Security and Privacy Standards

What is Privacy

- Security deals with how the data and resources are protected from all forms of intended and unintended misuse.
- Privacy, on the other hand relates to any rights a user has to control his/her personal information and how it's used.
- Privacy is concerned with regulating:
    - A list and description of information collected
    - Where the information is collected
    - Why is it collected
    - How it is collected
    - Who else can see it and whether it will be shared or sold
    - How users can use those rights
    - The rights that users have over their data
    - How users can use those rights

Need for Privacy

- In this era of digitization, every aspect of a person is digitised
- Private companies have information regarding:
  - the websites you visit
  - the places you visit
  - the products you buy
  - food you order
  - your friends, family
  - your daily habits
  - ……..

Need for Privacy

- Targeted advertisement
- Can manipulate elections - Example: Cambridge Analytica
- Healthcare system
- Can also affect personal safety

General Data Protection Regulation (GDPR)

- Privacy regulation in European Union
- Processing: Any operation on personal data such as collection, recording, organization, storage, alteration, use, transmission, destruction, etc.
- Profiling: Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements
- Controller: One who determines the purposes and means of the processing of personal data
- Processor: One who processes personal data on behalf of the controller

General Data Protection Regulation

- Right to be Informed: Data subjects have the right to be informed about the collection and use of their personal data.
- Right of access by the data subject: Data subjects have the right to view and request copies of their personal data.
- Right to rectification: Data subjects have the right to request inaccurate or outdated personal information be updated or corrected.
- Right to erasure (‘right to be forgotten’): Data subjects have the right to request their personal data be deleted.
- Right to data portability: Data subjects have the right to ask for their data to be transferred to another controller or provided to them.
- Right to object: Data subjects have the right to object to the processing of their personal data.

General Data Protection Regulation

- Right to restrict processing: Data subjects have the right to request the restriction or suppression of their personal data.
- Right to withdraw consent : Data subjects have the right to withdraw previously given consent to process their personal data.
- Right to object to automated processing : Data subjects have the right to object to decisions being made with their data solely based on automated decision making or profiling.

Data Protection in India

- In India the Ministry of Electronics and Information Technology is responsible for data protection related regulation
- The IT Act and IT Amendment Act 2008 specify laws regarding some aspects of cyber security
- It covers issues such as use of malwares, DoS attacks, Phishing, Digital Signatures, etc,
- Also gives a right to compensation for improper disclosure of personal information.

Data Protection in India

- The Digital Personal Data Protection (DPDP) Act 2023 applies to the processing of digital personal data within India
- It regulates how personal data can be collected, processed
- It applies to the processing of digital personal data within the territory of India where the personal data is collected––
    (i) in digital form; or
    (ii) in non-digital form and digitised subsequently;
- It also applies to processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India;

Data Protection in India

Does not apply to—

(i) personal data processed by an individual for any personal or domestic purpose; and

ii) personal data that is made or caused to be made publicly available

Key Objectives and Principles

- **Balancing Rights:** The Act aims to protect the rights of individuals regarding their personal data while enabling its processing for legitimate purposes.
- **Data Fiduciary Obligations:** The Act places obligations on "data fiduciaries," which are entities that determine the purpose and means of processing personal data.
- **Data Protection Board:** The Act establishes a Data Protection Board to oversee the implementation and enforcement of the Act.
- **Consent Management:** The Act emphasizes the importance of consent in data processing, requiring clear and informed consent from individuals.
- **Security Measures:** Data fiduciaries are required to implement reasonable security safeguards to prevent data breaches and ensure data accuracy.

Key Objectives and Principles

- Data Breach Notifications: The Act mandates that data fiduciaries notify affected individuals and the Data Protection Board in case of a data breach.
- Processing Children's Data: The Act includes provisions for the processing of children's data, with specific safeguards in place.
- Cross-Border Data Transfers: The Act addresses the issue of cross-border data transfers, requiring compliance with certain conditions.
- Exemptions for Research and Statistics: The Act includes exemptions for processing personal data for research and statistical purposes, subject to certain conditions.
- Significant Data Fiduciaries: The Act imposes additional obligations on "Significant Data Fiduciaries," which are entities that process a large amount of personal data.

