

NAVIGATING COOKIES

*Recalibrating your cookie strategy in light of the
DPDPA*





ACKNOWLEDGEMENTS

The ASCI Academy would like to extend its gratitude to the individuals and organisations whose support helped us put together this critical white paper for our stakeholders.

This report is put together by PSA Legal, Tsaaro Consulting and the ASCI Academy.

ASCI Academy is supported by - Diageo India, HUL, Mondelez, Nestle, Cipla Health, Coca-Cola, Colgate, Games 24X7, Pepsico, P&G, Kenvue, Bajaj Auto and Sporta Technologies.

DISCLAIMER

The contents of this white paper provides some basic information pertaining to the subject but are not intended to be, and should not be considered as, legal advice or opinion. Neither ASCI, PSA Legal, Tsaaro Consulting or any of the contributors to this white paper shall have any liability for any interpretation or information contained herein, including any errors or incompleteness.

TABLE OF CONTENTS

Foreword	01
Key Provisions of the DPDPA	03
Cookie Consent Practices & Gaps in India - A Dipstick	04
Understanding Cookies	06
A Look at Global Jurisdictions	08
Granular Consent for India	10
Other Considerations on Cookies	11
DPDPA's Industry-Wide Impact	13
Transparency & Fairness in Advertising	16
Conclusion	20
Some Key Judgements	21
Resources	27
About ASCI, PSA Legal, Tsaaro Consulting	



FOREWORD

Cookies create value for both advertisers and consumers, offering enhanced user experiences and personalized interactions. Advertisers use cookies to gather data on user behaviour, preferences, and browsing history, enabling the delivery of targeted, relevant ads that drive higher engagement and better ROI. For consumers, cookies can streamline browsing by personalizing content, remembering preferences, and simplifying website interactions.

However, the use of cookies raises concerns about privacy, data security, and user autonomy. Tracking across platforms and websites, often without explicit consent, can lead to mistrust as users remain unclear about how their data is collected, shared, or monetized. This lack of transparency undermines confidence in digital interactions.

While cookies can improve convenience, such as saving login credentials or delivering tailored ads, these benefits must be balanced with the need for transparency and control. To maintain trust, it is essential to prioritize user privacy, provide clear information about data practices, and empower users to make informed decisions about their online data.

Research by [Deloitte, Cookie Benchmark Study, April 2020](#),^[1] reveals the dichotomy in user sentiment toward cookies. **While 65% of surveyed e-commerce consumers expressed privacy concerns about cookie use, 60% were willing to share data in exchange for personalized benefits or discounts.** This demonstrates that consent management practices must prioritize user trust and transparency to ensure compliance while addressing user expectations. Alarming, the same study found that 55% of websites surveyed did not offer users an option to consent, highlighting a significant gap in compliance practices.

When used responsibly, cookies create a symbiotic relationship: advertisers achieve better outcomes with targeted marketing, and consumers enjoy a more customized and convenient digital experience. With an increased focus on privacy, advertisers must manage cookie consent responsibly, ensuring transparency and respect for user preferences.

The recent Digital Personal Data Protection Act (DPDPA) has several provisions regarding explicit consent. **This paper focuses on how cookies will be treated under the DPDPA and how advertisers can mindfully deploy cookies, balancing the need for consent with user experience.**



By embracing transparent practices and educating users about data usage, advertisers can not only enhance opt-in rates but also ensure campaign effectiveness while mitigating legal risks.

The report also explores global precedents, such as the European Union's (EU) General Data Protection Regulation (GDPR), to provide actionable insights for Indian advertisers.

With lessons from international case studies and a detailed overview of DPDPA requirements, this guide empowers advertisers to navigate the challenges of cookie consent management while continuing to deliver impactful campaigns in an increasingly regulated digital ecosystem.

Cookie consent management is no longer a mere legal checkbox; it is a vital element of building trust and brand credibility in a privacy-conscious marketplace.

Advertisers can leverage the findings of the paper to design strategies that respect user preferences while optimizing the use of cookies for targeted advertising, behavioural tracking, and personalized content delivery. Cookies power critical aspects of modern advertising, but their usage must now align with user preferences and legal mandates.



Manisha Kapoor
CEO & Secretary General, ASCI



KEY PROVISIONS OF THE DIGITAL PERSONAL DATA PROTECTION ACT (DPDPA) WITH RESPECT TO CONSENT

The DPDPA, notified on August 11, 2023, establishes a robust framework for processing personal data while balancing the rights of individuals with the lawful needs of businesses. For advertisers, this landmark regulation demands a shift in how data is collected and used, with particular focus on consent management.

The DPDPA emphasizes an individual's right to consent, requiring advertisers (as data fiduciaries) to obtain explicit, informed, and specific consent before processing personal data. Section 6 outlines that valid consent must be free, unambiguous, and provided through clear affirmative action. Consent requests must be straightforward, accessible in English and any of the 22 recognized Indian languages, and tailored to the specific purpose of data use. Moreover, users must retain the right to withdraw their consent at any time.

On January 3, 2025, the government released the draft DPDP Rules to clarify more detailed requirements, especially for consent, its withdrawal, and the processing of children's data. **Data fiduciaries are required to, before obtaining consent, provide a clear, understandable notice,** independent of any other information already given or made available to the individual, providing a description of the personal data to be collected and the specific purpose, including services, being made available to the individual as a result of this processing.

Additionally, the consent withdrawal mechanism has to be made simple, including by communicating the method for withdrawal. Regarding **children's data**, the draft rules mandate that platforms must secure verifiable parental consent before processing the personal data of users under 18 years of age, including by verifying the parent's age and identity, either through existing platform information or via legally authorized entities. Lastly, the rules specify the **time period** for which different kinds of data fiduciaries can retain data and how they must erase the same. While these rules are still under consultation and a final version is yet to be published, it is imperative that companies act quickly to ensure smooth and effective transitions into more compliant mechanisms.

Cookies, a cornerstone of digital advertising, are a key tool through which personal data is collected. Cookies collect sensitive user data such as browsing history, preferences, and even login credentials, necessitating clear and specific opt-in consent before use. In light of the DPDPA and rules, advertisers will have to design cookie consent notices and banners that clearly explain the purpose of data collection, offer options to reject non-essential cookies, and allow users to easily withdraw consent. Moreover, the notice will have to ensure granular consent is sought for, i.e., the individual must be asked to specifically consent to each unique action and purpose of processing and must also be allowed to withdraw their consent for each purpose.

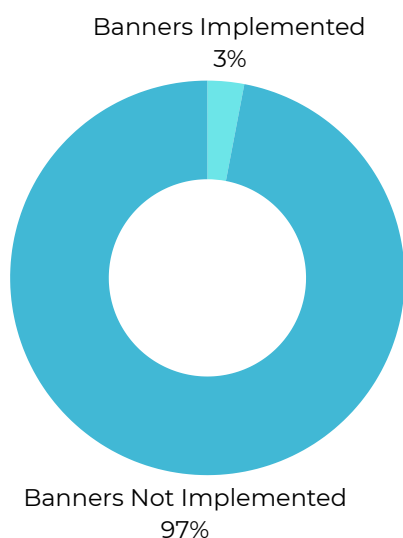


COOKIE CONSENT PRACTICES AND GAPS IN INDIA- A DIPSTICK

For the purpose of this paper, *a dipstick analysis of the top 50 most visited websites in India as of December 2024*, was undertaken by Tsaaro Consulting to identify the current scenario of cookie consent practices in India.

These websites were selected based on the list compiled by Semrush.com, with the top 50 websites accounting for over **3 billion visits in December 2024 itself**. The analysis revealed that:

- Only 3 websites (6%) currently implement cookie consent banners, underscoring a significant gap in compliance readiness;
- Among the websites with banners, most fall short of best practices, requiring improvements such as providing clear opt-out options and enabling users to give granular consent for different types of cookies.



It's important to note that this assessment reflects the status as of December 2024.

The websites analyzed span diverse sectors, including e-commerce, social media, aviation, banking, education, healthcare, sports, travel and tourism, news media, and hospitality. This broad evaluation provides an insightful view of the current state of cookie consent practices across industries.

A limited number of websites, primarily from the news media and banking sectors, featured cookie consent banners. However, these banners did not adhere to best practices. Key shortcomings included the absence of clear opt-out options and the lack of functionality for users to provide granular consent.

A key challenge observed in current practices is the lack of user-friendly design and transparency in cookie consent banners. Many websites fail to provide clear, easy-to-understand options for users to manage their cookie preferences, often presenting only a basic "accept all" option without offering sufficient control over individual cookie categories. This not only complicates the user experience but also increases the risk of non-compliance with data protection regulations.



COOKIE CONSENT PRACTICES AND GAPS IN INDIA- A DIPSTICK

Additionally, websites often lack mechanisms for users to easily withdraw consent, which further hinders compliance. These practical difficulties indicate that businesses will need to significantly overhaul their cookie management strategies, focusing on user control, transparency, and granular consent, to meet the evolving regulatory standards under the DPDP Act.

The absence of cookie consent banners on most analyzed websites points to the gap in preparedness to comply with the DPDPA. To align with global privacy standards and foster confidence among users, websites should implement:

The findings highlights a need for websites to enhance their cookie management practices to ensure compliance with the DPDPA, given that non-compliance is a serious risk, with the DPDPA envisioning the creation of a Data Protection Board that is empowered to levy fines against data fiduciaries, ranging from INR 10,000 to INR 250 crores.



**Transparent and user-friendly
cookie consent banners**



**Clear opt-out mechanisms for
non-essential cookies**



**Granular consent options - enable
users manage their cookie choices**



UNDERSTANDING COOKIES

In today's digitally driven world, advertisers operate at the intersection of personalization and privacy. As the internet continues to dominate every aspect of consumer interaction, the collection of user data has become integral to crafting targeted campaigns, enhancing engagement, and driving measurable Return On Investment (ROI). One of the most widely used tools for gathering such data are cookies—small pieces of data stored in a user's browser that track activity and preferences.

WHAT ARE COOKIES?

Cookies are small text files that websites place on one's device as they are browsing. These may collect and store information that can identify the user, including personal details, preferences, and browsing history. This stored information is used to help improve their browsing experience and generate targeted advertisements.

Simply put, cookies record information based on a user's session on a website to then identify the user when they revisit the site. The information is stored locally on the user's web browser so that, when the user revisits a particular website, the web browser returns the cookies to the website, recalling data from the previous session.

The stored information can consequently be used for personalization to tailor advertisements and to track a user's analytics of how much time was spent on a website, how many times the website was visited, and what, if anything, was purchased.

This allows the website to personalize suggestions similar to a previous purchase. On the flip side, cookies may be used to track browsing history and ban users if their activity is found to be violative of the website's terms and conditions.

HOW DO COOKIES WORK?

When a person uses their browser to visit a website, the browser sends a request to the website server for the page the user wants to view. The website server includes a set-cookie header in its response, which instructs the browser to store the cookie commonly referred to as the HTTP cookie.

This HTTP cookie is saved in a dedicated cookie file on the user's computer. It collects and stores basic information such as language preferences, time spent on a website, and website display preferences.

By understanding cookies and their purposes, advertisers and businesses can make informed decisions about compliance and user consent while maintaining functionality and effectiveness in digital campaigns.



6 TYPES OF COOKIES

Cookies can be categorized based on their purpose. Below is a list of commonly used cookies and examples from key platforms:



Essential / Strictly Necessary Cookies

These are fundamental for websites to function properly. They enable basic features like navigation and access to secure areas


Example: Session cookies that keep users logged in while browsing a website (e.g., shopping carts on e-commerce platforms)

These cookies collect anonymized data on how users interact with a website, helping businesses optimize performance

Google Analytics Cookies: `_ga`, `_gid`—Track user interactions and website traffic

Facebook Analytics Cookies: `datr`, `fr`—Help analyze user engagement and ad performance

Performance / Analytics Cookies




Functionality Cookies


They remember user preferences and settings, enhancing the user experience

- *YouTube Cookies: `PREF`, `VISITOR_INFO_LIVE` — Store user preferences for video playback, such as language*
- *Spotify Cookies: Save volume settings or preferences for curated playlists*

These track user activity to deliver personalized advertisements

- *Google Ads Cookies: `IDE`, `ANID`—Used for remarketing campaigns and ad personalization*
- *Facebook Pixel Cookies: `fbp`, `c_user`—Track conversions and user behavior for ad targeting*

Targeting / Advertising Cookies

Social Media Cookies


Deployed by social platforms to track user activity for sharing content and advertising

- *Twitter Cookies: `personalization_id` — Tracks engagement and recommends content*
- *LinkedIn Cookies: `bcookie`, `liap` — Authenticate users and track interactions for analytics and advertising*

Designed to maintain security and protect user data

- *Google Security Cookies: `SID`, `HSID` — Prevent fraudulent access and protect user accounts.*
- *Cloudflare Cookies: `__cfduid` — Identify trusted traffic and prevent attacks.*

Security Cookies








COOKIE CONSENT MANAGEMENT UNDER GDPR


Cookie consent management refers to a structured framework of systems and regulations that ensure organizations obtain valid, informed consent from users before storing or processing their data through cookies. The legal necessity for such frameworks is emphasized in Recital 30 of the GDPR, which highlights the potential for online identifiers, including cookies, to create detailed user profiles when combined with other identifying information.

