UNIT 3 CONSUMER PRIVACY AND DATA PROTECTION IN RETAIL: ETHICAL CONSIDERATIONS

Structure

3.0 Objectives

3.1 Introduction

3.2 Data Collection and Profiling in Retail

3.3 Consent

3.4 Confidentiality

3.5 Responsibility and Accountability for Retailers and Customers

3.6 Consumer Rights in Terms of Data Protection

3.7 Addressing Consumer Concern

3.8 Secured Data Storage

3.9 Transparency

3.10 Data Minimization

3.11 Data Access and Control

3.12 Third Party Sharing

3.13 Compliances

3.14 Let Us Sum up

3.15 Key Words

3.16 Answers to Check Your Progress

3.17 Terminal Questions

3.0 OBJECTIVES

After studying this unit, you will be able to:

- Explain consumers' rights regarding data protection;
- Identify customers' data privacy concerns;
- Explain the compliances regarding data protection;
- Identify the ways for secured data storage;
- Explain good practices regarding data minimization.

3.1 INTRODUCTION

In the previous unit, you learnt about different aspects of the Fair Trade practices and their significance, principles and standards. The collection and safe custody of the customers' data is another important activity in the retail business. In this unit, you will study about these factors in detail.

In this age of the advancement in information technology, retailers collect many types of data at many touch points of sales, such as at the time of billing, at the customer service desk if any data missing, while making loyalty cards for the customers or during promotional campaign when they redeem the consumer offers or coupons. It has become a general practice that customers are asked at least mobile number which has lot of data points related to the area customer is coming from, frequency of purchases, purchase mix, etc. helping the retailers to make availability of such products at any point of time based on frequency. While collecting data, it is absolutely necessary that the retailers follow some ethical considerations.. Data security is a retailer's moral obligation and the IT system should be strong enough to protect the data at any point of time. There, should be enough transparency on "who is permitted to access the data". If any data sharing is taking place, then the customers should be well informed about that. Retailers should pay special attention to the privacy of the vulnerable populations, such as children, and take extra precautions to protect their data.When using artificial intelligence and algorithms for customer profiling and recommendations, retailers must ensure fairness and avoid bias that can lead to discrimination. Retailers must teach their employees how to use customer data and some ethical data control training is needed, like which information is a public domain information and which one is personal. Complying with data protection regulations (e.g. General Data Protection Regulation, Central Consumer Protection Authority) is not just a legal obligation but also an ethical one. Retailers should strive to go beyond mere compliance and prioritize ethical data practices. In this unit, you will study all these ethical considerations in the process of the collection of customers' data and its use by the retailers.

3.2 DATA COLLECTION AND PROFILING IN RETAIL

Data collection of customers is a regular process. Data is collected in many forms like age, gender, address, occupation, mobile number, etc. All such data is collected to understand the buying behaviours of the customers, their frequency of purchases, their preferences in any category or product, etc. All such data gives valuable information about the customers which further helps in building special marketing campaigns. It also helps merchandising team to build minimum base quantity based on frequency and speed in purchasing specific products within the category.

Customer Profilinghas typically the following information:

1. **Customer Personal Information:** It includes customer name, photo, address, email id, mobile number, and some background information, such as key characteristics of customers based on the demographic and behavioural traits that define the segment.

2. **Customers'Preferences**: Information about the types of products, brands, or promotions that do well to a particular segment of the customers.

3. **Buying Patterns:** Insights into when, where, and how often this segment shops.
   Demographics alone are not enough to understand how, when, and why people make purchasing decisions, and that's where psychographics come in.

These factors relate to the attitudes and psychological makeup of a customer and may include:

Life-style
Goals
Pains
Habits
Values
Interests

Psychographics are helpful to understand the buying journey and even the customer journey after they have already purchased from you. For example, in southern India, there are many rice eaters and in north India, we have more wheat eaters. Psychographics means customers buying and consumption behaviour based on the society and acceptable norms within the city, region, or country. The Figure 3.1 shows the components of the customer personal information.

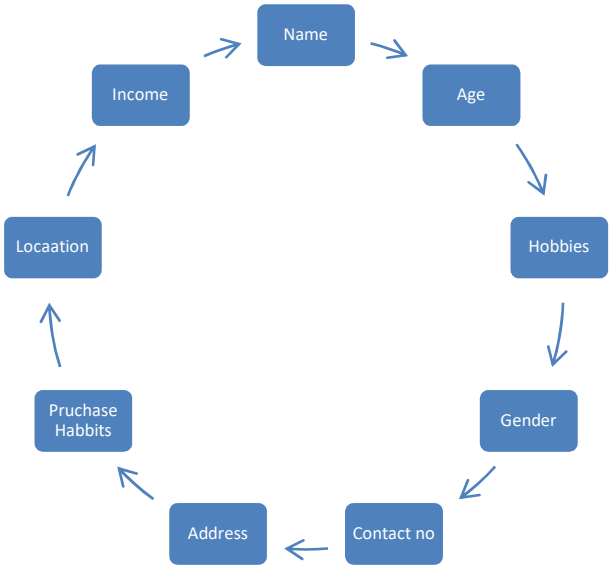

Fig. 3.1: Components of theCustomer's information.

Date to Assess the Customer's Profile

In some cases, PAN card and Aadhar card details are also asked. In the online space, since card payments are used, invoices are to be linked to the Pan card. Customers authentication is done through Aadhaar and PAN card details are also required to link purchases beyond a particular value.

Fig. 3.2: Data to be Assessed for the Customer Profile

Source: https://merehead.com/blog/successful-digital-marketing-strategies-for-retail-store/

Data collected from the customers generate further data based on the purchase pattern, frequency, preferences, etc. This data when linked with the above points gives some qualitative insights about the customer profile.

Benefits of the Customer Profiling

Sales: Retailers are always worried about sales targets and margin target achievements. The customer profiling always helps them stock right merchandise mix stocks. For example, Dmart which is a value store and not a premium store, cannot stock like Shoppersstop or lifestyle type merchandise. It has to offer value offering of the products but of the decent quality and right pricing. So, data become a crucial point of planning merchandise mix effectively.

Marketing: Retailers do Above The Line (ATL) marketing, Below The Line (BTL)and then digital marketing. All the types of campaigns need lot of marketing budget but when retailers have specific budgets to spend, then they must use the customer data based on the purchase preferences, demography, frequency, and income level of customers. This indicates to the retailer plan set for the products for campaign and put special offers accordingly.

Customer Support: Customer data is needed to understand customer behaviour over a period. Is he a loyal customer or a new customer. What is his frequency of purchases? Data available to the customer service team helps

to understand history of the customers' interaction, purchases, and frequency along with complaint ratio of a specific customer. It allows customer support team to plan effectively before handling the customer grievances.

Challenges in Collection of Data from the Customers

- **Data Privacy Concerns:** Customers these days are concerned about their data. There had been many instances where their data is made available to other businesses. It is difficult to question who has done it. Considering data privacy issues, customers generally avoid sharing too much of information about themselves unless they feel necessary to give to avail the services.

- **Data Security**: It is the responsibility of a business to keep the data with utmost security. In case customer does not have enough trust on a business, then he/she should avoid sharing sensitive information.

- **Data Accuracy:** Many a times, customers give incomplete information or person collecting the information is not able to collect complete information or coding to extract data is not done correctly.In such a scenario, it may be difficult to take right decisions.

- **Data Quality and Volume:,** Data collected from the customers must be checked on periodic basis to ensure right data information in the system. It can be done periodically, say on the quarterly basis to check data accuracy of all customers. Companies must focus on quality of data collection and then volume of data from the customers.

- **Regulatory Compliances:** Some countries have very strict norms on data security like GDPR and CCPA; their regulatory guidelines must be adhered to completely while dealing with the data of such customers. There are huge penalties on data privacy related issues.

- **Technology Challenges:** Using latest technology to collect the data is a key,esspecially when data is collected from web platforms, social media, own website, retail stores and third-party websites, etc. Integration is a key and terms and conditions must be absolutely clear on ownership of the data.

- **Opt-out Process for Customers:** When Opt-out process is clearly defined, then customers trust the retailer and give basic information. This must be easily available on company website or other channels so that if customers want, they should opt out from receiving email or instructing retailer or business to delete their data completely.

- **Monetization and Ethical Practices:** If companies convey clearly the guidelines on ethical practices in terms of the customer data that no monetization process is being done except for self-usage by the company. If companies follow their ethical practices, then convincing customers to give data is easily possible.

- **Changing Regulation:** The data privacy laws are still evolving in our country. A change in laws might affect customers data privacy; so companies before acting on it must inform customers in advance and provide opt out options to the customers. Sometime when data is migrated to other sister concern of the company internationally, then regulatory laws also affect the data collection process.

3.3 CONSENT

Consent is considered as the main factor in the consumer privacy and data protection in retail. Consent is a first step in ethical data collection and privacy, as it gives customers individual autonomy and their right to control their personal information.

Some ethical considerations are given below in regard to the consent of the customers in context of the retail industry.

Granular Consent: By sharing with the customers granular consent in the form of click options, customer may decide when to give consent and when not to give it. In this manner, customer can control the data for specific usage of the service only. Retailer then cannot use customer data for the purposes other than the mentioned one. It will give highest level of control to the customer.

Informed Consent: Informed consent means where customer is informed on the usage of their data purpose. It means customer will have a clear information and understanding of what data is being collected, for what purposes and usages, and how it will be used. Retailers and companies must avoid using vague or overly complex language in consent forms. Generally customer does not read it well and later issues come up.

Opt-In vs. Opt-Out: This process means retailers or ethical companies give customers the option to opt out the messaging services and data. They also ask to opt in from the customers.Companies which collect data in this manner are more vulnerable and may use the data of customers for their gains.

Revocable Consent: Ethical consent means companies should allow consumers to easily withdraw their consent at any point of time without facing any negative consequences or loss of their subscription or sign-up page usage, etc. Retailers and companies must make the withdrawal process straightforward and transparent.

Children Consent: These days children are using web, so it becomes necessary to seek child's consent. So instead of the child's consent, their parents may be asked to give the consent as the child being minor. The same normal process of OPT-in and OPT-out process be followed ideally.

Third-party Sharing consent: If retailers share some customers' data to-third-party organizations (e.g. marketing partners), consumers should be informed about this practice and given the option to consent or withhold

consent for such sharing. These days in this area, lot of malpractices are being followed which should be stopped for the benefit of the customers' data privacy.

Profiling and Personalization Consent: When retailers get into customer profiling or personalized marketing for them, consumers should be explicitly informed regularly about these practices, as they can have a significant impact on the shopping experience. If any customer is not interested to receive specific marketing communication, then some tool should be available to him to unsubscribe such services.

Transparent Process: Retailers must be transparent about their data collection and usage practices, including how long data will be retained and how it will be protected as data security is an important subject these days. Transparency builds trust and helps consumers make informed choices. It ultimately makes positive and loyal customers build brand image as well. All the loyalty programs' communication consent from the relevant customers must be obtained in advance before sharing anything with them.

Consent Documentation: Retailers should maintain records of consent, including when and how it was obtained, to demonstrate compliance with data protection regulations. They should keep a log of IP address of the customers along with location at the time of consent. The log information file of customer acceptance should be sent as a rule so that customers may remember for which purpose the data consent is given to the retailer.

Testing and Accessibility: The consent mechanism process must be tested for normal customers and customers with disabilities. They should be able to either subscribe or unsubscribe as per their choice. The platform should be able to provide all such customers with this process flow.

Ethical Data Usage and Handling Process: Retailers must use customer data only for the purposes for which consent was given and ensure that it is protected from unauthorized access or misuse. It requires all data security measures control as well.

Employee Awareness: Retailers must educate their employees about the importance of consent and ethical data practices fostering a culture of respect for customer privacy.

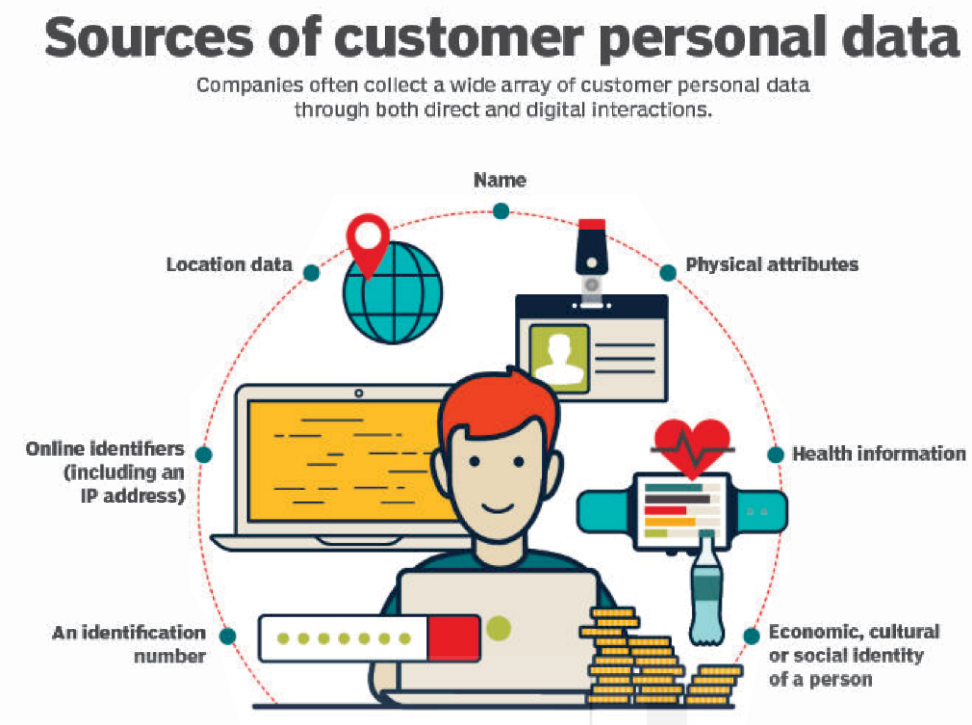

Fig. 3.3: Customers' Personal Data

Source:https://www.techtarget.com

3.4 CONFIDENTIALITY

Confidentiality is a prime point in building ethical practices in consumer privacy and data protection in retail. Many countries have different rules and regulations to control data privacy issues and confidentiality. Some companies have stricter rules, and others may not be having stricter rules. As the online and web usage by the customer has gone up, customer is more exposed to data privacy issues.Hence it makes sense to build confidentiality aspect in their business process.

Confidentiality aspect has the elements which the companies must focus on seriously to maintain it to an optimum level.

1. **Data Security** – Many types of customer information are collected. Companies try to keep the data confidentially, but their system should be strong enough to prevent data breaches by hackers. Enough budget must be spent to put in place the technology to control data security measures in the company.

2. **Data Minimization Approach** – Companies should collect only that data which is necessary to run the objectives effectively. It should be used by them. Legitimate usage of data and collection is a key aspect which every company must focus.

3. **Third PartyAccess Rights:** Companies must refrain themselves in giving or sharing data with third party for the commercial benefit or otherwise also. There may be serious complications if it goes out

from the company domain area. Trust can break and it may impact overall company's brand image.

4. **Employees Training on Data Management**: Every employee who is exposed to customer data be informed through the training that sharing of such information to anyone outside the business is related to integrity issues. They should be informed on impact on personal basis and on company due to data breaches of customer information.

5. **Data Access Control**:To maintain data confidentiality,some selected departments may have complete data access and for the departments using the information for customer service, etc. the same should be viewable with customers opt sharing process. This way company may control the data breaches issues within the company as well.

6. **Continuous Process of Management:** Data ethical practices is a continuous process. Companies also gain learning by managing data regularly. Companies may focus on newer technology adoption and internal processes to control the same. The data collected should never be retained for longer period.

7. **Audits and Regular Compliance Checks:** Audits of data confidentiality process must be checked regularly by the companies; the findings of audit trails be carefully analyzed, and corrective measures be taken regularly to control the process lapses situations. It makes employees also on toes to follow the process religiously.

8. **Having Ethical AI Algorithms:** Retailers and companies must assess the ethics of AI and machine learning algorithms used for customer data analysis to prevent discrimination and bias.

9. **Cross Border Data Share:** Retailers and companies must refrain from sending the data outside the country. They must have full understanding of the country rules and regulations related to the data management and privacy related clauses.

10. **Data Consent:** Customer must have clear understanding what kind of data company needs, how the companies will use it, how company will protect the data. Data consent process must be ethical to build trust with the customers. Retailers must look onto anonymizing customer data whenever possible to protect individual privacy. Anonymization involves removing personally identifiable information from the data.

11. **Vendor Management:** While integrating data, many a times vendors are used to do this difficult task as it requires specific skills. Companies must educate the vendors on company ethical data practice management. This is the way they control and educate vendors and follow the stricter data management practices within the company.

In summary, confidentiality in consumer privacy and data protection is a fundamental or basic ethical consideration for retailers and companies. Protecting customer data from unauthorized access and ensuring its confidentiality is not only a legal requirement but also a moral obligation to respect customer privacy and build trust in the retail relationship.

The responses revealed significant differences from country to country and from one type of data to another. Germans, for instance, place the most value on their personal data, and Chinese and Indians the least, with British and American respondents falling in the middle. Government identification, health, and credit card information tended to be the most highly valued across countries, and location and demographic information among the least. Look at the figure 3.4 which shows that the data can be assigned a monetary value

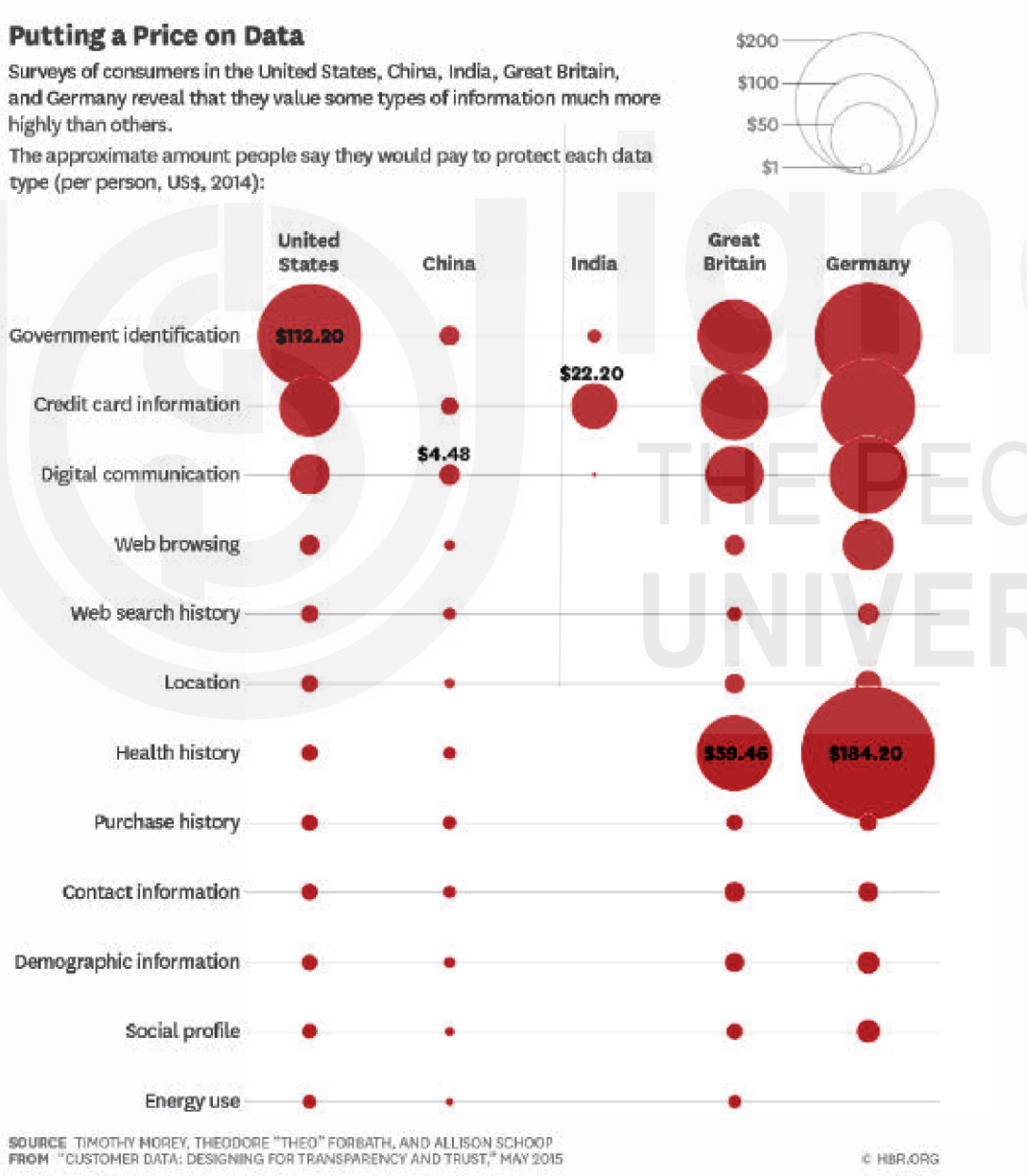

Figure 3.4: A monetary value can be assignedto the customers' data

Source: https://hbr.org **(Harward Business Review Article)**

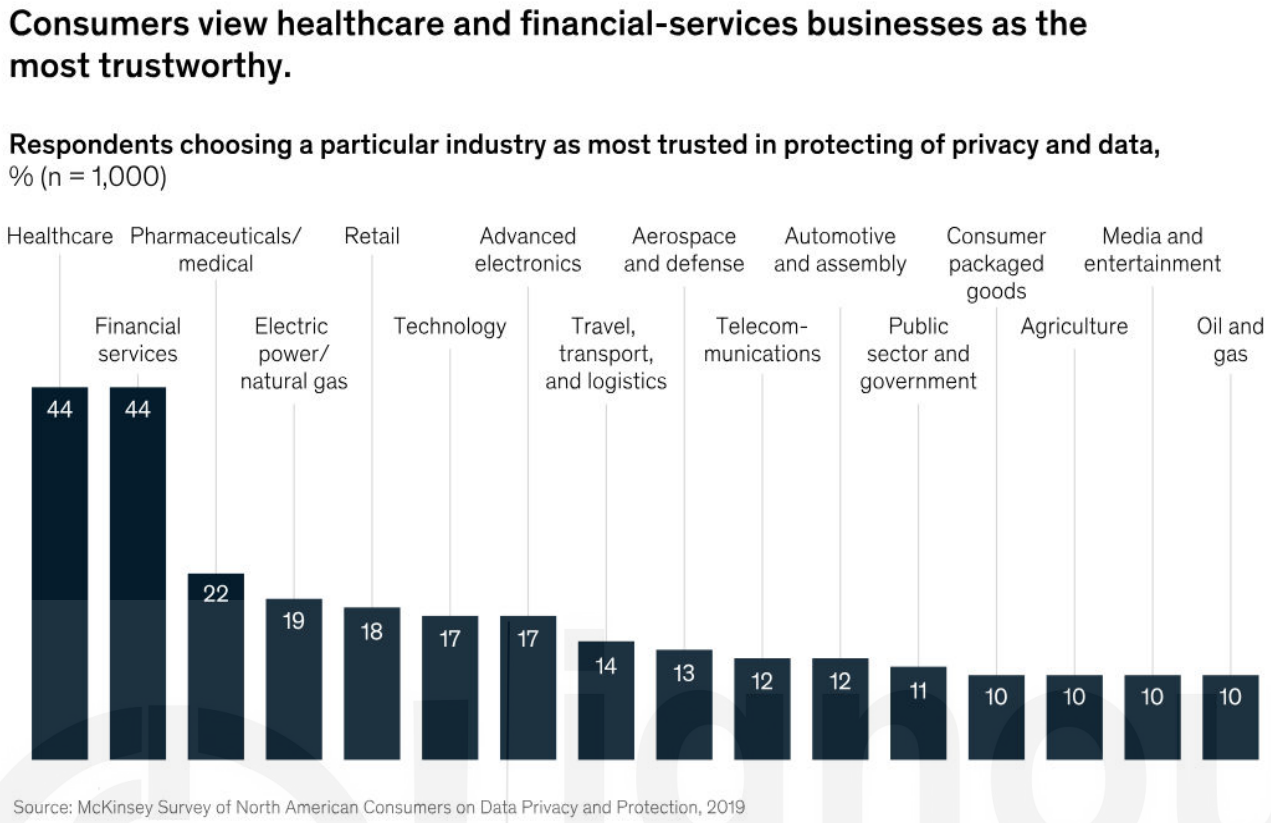

Fig. 3.5: Study on Most Trusted Company on Data Protection

Sources: McKinsey Survey on American Consumer on data Privacy and Protection, 2009

3.5 RESPONSIBILITY AND ACCOUNTABILITY FOR RETAILERS AND CUSTOMERS

Every company which is exposed to customer data collection must have clear cut responsibility and accountability of managing customer data judiciously. No customer today wants to give a lot of information. Companies which are having ethical ways of managing data may get data easily. In India,customers are exposed to sharing their lot of data and never care much about it. But due to bank related frauds, every customer is very cautious in sharing their information. In Figure 3.6, the extent of consumers' trust in the companies and the response of the latter to hacking and breaches are depicted.

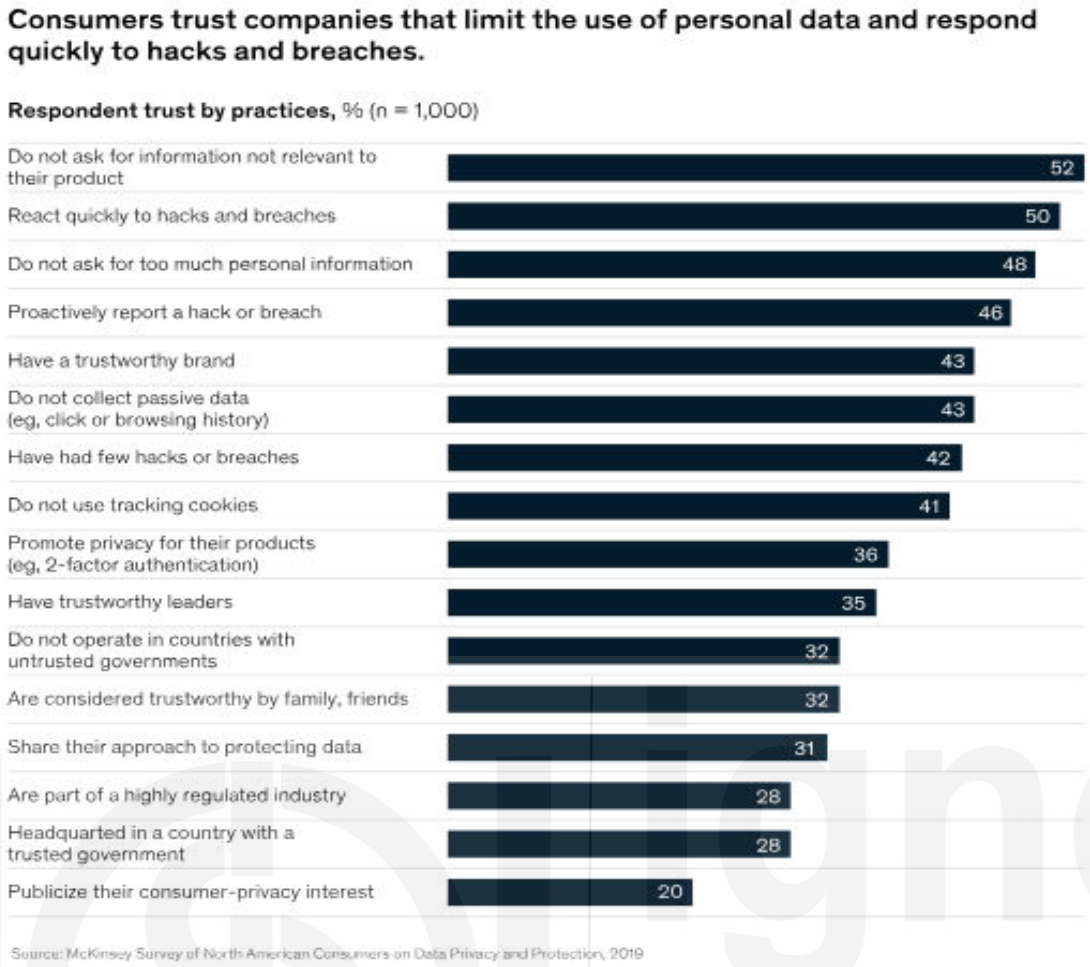

Fig. 3.6: Consumers' Trust Companies that limit the use of Personal data and Respond Quickly to Hacks and Breaches.

Sources: McKinsey Survey on American Consumers on Data Privacy and Protection 2019

Retailers must educate their customers on the policy of the company in dealing customers' data. The collection process and unsubscribe process must be very easy to understand and use.

Retailers' Responsibility Pointers

Data Minimization – Collect only that data which is needed.