Obligations of Data Fiduciaries

- Security Safeguards: Implement reasonable security measures to prevent data breaches.
- Data Breach Notification: Inform affected individuals and the Data Protection Board in case of a data breach.
- Data Accuracy: Make reasonable efforts to ensure the accuracy and completeness of data.
- Data Erasure: Erase personal data when it is no longer needed for the specified purpose or upon withdrawal of consent.
- Grievance Redressal: Have in place a grievance redressal system and an officer to respond to queries from Data Principals.
- Data Protection Officer: Significant Data Fiduciaries are required to appoint a Data Protection Officer.
- Data Protection Impact Assessment: Significant Data Fiduciaries are required to conduct periodic Data Protection Impact Assessments

Security Standards

- A standard is a document, established by consensus and approved by a recognized body, that provides, rules, guidelines, or characteristics for activities or their results.
- A cybersecurity standard is a set of guidelines or best practices that organizations can use to improve their cybersecurity posture.
- Cyber security standards cover a broad range of granularity, from the mathematical definition of a cryptographic algorithm to the specification of security features in a web browser, and are typically **implementation independent.**
- Numerous standards have been developed for cyber security to help organizations better manage security risk, implement security controls that meet **legal and regulatory requirements**, and achieve **performance and cost benefits**.
- Every organization has its own mission, structure, userbase, technology
- Depending on the organization, it can select the standards that applies to it

Advantages of Security Standards

- Security standards facilitate **sharing of knowledge and best practices** by helping to ensure common understanding of concepts, terms, and definitions, which prevents errors.
- Standards help e**stablish common security requirements and the capabilities needed** for secure solutions.
- Standards **reduce the number of technical variations** and allow consumers easy access to interchangeable technology.
- Standards compliance programs offer a way to measure products and services against objective criteria and **provide a basis for comparing products**, such as confirming that they offer certain sets of security features.
- Consumers often benefit from **cost savings** that result from the development, manufacture, sales, and delivery of standards-based, interoperable products and services.
- Well-developed cyber security standards **enable consistency among product developers** and serve as a reliable metric for purchasing security products.
- Cyber security standards **enhance security and contribute to risk management** in several important ways.

Characteristics of a Good Standard

- A standard must address user needs, but must also be practical since cost and technological limitations must be considered in building products to meet the standard.
- A standard's requirements must be verifiable; otherwise, users cannot assess security even when products are tested against the standard.

Types of Standards

- International Standards: one that is adopted by an international standards development organization (SDO) and made available to the public. Ex: ISO standards
- Regional standard: a standard adopted by several nations in a particular geographic region, for example, European Committee for Standardization (CEN) standards.
- National standard: a standard developed for use in a particular country either by a government entity or a national SDO.
- Industry standard: one that has been adopted by a particular industry for common use, for example, Security Industry Association (SIA) standards.
- Company standard/ proprietary standard: a standard developed and owned by a commercial entity that specifies practices or conventions unique to that entity.

Security Standards Examples

- ISO 27000 series
- NIST SP 800 series
- Federal Information Processing Standards (FIPS) : A standard for adoption and use by federal departments and agencies of the USA
- PCI: Payment Card Industry Security Standards

ISO 27000

- International Organization for Standardization (ISO) is an independent non-government organization with more than 150 member countries (including India)
- It develops various standards in the series
- ISO 27000 is an international standards that sets specification for an Information Security Management Systems (ISMS) to create a continuous program for applying security controls to an organization
- Certification agency will audit and issue certificates

ISO 27000

- ISO focuses on following:
  - Systematically examining security risks, threats, vulnerabilities, and their impact
  - Designing and implementing security controls to manage risks
  - Continuous management process to keep the system secure

ISO 27000

- ISO 27000 series has namy standards. Some of them are:
  - ISO 27018 addresses cloud computing.
  - ISO 27031 provides guidance on IT disaster recovery programs and related activities.
  - ISO 27037 addresses the collection and protection of digital evidence.
  - ISO 27040 addresses storage security.
  - ISO 27799 defines information security in healthcare

Other Guidelines and Frameworks

- Data Security Council of India (DSCI) established by National Association of Software and Services Companies (NASSCOM) publishes best practices in cybersecurity
- RBI has issued a cyber security framework for all commercial banks through Reserve Bank of India Act 1934
- Indian Medical Council issues guidelines for protection of healthcare data

References

1. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152153#:~:text=A%20cyber%20security%20standard%20defines,metric%20for%20purchasing%20security%20products.
2. https://gdpr-info.eu/
3. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf