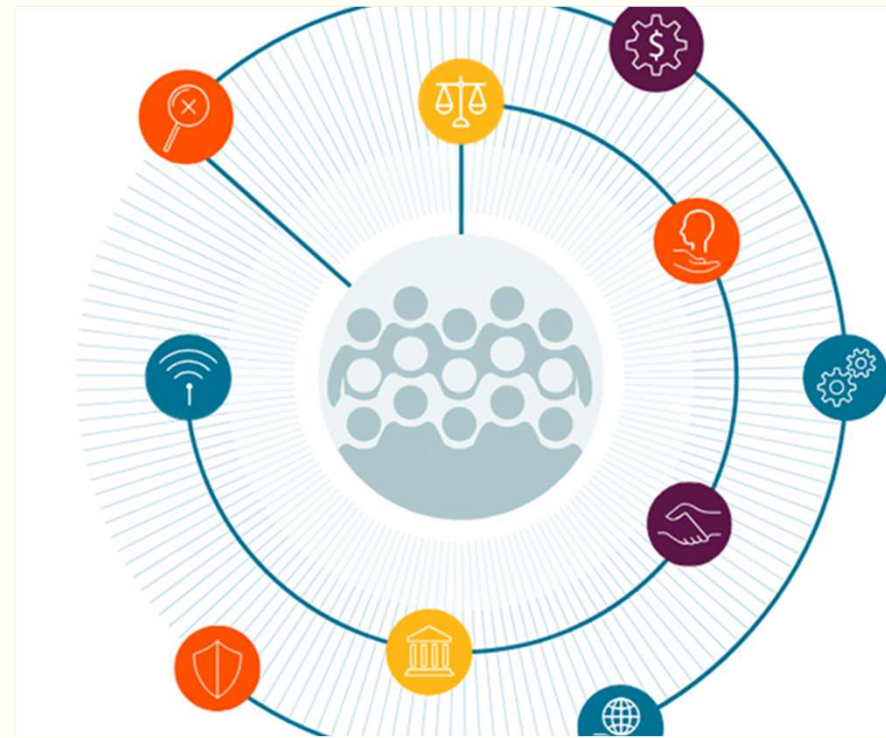




CONSUMER RIGHTS AND DATA PROTECTION

Dr. Kanti Singh Sangher
Scientist-E
kantisingh@cdac.in
C-DAC Noida





Introduction



- Consumer Rights and Data Protection are increasingly recognized as fundamental rights globally.
- Every day, more than 5.3 billion people use the internet. Yet only a fraction of consumers are aware and can control, how their information is collected, used and protected. Only 59% of countries have laws covering online consumer protection.
- The Consumer Protection Act, 2019 has expanded protections for e-commerce transactions but does not comprehensively address data privacy concerns.

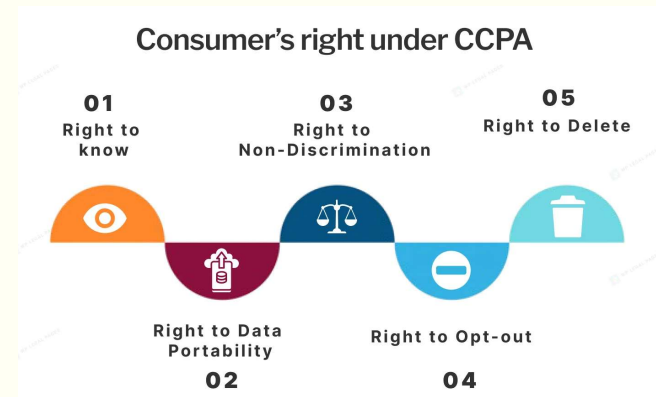




Need of Consumer Rights and Data Protection



- Need for harmonized approach between privacy rights and consumer interests.
- Potentially transformative changes by establishing data fiduciary responsibilities and robust enforcement mechanisms.
- The GDPR's consumer-centric provisions offer useful models for balancing innovation with protection.
- The implementation challenges including technological complexities, cross-border data flows, and enforcement capacity constraints that must be addressed through multi-stakeholder governance approaches.





Growth of Digital Economy and Increased Consumer Vulnerability



- India's digital economy is projected to reach \$1 trillion by 2025. This growth creates immense opportunities but also heightens consumer vulnerabilities. Most digital services operate on a data-for-service model.
- Consumers often surrender personal information in exchange for "free" services. This transaction creates fundamental information asymmetries. Businesses possess sophisticated data analytics capabilities.
- Consumers typically lack awareness about how their data is used. This imbalance weakens consumer's bargaining position in the digital marketplace.
- It undermines their ability to protect their privacy interests effectively.





