COOKIES UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Amartya Gumaste, DES Shri Navalmal Firodia Law College

ABSTRACT

This essay provides an analysis of the regulations surrounding cookies under the Digital Personal Data Protection Act, 2023 **("DPDPA").** Cookies are small data files stored on a user's device, It may collect personal data to enhance user experience by storing login credentials and preferences. The essay discusses the types of cookies, the applicability of the DPDPA to cookie usage, and the consent mechanisms under the DPDPA. The essay also provides a comparison between existing regulations under the Information Technology Act and the GDPR. The paper also addresses the issues of dark patterns in obtaining consent, cookie-related fines, and steps for compliance along with best practises under the Indian Context.

Introduction

In the realm of web browsing, Cookies are essentially small data files which are deposited on a user's device by the web server associated with relevant website being visited, these cookies are normally used to collect personal data. These files serve the function of improving the user's surfing experience by storing login credentials, user preferences, and advertisements. There are several kinds of cookies, including first-party cookies, third-party cookies, session cookies and persistent cookies.

Applicable Law relating to cookies

Digital Personal Data Protection Act, 2023

Under the Digital Personal Data Protection Act, 2023 ("**DPDPA**") personal data means any data about a person who is identifiable by or in relation to such data. Since cookies store information on a user's device, The Data collected by cookies, that can later be used to identify and profile the user can qualify as personal data under the Act. Although, since the DPDPA is yet to undergo implementation, cookies collecting certain categories of personal data are subject to the provisions of the IT Act and a few IT Rules.

Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Currently, there are no specific laws, regulations, or guidelines addressing cookie-related compliance. However, if cookies on a user's system access any sensitive personal data, this is regulated by the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**SPDI Rules**"). Sensitive personal data as defined under Rule 3 includes passwords, financial details (bank, credit, debit, payment instruments), health conditions (physical, physiological, mental), sexual orientation, medical records, biometric data, and any related details provided for service provision or processed under lawful contracts. Publicly available information or data furnished under the Right to Information Act, 2005, is not considered sensitive[1].

[1] Athavale, Varsha Vishnu. "The Study of Right to Privacy with Reference to Information Technology Act, 2000.", Maharaja Sayajirao University of Baroda (India), 2021

Obtaining Consent for cookies

Under the DPDPA, according to section 6, consent has to be:

- Given freely
- Specific
- Informed
- Unambiguous
- Unconditional
- With a clear affirmative action
- The user's consent is restricted to the precise information required for a certain legal purpose

Section 6 mandates every request made to a data principal for shall be accompanied by a notice given by the data fiduciary. The notice must specify the following: the personal data being processed and its intended use; how the individuals may exercise their DPDPA rights about the personal data; and how they may file a complaint with the Data Protection Board.

According to section 7 of the DPDPA, a Data Fiduciary may process a Data Principal's personal data for the specified purpose voluntarily provided by the Data Principal, as long as they have not withdrawn consent.

The Data Principal can manage consent through a Consent Manager. The Consent Manager must be registered with the Board, and in any proceeding, the Data Fiduciary must prove that the Data Principal was notified and gave consent as per the Act's provisions.

SPDI Rules

According to Rule 5 of the SPDI Rules, body corporates must obtain written consent (via email, fax, or letter) before collecting sensitive personal data. This consent must be acquired prior to the data collection. It also must be ensured that the data subject is aware of:

- the data being gathered
- the reason for the data collection
- the intended recipients
- the name and address of the organisation collecting the data as well as the organisation keeping it.

Rule 5(7) mandates that data subjects be given the option to refuse the collection of their data. Additionally, A Grievance officer must be appointed whose details must be given on the website. All grievances must be resolved within 1 month of receipt of such grievance.

Cookie Regulations under GDPR

Recital 30 of the GDPR specifically concerns cookies, Cookies which are used to identify users are considered as personal data and are subject to the provisions of the GDPR. Companies can process user data if they obtain consent or have a legitimate interest. Recital 30 of the GDPR explains that individuals may be associated with online identifiers originating from their devices, applications, tools, or protocols, including IP addresses, cookies, or identifiers like RFID tags. These identifiers can leave traces that, when combined with unique identifiers and other data collected by servers, may be used to build profiles and identify the individuals.

The ePrivacy Directive covers cookies, email and telephone marketing, spyware, and more. Every EU country, plus the UK, Iceland, Liechtenstein, and Norway, has implemented the ePrivacy Directive into national law. Ireland has its ePrivacy Regulations, the UK has its Privacy in Electronic Communications Regulations, and France incorporates it in Article 86 of its Data Protection Law. The guidelines for cookies are largely the same across various legislation, despite slight differences.

Recital 25, ePrivacy Directive[2] categorizes cookies as a legitimate and useful tool, provided that cookies are used for permitted purposes their use should only be on the stipulation that users are provided with clear and accurate information as mentioned under Directive 95/46/EC

[2] Directive 2002/58, of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002 O.J. (L 201) 37 (EC).

about the purposes of cookies. Users also must have the option to refuse cookies and the methods for giving this information, offering a right to refuse or requesting consent must be in a user friendly manner.

Article 5(3) of the ePrivacy Directive emphasizes the importance of consent in storing of information or gaining of access to information in the equipment of the user

The consent requirement does not apply to the following types of cookies:

- Cookies used solely for transmitting communications.
- Cookies that are absolutely necessary to provide a service the user clearly requested.

Consent needs to be given freely, explicit, informed, unambiguous, granted by a straightforward affirmative action, and simple to withdraw. The ePrivacy Directive is set to be repealed by another law called the ePrivacy Regulation. This new law has been majorly delayed, but it is expected to pass within the next few years.