The Directive 2002/58/EC of the EU on privacy and electronic communications (EPD) introduced key principles for cookie consent, emphasizing that cookies serve legitimate purposes, such as analyzing website effectiveness and facilitating online transactions, provided users are informed of their purpose. Clause 25 of the EPD mandates that users must

 *be given the opportunity to refuse cookies, particularly when privacy-sensitive information is at stake*

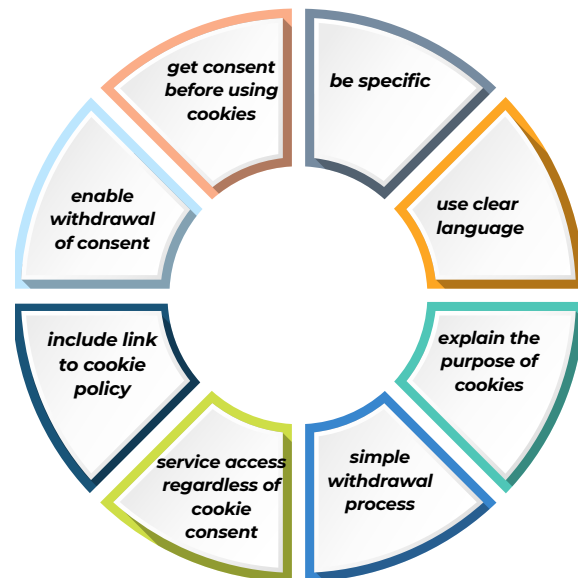
 *be informed about the purpose and nature of stored data*

 *have user-friendly methods to give consent or refuse cookies*

 *be allowed conditional access to website content if cookies serve legitimate purposes*

These principles, read with GDPR requirements for consent to be freely given, specific, informed, and unambiguous, form the basis for structuring cookie consent notices.

STRUCTURING NOTICES OF COOKIE CONSENT UNDER GDPR



THE PRINCIPLE OF GRANULARITY IN COOKIE CONSENT

Granularity is a cornerstone of lawful consent under GDPR. It mandates that users must have the freedom to consent separately to distinct processing purposes rather than being forced to accept bundled permissions. Recital 32 specifies that consent must be purpose-specific, while Recital 43 presumes consent is not freely given if users cannot grant or withhold consent for each distinct purpose. For cookies, this means:

- **Separate Consent:** Consent must be obtained for each cookie purpose individually (e.g., functional cookies, analytics cookies, or advertising cookies).
- **Right to Withdraw:** Users must have the ability to refuse or withdraw consent without detriment. For example, the functionality of a website must not degrade for users who opt out of non-essential cookies.



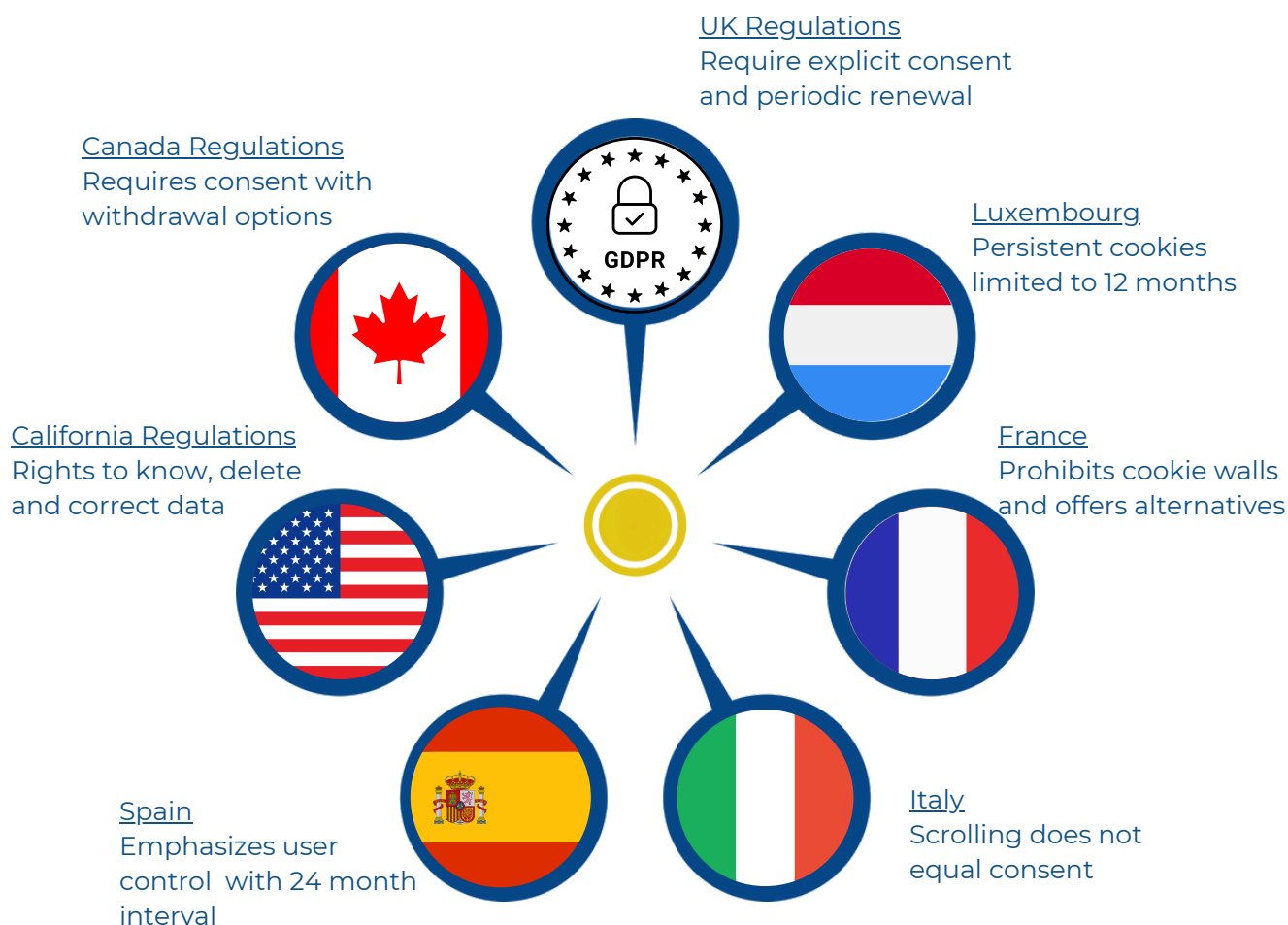
REGULATORY IMPLICATIONS FOR ADVERTISERS

EU data protection agencies have imported granularity requirements into cookie consent regulations. For advertisers, this translates into:

- ✓ Detailed Cookie Banners: Clear breakdowns of cookie types, purposes, and data collected
- ✓ Granular Opt-Ins: Users must have the option to selectively consent to specific cookies
- ✓ Ongoing Compliance: Mechanisms for withdrawing consent must be straightforward and readily accessible

COOKIE REGULATIONS ACROSS KEY JURISDICTIONS

Understanding cookie regulations across jurisdictions is essential for advertisers to maintain compliance and build trust with users. Below is an overview of how cookie consent is regulated in various regions:





GRANULAR CONSENT FOR INDIA

While there is no specific cookie law in India, the **DPDPA provides the principles for granular consent** to be obtained from users in cookie banners and privacy statements. Since cookies collect and store information, they would require consent in line with sections 5 and 6 of the DPDPA.

Under Section 5(1)(i) of the DPDPA, every request made to a data principal for consent must be accompanied or preceded by a notice given by the data fiduciary informing the personal data collected and the purpose for which the same is proposed to be processed. This is similar to Article 6(1)(a) of the GDPR requiring that the data subject be informed about each purpose for which their data is being processed before providing consent.

Section 6(1) of the DPDPA specifies that consent given by the data principal shall be free, specific, informed, unconditional, and unambiguous, which shall signify an agreement for processing her personal data for the specific purpose, and it is only limited for that specific purpose. Section 6(3) requires that the request for consent be provided to the data principal in a clear and plain language. Section 6(4) states that a data principal shall have the right to withdraw consent at any time.

These bear similarity to Article 4(11) of the GDPR, which defines consent as being freely given, specific, informed, and unambiguous, given through a statement or by clear affirmative action, and Article 7 of the GDPR, which lays down the conditions for valid consent, including that the request be made in an easily understandable and accessible form in clear and plain language, and that the right to withdraw consent be available at all times.

The DPDPA enshrines the requirements of consent being specific, and granular consent would therefore fulfil this requirement.



OTHER CONSIDERATIONS ON COOKIES

DARK PATTERNS: VIOLATING THE SPIRIT OF USER CONSENT

Dark patterns are deceptive user interface designs, that manipulate users into making choices that are detrimental to their interest, such as buying a more expensive product, paying more than what was initially disclosed, sharing data, or making choices based on false or paid-for reviews, and so on. These are concerning as they bar users from acting in accordance with their preferences. They undercut individual autonomy through deception and coercion. As stated in a [2022 report by the Advertising Standards Council of India](#), “Dark patterns eventually undermine how consumers view advertising. The increasing presence of dark patterns forces consumers to be on guard and suspicious of the online space. In the long run, such tactics ruin customer experience, lower brand image and loyalty, and increase abandonments.”^[1]

In cookie consent banners, dark patterns sometimes appear in the form of visually biased designs. For instance, the “accept all cookies” button might be brighter, more accessible, and more aesthetically pleasing than the option to customize or reject non-necessary cookies.

Such aesthetic manipulation, such as using larger fonts and high contrast colour on the accept cookie option steers users toward agreeing without considering their actual preferences.

Other common examples include pre-selected checkboxes that automatically opt users into privacy policies or data sharing practices. These methods contravene global privacy standards, such as the GDPR and India’s DPDPA, which mandate clear, informed, and voluntary user consent. Several jurisdictions have already ruled pre-checked boxes invalid, emphasizing the need for explicit and unambiguous choices.

THE “CONSENT OR PAY” DEBATE

The “consent or pay model” is based on the fact that a user can either accept the cookies, which would lead to their information being used by different third parties, or pay a small subscription fee to ensure their data is not shared with third parties. Such models are most commonly used and oriented towards behavioral advertising.

An issue would arise if the user is not provided an option to reject all cookies, i.e., even under the “pay” option, performance cookies are deposited.

This constitutes the creation of a cookie wall, i.e., it forces the user to either accept all cookies being shared through the “consent option” or some essential cookies being deposited but not shared through the “pay option.”

Consequently, if the user does not want to consent or pay, they will not be permitted to proceed with using the website.



There is no definite legal stance on whether the consent or pay model is legally sound as per the GDPR and various data privacy laws.

However, the EPDB opinion on “valid consent in the context of consent or pay models implemented by large online platforms dated 08/2024” states that, if controllers offer a paid service to avoid all cookies, they must also offer an alternative where only personalisation-based cookies are accepted and cookies used for behavioural advertisement are rejected.

Options Users Must Have



ACCEPT ALL

Free browsing through acceptance of content personalisation cookies and behavioural advertising cookies



ACCEPT ONLY ESSENTIAL

Free browsing through acceptance of content personalisation cookies



PAY AND REJECT ALL

Subscribe and Reject all cookies



DPDPA'S INDUSTRYWIDE IMPACT

This section looks at some practices and use-cases that are likely to be impacted by the provisions of DPDPA as interpreted for cookie consent:

E-COMMERCE

E-commerce retailers in India commonly use cookies to enhance user experience and provide personalized recommendations. With the implementation of cookie consent requirements under the Indian data protection law, businesses will need to adopt mechanisms to ensure transparency and obtain user consent for different purposes of cookie usage. This includes providing clear information on the purpose of each cookie, the data being processed, and allowing users to make granular choices, such as consenting to essential cookies while rejecting others. These adjustments will require businesses to redesign their cookie management practices and user interfaces to comply with the law while balancing user expectations and operational needs.

SOCIAL MEDIA PLATFORMS

Social media platforms and video-based applications often use cookies to enhance user experience by tailoring content feeds, providing personalized recommendations, and suggesting connections. With the Indian data protection laws creating implications for cookie consent requirements, these platforms will need to ensure greater transparency and obtain specific user consent for cookie usage, particularly for tracking browsing and watch histories. Platforms may also need to implement mechanisms for periodic consent renewal and offer users more granular control over their data.

TECH AND SOFTWARE-AS-SERVICE (SAAS) COMPANIES

These deploy cookies for user authentication of their software products licensed out to other companies and to optimize performance and user interaction on their websites. The GDPR classifies cookies into strictly necessary, preference, statistics, and marketing cookies and specifies that for strictly necessary ones, the company is not required to obtain consent and must merely explain what they do and why they are necessary to the user. Performance cookies are considered strictly necessary when they are required for the website to function. Compliance with data protection laws will require these companies to clearly explain the purpose of the cookies they deploy and implement mechanisms for obtaining user consent where necessary. This includes ensuring transparency about how cookies function and offering users the ability to make informed choices about their use. Companies will need to align their practices with legal requirements while maintaining service efficiency and user accessibility.



DIGITAL ADVERTISING AND MARKETING

This industry relies heavily on cookies to deliver targeted advertisements tailored to users' browsing and purchasing histories. With stricter norms under data protection laws, businesses in this sector will need to ensure that users are informed about the purpose of cookies and provide mechanisms for obtaining specific consent for their use. Additionally, users will have the right to withdraw consent at any time, requiring companies to adapt their practices and technologies to accommodate these changes while maintaining compliance. These adjustments will play a significant role in shaping the industry's approach to targeted advertising.

HEALTHCARE

Organizations often rely on cookies to facilitate access to critical health-related information and medical histories. These cookies enable seamless functionality for patients, such as retrieving prescriptions, viewing diagnostic reports, managing appointments, and accessing health records. However, given the sensitive nature of health data, stricter compliance with data privacy regulations is paramount.

FINANCE

Financial platforms often use cookies to facilitate access to sensitive user data, such as account details, transaction histories, and payment information. While these cookies are essential for secure authentication and seamless online banking experiences, they pose significant privacy challenges due to the highly sensitive nature of the data involved.



TRANSPARENCY & FAIRNESS IN ADVERTISING

While the Consumer Protection Act, 2019 (CPA) does not explicitly regulate the use of cookies, its principles on transparency and fairness in advertising and marketing impose important obligations for advertisers:

TRANSPARENCY IN COOKIE CONSENT MECHANISMS

Cookies play a discreet but indispensable role in facilitating targeted advertising.

Cookie banners must clearly articulate:

- The type of data being collected.
- The purpose of data collection, especially if consumer data is shared with third parties for personalized advertising.

RIGHT TO AWARENESS AND CONSUMER EMPOWERMENT

The CPA enshrines the right to awareness as a core consumer right, implying that consumers understand the consequences of their consent.

Cookie banners should be:

- Be simple and written in easily understandable language.
- Provide unambiguous options for users to consent or reject cookies.
- Clearly disclose how data will be used, especially in direct marketing.

PROTECTION AGAINST UNFAIR TRADE PRACTICES

Under the CPA, disclosing personal information shared in confidence without explicit consent could be considered an unfair trade practice.

For advertisers, this means:

- Personal data obtained via cookies must remain confidential unless explicit user permission is obtained.
- Transparent cookie policies should outline how personal data will be managed and safeguarded.

Failing to align cookie practices with CPA principles could expose organizations to allegations of misleading advertisements or unfair trade practices



CORE PRINCIPLES FOR COMPLIANCE



CLEAR COOKIE CONSENT BANNER

- Accept Option
- Reject Option
- Customize Preferences



TRACK AND STORE CONTENT

- Audit demonstration
- Legal scrutiny



CATEGORIZE COOKIES

Classify cookies to enable informed user choices

- Functional
- Performance
- Targeting
- Strictly necessary



CONSENT WITHDRAWAL OPTIONS

- Modify Consent
- Withdraw consent



REGULAR AUDITS

- Compliance review
- Outdated cookie removal



DETAILED PRIVACY POLICY

- Data Collection
- Data Usage
- User Rights

DESIGNING A USER-CENTRIC COOKIE PREFERENCE CENTER

A Cookie Preference Center is a website tool that empowers its users to manage their cookie settings, granting or withdrawing consent and choosing specific cookie categories, ensuring compliance with relevant data privacy regulations.

FEATURES

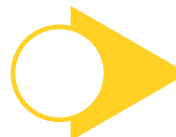


Categorized cookie options (necessary, analytics, advertising)



Mechanisms for consent withdrawal and modifications

ADVANTAGES



Compliance

Adherence to privacy laws like GDPR, DPDPA, and the e-Privacy Directive



User Trust

Transparency and control over data usage



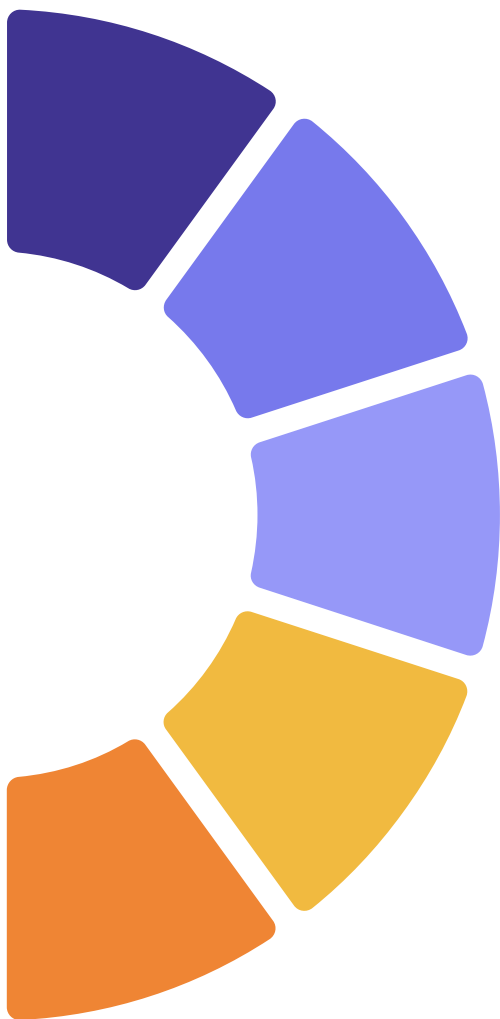
Risk Mitigation

Avoid penalties by maintaining compliance



CRAFTING AN EFFECTIVE COOKIE POLICY

An effective cookie consent policy should encompass comprehensive transparency and granular control mechanisms that align with applicable data protection regulations. The policy must explicitly delineate the following elements:



- 1 CATEGORY OF COOKIES**
 - Strictly necessary/essential cookies
 - Functional/preference cookies
 - Performance/analytics cookies
 - Marketing/targeting/advertising cookies
- 2 TECHNICAL SPECIFICATIONS**
 - Cookie identifiers
 - Storage duration/expiration periods
 - First-party vs. third-party cookie deployment
 - Data processing purposes and legal bases
- 3 CONSENT MANAGEMENT:**
 - Clear opt-in/opt-out mechanisms
 - Granular consent options for each cookie category
 - Real-time consent recording and documentation
 - Mechanism for consent withdrawal
- 4 INFORMATION TRANSPARENCY**
 - Detailed data collection methodologies
 - Specific data processing purposes
 - Third-party data recipients and transfers
 - Cross-border data flow implications
- 5 USER CONTROL INTERFACE**
 - Easily accessible cookie preferences dashboard
 - Cookie settings modification capabilities
 - Persistent consent preferences storage
 - Browser-level cookie control information

The policy should maintain compliance with evolving regulatory frameworks while ensuring user-friendly implementation and regular updates to reflect technological advancements and emerging privacy standards.



PRACTICES TO AVOID

- ✓ **Assume Implied Consent:** Avoid pre-ticked checkboxes or banners without explicit consent options, as these violate laws like GDPR and DPDPA
- ✓ **Conceal Consent Options:** Don't hide cookie settings or make them difficult to access. Such practices can lead to user dissatisfaction and non-compliance
- ✓ **Use Non-Compliant Dark Patterns:** Manipulative design patterns that pressure users into accepting cookies can lead to non-compliance and harm user trust.
- ✓ **Neglect Third-Party Cookies:** Failing to manage third-party cookies can lead to compliance gaps and security risks.

LEVERAGING AUTOMATION FOR COMPLIANCE

Automation tools simplify and enhance cookie consent management by streamlining compliance processes, reducing manual effort, and ensuring consistent compliance with data privacy regulations. These tools are particularly valuable for businesses managing websites with high traffic or operating across multiple jurisdictions. They provide the technical capabilities needed to handle dynamic consent requirements effectively.