Continue..

- The monetization of consumer data has become a primary business model in the digital economy.
- Personal data serves as the new currency in this ecosystem. Consumer profiles are created, analyzed and traded between businesses.
- These practices often occur without meaningful transparency or consent.



Evolution of Privacy as a Fundamental Right in India

- The landmark judgment in “Justice K.S. Puttaswamy v. Union of India (2017)” transformed
- India's privacy landscape. A nine-judge bench unanimously held that privacy is a fundamental right under Article 21. The Court established that privacy is "the constitutional core of human dignity.
- This judgment established a three-fold test for privacy restrictions. Any limitation on privacy must satisfy the requirements of legality, necessity, and proportionality.
- This constitutional recognition significantly impacts data protection and consumer rights. It establishes privacy as a cornerstone of India's constitutional framework.



Consumer rights are a set of legal protections that ensure consumers are treated fairly in the marketplace



Right to safety:

· Protection from products and services that are hazardous to life and property. Consumers should insist on quality and certified products, like those with ISI or AGMARK marks.

Right to be informed:

· The right to receive clear and accurate information on the quality, quantity, potency, purity, standard, and price of goods and services. This helps consumers make informed choices and protects them from misleading advertising.

Right to choose:

· The ability to select from a wide range of goods and services at competitive prices. In cases of monopoly, it means the right to be assured of satisfactory quality and service at a fair price.

Right to be heard:

· The right to have grievances heard and to receive due attention from businesses and consumer forums.

Right to seek redressal:

· The right to fair settlement for genuine grievances, including receiving compensation for faulty goods or services.

Right to consumer education:

· The right to be educated about one's rights as a consumer to avoid exploitation due to ignorance.



Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011



- IT Rules 2011 – Key Points (SPDI Rules)
 - Applies to body corporates (companies, firms, sole proprietorships, associations) handling personal information or sensitive personal data or information (SPDI).
 - Applies when SPDI is collected, processed, stored, transferred, or disclosed.

Sensitive Personal Data or Information (SPDI) includes:

- Passwords
- Financial information (bank account, card details, etc.)
- Health conditions & medical records
- Biometric information
- Sexual orientation
- Physical, physiological, and mental health condition
- Any detail related to above categories
- Any information received for providing a service, which is stored/processed



The CENTRAL CONSUMER PROTECTION AUTHORITY (CCPA)



- The CCPA has been established under the Consumer Protection Act, 2019 and has come in to force w.e.f 24th July 2020 to regulate matters relating to violation of rights of consumers, unfair trade practices and false or misleading advertisements.

POWERS OF CENTRAL CONSUMER PROTECTION AUTHORITY (CCPA) -

- Protect, promote and enforce the rights of consumers as a class, and prevent violation of consumers rights under this Act;
- Prevent unfair trade practices and ensure that no person engages himself in unfair trade practices;
- Ensure that no false or misleading advertisement is made of any goods or services which contravenes the provisions of this Act or the rules or regulations made thereunder;
- Ensure that no person takes part in the publication of any advertisement which is false or misleading.
- E-prejudicial to the interests of consumers as class and public at large.



Consumer Protection Act, 2019 - Key Features:

Establishment of Central Consumer Protection Authority (CCPA):

- The Act introduced the CCPA to regulate matters related to violations of consumer rights, unfair trade practices, misleading advertisements, and ensuring the rights of consumers.

E-filing of Complaints:

- The Act provides for the e-filing of complaints in consumer commissions (formerly consumer courts) and has introduced provisions for hearing complaints via video conferencing to streamline the process.

Product Liability:

- The new Act introduced the concept of product liability, holding manufacturers, sellers, and service providers accountable for any harm caused by defective products or services. This provision ensures consumers can seek compensation in case of injury or damage due to faulty goods or services.

Misleading Advertisements:

- The CCPA can impose penalties on celebrities, endorsers, and advertisers for promoting misleading advertisements. There is also a provision for banning such advertisements and taking corrective measures.

Unfair Trade Practices:

- The Act defines and prohibits unfair trade practices, including unfair contracts, misleading advertisements, and denial of services, among others. It also offers provisions for penalty and redressal in such cases.



Continue..



