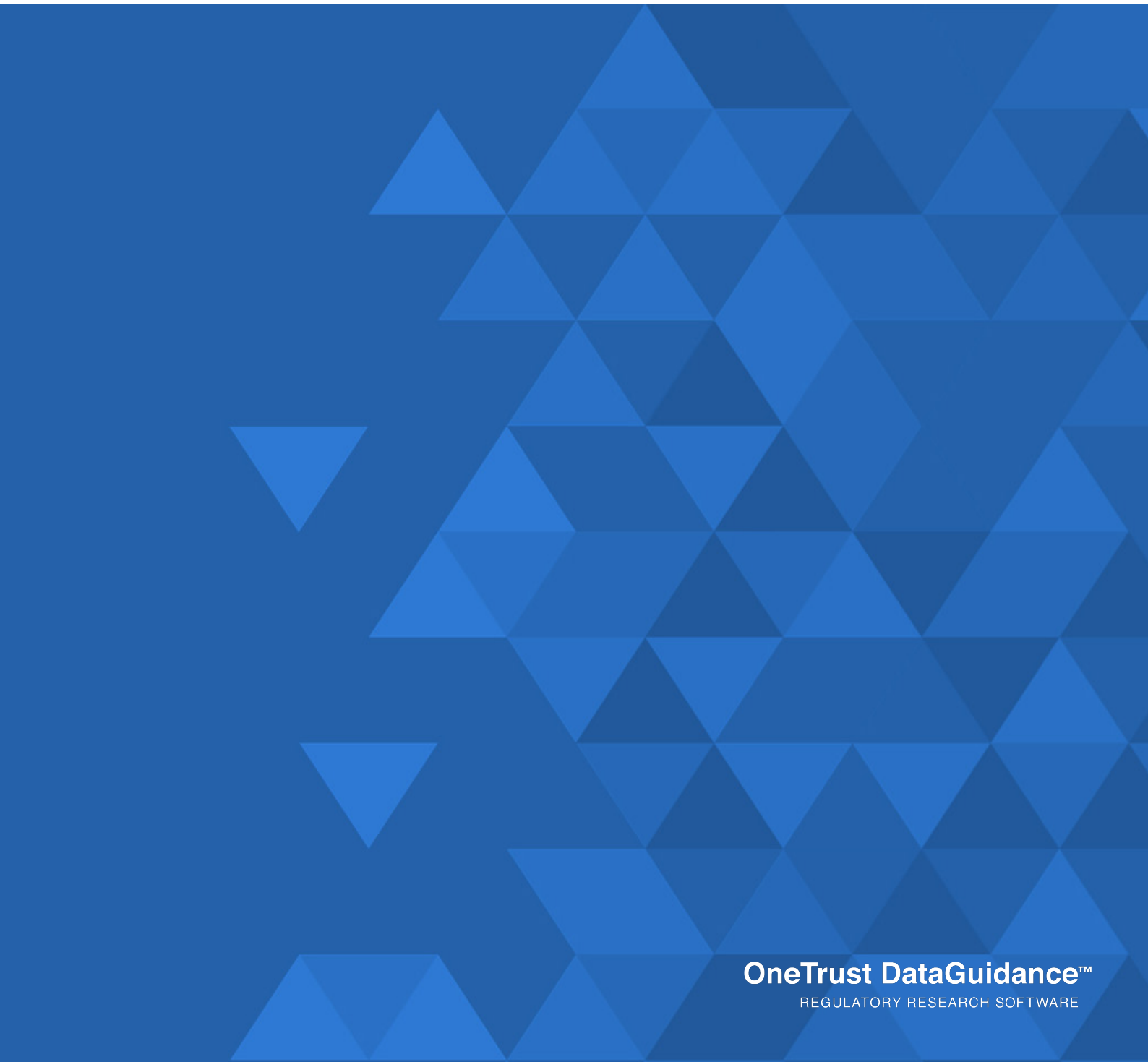
With focused guidance around core topics, Comparison Charts, a daily customised news service and expert analysis, OneTrust DataGuidance provides a cost-effective and efficient solution to design and support your privacy program

- Legal Guidance & Opinion
- Law Comparison Tools
- Breach & Enforcement Tracker
- Ask-An-Analyst Service



SCAN TO ACCESS
FREE TRIAL
Use your camera or a QR code reader

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE


OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE