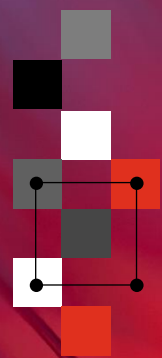
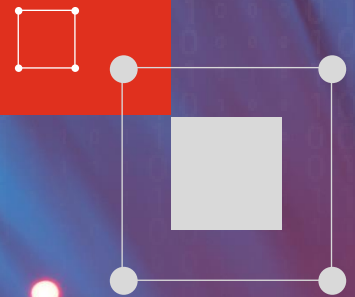
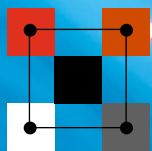


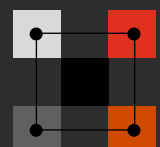
White Paper on User Consent Practices under EU Regulatory Requirements

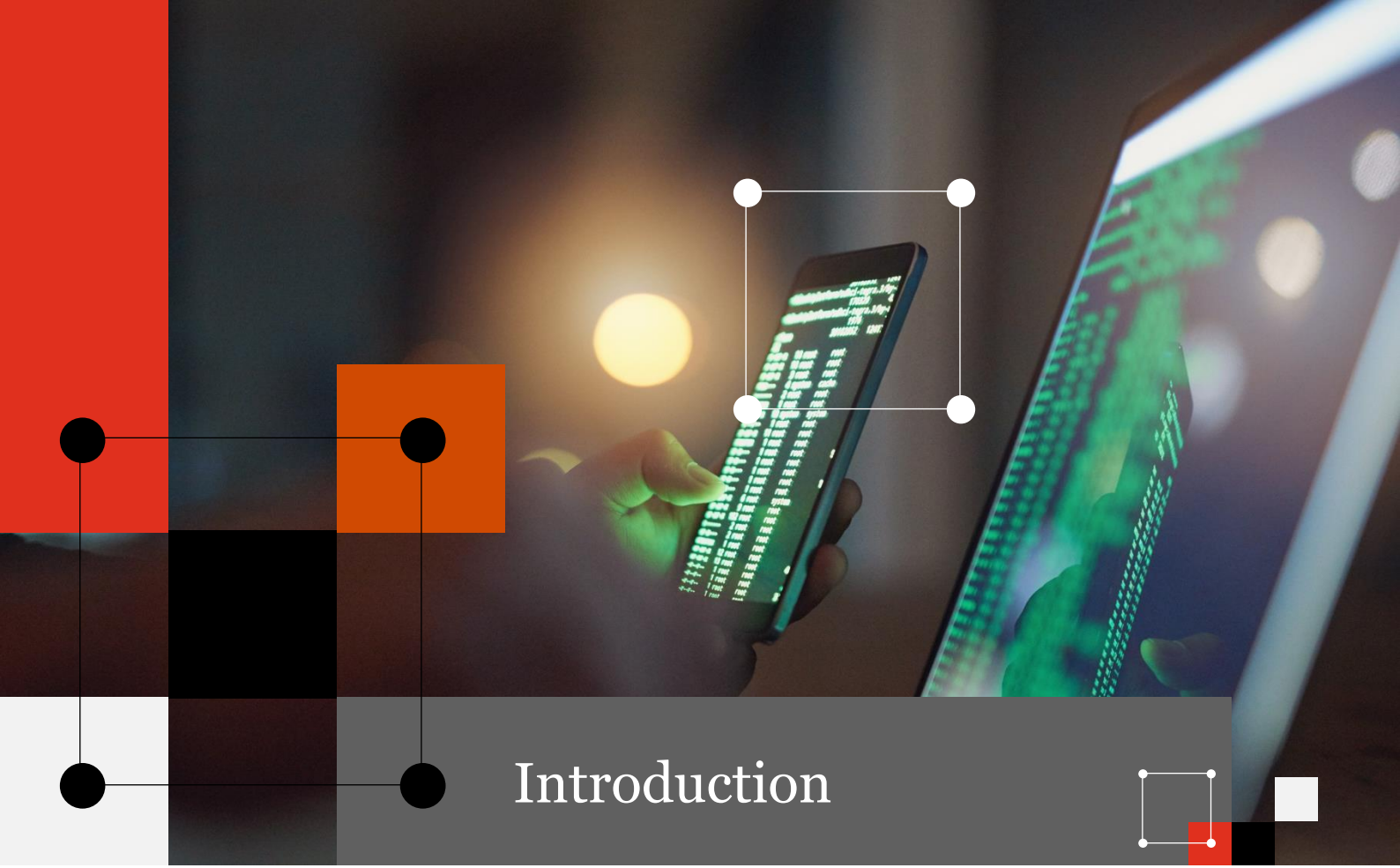




Contents

Introduction	02
Chapter 1: What are the GDPR's and ePD's user consent requirements for businesses?	04
Chapter 2: How to build an effective and compliant consent banner for the EEA?	10
Chapter 3: Q&A	20
Conclusion	21
Contacts	22





Introduction

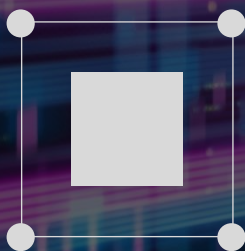
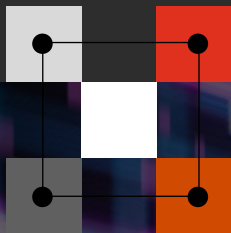
The General Data Protection Regulation (GDPR), implemented by the European Union, has established a global trend towards stricter data protection laws, granting consumers greater privacy rights. It is important for companies operating in the European Economic Area (EEA) to comply with privacy protection regulations to avoid significant penalties (administrative fines up to 20,000,000 EUR or up to 4% of the total worldwide annual turnover), which can severely impact their financial position, reputation, and consumer trust. Therefore, it is recommended that organisations enhance their data protection compliance capabilities to align with EEA regulations. By doing so, they can mitigate legal and economic risks, ensuring the continuity of their business. GDPR-compliant

organisations can also inspire trust from consumers, enhance their brand image, and foster greater customer loyalty.