- **Enhanced Pecuniary Jurisdiction:** The pecuniary jurisdiction (the monetary limit for filing complaints) of consumer commissions has been revised:
 - **District Commission:** For cases up to ₹1 crore.
 - **State Commission:** For cases between ₹1 crore and ₹10 crores.
 - **National Commission:** For cases above ₹10 crores.

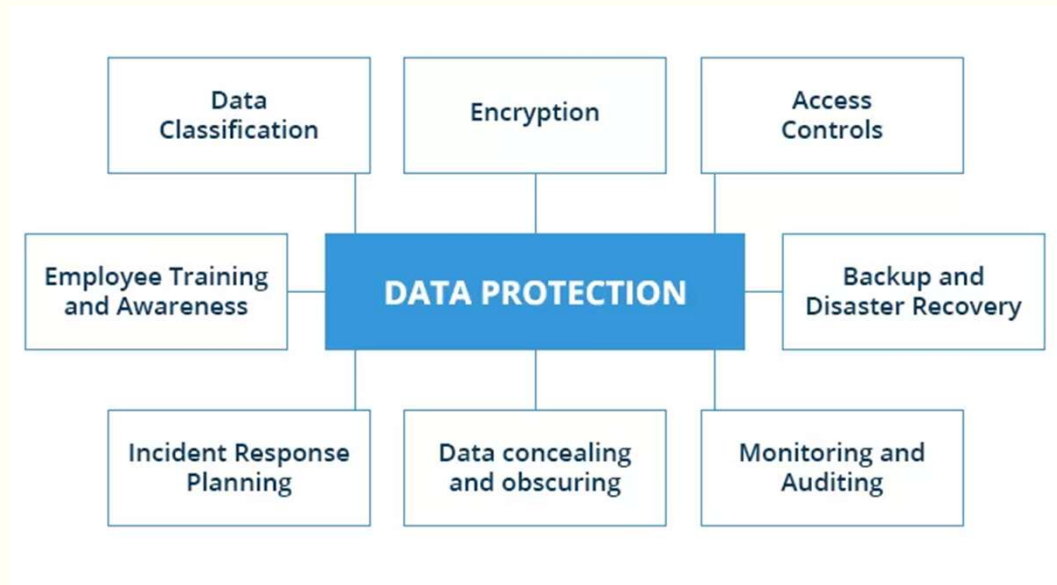
- **Alternate Dispute Resolution:** The Act encourages mediation as an alternative dispute resolution mechanism. A mediation cell will be attached to the consumer commissions to provide faster and amicable settlements of disputes.



Data protection



- India's Digital Personal Data Protection Act uses the term "data principals" rather than "data subjects," referring to individuals "to whom the personal data relates and where such individual is a child includes the parents or lawful guardian of such a child."





For all stakeholders: Recognize the growing vulnerability of consumers in the digital age



- The changing digital landscape, with its concordant growing power and information asymmetries, means that consumer vulnerability manifests in new and growing ways that are important to monitor.
- It is essential that public and private entities consider this in any process for exercising consumer rights, ideally by working with advocates to understand, refine and track definitions, factors and conditions of vulnerability.



For policy-makers:

- Strengthen the options for collective redress

Strengthening collective redress mechanisms is essential for addressing widespread data protection issues, as collective actions can better enforce rights for many individuals, compared to rare individual legal actions in this field.





Data Protection – Data & Policies

Data Protection					
Security			Privacy		
Encryption	Network Security	Access Control	Discovery & Classification	DSARs	Alerting
Activity Monitoring	Breach Response	DLP/CASB	Regulations	Contracts	Policies
How those policies got enforced			What data is important and why		