The Planet49 Gmbh Judgement[3] clarified certain additional requirements pertaining to cookies

Active Consent - Pre-checked boxes in cookie notices do not offer valid consent under the GDPR and the ePrivacy Directive. Active consent is necessary, as outlined in Article 4(11) and Recital 32 of the GDPR.

Cookie Information- Users must be informed about the lifespan of cookies and third-party access. This ensures consumers can make well-informed decisions, complying with Article 5(3) of the ePrivacy Directive and Article 13(2)(a) of the GDPR.

Specific Consent- Consent must be specific and cannot be bundled. It must directly relate to the data processing in question, as confirmed by the CJEU.

Since the rules pertaining to cookies in India are still developing, It would be optimal to follow EU jurisprudence on cookies due to the similarity in consent requirements across the two

[3] CURIA, ‘Judgment of the Court (Grand Chamber) of 1 October 2019, Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände’ (Case C-673/17) [2019] ECLI:EU:C:2019:801 https://curia.europa.eu/juris/document/document.jsf?docid=218462&text=&dir=&doclang=EN&part=1&occ=first&mode=DOC&pageIndex=0&cid=703991 accessed 1 September 2024.

jurisdictions.

Dark Patterns in Obtaining Cookie Consent

There are often certain deliberate design practices that induce users make decisions they wouldn't otherwise make; these are termed to be dark patterns[4]. For example, A cookie consent banner that has hidden the reject button and made the Accept button much larger.

Clause 2(e) of the CCPA's "Dark Pattern Guidelines[5]" states that dark patterns refer to any methods or deceptive design patterns that use UI or UX (user interface/user experience) on any platform; intended to trick or mislead users into doing something they did not intend to do; by undermining or impairing their autonomy, choice, or decision-making; amounting to unfair trade practices, misleading advertisements, or violations of their rights as consumers;

French Data Protection Regulator fines google

Google LLC was fined €90 million by CNIL, while Google Ireland Limited was fined €60 million for having insufficient cookie consent procedures[6]. The rule stipulates that data controllers have to provide users with an equal level of simplicity in order to allow them to accept or refuse cookies and other trackers. CNIL found that google.fr and youtube.com had an immediate cookie acceptance button but no equivalent for rejection. Users had to perform five steps to refuse cookies (click 'customise' disable three options for 'search personalization' 'YouTube history' and 'ad personalization' then click 'confirm') compared to a single step to accept them.

Annexure 1 of the Dark Patterns Guidelines specifies ten categories of dark patterns. The following might apply to cookies.

[4] Trilegal, 'Guidelines for Prevention and Regulation of Dark Patterns 2023' (Trilegal, 12 December 2023) https://trilegal.com/wp-content/uploads/2023/12/Guidelines-for-Prevention-and-Regulation-of-Dark-Patterns-2023.pdf accessed 1 September 2024

[5] Government of India, 'Draft Guidelines for Prevention and Regulation of Dark Patterns' (Department of Consumer Affairs, 2023)https://consumeraffairs.nic.in/sites/default/files/fileuploads/latestnews/Draft%20Guidelines%20for%20Prevention%20and%20Regulation%20of%20Dark%20Patterns%202023.pdf accessed 1 September 2024.

[6] DataGuidance, 'France: CNIL Fines Google for Inadequately Facilitating Cookie Refusal' (DataGuidance, 7 January 2022) https://www.dataguidance.com/news/france-cnil-fines-google-150m-inadequately-facilitating accessed 1 September 2024

Confirm shaming- Using any means to create fear, shame, ridicule, or guilt to nudge users into purchasing a product, subscribing to a service, or continuing a subscription.

For e.g., Some platforms may employ negative framing to imply that users will miss out on certain functionalities if they do not consent. For example, "If you decline cookies, some features of the site may be unavailable."

Interface interference- refers to design elements that manipulate the user interface by (a) highlighting specific information and (b) obscuring other relevant information to misdirect the user from their desired action.

These types of practices can include

- Pre checked cookie categories
- A notice only banner with no accept or reject option
- A Deceptive link design
- Using unfavourable fonts, colours and contrasts to tamper with visibility

Steps towards compliance

Data fiduciaries can use standalone consent management platforms ("**CMP**") to collect, track, manage, and synchronize consents, automating the process and ensuring compliance with the DPDPA. CMPs can manage cookie permissions, update preferences, and block third-party scripts until consent is given. They can also display cookie banners and provide information as required by the Act.

In India, like the GDPR and unlike the CCPA (Opt-out mechanism) an opt-in consent framework would be required where a user gives consent by affirmative action, This could be done by checking boxes to signify acceptance or giving express approval by other forms concerning the processing of data. Here are some steps organisations can implement to remain compliant with the provisions of the DPDPA, although there may be additional requirements with the notification of Digital Personal Data Protection Rules.

1. Cookie Banners: Implement cookie banners that inform users of the use of cookies and

allow them to accept or change cookie settings.

2. Cookie Policy: Develop a cookie policy that describes the types of cookies used, their purpose and how users can manage their preferences.

3. Consent management: Implement consent management systems that allow users to quickly grant and withdraw consent. These forums must keep records of user consent in compliance with the DPDPA.

4. Regular Audits: Conduct regular reviews of the site's cookie usage to remain compliant with the DPDPA.

Conclusion

The DPDP Act will replace Section 43A of the IT Act, 2000, and the SPDI Rules, 2011, which have been India's data protection law until now. The new framework will consist of the DPDP Act and additional rules issued by the Central Government. The Rules supplementary to the DPDPA are still yet to be notified and will undergo implementation soon. The DPDPA will supersede the IT Rules regarding data protection. The IT Rules will likely be amended or repealed altogether.