GDPR is widely recognised as a major milestone in privacy legislation and has had a profound impact on the regulations governing the digital advertising industry. The legislation imposes restrictions on businesses that collect and process personal data from EU IP addresses. Similarly, after Brexit, the United Kingdom General Data Protection Regulation (UK-GDPR) and Data Protection Act 2018 affect how businesses, as website or application owners, must obtain and store user consent. Therefore, the same requirements apply in the UK as in the GDPR.

Advertisers and publishers are required to obtain clear and explicit consent from users, which can be withdrawn at any time, regardless of whether the service provided by the business is via a website or an app. Hence, it is crucial for businesses to have a thorough understanding of their legal obligations. This white paper provides a comprehensive overview of the EU regulatory requirements for obtaining user consent and offers examples of good practices.

- Chapter 1 provides a general interpretation of GDPR and ePrivacy Directive (ePD) requirements regarding user consent. It includes examples and in-depth explanation of relevant case studies related to topics such as cookies or personalised advertising.
- Chapter 2 is a practical guide on how to build an effective consent banner in compliance with EU regulations.
- Chapter 3 lists frequently asked questions shared by our customers and our responses to those questions.



Chapter 1: What are the GDPR's and ePD's user consent requirements for businesses?

While ePD emphasizes the consent requirement of cookies or similar technologies, the GDPR provides general principles regarding consent for personal data processing activities. And in its guidance on “consent” under the GDPR, the European Data Protection Board (EDPB) clarifies that the conditions for obtaining valid consent under the GDPR also apply to situations within the scope of the ePD. So, we focus more on the consent requirements of the GDPR. As required by GDPR, businesses must have a legal basis for processing personal data, with consent from the data subject¹ being the most commonly used legal basis. As defined by the GDPR, personal data means any information relating to an identified or identifiable natural person (“data subject”), such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. Overall, if consent is used as the legal basis for data processing in your company website or App, it is essential to comply with the following requirements regarding user consent.

1 Obtaining valid user consent

To be considered “valid”, the consent given by the data subject must meet certain criteria. It should be freely given, specific, informed, and indicate unambiguously that the data subject wishes to agree, by a statement or by a clear affirmative action, to the processing of personal data. Four key elements should be noted:

- **Freely given:** The “free” aspect of the requirements implies real choice and control on the data subjects’ part. Any inappropriate pressure or influence exercised upon the data subject (which may be manifested in many different ways) preventing them from exercising their free will shall render the consent invalid.
- Consent cannot be bundled up as a non-negotiable part of terms and conditions.

¹ A data subject is defined by GDPR as an “identified or identifiable natural person” from whom or about whom information is collected.



Example: A website provider sets up a script that will block content from being visible unless the data subject agrees to a request to accept cookies and the information about which cookies are being set and for what purposes data will be processed. There is no option to access the content without first clicking on the “Accept cookies” button. Since the data subject is not presented with a genuine choice, their consent is not freely given.

- Consent should not be provided in a bundle of processing purposes. Instead, data subjects should be free to choose which purposes they accept or decline.



Example: Using the same consent request, a retailer asks its customers for consent to use their data to send them marketing materials by email and sharing their details with other companies within their group. This consent request is not granular, as there are no separate choices for these two purposes, therefore the consent is not considered valid.

- Refusing to give or withdrawing consent cannot be detrimental to data subjects (e.g., in the form of additional cost and downgraded service quality).

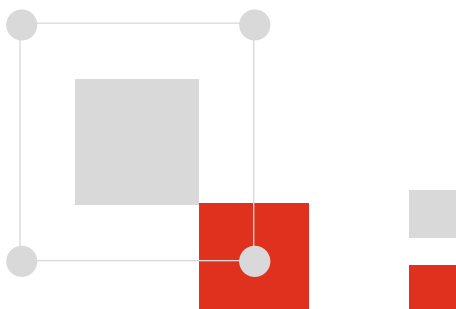


Example: A customer subscribes to a fashion retailer’s newsletter offering general discounts. The retailer asks the customer for consent to collect their data on shopping preferences for the purpose of tailoring the offers based on their preferences, shopping history, or information collected from a voluntary questionnaire. When the customer later withdraws consent, he or she should still receive the same discounts without personalised marketing information.

- **Specific:** The “specific” aspect aims to ensure a degree of user control and data transparency. Consent from data subjects must be obtained for a specific processing purpose without function creep, and users should be informed of that specific purpose. If consent is sought for different purposes, separate options should be provided for each purpose to allow users to give specific consent for each one.



Example: A game App collects users’ personal data, with their consent, to provide personalised suggestions for game content based on their operating habits. If the application later decides to enable third parties to send or display targeted advertising based on the subscriber’s habits, new consent is required for this new purpose.

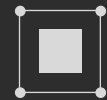


- **Informed:** The “informed” aspect requires providing information to data subjects prior to obtaining their consent, thus enabling them to make informed decisions. The request for consent should be clearly distinguishable from other matters and presented in an intuitive and easily accessible form using clear and plain language. For example, information relevant for making informed decisions on whether or not to give consent should not be hidden in the general terms and conditions.

The minimum information to be provided for obtaining a valid consent includes:

- i. the controller’s identity;
- ii. the purpose of each of the processing operations for which consent is sought;

- iii. the type of data to be collected and used;
- iv. the existence of the right to withdraw consent;
- v. information about the use of the data for automated decision-making in accordance with GDPR Article 22 (2)(c)² where relevant;
- vi. on the possible risks of data transfers to a third country in the absence of an adequacy decision from the European Commission and of appropriate safeguard measures as described in GDPR Article 46³, where relevant.



² Required by GDPR Article 22 (2): The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, unless there is a legal basis for one of the three following: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or (c) is based on the data subject’s explicit consent.

³ Required by GDPR Article 46: The controller or processor should provide appropriate safeguards before transferring personal data to a third country or an international organisation.



- **Unambiguous indication of wishes:**
To be valid, consent requires an unambiguous indication by means of a statement or by a clear affirmative action. Consent can be collected through written or oral statements, including through electronic means. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service, cannot be considered as an active indication of choice. Therefore, it is important to ensure that user consent is collected in a way that allows for easy feedback. This can be achieved by providing buttons or unticked boxes. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal data. Businesses should design their consent mechanism in ways that are clear and unambiguous to data subjects, while ensuring that the action by which consent is given can be distinguished from other actions.



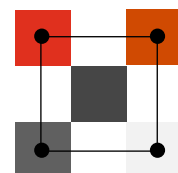
Example: When users visit a website for the first time, they are informed that cookies are used to collect information about their interactions. This information is used to improve and customise their browsing experience. By clicking the “Accept” button, the user is able to validly perform a “clear affirmative action” to consent to the processing. Users also need to be provided with a “Decline” button and the information regarding their interactions should no longer be collected when they click “Decline”.

2 “Explicit” consent should be obtained under certain circumstances

If consent is used as legal basis in the following situations, an “explicit” consent is required. Explicit content, which tends to be stringent than regular content, should be required in the following situations:

- processing of special categories of personal data as defined in Article 9 of GDPR, including the personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or membership status in a trade union, genetic data or biometric data for the purpose of uniquely identifying a person, data concerning health or data concerning a person’s sex life or sexual orientation;
- personal data processing for automated individual decision-making, including profiling⁴ ;
- personal data transfers to third countries or international organisations in the absence of adequate safeguards.

⁴ Means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.



We recommend consulting with a professional third party for a detailed analysis regarding the above scenarios.

To obtain the explicit consent of a data subject, companies may consider using one of the following methods:

- **Written statement:** The data subject expressly consents by providing a written statement, which may require a signature where appropriate.
- **Digital or online context:** In this scenario, consent of a data subject can be expressed through filling in an electronic form, sending an email, uploading a scanned document carrying the signature of the data subject, or using an electronic signature.
- **Verification of consent in two stages:** Consent can be verified in two stages to ensure its authenticity and validity.

To avoid compliance issues, it is advisable to refrain from using the aforementioned special categories of data and precise location data for advertising purposes.



3 Additional requirement to obtain children's consent

According to GDPR, additional requirements apply when processing the personal data of vulnerable individuals, especially children. Such protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. For websites or apps that target children, companies should pay attention to the additional requirements as far as consent-based data processing is concerned:

- When the child is below the age of 16 years (may be different based on individual country's law within the EEA), such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.
- Reasonable efforts should be made to verify in such cases where consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

To minimise any potential compliance issues, it might be advisable not to implement personalised advertising to children altogether.

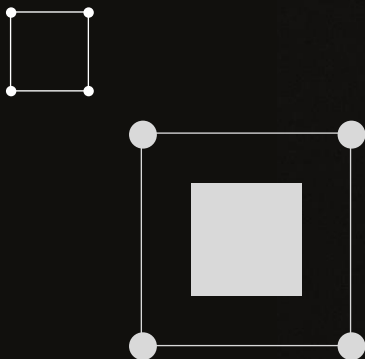
4 Consent withdrawal requirement

Article 7(3) of GDPR prescribes that the data subject has the right to withdraw his or her consent at any time. Some specific requirements related to consent withdrawal are as follow:

- Data subjects should be able to withdraw their consent as easily as they provide it. For example, if consent is obtained through the use of a service-specific user interface via a website or an app, it must contain the option to withdraw via the same electronic interface.
- The withdrawal of consent should be free of charge and not result in a lowering of service quality.
- The data subject must be informed of the right to withdraw consent as a part of the information required to be provided for obtaining a valid consent.
- If the data subject withdraws consent, the processing of data must be terminated immediately. If there are no other lawful basis, such data must be deleted.

5 Consent record requirement

In Article 7(1), the GDPR clearly outlines the explicit obligation of the controller to demonstrate a data subject's consent. In other words, companies should maintain a record of consent obtained from data subjects. For as long as a data processing activity in question lasts, the obligation to demonstrate consent remains applicable. After the processing activity ends, proof of consent should be kept no longer than strictly necessary for compliance with a legal obligation or for the establishment, exercise, or defence of legal claims.



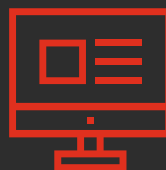
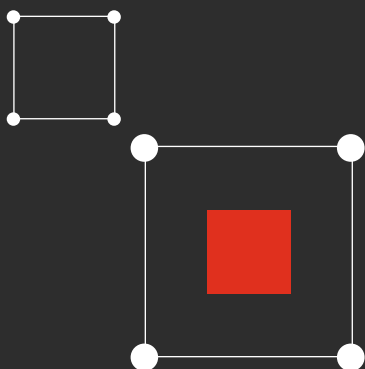
Chapter 2: How to build an effective and compliant consent banner for the EEA?

1 Best practices for building a good website consent banner



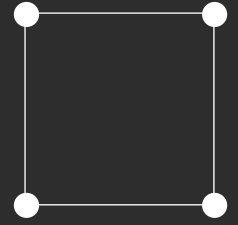
Step1: Understand regulatory requirements regarding user consent.

You can refer to Chapter 1 for an overview of regulatory requirements in EEA and UK regarding user consent. Please note that these are general requirements and there can also be other legal differences (e.g., the age at which a person is considered to be a child).



Step2: Audit your website to identify cookies and other trackers.

Conduct a thorough scan of your website to learn about cookies, beacons, and other tracking technologies being used on your website. Verify that the use of cookies complies with your privacy policy or the privacy policy of the third-party website where the cookies are placed. Auditing your website allows you to automatically detect and classify cookies and tracking technologies, enabling consumers to understand and make informed choices. Cookies generally have the following types: strictly necessary, functional, statistical, marketing, etc. Only strictly necessary cookies can use implied consent, granular options for accepting or rejecting other types of cookies should be available to the user. This is explained further in Step 3.



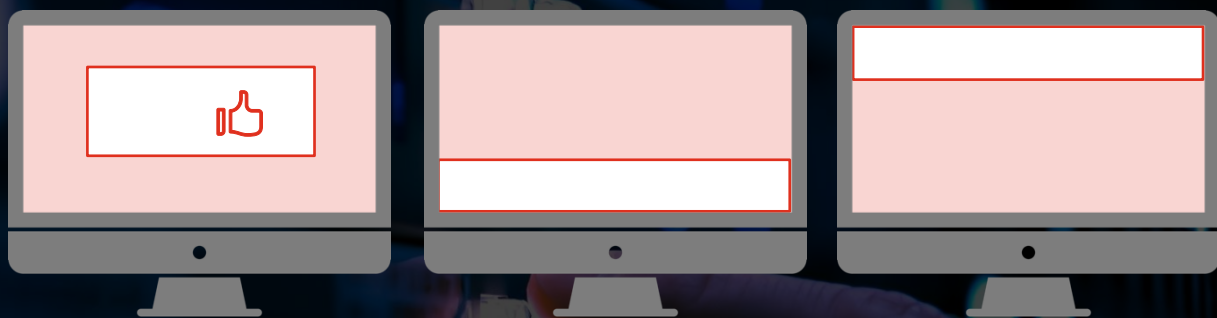
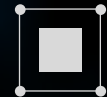
Step3: Design and set up your banner.

When designing your consent banner, you may need to consider how you can enhance the user experience and potentially increase the user consent rate while still meeting regulatory requirements. However, additional requirements should be based on guidance issued by local data protection authorities. Relevant guidance can also be found on some consent management platforms. Here we offer some practices:


- **Banner position:** The placement of the banner is the key factor that affects the consent rate. It is commonly placed in the middle of the webpage, the footer of the website, and the top of the webpage. Placing the banner in the middle tends to attract more attention. Industry research had found that the position of the consent layer in the middle of the website had the highest consent rate.

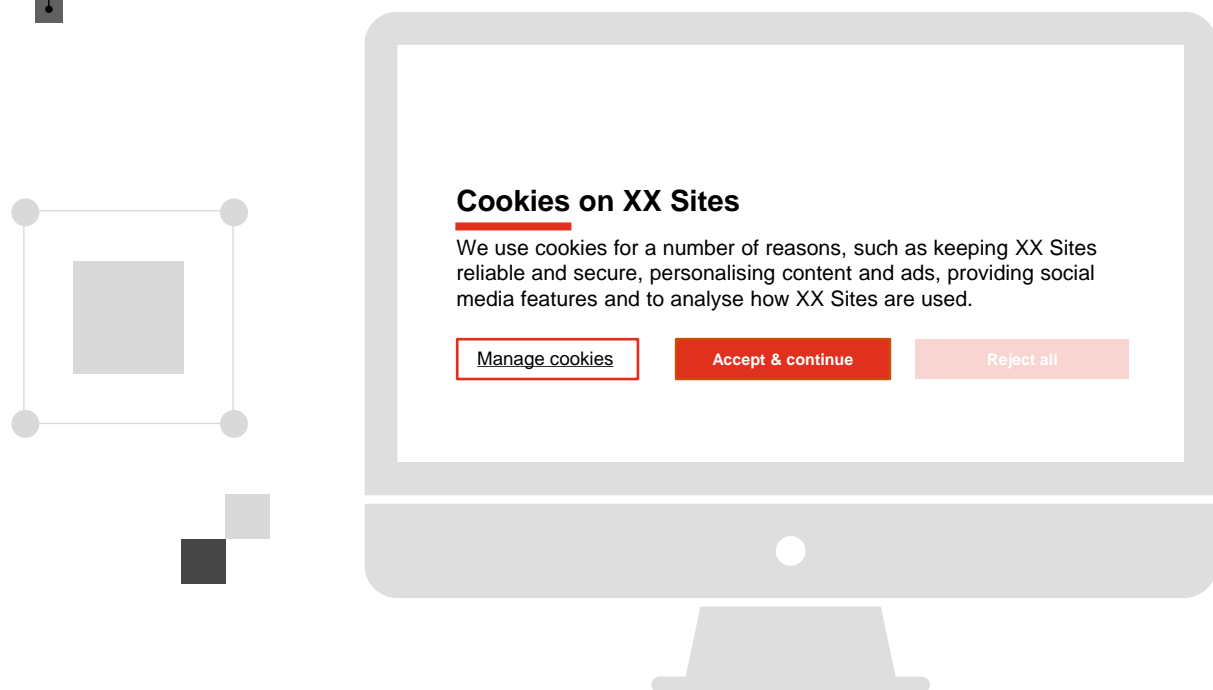


Figure 1: Position of the 3 main categories banner



- Content: Fully consider the compliance requirements regarding user consent as explained in Chapter 1. Inform users about cookie usage in plain and jargon-free language. The following steps are advised:
 - Clearly identify your organisation. Display your company name or logo on the banner; if your website shares the data collected through cookies with third parties, such as advertising or analytics partners, the consent banner should inform users about such data sharing practice;
 - Describe what (type of) data will be collected and used;
 - Explain the purposes for data processing. For example, use cookies to serve users relevant promotions (marketing) or to give users a better experience of the website (functional);
 - Communicate the right to withdraw consent at any time and the withdrawal method;
 - Link to website cookies and privacy policies; we also recommend that the consent banner link to a list of vendors with whom they share this data.
- Button: Display “Accept” and “Reject” or words with similar meanings buttons on the banner in a clear way. Only when the user actively clicks “Accept” can it be regarded as valid consent. However, some studies show that the consent rate of this setup is relatively low because users will often say no if they don’t understand the implications of such action. The “Accept + Settings” combination shows the highest acceptance rate. You can also increase user consent with a pleasant or trusting tone of voice. For example, the use of “Please accept!” and [website name] values your privacy” can increase the acceptance rate of users to a certain degree.