Protect your customer data

Reputational damage

Meeting compliance requirements

Financial losses

Gaining competitive advantage



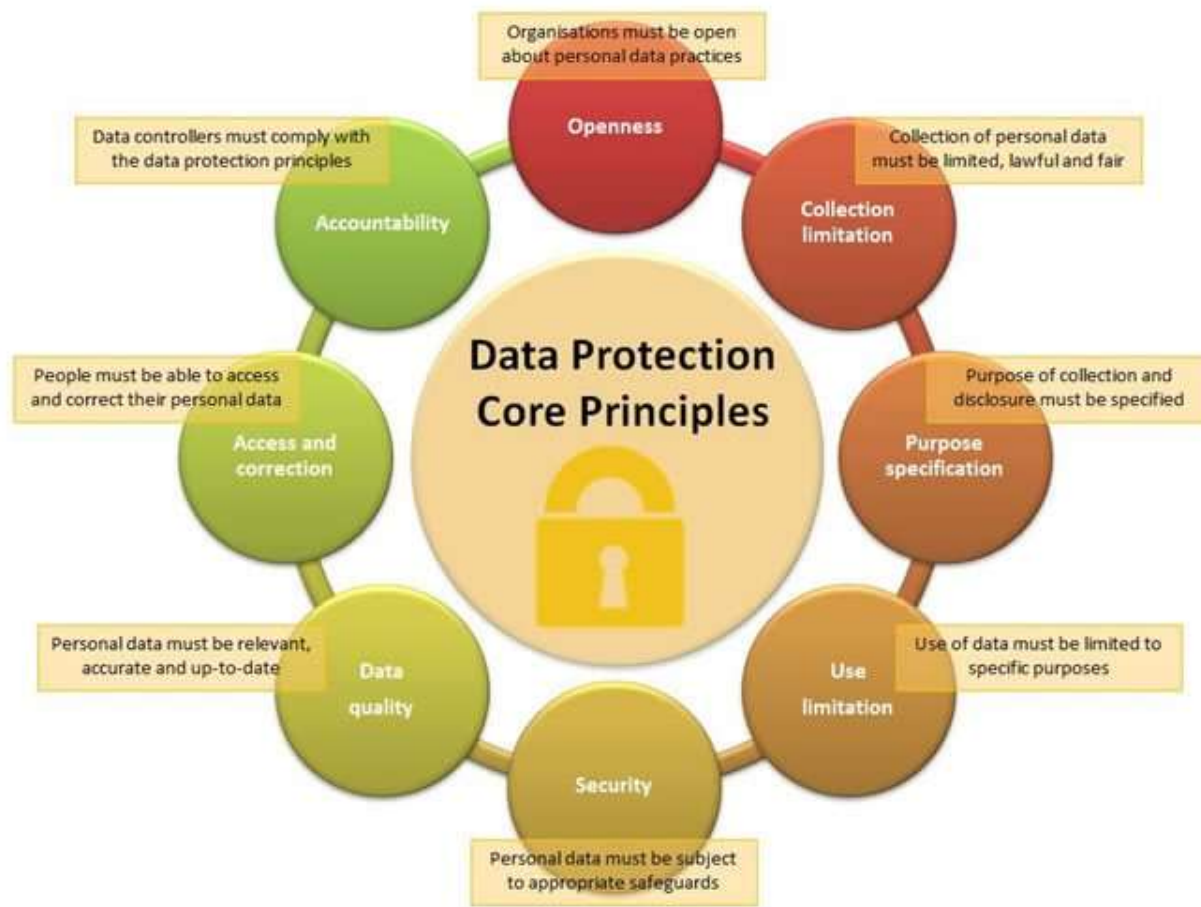
Data Privacy



- Data privacy, is legal control concerning data access or use. Data security plays a significant role in data protection.
- Data privacy incorporates all the steps to handle, process, and store and use personal information. Data privacy takes into consideration consumer rights as an individual. Such include proper management of consumer data.
- Data privacy looks at policies or contracts around the collecting of such information. It also covers all the applicable regulatory laws.



Data Protection Core Principles





Intersection Between Data Protection and Consumer Interests

- ✓ Consumer protection traditionally focused on quality, safety and fair pricing.
- ✓ Consumer vulnerability extends beyond traditional market failures, encompasses informational privacy and algorithmic decision-making.
- ✓ The absence of comprehensive data protection legislation creates leaves consumers without adequate safeguards for their personal information.
- ✓ The Consumer Protection Act, 2019 represents a significant advancement in digital consumer protection.
- ✓ It recognizes e-commerce transactions and establishes relevant consumer rights. The Act created the Central Consumer Protection Authority with enhanced enforcement powers.



Cybersecurity Categories



Network security that uses appropriate measures to guard your computer network

Information Security gives privacy to data while in storage or transit

Application security aims at keeping devices or software free from threats

Operational security determines who has access to data in an organization. It also looks at the handling and decision-making around networks and procedures

End-user security that aims at educating people on proper internet use.



