



## Safeguarding Personally Identifiable Information

**For Prelims:** [Personally Identifiable Information](#), [Computer Emergency Response Team of India \(CERT-In\)](#), [Social Engineering Attacks](#), [Privacy](#), [Cybercrime](#), [Digital Personal Data Protection Act, 2023](#), Extended detection and response (XDR) tools.

**For Mains:** Data Breach, Cyber Crime, Related Challenges and Measures to Deal with it.

[Source: TH](#)

### Why in News?

Recently, the **Ministry of Corporate Affairs** fixed a critical vulnerability in its online portal after a cybersecurity researcher reported it to the [Computer Emergency Response Team of India \(CERT-In\)](#).

- The vulnerability reportedly exposed [Personally Identifiable Information \(PII\)](#) like [Aadhaar](#), [Permanent Account Number \(PAN\)](#), [Voter identity](#), date of birth, contact number, and communication address of more than 98 lakh directors of Indian companies.

### What is Personally Identifiable Information (PII)?

- **About:**
  - PII is any **data or information maintained by an organisation or agency** that can potentially be **used to identify a specific individual**.
    - This could include information such as **Aadhaar, PAN, voter identity, passport, date of birth, contact number**, communication address, and biometric information.
  - The constituents of PII vary depending on an **individual's home country**.
- **Types of PII:**
  - PII comes in two types: **direct identifiers and indirect identifiers**.
    - **Direct identifiers are unique to a person** and include things like a passport number or driver's license number.
      - A single direct identifier is typically enough to determine someone's identity.
    - **Indirect identifiers are not unique**. They include more general personal details like race and place of birth. While **a single indirect identifier can't identify a person, a combination can**.
- **Sensitive vs. Non-sensitive PII:**
  - Among PII, some pieces of information are more sensitive than others.
  - **Sensitive PII:**
    - It is sensitive information that **directly identifies an individual and could cause significant harm** if leaked or stolen.
    - **Sensitive PII is typically not publicly available**, and most existing data privacy laws require organizations to safeguard it by encrypting it, controlling who accesses it, or taking other cybersecurity measures.

- **Non-sensitive PII:**
  - It is personal data that, in **isolation, would not cause significant harm to a person if leaked or stolen.**
    - It **may or may not be unique to a person.**
  - For example, a social media handle would be non-sensitive PII. It could identify someone, but a malicious actor couldn't commit identity theft armed with only a social media account name.
  - This also includes information such as **zip code, race, gender, and religion.** They cannot be used to accurately identify an individual.
- **Non PII:**
  - **Non-personally identifiable information (non-PII)** is data that cannot be **used on its own to trace, or identify a person.** However, non-PII in tandem with **additional information can be used to identify an individual.**
    - Non-PII information includes photographic images (especially of the face or other identifying characteristics), place of birth, religion, geographic indicators, employment information, educational qualifications, and medical records.

## What are the Risks of PII Exposure?

- **Identity Theft:**
  - PII exposure increases the risk of identity theft, where criminals use stolen personal information to impersonate individuals for fraudulent activities.
  - **Cyberattacks and weaknesses in [digital infrastructure](#)** can lead to the exposure of citizens' PII.
- **Financial Fraud:**
  - Exposed PII, such as **bank account numbers or credit card information**, can lead to **financial fraud.**
    - Criminals may access bank accounts, make unauthorized transactions, commit payment fraud, and **siphon funds from accounts allotted to beneficiaries of government [welfare programmes](#)**, resulting in **financial loss for the victim.**
- **Privacy Violations:**
  - PII exposure can **violate privacy**, compromising individuals' **confidentiality and autonomy.**
    - Unauthorized access to personal information can result in **stalking, harassment, or intrusion into individuals' private lives.**
- **Phishing and Social Engineering Attacks:**
  - Cybercriminals may use exposed PII to conduct **phishing attacks**, tricking **individuals into disclosing further sensitive information** or clicking on malicious links.
    - Social engineering attacks, such as impersonation scams or pretexting, exploit exposed PII to manipulate individuals into **revealing confidential data or granting unauthorized access.**
- **Data Breach Fallout:**
  - PII exposure often occurs through **data breaches**, leading to significant financial losses, remediation costs, and damage to the organization's reputation.
    - Organizations may suffer from diminished customer trust, decreased revenue, and increased scrutiny from regulators and stakeholders.
- **Reputation Damage:**
  - Exposure of sensitive PII, such as compromising photos or personal messages, can damage individuals' reputations and relationships.
    - Information leaked online may be used for **blackmail, extortion**, or **public humiliation**, leading to social and professional consequences.