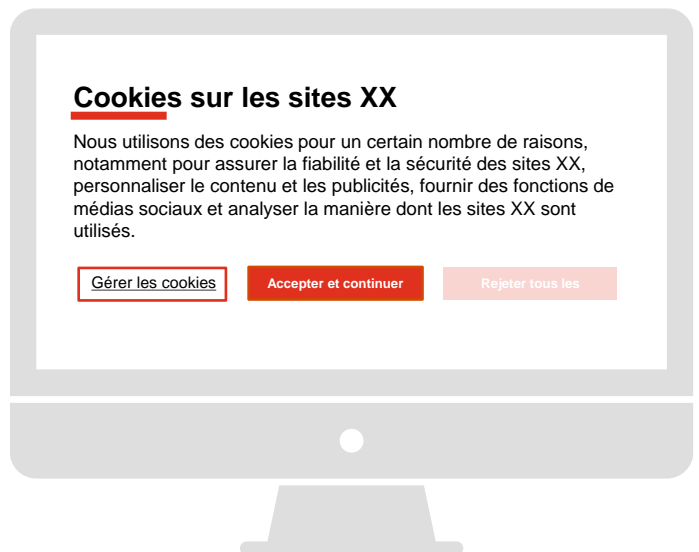
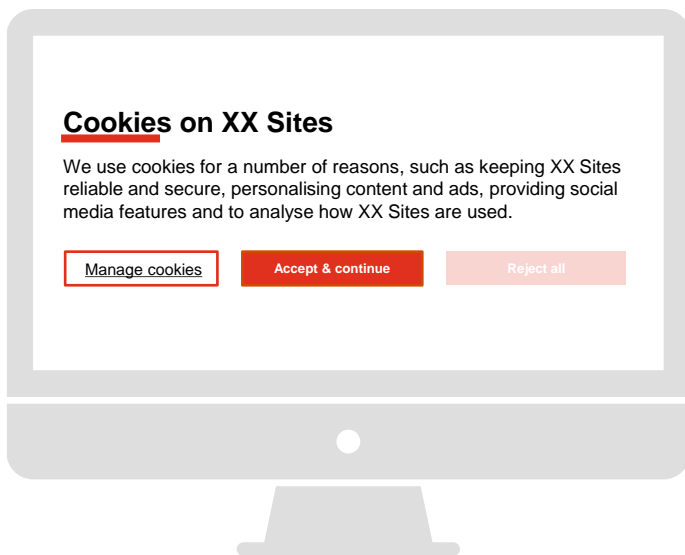
 Figure 2: Good practice for buttons on consent banner



- **Colour:** You can customise consent banners' colours to match the business's brand style. In terms of font colours, try reversing the theme (dark background and bright text, rather than bright background and dark text), this could influence the agreement rate positively. For example, unlike the text on the "Decline" button, the "Accept" button can be darker in colour with border font and shows an icon in a convenient position.
- **Font:** Generally, the title text, such as the name of the organisation and button text, should be large enough for viewing; the text describing the purpose of collecting information should be in a smaller font and should not be too long or too short in length; the links to the privacy policy and cookie policy should also be distinguished by different fonts (e.g., italic, bold, etc.) and colours.
- **Language:** Display banners in local languages depending on the country or jurisdiction where the site is hosted, allowing users to understand the content effectively.



Figure 3: Practice reference for different language display



- Consent management mechanism:
 - After the consent banner, users can access the consent management interface via a “Manage my cookies” button or link. Users should be given the option to choose which cookies they want to accept before their personal information is collected. As mentioned in Step 2, classifying the cookies, and informing the user about the role of each category of cookies. Except for strictly necessary cookies,

all other types of cookies require users to actively tick the box.

- You should have a clear and simple opt-out mechanism. Users must be able to withdraw their consent any time. You may provide users the link to cookie management in the footer of the web page. After the cookie pop-up window appears, users should be able to enter the webpage in a simple way to access cookie settings, such as changing consent preferences.



Figure 4: Practice reference for consent management mechanism

Cookies on XX Sites

We use cookies for a number of reasons, such as keeping XX Sites reliable and secure, personalising content and ads, providing social media features and to analyse how XX Sites are used.

[Manage cookies](#) [Accept & continue](#) [Reject all](#)

We use cookies for a number of reasons, such as keeping XX Sites reliable and secure, personalising content and ads, providing social media features and to analyse how our Sites are used. [Manage cookies](#)

Manage Cookies

You can manage which cookies are set on your device, but if you disable cookies, some part of the XX site may not work properly. Some cookies are essential for the operation of our sites. By clicking the Save button below you are accepting cookies in accordance with our [Cookie Policy](#).

What cookies does this toggle cover?
Please [sign into your account](#) before submitting your preferences to ensure these changes are applied across all of your device

<p>Allow</p> <p>See personal advertising and allow measurement of advertising effectiveness <input type="radio"/></p>	<p>Block</p> <p>Block personalised advertising and measurement of advertising effectiveness <input type="radio"/></p>
---	---

[Save](#)

If you turn this off, you will still see the same number of adverts but they may be less relevant.

Third party technology that helps us deliver other functionality

We used third party cookies to optimize marketing performance and to measure the effectiveness of our advertising on other websites. Due to technical limitations please follow the links below for each provider's policies and instructions to opt out. You will need to make these changes on every browser you use.

XXXXXX(third party)	XXXXXX is a digital measurement platform that enables us to monitor advert viewability and analyse invalid traffic.
---------------------	---

Other ways to opt out

Alternatively, you can manage cookies via your browser settings or by using the below two links: this will impact your cookie settings across the Internet, not just on XXXXX:

[Your Ad Choices](#)
[Your Online Choices](#)

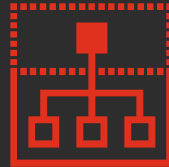
Some advertisers and third parties will personalize adverts based on data you have provided to them, to the extent that you have consented to this. To fully understand how these third parties process personal information, please review their policies. You can manage your cookie settings with these partners by visiting the links below.

For more details of the cookies used for advertising please visit: XXXXXX website



Step 4: Double check.

