**Data Privacy**

* **Data Privacy** = Protecting people’s personal information (like your name, email, phone number, medical history, financial data) and ensuring it is collected, stored, and shared responsibly.
* **Why it matters**:
  + Prevents **identity theft** and fraud.
  + Protects people’s **freedom and rights** (e.g., not being tracked without consent).
  + Builds **trust** between users and organizations (you wouldn’t trust a bank that leaks your details).
  + Many countries have **laws** that punish mishandling of personal data.

**Data Privacy vs Data Security**

* **Data Privacy**: About **who has the right** to access/use your data.
  + Example: A company asking your consent before collecting your location.
* **Data Security**: About **how data is protected** from hackers, leaks, or unauthorized access.
  + Example: Encrypting your banking details so hackers can’t steal them.

Privacy = the rules, Security = the lock & alarm system.

**Examples of Personal Data**

This is also called **PII (Personally Identifiable Information)** and other sensitive categories:

* **PII (Personal Identifiable Information)**: Name, email, phone number, date of birth, Aadhaar number, driver’s license.
* **PHI (Protected Health Information)**: Medical records, prescriptions, test results.
* **Financial Data**: Credit card numbers, bank account details, tax information.
* **Digital Identifiers**: IP address, location, browsing history, device IDs.

Basically, **any data that can identify you or be linked back to you.**

**Personally Identifiable Information (PII)**

* **Definition**: Any data that can identify a specific person.
* **Examples**:
  + **Direct identifiers**: Name, Aadhaar number, passport, phone number.
  + **Indirect identifiers**: Date of birth + location + gender (combined, these can identify you).
* **Why important?**: PII must be protected because misuse can lead to identity theft, fraud, or surveillance.

**Data Lifecycle**

Every piece of data goes through these stages:

1. **Collection** – Gathering data (forms, apps, sensors, websites).
   * Example: You sign up for Instagram and give your email & phone number.
2. **Storage** – Saving the data securely (databases, cloud).
3. **Use** – Processing the data for services (recommendations, billing, healthcare).
4. **Sharing** – Passing data to 3rd parties (ad companies, research partners).
5. **Deletion/Destruction** – Securely erasing data when no longer needed.

**Privacy by Design (PbD)**

A principle that says **privacy should be built into systems and processes from the start** (not added later as an afterthought).

* Example:
  + Apps asking for **minimum permissions** instead of everything.
  + Default settings should be **privacy-friendly** (opt-in, not opt-out).
* PbD has **7 principles** (high-level for beginners): proactive, default, embedded, full functionality, end-to-end security, visibility, user-centric.

**Data Minimization & Consent**

* **Data Minimization**: Collect only the data you truly need.
  + Example: A food delivery app doesn’t need your passport number – just address & phone.
* **Consent**: Users should have clear control over whether their data is collected and how it’s used.
  + Example: Websites asking you to **accept/reject cookies**.

**Difference Between Anonymization, Pseudonymization, and Encryption**

* **Anonymization**: Irreversibly removing personal identifiers so the person can’t be identified.
  + Example: Removing names, phone numbers, and replacing with random codes permanently.
* **Pseudonymization**: Replacing identifiers with fake ones, but you can reverse it with a key.
  + Example: Replacing “Rohit” with “User123” in a dataset, but the company can still map it back.
* **Encryption**: Converting data into unreadable form, only accessible with a key.
  + Example: Encrypting your WhatsApp chats – only you and the recipient can read them.

## ****India’s Digital Personal Data Protection Act (DPDP Act, 2023)****

* India’s **first major data privacy law**, passed in 2023.
* **Key Features**:
  + Applies to **digital personal data** (online data, or offline data that’s digitized).
  + Data can only be collected for a **lawful purpose** with **consent**.
  + Data subjects (called “Data Principals”) have rights: access, correction, deletion, grievance redressal.
  + **Children’s data**: parental consent needed for under 18.
  + Data Protection Board of India will enforce compliance.
* **Penalties**: Up to ₹250 crore (~$30M) for violations.

## ****Other Global Regulations (High-Level Overview)****

* **HIPAA (USA – Health Insurance Portability and Accountability Act)**
  + Protects **health data (PHI)** like medical records.
  + Hospitals, doctors, and insurers must follow strict rules.
* **LGPD (Brazil – Lei Geral de Proteção de Dados, 2020)**
  + Brazil’s version of GDPR, covers both online & offline data.
* **PIPEDA (Canada)**
  + Protects personal info collected by businesses in Canada.
* **China’s PIPL (Personal Information Protection Law, 2021)**
  + Very strict, regulates both local and foreign companies processing Chinese citizens’ data.

