

**Experiment No.: 07**

**Title: Privacy Policies of Social Media Websites.**

**Batch: A-4** **Roll No.:16010422211**  **Experiment No: 07**

**Aim: Privacy Policies of Social Media Websites**

To understand the privacy policies of Social Media Websites in the context of GDPE

and DATA Protection Bill

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Resources needed:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Theory:**

A privacy policy is a document that explains how an organization handles any customer, client or employee information gathered in its operations. Most websites make their privacy policies available to site visitors. The privacy policy must describe the information collected, the purpose of use of the information, to whom and how to disclose the information and reasonable security practices followed to safeguard such information. As per the Information Technology Act, all businesses require to have a privacy policy that is published on their website. The privacy policy must describe the information collected, the purpose of use of the information, to whom and how to disclose the information and reasonable security practices followed to safeguard such information. The Information Technology Act also requires the appointment of a Grievance Officer whose name and contacts are published on the website. The

Grievance Officer requires to act on any compliance within 30 days relating to the

Privacy policy or user information collection.

The relevant Indian laws governing online data protection are the Information Technology Act,2000 (IT Act) and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The Digital Personal Data Protection Bill, 2023 The Bill applies to the processing of digital personal data within India where such data is: (i) collected online, or (ii) collected offline and is digitised. It will also apply to the processing of personal data outside India if it is for offering goods or services in India. Personal data is defined as any data about an individual who is identifiable by or in relation to such data. Processing has been defined as wholly or partially automated operation or set of operations performed on digital personal data. It includes collection, storage, use, and sharing.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**



**Results: (Queries printout with output)**

**Students need to select any social media site or companies website and compare their privacy policies with respect to our final data protection bill 2023.**

**Example**

| **Aspect** | **Privacy Policy (Twitter)** | **Data Protection Act of India(2023)** |
| --- | --- | --- |
| **Information**  **Collection** | **Collects various user data, including**  **personal, usage, device, location,**  **and biometric information.** | **Regulates the processing of personal data**  **and imposes obligations on data**  **Fiduciaries.** |
| **Data Usage** | **Uses data for purposes like**  **improving services, personalization,**  **research, and marketing.** | **Data processing should align with lawful**  **purposes defined by the Act.** |

***INSTAGRAM:***

| ***Aspect*** | ***Instagram's Privacy Policy*** | ***Data Protection Act of India (DPAI)*** |
| --- | --- | --- |
| ***Data Collection and Usage*** | *- Describe how Instagram collects and uses user data* | *- Compare Instagram's practices with DPAI requirements* |
| ***Consent Mechanisms*** | *- Explain how users can provide or withdraw consent* | *- Check if Instagram's consent mechanisms align with DPAI* |
| ***Data Sharing and Third Parties*** | *- Outline Instagram's data sharing practices* | *- Compare these practices with DPAI regulations* |
| ***Data Security*** | *- Detail security measures to protect user data* | *- Assess Instagram's security practices in line with DPAI standards* |
| ***Data Retention Policies*** | *- State how long Instagram retains user data* | *- Ensure Instagram's retention policies comply with DPAI guidelines* |
| ***User Rights*** | *- Describe how users can exercise their rights* | *- Compare with DPAI-mandated user rights and compliance mechanisms* |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Outcomes:**

**Relate cyber laws to its applications in business and e-commerce.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1)Write the highlights of DATA Protection Bill

2) Differentiate between GDPR and DATA Protection Bill.

3) Compare the privacy protection of data with respect to IT ACT and Data Protection Bill.