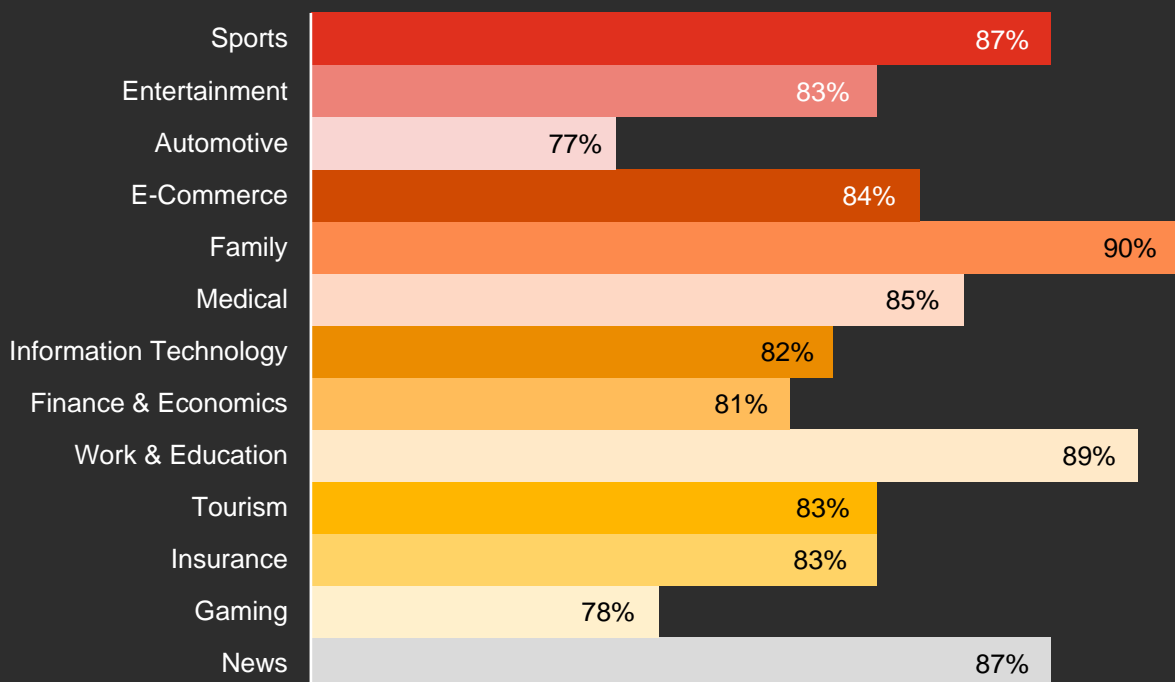
You should ensure trackers are automatically blocked until user consent is obtained. Ensure that banners are set, and that cookies are executed in a manner consistent with your public privacy policy. Show the right consent banner to the right person at the right time.



Step 5: Measure success.

Once you have a basic banner set up on your website, it is also important to monitor the approval rate using an interactive dashboard. If opt-ins are low, it's time to do some testing. Through A/B testing, experimentation, and easy testing of template design, layout, copy, CTA, text, colour, and so on, you can determine which changes produce the highest conversion rate. According to the practice of some consent management platforms, the consent rate varies considerably across industries, as shown below.

Figure 5: Consent rate of major industries⁵



⁵ Source: Statistical analysis of more than 1 billion consent layers across 15,000 websites using the consent manager platform from Consent Manager.

2 Best practices for building a good APP consent banner

Since APP consent is a much more complex topic, we just give some general advice for reference here. Further guidelines should refer to the requirements for developers provided by the APP distribution platform, such as Google Play's guidance or Apple App Store's guidance. And it is very important to start thinking about privacy by design before development itself.

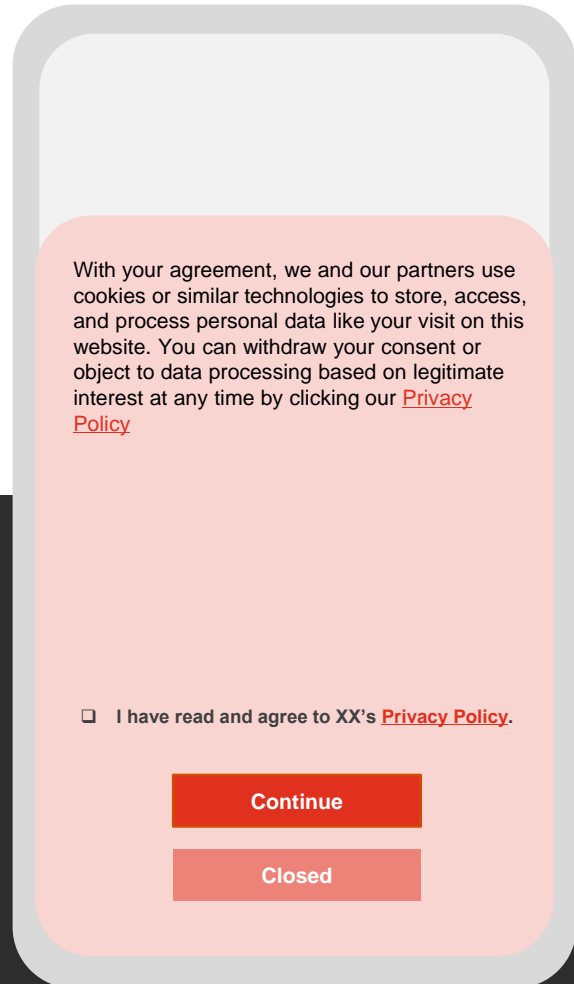


Step 1: Understand regulatory requirements regarding user consent.

For APP providers, the regulatory requirements you need to comply with to publish your app in the EEA and UK are the same as those mentioned in Chapter 1. Additionally, you need to comply with the privacy policy of the application platform where your APP will be published.



Figure 6: Practice reference for App



Step 2: Audit services and APIs for compliance in your APP.

Perform a thorough scan of the app and consider GDPR obligations when integrating your app with third-party services or APIs. These details need to be documented in your privacy policy.



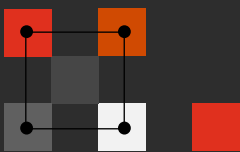
Step 3: Design and set up a consent banner or consent box on APP.

If you choose consent as the legal basis of processing the data on the APP, user consent should be obtained before any processing at the first time. We strongly recommend displaying a consent screen (the form of banner, box, etc) on app launch as this is the only way to be fully GDPR compliant.

When providing an app on iOS devices, it is necessary to follow the additional requirements regarding App Tracking Transparency⁶. Obtaining user consent for Application Tracking Transparency (ATT) is a distinct process from obtaining user consent to comply with GDPR regulations.

Same as with the consent banner on the website, you need to make similar settings for content, button, colour, font, and language. (Not to be repeated here.)

- Position: It is recommended that the APP pop-up window be placed in the middle or lower part of the screen, so that it is easier to attract the user's attention as well as convenient for the user to click.