**Tools & Techniques for Privacy**

## ****1. Basic Encryption Concepts (AES, RSA – Beginner Level)****

**Encryption** = converting readable data (plaintext) into unreadable form (ciphertext) using a key.  
Only someone with the right **decryption key** can unlock it.

* **AES (Advanced Encryption Standard)**
  + Symmetric encryption (same key for encryption & decryption).
  + Very fast, used in Wi-Fi security, cloud storage, banking.
* **RSA (Rivest–Shamir–Adleman)**
  + Asymmetric encryption (public key to encrypt, private key to decrypt).
  + Slower, but secure. Often used in digital signatures and HTTPS certificates.

Example: WhatsApp uses **end-to-end encryption** (AES + RSA hybrid) so only sender & receiver can read messages.

## ****2. Data Masking and Tokenization****

* **Data Masking**: Replacing sensitive data with fake but realistic-looking values.
  + Example: Credit card 1234-5678-9012-3456 → XXXX-XXXX-XXXX-3456.
  + Often used in testing environments to protect real data.
* **Tokenization**: Replacing sensitive data with a random token (reference ID).
  + Example: When you save your card on Amazon, they store a **token** instead of your real number.
  + The token has no meaning outside the system.

## ****3. Secure Data Storage & Transmission****

* **HTTPS (HyperText Transfer Protocol Secure)**
  + Encrypts communication between your browser and websites.
* **VPN (Virtual Private Network)**
  + Creates a secure, encrypted tunnel for your internet traffic.
  + Hides your IP address and prevents tracking on public Wi-Fi.
* **SSL/TLS (Secure Sockets Layer / Transport Layer Security)**
  + Protocols that power HTTPS.
  + Protects data in transit from being intercepted (man-in-the-middle attacks).

## ****4. Understanding Cookies, Trackers, and Browser Privacy****

* **Cookies**: Small text files stored by websites in your browser.
  + Useful (session cookies, shopping carts).
  + Risky (tracking cookies used for ads).
* **Trackers**: Scripts that follow your online activity (Facebook Pixel, Google Analytics).
* **Browser Privacy Tools**:
  + **Incognito/Private Mode**: Prevents local history storage (but not total anonymity).
  + **Ad-blockers & Anti-tracking extensions**: Stop trackers.
  + **Privacy-focused browsers**: Brave, Firefox with strict settings, Tor (for anonymity).

## ****Organizational & Personal Privacy Practices****

## ****1. Privacy Policies – What to Look For****

A **privacy policy** tells you how a company collects, uses, shares, and protects your data.  
When reading one, check:

* **What data is collected?** (name, location, browsing history, etc.)
* **Why is it collected?** (service improvement, ads, analytics).
* **Who is it shared with?** (partners, advertisers, third parties).
* **How long is it stored?** (indefinite storage = red flag).
* **What rights do you have?** (opt-out, delete data, access info).

Example: Apple’s policy focuses on **minimal data collection**, while Meta/Facebook collects **a lot** for ads.

## ****2. Data Handling Best Practices for Employees****

Organizations train employees to avoid privacy breaches. Best practices:

* Collect **only necessary data**.
* Store data in **secure systems** (encrypted databases).
* Avoid sending sensitive data over email without encryption.
* Use **role-based access control (RBAC)** → employees only access data they need.
* Report data breaches immediately.

## ****3. Cyber Hygiene****

Like personal hygiene, but for your digital life.

* **Strong Passwords**:
  + At least 12 characters, mix of letters, numbers, symbols.
  + Avoid birthdays, names, or “12345.”
  + Use a **password manager** (Bitwarden, 1Password).
* **2FA (Two-Factor Authentication)**:
  + Extra layer of security (SMS, authenticator app, biometric).
  + Even if password leaks, account stays safe.
* **Avoiding Phishing**:
  + Don’t click on suspicious links or attachments.
  + Check sender email carefully (e.g., support@paypal-secure.com is fake).
  + Phishing can happen via **email, SMS, calls, or fake websites**.

## ****4. Safe Browsing & App Permissions****

* **Safe Browsing**:
  + Use trusted websites (look for https://).
  + Don’t download from unknown sources.
  + Keep browser & plugins updated.
* **App Permissions**:
  + Give apps **only what they need** (a calculator doesn’t need your location).
  + On Android/iOS, regularly review which apps have access to your camera, mic, location.
  + Disable background permissions if not needed