HOW CAN AUTOMATION HELP



Compliance Across Jurisdictions: Automatically adapts cookie banners and policies to comply with region-specific regulations like GDPR and the DPDPA, ensuring compliance.



Real-Time Cookie Scanning: Regularly scans websites to detect and categorize cookies, including third-party cookies, for comprehensive management and compliance.



Centralized Consent Tracking: Maintains detailed records of user consents in a centralized dashboard, aiding in audits and regulatory reporting.



Customizable User Interfaces: Enables businesses to design user-friendly and brand-consistent cookie banners with customizable consent options.



Seamless Integration: Integrates with analytics tools, CRM systems, and Content Management Systems (CMS) to synchronize cookie preferences across platforms.



Automated Updates: Keeps cookie banners and policies updated with regulatory changes or changes in cookie usage, minimizing the risk of non-compliance.



CONCLUSION

The evolving landscape of cookie consent management underscores the delicate balance advertisers must strike between leveraging data for targeted marketing and respecting user privacy. With the advent of the DPDPA and the draft Rules, the responsibility to ensure transparent, user-friendly, and legally compliant consent mechanisms is no longer optional but imperative.

Advertisers will face significant challenges, particularly those who rely heavily on non-consensual and unchecked data collection through cookies for personalized marketing campaigns. The user's right to withdraw consent at any time introduces operational complexities. The requirement for explicit, informed, and revocable consent may lead to reduced data availability, impacting targeting accuracy and campaign effectiveness. On the bright side, this will ensure quality data instead of quantity since data available for processing will primarily be from users who voluntarily want to receive targeted and customized ads and services.

Compliance, if done effectively, will empower advertisers will be able to position themselves as privacy-conscious brands. For this, advertisers will have to prioritize designing granular cookie consent banners that ensure users can easily opt-out of non-essential cookies, and investing in automation and tools for automated consent tracking and withdrawal management. The overarching objective is to empower users with informed choices, and the experiences of jurisdictions like the EU provide valuable insights into avoiding pitfalls and embracing effective strategies. Ultimately, the path forward demands a proactive approach from advertisers; one that prioritizes transparency, user autonomy, and ethical data usage. The transition to compliant and user-centered cookie practices is not merely a regulatory necessity but a cornerstone of sustainable and responsible digital marketing



SOME KEY JUDGEMENTS

FINLAND DPA, 2019

FACTS

The data subject filed a complaint with the Finnish DPA regarding a website's cookie consent banner, alleging that the banner did not allow for the refusal of cookie storage.

WORDING OF THE NOTICE

The banner only had two options: "OK" and "Additional Information." The second option sent the user to the website's privacy statement.

HOLDING

The Finnish DPA held that consent will not be considered voluntary till there is a right for the user to refuse the storage of the cookies. Under the EPD, there has to be an easy mechanism for the withdrawal of consent, which was not available. They ordered that there must be a change in the banner to explicitly include a refusal for storage of cookies and that there must be an easier process to withdraw consent.

DSB AUSTRIA, DER STANDARD, 2023-O.174.027, 2023

FACTS

An Austrian newspaper "Der Standard" in the cookie banner only had two options: "Ok" or "Pay." When a user selected the "Ok" button, it led to their data being shared with 125 third parties. Alternatively, the "Pay" option required the user to purchase a subscription to the paper in order to reject the cookies from collecting and sharing information with third parties.

HOLDING

The DPA looked at the granularity of consent and reiterated that if there are multiple processes taking place, there must be consent obtained for all of them; there cannot be a singular blanket acceptance for all of these processes. Each user must have the right to withdraw from a process if they wish to; it is not permissible that, if a user cannot afford a subscription, there is significant impairment on their data protection rights. Under the EPD, there must be a right of refusal and a right to withdraw consent, neither of which was available. Therefore, they held that the processing was unlawful.

CHRISTIAN SCHMIDT VS. DANISH METEOROLOGICAL INSTITUTE, DENMARK DPA, 2018-32-0357, 2020

FACTS

A complaint was filed against the Danish Meteorological institute ("DMI") alleging they improperly collected and used personal data to display ads based on user behaviour jointly with Google and their ad management tools.

WORDING OF THE NOTICE

The initial consent banner on DMI's website only displayed an "Ok" button and no way to refuse the cookie storage. The DMI then changed their banner to include an "Ok" button and an additional "Show Details" button wherein users had to de-select the pre-checked boxes representing different purposes.

HOLDING

The DPA found that the DMI's cookie consent banner was not in line with the way consent must be obtained to process personal data under Article 4(11) and Article 5(1)(a) of the GDPR. They also stated that consent must be obtained granularly, i.e., consent must be obtained for each purpose for data processing and sharing, and cannot be a singular choice, which allows for multiple processes under one consent banner.

They also rejected the modified version adopted by the DMI on the ground that it was not sufficient as the option of rejection of cookies and processing of personal data was not provided in the first interaction. They also stated that the consent banner did not reflect that Google would also have access to the data as a joint controller. Furthermore, they held that the banner is not sufficiently transparent since it provides only "Ok" and "Show details" buttons.



AMAZON FRANCE LOGISTIQUE CASE, 2023

FACTS

Amazon France deposited a large number of cookies with an advertising purpose on users' computers without their consent. The cookie consent banner did not inform users beforehand about the deposit of the cookies, the purpose, and how a user could reject them. Furthermore, cookies were deposited on a user's device if they clicked on an advertisement for Amazon France on another website.

HOLDING

The authority held that the cookie consent banner must fully inform the user of their purpose and their right to refuse such cookies, which Amazon's cookie banner failed to do in clear and express terms. Furthermore, in regards to the Amazon ads on third-party websites, Amazon argued that a small button was provided at the top of each ad to prevent cookies from being deposited if the ad was clicked on.

However, the court held that the button only ensured the ad was not shown again and did not explicitly provide for an option to reject cookies. Resultantly, Amazon was fined € 35 million.

SPANISH DPA, 2023

FACTS

A data subject represented by the European Centre for Digital Rights filed a complaint with the Spanish DPA that a website installed non-essential cookies even before the user could interact with the cookie banner.

HOLDING

The Spanish DPA entered the website of the controller and verified that, without accepting cookies or performing an action on the page, performance cookies and targeting cookies were installed on the user's device. They also found that the cookies were neither technical nor necessary but belonged to a third party who was not the controller of the website. The Spanish DPA also found that there was no option to withdraw their consent or disable certain cookies. The Spanish DPA fined the company € 2000.

FEDERATION OF GERMAN CONSUMER ORGANISATIONS VS. PLANET49, 2019

FACTS

A German company called Planet49 organised an online lottery on their website. Underneath the details input field, there were two checkboxes. The first checkbox required the user to consent to be contacted by firms for promotional offers and the second checkbox required the user to consent to cookies being installed on their device. The first checkbox was not pre-ticked while the second checkbox was. To participate in the lottery, a user had to tick at least the first checkbox.