- Consent management mechanism:
 - You can select a sidebar or menu item to link to the interface for managing privacy and data collection. Show users your privacy policy, information about the types of data being collected, and allow them to change their consent choices. Additionally, you should provide users with the option to or not to enable personalised advertising on the setting page.
 - Similarly, with a GDPR-compliant mobile App there should also be a dedicated page where the user can opt out of communication with the App or ask for their data to be deleted. The entry to this page should be simple and clear.
 - In addition, it is necessary to implement other GDPR-required compliance measures, such as providing mechanisms for data subjects to exercise their rights. We recommend consulting with a professional third party for a detailed analysis regarding the further scenarios.

⁶ You need to receive the user's permission through the App Tracking Transparency (ATT) framework in order to track them or access their device's advertising identifier. More information please refer to the Apple.



Step 4: Double check.

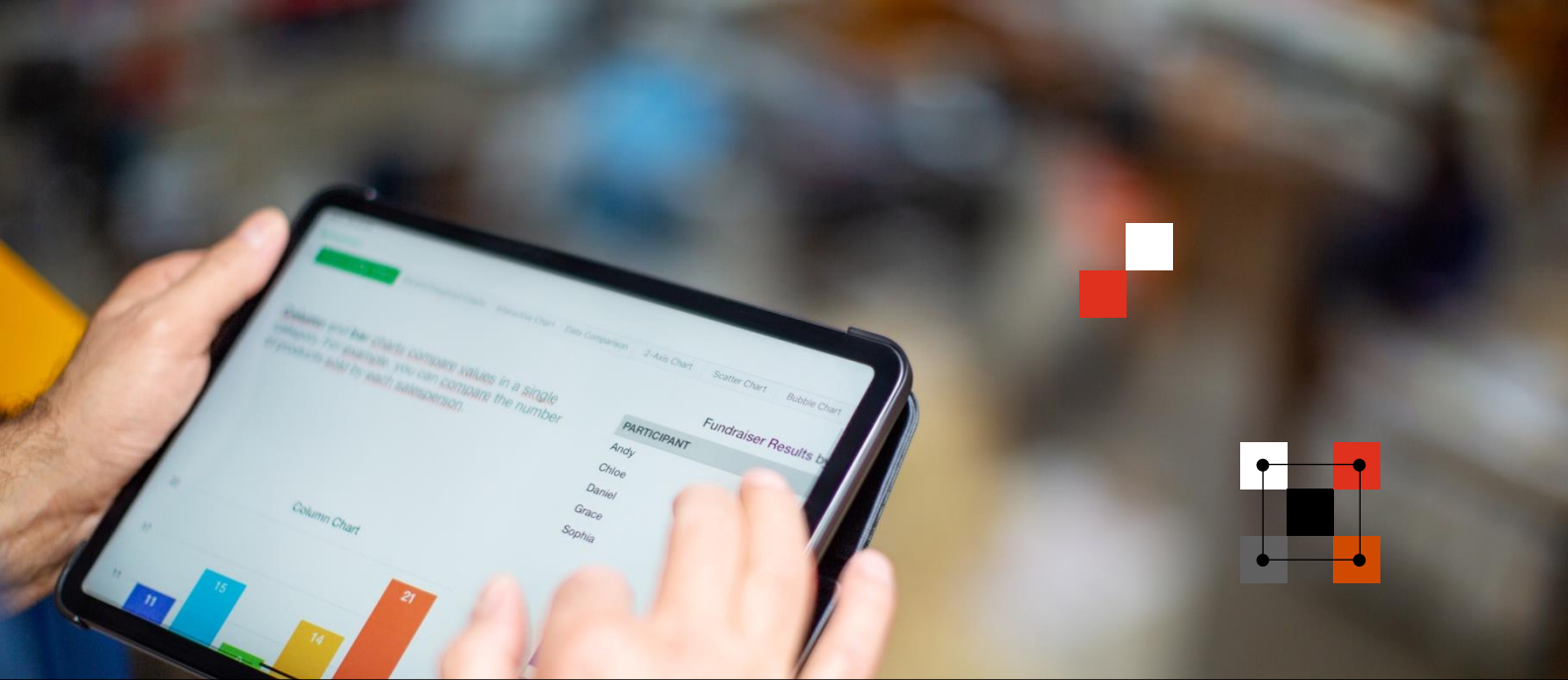
User information cannot be captured until consent has been obtained from the user. Make sure that the app's data collection is performed in a way that is consistent with your privacy policy.



Step 5: Measure success.

Finally, you also need to monitor the consent rate on the app and test it with the suitable methods to find the changes that will have a positive effect.





3 Checklist for a compliant consent banner

The following checklist might help you avoid common mistakes when implementing consent banners:

- Have you checked that your consent notification is displayed when users from all EEA countries visit your website or app?
- Have you automatically blocked trackers before obtaining user consent?
- Have you clarified to users what personal data is being collected and why when users consent to the collection of their personal data on your website or app? (e.g. are they aware that their personal data will be used for personalised advertising?)
- Have you informed users who will use the data (including third parties) and for how long?
- Have you provided separate consent options for each purpose, rather than bundling consent to cover multiple purposes or activities?
- Does the user have the option of taking a clear and positive action to indicate consent, i.e. by clicking on the “OK” button or the “I agree” button?
- Have you provided an easy access for users to modify their consent preferences or withdraw consent in the future?
- Have you recorded and stored this consent data to be used to verify user consent in case of an audit by a data protection authority (DPA) after obtaining it?



Chapter 3: Q&A

? Can I present an “accept” button alone?

... According to GDPR, you need to provide an opt-out option for users. You should present both “accept” and “reject” button, or present only “accept” button but also allow users to enter a “manage cookies” page to set their cookie preferences.

? What if I don’t allow the user to play the game if no consent is given?

... For a consent to be valid, it must be “freely given” by a user, which means consent to process personal data that are not necessary for the performance of a contract or service cannot be tied to the provision of that contract or service. Therefore, it is not suggested to bind the basic service purpose (play the game) with advertising purpose for a user to consent together.

? Do I need to include all third parties?