Common examples of personal data misuse include:



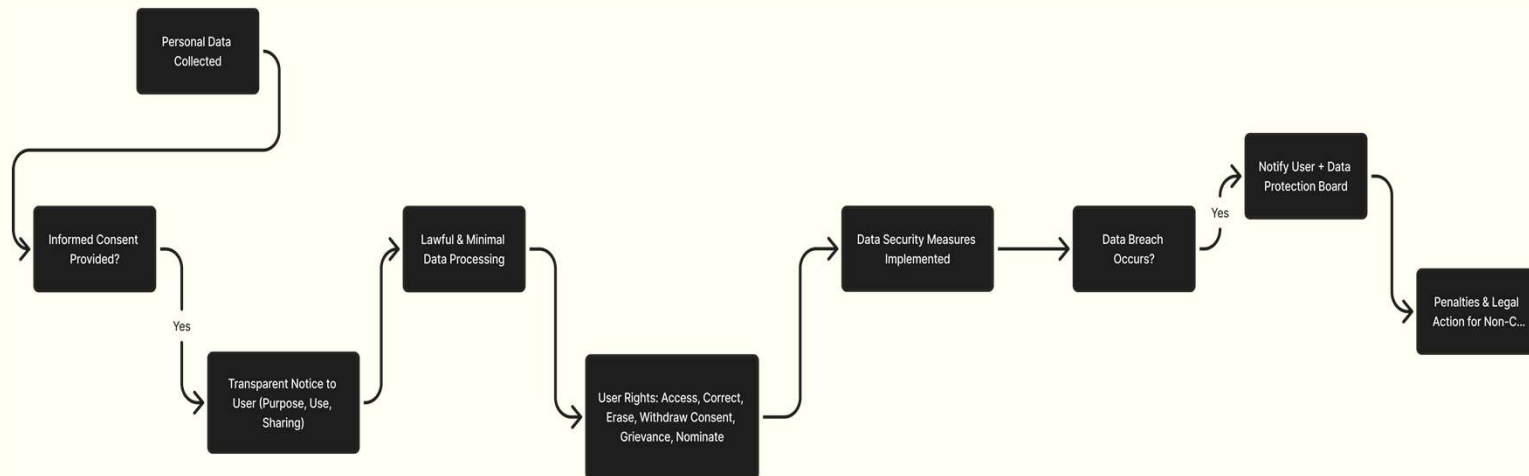
- The misuse of personal data means any non-compliant processing of personal data.
 - Breach of personal data
 - Collection error - personal data is incorrectly or unnecessarily collected without a legitimate legal basis
 - Unauthorized use - when personal data is processed for a certain purpose, but is ultimately used by the data controller for another purpose.



Other Consumer Protection Laws and Regulations



- Bureau of Indian Standards (BIS) Act, 2016: Ensures standardization and quality certification of goods.
- The Legal Metrology Act, 2009: Regulates weights, measures, and labels to prevent deceptive practices.
- The Food Safety and Standards Act, 2006: Regulates food quality standards to ensure consumer safety in food products.





Consumer Responsibilities:



- While consumers have rights, they also have responsibilities to ensure fair practices in the market:
 - Being aware of the quality and quantity of products and services.
 - Reading labels and instructions carefully.
 - Demanding bills and warranties for purchases.
 - Reporting genuine grievances and avoiding false complaints.



Key Data-Protection & Consumer-Rights Aspects under DPDP



Explicit rights for individuals (data principals)

- Under DPDP, persons whose data is processed (“data principals”) get a suite of rights — giving them significant control over their personal information. These include:
 - Right to give or refuse consent — organizations must get clear, informed, voluntary consent before processing data.
 - Right to know how and why data is used — data fiduciaries must explain purpose, categories of data collected, processing methods, third-party sharing, etc.
 - Right to access personal data — individuals can request a copy or summary of their data held by a fiduciary.
 - Right to correction or update inaccurate or outdated data. [Mondaq+2privacypulse.co+2](https://www.mondaq.com/india/privacy/2018/06/20/1000000)
 - Right to erasure (“right to be forgotten”) — request deletion of data under certain conditions.
 - Right to data portability / transfer, in certain cases — ability to move personal data from one service provider to another.
 - Right to nominate someone else to exercise these rights (useful in cases of incapacity or death).
 - Right to grievance redressal — mechanisms to complain or challenge misuse of data or breach of rights.



Obligations on data-handling entities (data fiduciaries) — boosting consumer protection



- To safeguard data principals and ensure fairness/transparency, DPDP imposes several obligations on entities (companies, organisations) that collect or process data:
- **“Purpose limitation” & “data minimization”** — data may be collected/processed only for clear, lawful, specified purposes; “just-in-case” mass data collection is disallowed.
- **Transparent consent notices** — before collecting data, organisations must inform individuals (in clear, plain language) about what data they collect, why, how it will be used, how long kept, and with whom shared.
- **Security safeguards** — fiduciaries must implement reasonable security measures (encryption, access control, logging, backups) to prevent unauthorized access or data breaches. **Breach-notification requirement** — in event of a personal data breach (unauthorised access, leak, loss, etc.), organisations must promptly notify affected individuals (and the supervisory authority) in plain language about what happened, risks, and remedial steps. [The Times of India+2](#)[India Briefing+2](#)
- **Special safeguards for children and vulnerable groups** — when processing data of minors or persons with disabilities, fiduciaries must obtain verifiable consent from guardians; tracking, profiling or targeted advertising for minors is restricted. [VISION IAS+1](#)
- **Obligations apply also in cross-border contexts** — if service/provider is outside India but offers goods/services to Indian users, DPDP may still apply (making it relevant to many global online platforms). [Techlegis | +2](#)



Means for Consumers / Users



- With DPDP in force (and its Rules notified in November 2025), consumers using digital services, e-commerce, social media, apps, online banking etc. get legal tools to:
 - Understand what personal data is being collected and why (transparency)
 - Control to accept or refuse, whether their data is collected/used (consent)
 - Access, correct, or delete their data e.g. if wrongly stored
 - Transfer their data if they switch service providers (portability)
 - Demand security, and seek redress if data is misused or breached
 - Expect better safeguards for sensitive groups (children, persons with disabilities)



Safeguards for Children & Vulnerable Users



- No targeted ads, tracking, or profiling of children.
- Strict parental/guardian consent required.



Accountability & Penalties



- Heavy financial penalties (up to crores) for data breaches, misuse, or failure to protect user rights.
- Data Protection Board can investigate and impose penalties.



BEST PRACTICES



Physical Workspace



- It's easy to fall into patterns that expose sensitive data to would-be cyber criminals. Employees should be trained to exercise these steps around their workspace:
 - When you walk away from your workspace or phone, make sure it locks or times out.
 - Keep sensitive documents secure.
 - Grab documents off printers immediately, and require access codes on printers.
 - Keep desks clean.
 - Avoid leaving sensitive notes, information, and documents on a desk.



Online/Network Practices



- Passwords
 - Keep passwords separate
 - Ensure passwords vary for all accounts
 - Offer appropriate and regular password update cadence
- Phishing/social engineering awareness
 - Guidance around what spoofed emails and text messages look like
 - Insights as to how cyber criminals can take advantage of your employee's information
- Suspicious websites, links, and files
 - Verify the source of website, links, and files prior to clicking, downloading, or taking other actions
 - Telltale signs of suspicious schemes, such as odd spelling or inclusion of out-of-place characters
- Mobile device management
 - Lock devices automatically after a short period of inactivity
 - Have IT backup devices regularly
 - Deploy antivirus and malware protection across all mobile devices
- Creating accurate policy documentation is a necessary step before delivering training and best practices at workforce.
- Company-issued devices can also be forced to automatically lock, enroll in backup services, and install security and antivirus software.



Systems: Network, Software, and Hardware



▪ Software

- Updates: Operating Systems, Anti-Virus, and Malware
- As threats and vulnerabilities appear in systems, patches are developed and must be deployed to keep your business safe.
- Often, employees will not act with the same level of urgency to keep their software up to date, and automatic updates take the guesswork out of keeping your network and devices safe.

▪ Network

- Network Access Control/ Firewall
 - Use Access Control to keep unwanted and potentially insecure devices off your network.
 - Access Control software will monitor your network traffic and block unidentified or unauthorized devices from transmitting potentially damaging data.
 - Firewalls, on the other hand, ensure that you have access to all the data you need while also limiting harmful and undesired activity on your network.
 - Using a firewall to screen suspicious websites and restrict the use of harmful web-based applications complements all the other security measures in place to keep cybercriminals out of your network.
- Data Encryption
- A great method of data protection, encryption is used primarily for two things:
 - To encrypt the data traveling through the network so it cannot be intercepted and disseminated

▪ Backups

- Having an automatic backup of data regularly occur helps ensure data doesn't get lost.
- Backups require monitoring and periodic testing to ensure they are working properly and that the data is recoverable.

▪ Hardware

- Updated Hardware's should be used.



References:

- Department of Consumer Affairs (DOCA)
- National Consumer Helpline (NCH)
- Jago Grahak Jago
- National Consumer Disputes Redressal Commission (NCDRC)
- <https://consumerhelpline.gov.in/public/>



Thanks