WORDING OF THE NOTICE

I agree to the web analytics service Remintrex being used for me. This has the consequence that, following registration for the lottery, the lottery organiser sets cookies, which enables Planet49 to evaluate my surfing and use behaviour on websites of advertising partners and thus enables advertising by Remintrex that is based on my interests. I can delete the cookies at any time. You can read more about this here.'

HOLDING

The court held that a key component of valid consent is that it must be given by a clear affirmative act. Mere unticking of a box is not sufficient. The court held that Planet 49's consent model was inadequate with regards to securing consent to place cookies on the user's device. Consent must be given on the basis of clear and comprehensive information communicated to the user.

This implies that in cases where cookies aim to collect information for advertising purposes, there should be a clear mention of the duration of the operation of cookies and whether the information collected would be shared with third parties or not. The court concluded that the opt-in policy under the GDPR is not satisfied by pre-ticked checkboxes



DENMARK, DECISION AGAINST META OF OCTOBER 30, 2023

FACTS

The Danish Agency for Digital Government addressed a consultation letter to Meta requesting to elaborate on the cookies it uses and on cookie banners it displayed on its website. Meta, in its response, stated that it uses technically necessary cookies for non-registered users and a cookie banner for registered users.

WORDING OF THE NOTICE

In case of registered users, Meta grouped “Cookies on other apps and websites” and “Cookies from other entities” under a single consent banner. For non-registered users, only two options were made available: “Allow only necessary cookies” and “Allow necessary and optional cookies.” In 2022, Meta changed their policy for unregistered users and allowed them to visit their cookie policy. However, there was one blanket consent for the data being used for several purposes

HOLDING

The authority held that Meta’s cookie banner did not allow its registered and unregistered users to give granular consent, i.e., separate consent for their data being used for different purposes. They further went on to hold that a permanent and clear option to withdraw one’s consent was not available to users, and they had to click three times before they could withdraw consent.

The authority asked Meta to make their website compliant with certain recommendations –

- Make it possible for users to grant granular consent;
- Give users a permanent option to withdraw consent directly and clearly;
- Information about each cookie and their purpose must be continuously available on their website, and this must be provided in a clear, precise, and easily understandable language.

PLAINTIFF VS. LINKEDIN NETHERLANDS B.V., MICROSOFT CORPORATION, MICROSOFT IRELAND OPERATIONS, MICROSOFT B.V., XANDER INC., 2024, AMSTERDAM

FACTS

The data subject visited several websites and refused all the cookies via their cookie banner. However, it was found that tracking cookies were still present on the data subject’s laptop. The controllers were LinkedIn Ireland, LinkedIn Netherlands, Microsoft, Microsoft Ireland Operations, Microsoft Northern Ireland, and Zandr. The user hired an independent analyst to view the data, and it was found that out of 30 websites visited, 27 had deposited cookies despite explicit rejection of the cookies.

HOLDING

The court held that there was a clear violation of the GDPR and the Dutch Telecommunications Act by placing reading cookies without the consent of the data subject. The court prohibited the controllers from placing or reading tracking cookies on data subject’s devices without their consent. The court also imposed a penalty of €500 per violation or €1000 per day, up to a maximum of €25,000 per company until they complied. Additionally, they asked the controllers to pay the data subjects legal costs.



UNITED STATES OF AMERICA, PLAINTIFF VS. GOOGLE INC., DEFENDANT, 2012, UNITED STATES OF AMERICA [3]

FACTS

The Federal Trade Commission (“FTC”) filed a complaint alleging that, for several months in 2011 and 2012, Google was placing certain advertising tracking cookies on the computers of individuals using Safari browser who visited sites within Google’s DoubleClick advertising network, without their knowledge or consent. According to the complaint, Google assured that Safari browser’s default setting to block third-party cookies had the same effect as opting out of this particular advertising tracking cookie. Despite this, an investigation found that Google was placing these cookies on consumers’ computers by circumventing Safari browser’s default setting.

Google had exploited an exception to this default setting to place a temporary cookie from the DoubleClick domain. This initial temporary cookie then opened the door to all cookies from the DoubleClick domain, including the Google advertising tracking cookie.

HOLDING

The court held that there was a clear violation of the GDPR and the Dutch Telecommunications Act by placing reading cookies without the consent of the data subject. The court prohibited the controllers from placing or reading tracking cookies on data subject’s devices without their consent. The court also imposed a penalty of €500 per violation or €1000 per day, up to a maximum of €25,000 per company until they complied. Additionally, they asked the controllers to pay the data subjects legal costs.

IN THE MATTER OF SCANSCOUT, INC., A CORPORATION, 2011, UNITED STATES OF AMERICA [4]

FACTS

FTC filed a complaint alleging that, from April 2007 to September 2009, the privacy policy of ScanScout, an online advertiser that engaged in behavioral advertising by collecting information about consumers’ online activities and then serving video ads targeted to their interests, stated users could opt out of receiving a cookie by changing their browser settings to prevent receipt of cookies. However, an investigation found that the company was using Flash cookies, which could not be removed or blocked by changing browser settings.

HOLDING

The claims by ScanScout were deceptive and violative of the FTC Act. ScanScout agreed to settle the charges. The settlement directed that, within 30 days from when it took effect, ScanScout place a prominent notice on its home page stating, “We collect information about your activities on certain websites to send you targeted ads. To opt out of our targeted advertisements, click here.”

Additionally, the hyperlink must take consumers to a mechanism that allows them to prevent the company from collecting information that can identify them or their computer and associating any previously collected data with them. Additionally, the consumer’s choice was to last for at least five years, unless the consumer changed it. In addition, next to each targeted ad, ScanScout was required to embed a hyperlink to take consumers to the choice mechanism that allowed them to opt out of receiving targeted ads.



IN RE: NICKELODEON CONSUMER PRIVACY LITIGATION, UNITED STATES COURT OF APPEALS FOR THE THIRD CIRCUIT, 2016 [5]

FACTS

Viacom owns children's television station Nickelodeon and operates Nick.com, a website that caters to children. Children have to register to use the website with a username and password and details such as birthdate and gender. Certain individuals filed a suit alleging its registration form informs children's parents that it does not collect any personal information about the child and therefore does not share any. However, Viacom and Google unlawfully use cookies to track children's web browsing and video-watching habits on Viacom's websites. It was further alleged that when a user visits one of Viacom's websites, Viacom places its own first-party cookie on that user's computer. This permits Viacom to track a child's behavior, including which games a child plays and which videos a child watches. Google then contracts with Viacom to place advertisements on Viacom's websites. As a result, Google is able to place third-party cookies on the computers of persons who visit those websites, including children. Once Google places a cookie on a person's computer, it can track that person across any website on which Google displays ads. Google uses "DoubleClick.net cookies" to accomplish this task. Therefore, Viacom discloses to Google, and Google collects and tracks children's information, including username, gender, birthdate, IP address, browser settings, unique device identifier, operating system, and web communications, including detailed URL requests and video materials requested and obtained from Viacom's children's websites. All this information is then used to sell targeted advertising, especially to children.

HOLDING

The plaintiffs have adequately alleged that Viacom collected personal information about children despite its promise not to do so and invaded their privacy in violation of New Jersey privacy law. The primary issue here is not whether Viacom collected personal information or disclosed it, but that it created an expectation of privacy on its website and obtained personal information under false pretense. Such a claim survives if a company promises to respect consumer privacy and then disregards its commitment.

Viacom's message to parents about not collecting children's personal information may have created an expectation of privacy on Viacom's websites and may also have encouraged parents to permit their children to browse those websites under false pretenses. However, the practice adopted by Google in this case of deploying third-party cookies on Nick.com is not unusual or sufficiently offensive; Google deploys such cookies on several other websites too. Additionally, Google was allegedly a mere recipient of personal information.

FACEBOOK INC. VS. AUSTRALIAN INFORMATION COMMISSIONER, AUSTRALIA, 2022 [6]

FACTS

A suit was filed regarding an application called This Is Your Digital Life which required users to log in using their Facebook account and did not offer any alternate means of logging in. The app then asked for permission to access the personal information held by Facebook about the user and for access to the personal information of their Facebook friends. Upon obtaining the user's permission, the developers then requested that Facebook provide them with access to that user's and their friends' personal information. Facebook provided this information under certain terms, including that the developer was not permitted to use the information other than for the purposes of the application. The developers, however, breached this requirement by permitting the personal information to be used for political campaigns. The primary contention raised was that the Privacy Act in Australia prevents organizations that have collected information for a particular purpose from using it for another purpose. Facebook Ireland and Facebook Inc. were also made defendants. Facebook Inc. challenged the jurisdiction of the Australian authorities to serve notice on it given Facebook Inc. is incorporated in Delaware and based in California.



HOLDING

The Privacy Act applies to acts done or practices engaged in outside Australia if they are done or engaged in by an organization with an Australian link. For a body corporate such as Facebook Inc. or Facebook Ireland, an Australian link will be present if the body corporate carries on business in Australia and it has collected or held personal information in Australia. As part of its business, Facebook Inc. was installing cookies on the devices of users in Australia.

Cookies are central to the Facebook platform. In its 2013 Data Use Policy, users are informed that whenever they visit a game, an application, or a website that uses the Facebook platform, Facebook will collect through cookies data including date and time one visits the site, web address of URL, technical information about the IP address, and browser and operating system being used. Facebook Inc. had used cookies to store the personal information on the devices of Australian users and had therefore held the personal information in those devices. There is a prima facie case that an Australian link exists, and the Privacy Act will apply to Facebook Inc.



GLOSSARY OF TERMS AND ABBREVIATIONS

- **DPDPA:** Digital Personal Data Protection Act.
- **Cookies:** Small text files stored on a user's device by websites to remember preferences, track activities, or enhance the browsing experience.
- **Data Fiduciary:** Section 2(i) of the DPDPA defines data fiduciary as “any person who, alone or in conjunction with other persons, determines the purpose and means of processing personal data.”
- **Data Principle:** The individual to whom the personal data being processed relates, typically the person whose data is being collected or processed.
- **DPDPA:** The Digital Personal Data Protection Act, 2023, is an Indian law that governs the processing of personal data to protect individuals' privacy while enabling data-driven innovation.
- **GDPR:** The General Data Protection Regulation is a comprehensive EU law that regulates the collection, processing, and protection of personal data to safeguard individuals' privacy rights.
- **EDPB:** The European Data Protection Board is an EU body that oversees the consistent application of the GDPR and promotes cooperation among data protection authorities across Europe.
- **CPA:** Consumer Protection Act, 2019

REFERENCES

1. **Deloitte, Cookie Benchmark Study**, April 2020,
2. The Advertising Standards Council of India, **Dark Patterns – The New Threat to Consumer Protection**, Discussion Document, November 2022.
3. United States of America, Plaintiff, vs. Google Inc., Defendant, Docket Number: C-4336, United States of America, Federal Trade Commission, November 20, 2012
4. In the Matter of ScanScout, Inc., a corporation, Docket No. C-4344, United States of America, Federal Trade Commission, December 14, 2011
5. In re: Nickelodeon Consumer Privacy Litigation, 827 F.3d 262 (3d Cir. 2016), United States Court of Appeals for the Third Circuit, June 27, 2016
6. Facebook Inc. vs. Australian Information Commissioner (2022) FCAFC 9, Federal Court of Australia, February 7, 2022

ABOUT ASCI ACADEMY

The ASCI Academy is a flagship program of the Advertising Standards Council of India to build the capacity of all stakeholders in creating responsible and progressive advertising. ASCI Academy aims to raise standards of advertising content through training, education, outreach, and research on the preventive aspects of advertising self-regulation. Be it advertisers, agencies, industry bodies, educational institutions, consumer bodies, government and research and insight organisations, all are joining hands to create a more responsible future!

ABOUT TSAARO CONSULTING

Tsaaro Consulting is a leading authority in helping businesses navigate the complexities of data privacy and cybersecurity regulations. With a mission to assist organizations in achieving compliance and safeguarding client data, Tsaaro Consulting empowers businesses to confidently manage their privacy obligations. Tsaaro Consulting's professional services include Privacy, Cybersecurity, Governance, Risk, and Compliance (GRC), Environmental, Social, and Governance (ESG), and AI Ethics & Governance. With a meticulous, risk-based approach, Tsaaro Consulting delivers tailored solutions, monitors threats, and ensures that compliance is not a deterrent, but a business enabler, creating an environment where trust thrives and businesses succeed without worrying about regulatory fines. Tsaaro's offices are located in key business hubs across the globe, including Amsterdam, Bengaluru, Mumbai, Noida and Pune.

ABOUT PSA - LEGAL COUNSELLORS

PSA is a full-service business law firm with a driven and dynamic legal team that is trained to think out-of-the-box. Known for its business-oriented and resolution-centric reputation, they are now recognized among the top legal firms in India. The strength of the Firm lies in the ability of its legal experts in providing holistic and analytical advice. The range, breadth, and depth of the firm is broad-based and full-service, with its commercially savvy and dynamic lawyers experienced across the range of its practice areas. Be it start-ups, or large conglomerates with global footprints, PSA provides legal services in a timely and cost-effective manner. The USP of the firm is a global mindset coupled with a focus on practical and innovative legal solutions to their clients. PSA has been working with some of the largest companies on their privacy compliance and data governance requirements, especially around the DPDP Act, 2023, as well as represented companies in complex M&A, regulatory advisory, litigations and arbitrations.



ASCI, 402/A, Aurus Chambers,
S.S. Amrutwar Marg, Worli,
Mumbai 400 013



contact@ascionline.in



www.ascionline.in