## Instances of Data Breach in Past:

- **CoWIN Data Breach Allegations:**
  - Reports emerged about a **Telegram bot** returning the **personal data of Indian citizens registered** on the **CoWIN portal.**
    - A similar data breach was reported when an **American cybersecurity company** claimed the PII of 815 million Indian citizens, including Aadhaar numbers and

passport details, were being sold on the dark web.

- The Indian government denied allegations of biometric data leaks and CoWIN portal breaches and stated that the CoWIN website is safe and has adequate safeguards for data privacy.

- **Aadhaar:**

- Aadhaar data leaks were also reported in 2018, 2019, and 2022, with three instances of **large-scale leaks being reported**, including one in which farmer's data stored on the [PM Kisan website was made available on the dark web](#).

- **RailYatri Platform Data Breach:**

- A data breach was also reported in the RailYatri platform in January 2023.

- **Increase in Cyberattacks on Government and Essential Services:**

- Additionally, 67% of Indian government and essential services organisations experienced over a **50% increase in disruptive cyberattacks**, a report from Resecurity (an American cybersecurity company) said.
- Furthermore, a survey of 200 IT decision-makers noted that **45% of Indian businesses experienced more than a 50% increase in cyberattacks**.

## Provisions Related to Data Governance in India:

- [Information Technology \(Intermediary Guidelines and Digital Media Ethics Code\) Rules 2021](#).

- [Justice K. S. Puttaswamy \(Retd\) vs Union of India 2017](#).

- [Digital Personal Data Protection Act, 2023](#):

- Regulates the **processing of personal data in India**. The act applies to both online and offline data collection and processing, including activities outside India if they involve offering goods or services in India.

- **Computer Emergency Response Team - India (CERT-In):**

- In the **Information Technology Amendment Act 2008**, CERT-In has been designated to **serve as the national agency** to perform several functions in the area of cyber security: Collection, analysis and dissemination of information on cyber incidents also issue alerts on cybersecurity incidents.
  - It is an organisation of the **Ministry of Electronics and Information Technology**.
  - **CERT-In's objectives include:** Preventing cyber attacks against the country's cyberspace, Responding to cyber attacks and minimizing damage and recovery.

## What are the Challenges in Protecting PII?

- **Diverse Sources:**

- PII may be stored and processed across multiple locations due to the growth of cloud computing and SaaS services.

- **Increasing Data Volume:**

- The amount of sensitive data stored in public clouds is projected to double by 2024, posing challenges in ensuring its security.

- **Evolving Threat Landscape:**

- Cybercriminals employ various techniques, including [social engineering attacks](#) and **purchasing data** on the dark web, to steal PII.

- **Complex Regulatory Environment:**

- Organizations must navigate different **data privacy regulations and tailor their protection measures accordingly**.

## Way Forward

- **Encryption:**

- Employ encryption techniques **to protect PII**, regardless of the data's state whether **it is at rest in a database, in transit across the internet, or even in use**.

- **Identity and Access Management (IAM):**
  - Utilize **two-factor or multifactor authentication** and **zero-trust architecture (ZTA)** to limit access to sensitive data.
    - ZTA is based on the **principle of “never trust, always verify.”** It requires organisations to verify the identity of each user and continuously monitor user behaviour for malicious activity.
- **Training:**
  - Provide employees with **training on handling and protecting PII**, including anti-phishing and social engineering awareness.
- **Anonymization:**
  - Anonymize sensitive data to remove identifying characteristics.
- **Cybersecurity Tools:**
  - Deploy **data loss prevention (DLP) and extended detection and response (XDR) tools** for tracking and detecting PII misuse.
    - XDR tools are security tools that gather data from across a network and **manage automated responses to threats.**
- **Collaboration and Partnerships:**
  - Collaborate with cybersecurity experts, regulatory bodies, and industry peers to stay informed about emerging threats and best practices in PII protection.

## UPSC Civil Services Examination, Previous Year Questions (PYQs)

### Prelims

**Q1. 'Right to Privacy' is protected under which Article of the Constitution of India? (2021)**

- (a) Article 15
- (b) Article 19
- (c) Article 21
- (d) Article 29

**Ans: (c)**

**Q.2 In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)**

1. Service providers
2. Data centres
3. Body corporate

**Select the correct answer using the code given below:**

- (a) 1 only
- (b) 1 and 2 only
- (c) 3 only
- (d) 1, 2 and 3

**Ans: (d)**

### Mains

**Q. What are the different elements of cyber security ? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. (2022)**