**Answers:**

**1)** *Some common highlights or provisions typically found in data protection bills or regulations***:**

**1. *Personal Data Definition:*** *The bill typically defines what constitutes personal data, encompassing any information related to an identified or identifiable natural person.*

***2. Data Subject Rights:*** *Data protection bills often include provisions outlining the rights of data subjects, which may include the right to access, correct, delete, or export their personal data****.***

***3. Consent and Consent Withdrawal:*** *Regulations frequently require organizations to obtain explicit and informed consent from individuals before collecting and processing their personal data. Data subjects usually have the right to withdraw their consent at any time.*

***4. Data Processing Principles:*** *Data protection laws often include principles for lawful and fair processing of personal data, such as data minimization, purpose limitation, and storage limitation****.***

***5. Data Security:*** *The bill may set security standards and require organizations to implement appropriate measures to safeguard personal data from breaches and unauthorized access****.***

***6. Data Breach Notification:*** *Many data protection regulations mandate that organizations report data breaches to both authorities and affected**individuals within a specified timeframe.*

***7. Data Protection Impact Assessments (DPIAs):*** *DPIAs are used to assess the potential risks of data processing activities, and data protection laws may require organizations to conduct these assessments in certain situations***.**

***8. Data Transfer Restrictions:*** *Some regulations restrict the transfer of personal data outside the jurisdiction unless certain conditions or safeguards are met.*

***2)*** *However, for the purpose of this response, let's compare GDPR with a hypothetical generic "DATA Protection Bill" to highlight the key differences:*

***1. Scope and Applicability:***

***- GDPR:*** *The GDPR is a comprehensive data protection regulation that applies to all European Union (EU) member states. It also extends its reach to organizations outside the EU that process the data of EU residents.*

***- DATA Protection Bill:*** *This term is generic and could refer to any specific data protection legislation. Depending on the specific bill, its scope and applicability may vary. It might be a national or regional law applicable to a specific country or area.*

***2. Jurisdiction:***

***- GDPR:*** *It has a wide territorial scope, impacting organizations globally if they handle the data of EU citizens****.***

***- DATA Protection Bill:*** *Depending on the specific bill, it may have a narrower jurisdiction, applying only within a specific country or region****.***

***3. Penalties and Fines:***

***- GDPR****: It has stringent penalties for non-compliance, with fines of up to 4% of the annual global turnover or €20 million, whichever is higher.*

***- DATA Protection Bill:*** *Penalties and fines would vary based on the specific legislation. They may be less severe than those outlined in the GDPR, or they could potentially be even more stringent depending on the jurisdiction****.***

***4. Specific Requirements:***

***- GDPR:*** *GDPR imposes specific requirements like data subject rights, data protection impact assessments, mandatory data breach notifications, and the appointment of data protection officers, among others.*

***- DATA Protection Bill:*** *The specific requirements would depend entirely on the content of the individual bill. It might include similar provisions to GDPR, or it might have a different set of requirements altogether****.***

***5. Data Subject Rights:***

***- GDPR:*** *GDPR grants individuals a range of rights, including the right to access their data, the right to be forgotten, and the right to data portability, among others.*

***- DATA Protection Bill:*** *The rights granted to data subjects would depend on the specific provisions of the bill. They might align closely with GDPR, or they could differ significantly.*

***6. GDPR Specifics:***

***- GDPR:*** *GDPR includes provisions for data protection officers (DPOs), the right to erasure ("right to be forgotten"), and strict rules for obtaining valid consent for data processing****.***

***- DATA Protection Bill****: Depending on the specific bill, it may or may not include similar provisions. The inclusion of these specifics would be outlined in the content of the individual legislation****.***

***3)***

***1. Scope and Applicability:***

***- IT Act:*** *The IT Act is the primary legislation in India that addresses various aspects of electronic commerce, digital signatures, cybercrime, and digital communication. While it includes provisions related to data protection, it doesn't provide comprehensive privacy regulations like a dedicated data protection law.*

***- Data Protection Bill:*** *A Data Protection Bill, if enacted, would specifically focus on privacy protection, encompassing a broader set of rules and regulations for handling personal data. It would likely provide more robust privacy safeguards.*

***2. Data Subject Rights:***

***- IT Act:*** *The IT Act includes some provisions related to the protection of sensitive personal data and information, but it doesn't outline specific data subject rights as comprehensively as a dedicated data protection law would.*

***- Data Protection Bill:*** *A Data Protection Bill is expected to define and enumerate specific data subject rights, such as the right to access, rectify, erase, and port personal data. It would provide individuals with more control over their personal information.*

***3. Consent and Purpose Limitation:***

***- IT Act:*** *The IT Act contains provisions regarding obtaining consent for collecting and processing data, but it may not go into as much detail as a dedicated data protection law would****.***

***- Data Protection Bill:*** *A Data Protection Bill is likely to include explicit provisions on obtaining informed consent for data processing. It would also likely specify the purposes for which data can be collected and processed.*

***4. Data Localization:***

***- IT Act:*** *The IT Act, as of my last knowledge update, does not include specific provisions on data localization.*

***- Data Protection Bill:*** *Depending on the content of the specific Data Protection Bill, it may include provisions regarding data localization, specifying where certain types of data must be stored and processed****.***

***5. Data Breach Notification:***

***- IT Act:*** *The IT Act contains provisions for reporting and investigating cyber incidents, but it may not provide as detailed guidance on data breach notification requirements as a dedicated data protection law.*

***- Data Protection Bill:*** *A Data Protection Bill is likely to have explicit requirements for organizations to notify authorities and affected individuals in the event of a data breach within a specified timeframe****.***

***6. Penalties and Fines:***

***- IT Act:*** *The IT Act includes penalties for various cybercrimes and offenses, but it may not specify fines related to data protection violations.*

***- Data Protection Bill:*** *A Data Protection Bill would likely include specific provisions for penalties and fines for non-compliance with data protection regulations, potentially imposing substantial financial consequences****.***

*Privacy policies for social media websites are important documents that outline how these platforms collect, use, share, and protect user data. with a general overview of what such policies typically cover:*

*1. Data Collection: Social media platforms explain what types of data they collect from users. This can*

*include personal information like names, email addresses, phone numbers, and sometimes more*

*sensitive information like location data.*

*2. Cookies and Tracking: They describe the use of cookies and other tracking technologies, which are*

*used to gather information about users' online activities for various purposes.*

*3. User-generated Content: They detail how the platform handles the content users upload, post, or*

*share, including text, images, videos, and other media.*

*4. Profile Information: The policy typically covers the information provided in user profiles, such as profile*

*pictures, bios, and other details.*

*5. Usage Information: Platforms explain how they track and use data related to users' interactions with*

*the platform, such as likes, comments, shares, and the pages or accounts they follow.*

*6. Communication and Messaging: The policies outline how the platform handles user communications,*

*including messages, chats, and comments.*

*7. Third-party Access: They may mention whether and how third-party services and advertisers can*

*access or interact with user data.*

*8. Advertising and Personalization: Social media platforms often use data to target ads to users. The*

*policy should cover how this is done and what options users have for controlling personalized*

*advertising.*

*9. Data Sharing: They specify whether and how user data is shared with third parties, including affiliates,*

*partners, advertisers, and service providers.*

*10. Security Measures: Platforms explain the measures they take to secure user data and protect it from*

*unauthorized access or breaches.*

**Conclusion:**

**Relate cyber laws to its applications in business and e-commerce.**

**-----------------------------------------------------------------------------------------------------------------**

**Grade: AA / AB / BB / BC / CC / CD /DD**

**Signature of faculty in-charge with date**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**References:**

**Books:**

1. Nina Godbole, Sunit Belapure Cyber Security Understanding Cyber Crimes,Computer Forensics and Legal Prespectives” Wiley- India 1st Edition,

2 N S Nappinai Technology Laws Decodded LexisNexis 1 st Edition, 2017

https://enhelion.com/blogs/2022/09/01/role-of-intellectual-property-in-cyber-law/#:~:text=The%20IPR%20protects%20these%20works,available%20even%20for%20online%20infringements.