... Yes, under GDPR you should include all third party vendors that you will be sharing user information with and link clearly to their data policies.

? If a user rejects, how soon can I pop up the consent banner again?

... Legally, when a user doesn’t give consent, no information of such user should be recorded. That means you wouldn’t know that the user didn’t give consent and came back again. You should treat a non-consent user as a new visitor.

? Can I include the consent notice in my terms and conditions statement?

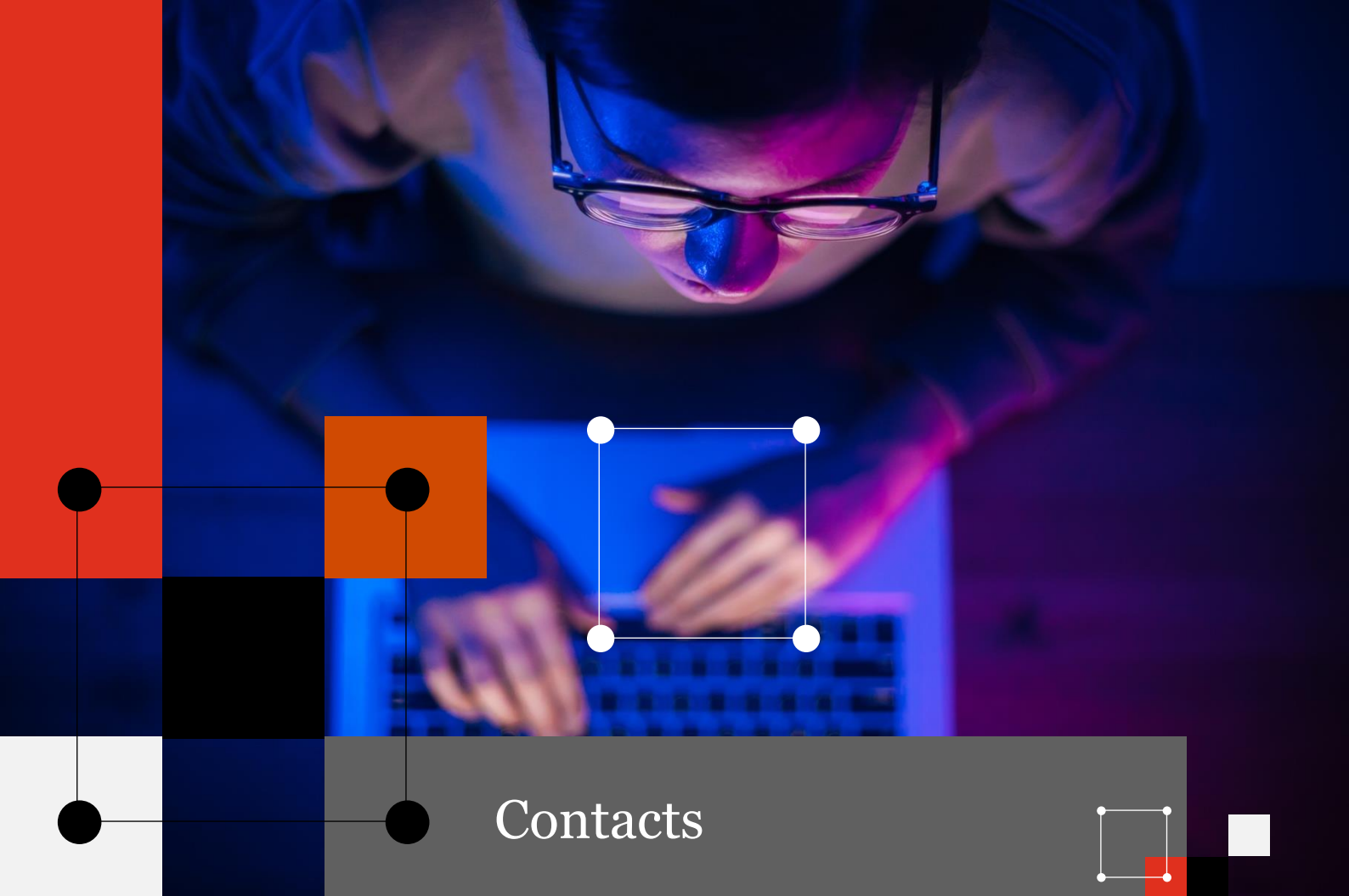
... No. Combining consent notice with terms and conditions can often lead to a long, complicated document that is difficult to read. It is recommended that consent notices be provided separately so that users have a clearer understanding of how their data will be used and give explicit consent.



Conclusion

In the current era of rapid digitalisation, businesses are encountering compliance challenges due to stricter regulations imposed by data protection authorities. This whitepaper serves as an introduction to EEA regulations on user consent, provides examples of good practices, and offers guidance on reducing compliance risks. Businesses can refer to this whitepaper to gain insight into EEA regulations on user consent, learn from good practices, and take necessary steps to mitigate compliance risks.





Contacts

Jane Wang

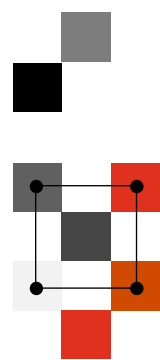
New Law Reporting and Strategy Service Advisory Leader, PwC China
jane.y.wang@cn.pwc.com

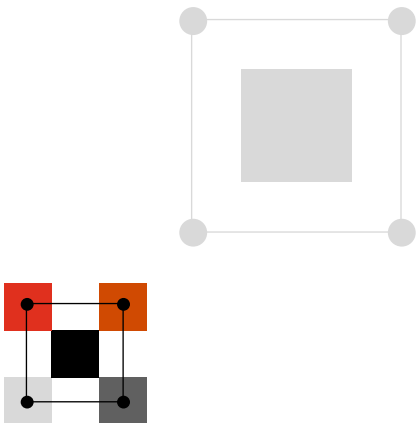
Elle Zhou

New Law Reporting and Strategy Service Advisory Partner, PwC China
elle.zhou@cn.pwc.com

Tianbin Ye

Digital and Technology Consulting Services Partner, PwC China
tianbin.ye@cn.pwc.com





This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

© 2024 PricewaterhouseCoopers All rights reserved. PwC refers to the China member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.