Data Secrecy – Robust technology should be used. Cyber security should be at the optimum level.

Customer Information- The customers must be informed on actual usage of the data.

Third Party Share- Retailers must not share any data with any third-party business whether on commercial basis or otherwise .

Opt-in and Opt-out- It is a choice of a customer. Retailers must give option to do so. Once a customer opts out, no message should flow. Flag should be created so that all the channels used by the retailer cannot send any data information.

Choice – It is the choice of a customer to give data. It is not a compulsion of any kind. Customer must read the terms in clarity.

Customer Rights – In case any information is missing in retailer's website related to usage of data, the customer must ask for it in writing. Without asking any question, if you give data then your data may be used by some unidentified people. It is always at the risk.

Unidentified link- Do not click on any unidentified link, as it might steal your valuable information silently.

Customer Password- Customer must keep changing their password so that some additional information may not be passed on to unidentified people.

3.6 CONSUMER RIGHTS IN TERMS OF DATA PROTECTION

The General Data Protection Regulation (GDPR) is legislation that updated and unified data privacy laws across the European Union (EU). GDPR was approved by the European Parliament on April 14, 2016 and went into effect on May 25, 2018. GDPR replaces the EU Data Protection Directive of 1995.

GDPR has not been implemented till now in India, but talks are on to understand the challenges and other processes in this regard. Possibly, India would like to discuss GDPR laws from the customer standpoint for more clarity.

The GDPR offers Individuals with Eight Rights

1. The Right to be Informed Related to Data Shared by Individuals

The companies are supposed to tell individuals what data is being collected, how it is being used, how long it will be kept and whether it will be shared with any third parties.

This information must be communicated concisely and in plain language.

2. The Right to Access the Data by Individuals

Individuals can always submit data access requests, which makes it necessary for the companies to provide a copy of any personal data concerning the individual.Companies have one month to produce this information, although there are exceptions for those requests if it is repeatedly asked.

3. The Right to Rectification

Individuals may access the data and correct it if it is incorrect or new information is to be added or updated. Company will have one month time to update the same as a process.

4. The Right to Erasure (also known as 'the right to be forgotten')

Individuals can request the companies to erase their data in certain circumstances, such as when the data is no longer necessary, the data was unlawfully processed or it no longer meets the lawful ground for which it was collected. This includes instances where the individual withdraws consent.

5. The Right to Restrict Processing

Individuals can request the companies to limit the way an organization is using personal data.It is an alternative to requesting the erasure of the data, and might be used when the individual contests the accuracy of their personal data or when the individual no longer needs the information but the company requires it to establish, exercise or defend a legal claim.

6. The Right of Data Portability

Individuals are permitted to obtain and reuse their personal data for their own purposes across different services. This right only applies to personal data that an individual has provided to data controllers (company) by way of a contract or consent.

7. The Right to Object

Individuals can always object to the processing of personal data that is collected on the grounds of legitimate interests or the performance of a task in the interest/exercise of official authority.Companies should stop processing the information unless they can demonstrate compelling legitimate grounds for the processing that overrides the interests, rights, and freedom of the individual or if the processing is for the establishment or exercise of defense of legal claims.

8. Rights Related to Automated Decision-Making Including Profiling

The GDPR also includes the provisions for decisions made with no human involvement through some technology usage, which uses personal data to make calculated assumptions about the individuals.

There are strict rules for it and individuals can challenge the process and request to review the processing if they believe that something is incorrect considering their profile.

India is not following the data privacy laws and regulations. If GDPR is implemented in India, there will be major changes with all the companies' asking data from customers. There will be more transparency and clarity in terms of the data collection, its usage, updation, and removal process by customers. Companies may not be able to use the data other than self-usage. Third party sharing of data which currently happens illegally may be stopped to some extent. Figure 3.7 shows that the current global approach to data protection is inadequate.

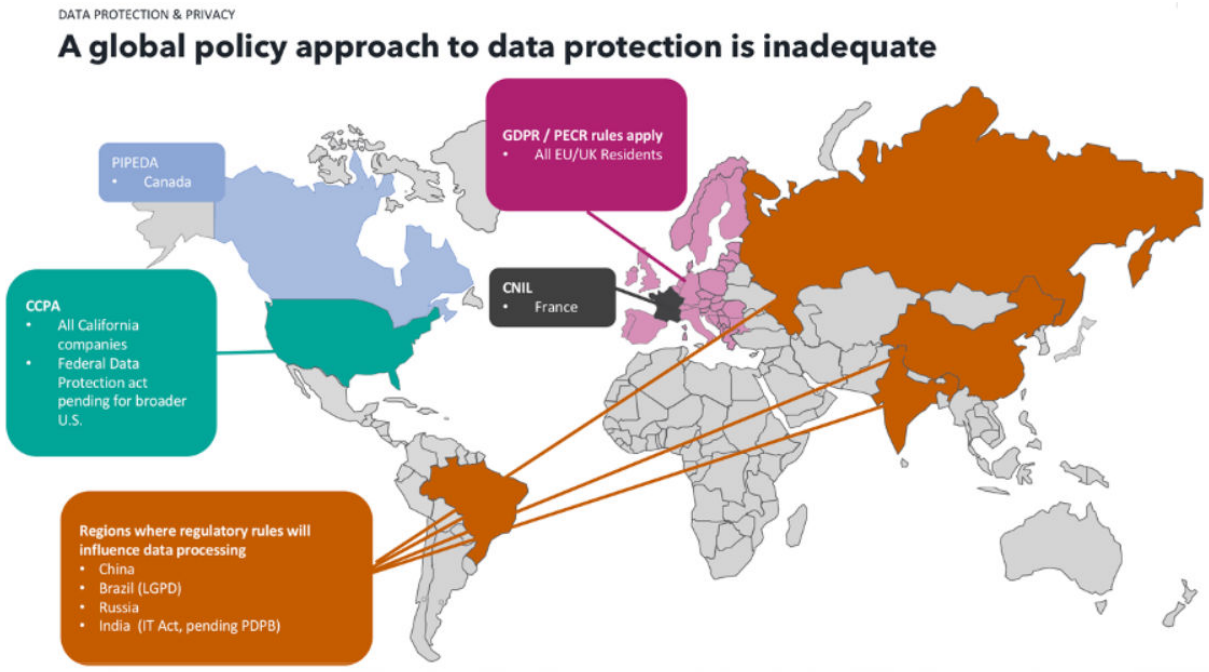

Fig. 3.7: It shows Global Policy Approach to Data Protection is inadequate

Source: https://www.investisdigital.com/blog/technology/keeping-consumer-privacy-compliance

Check Your Progress A

1. List typical points in the customer profiling.
2. List three benefits of the customer profiling.
3. Explain data privacy concerns.
4. List customers' rights in terms of data protection?
5. Which of the following statements are **True** or **False**?
   (i) All data is collected to understand buying behaviours of the customer.
   (ii) The customers profiling helps retailers to stock right merchandise mix.
   (iii) Company which is exposed to customer data collection does not have accountability of managing customer data judiciously.
   (iv) Granular consent gives customers click option for opt-in or opt-out.
   (v) General Data Protection Regulation does not give the customer right to rectify the profile.

3.7 ADDRESSING CONSUMER CONCERNS.

Every company or retailer who is in possession of the customer data has an obligation to clear or answer customer concerns related to the data privacy. Every customer is unique and has a unique data known as the customer profile. Let us discuss the consumer concerns and some solutions which companies can clarify to their customers ongoing basis.

Concern 1 – What will happen to my personal data? Hope it will not be leaked to third party?

Concern 2 – If I share my data, will it impact me with financial frauds because of data being leaked to other unscrupulous companies.

Concern 3 – Can company allow me to delete my data? If deleted 100%, will a copy of the same be still available to them for future.

Concern 4 – If I get spam emails and calls after sharing the data, which company should I contact?

Concern 5- Can I update my data as per current records regularly?

Concern 6 – I have shared my data to many companies. How can I know if any company shares my data with unscrupulous companies and individuals?.

The above pointers are very legitimate in their own way. Companies and retailers should explain the same to all their customers in simple language. This can bring trust and transparency to the customers' group.

3.8 SECURED DATA STORAGE

Securing customer data storage is a critical component of data privacy. Data privacy refers to the protection of personal and sensitive information from unauthorized access who can misuse the customer data for their gain.

There are many ways companies and retailers can secure customer data.

Encryption of Customer Data: Encryption means that the data is transformed into unreadable text or code that can only be decrypted by authorized users or systems with the appropriate encryption keys and passwords.These days hardware and software encryption technologies are available which can make it easy for companies to encrypt and decrypt data as per the need and controls.

Strong Data Access Control: Companies have implemented strong access controls of data to ensure that only authorized individuals or systems can access and modify stored data. It means authentication (e.g., usernames and passwords), role and designations -based access control.

Data Classification of Customers: Companies may classify the data based on its sensitivity. Generally, not all data will require the similar level of protection. Companies may implement access control measures based on the sensitivity to classify the data as sensitive, semi-sensitive, normal, etc. Companies may classify the data based on their understanding and give names accordingly.

Data Masking and Anonymization: Companies may use methods like data masking or anonymization to protect sensitive data. Data masking means replacing sensitive data with fictional or scrambled information, while

anonymization removes personally identifiable information (PII) to protect privacy.

Customer Data Backups and Disaster Recovery: Companies ensure regular data backup procedures periodically as per processes laid down and encryption of backup is extremely important. Storage of data be available in multiple servers to manage well the disaster recovery plans in case of data breaches.

Physical Security of Premises: Companies ensure physical security of data storage facilities. They have enough security measures of the centers or server rooms from unauthorized access, theft, and environmental threats such as fire and floods.

Customer Data Retention Policies: Companies build a retention policy to determine how long data should be stored. There is a plan to delete the data which is no more required to reduce risk associated with it.

Auditing and Monitoring: There is regular audit according to the laid down processes of data storage, access, and deletion process. It should have all key action points including data storage server management, team deployment, data encryption technology, etc. Keep track of audits with logs and regular security assessments including finding newer technology to ensure data management further robust.

Regulations and Compliances: Depending on the location and industry, it may be necessary to comply with specific data privacy regulations, such as the General Data Protection Regulation (GDPR) in Europe or the Health Insurance Portability and Accountability Act (HIPAA) in the United States. It is necessary to align data storage practices with these regulations.

Make Employee Aware Through Training: Training regularly employees on data privacy best practice is good for the company as it can create a culture of awareness and responsibility. Many data breaches occur due to human error or negligence. Negligence is a major cause of data breaches which can be avoided with the help of timely and regular training programs on every aspect of data privacy and management.

Secured Transmission is a Key: Data security is not necessary just for the storage alone. Companies must ensure that data is transmitted securely using encryption protocols like SSL/TLS while transferring data over networks.

Vendor Security: When using third party vendors or cloud storage for data storage, it is necessary to ensure that robust security measures are in place. It is necessary to follow due diligence of vendor security protocols regularly to safeguard the company data.

Secured data storage is a fundamental aspect of protecting data privacy. Companies following good practices always have long lasting positive impact on consumer value management. It builds brand image as well.

3.9 TRANSPARENCY

Data Transparency is a key concern from the customer stand point. Today in India, every online company is collecting information in some form; we share at least telephone no.s in every billing. Even in the offline retail business, consumer is sharing information at the following touch points:

- At the POS / billing machine by giving mobile number
- At the customer service desk (Online and Offline)
    - Telephone number
    - Name
    - Email id
    - Address
    - Sometimes profession is also asked.
    - Credit card and debit card details
    - UP ID's
- In Financial transaction website / physically
    - We add the above data points.
    - We also give PAN card.
    - AADHAR number
- Today for any services, AADHAR Authentication KYC is a must

Literally the customer is sharing complete information of self. So, it becomes imperative for a customer to see how these companies are securing his data with complete transparency. Today none of the companies is transparent in informing to the consumer that how they are securing their data efficiently. We get lot of spam calls. This may be a result of sharing of data by such companies at a price to them. So currently consumer data has reached a vulnerability point where nothing is secret from the world. If companies want, they can release the data to anyone on some commercial transactions. GDPR rules and regulations are still not implemented in India. Customer today shares his data to genuine businesses or reputed businesses where data is secured in some way.

3.10 DATA MINIMIZATION

Companies collect the customer data so that they can understand the frequency of customers' purchases and build focus on marketing promotions and schemes for the customers.

Basic data is always required as mentioned in 3.9, but collecting extra data is a wastage of time for the company and data handling costs also go up. Only

on completing one cycle, data starts showing relevancy for its effective usage. Data compilation and then making the data ready based on some parameters is a key which company does when they have enough data to understand. Some data over a period reach to a garbage level; beyond that data is not to be stored further and companies should work on deleting the data. Companies can follow certain key good practices:

- Collection of data in basic manner
- Identifying some action points for customers' benefit
- Use till a maturity level is reached.
- Post maturity level of data, delete some data points.
- Ensure data security is always the best in technology terms.
- Companies should be open for data portability to some other platform based on customer request.
- Opt-in and Opt-out policy be in place
- Customer data be deleted from main server if customer wants.
- Periodic reviews by companies on data security, access control of data and data audits and process reviews, etc.

The companies should always refrain from sharing the customer data with third party company. This is the biggest concern with the customers at large.

3.11 DATA ACCESS AND CONTROL

Data access and control is a process related action point for any company which has collected customer data. It is an obligation of the company to ensure that all the customer data is managed well. The utmost requirement here is control on data privacy related issues which means data is not leaked to third party or intentionally sold to third party for commercial gains.

If a customer has shared the following data

1. Name
2. Telephone number
3. Address
4. Email id
5. AADHAR card details
6. Credit card or debit card details
7. UPId's
8. Buying behaviour data and frequency of purchases.

This data always belongs to the customer and storage and control is a key control measure which the company must ensure. The data is always used by human being under some process protocols as planned by the company.

Companies must very strictly do the followings.

- Set the process of managing customer data confidentially.
- Define the roles of people handling the data. Employees at different roles use data based on the exposure define.
- Regular training to employees on GDPR rules and regulations and each member understands the repercussions on company and individuals with clarity.
- Data encryption and decryption protocol must have been implemented with seriousness.
- Mirror copy of the data always be maintained in encryption form to avoid any loss of data or leakage of data at other servers' levels.

3.12 THIRD PARTY SHARING

Let us understand who are third parties.

- Suppliers
- Distribution channels partners and resellers
- Network security tools
- Monitoring solutions
- Customer Relationships Management (CRM) tools
- Digital marketing systems
- Employee and customer screening and reputation services
- Media agencies

What do we mean by Third-Party Risk?

Third-party risk involves the following factors:

- **Data Breach** – When data shared with third party is compromised and shared to some other third party that is called data breach.
- **Rapid Response** – In most cases, a data breach will be followed by a rapid response process driven by the organization's data privacy team. When multiple parties are involved, this process becomes more complicated.

- **Data Governance Practices Issues**– If dealing with small organizations and immature organizations, the data governance issues may be present. Company must be very vocal in agreement with penalty clause on data related privacy issues.

- **Control Lapses or Losses**– data is a transient object; it is being moved and aggregated by different backup systems or data pipelines and may end up in the hands of subsequent parties who have no legal obligations to you (fourth or fifth parties).

- **Traceability** – Traceability and questioning are very difficult when multiple parties are working on a project and using the data. Although logs and other tools are present, but these are cumbersome processes to establish ultimately who compromised on data loss.

The goal of the Third-Party Risk Management program must be to eliminate the following risks:

- **Strategic Risk:** Risks arising from adverse business decisions and failure to meet business objectives due to third-party vendors.

- **Financial Risk:** This risk is created when a third-party business performance lapses on the service created which leads to financial risk to the company. Companies must protect themselves in agreement with the third party with penalties etc.

- **Operational Risk:** A risk that a third party will impact / slowdown / stop internal processes, people, and systems essential for day-to-day operations.

- **Reputational Risk:** Risk arises from negative public opinion formed due to dissatisfied customer service, inappropriate recommendations, security breaches, and other flaws by third parties.

- **Compliance Risk:** A risk with a third party may impact business compliance with laws, rules, or regulations negatively.

- **Cyber security Risk:** A risk arises from cyber attacks, cyber security, data breaches, and other security breaches by third-party vendors. Using data discovery tools, sensitive data can be searched and detected for better protection.

How to Mitigate Such Risks

- Always work with a company of reputation which has knowledge of data privacy. They must have past experience of managing customer data well with no compromises related issues.

- Team training and proactive approach of such companies decide the fate of tie up with these companies.

- Always put penalty clause which should work as a strong deterrent to the companies.
- Third party must have strong technical team of managing such large data with 100% confidentiality and performance.

3.13 COMPLIANCES

- If company follows GDPR rules, even if not applicable, will always help in compliances related issues.
- Data security at server levels, cyber security implementations, mirroring of data always protect companies from data breaches.
- Sensitization of data security and confidentiality at employee levels and third-party vendors levels is highly recommended.
- Employee levels-based exposure of data can help in protecting data.
- Terms and conditions mentioned in online space must be clearly defined in simple words so that customers can understand it well.
- Opt-in and Opt-out option to customers must be easily available to update or delete the data and data portability also must be addressed.
- In order to be at the top of compliances, companies must ensure that they use latest technologies to control the compliances related issues.

Check Your Progress B

1. Explain any two important concerns of the customer related to the data privacy?
2. What is meant by encryption of the data?
3. How can the third-party risk be mitigated?
4. What is data minimization? ?
5. Which of the following statements are **True** or **False**?

   (i) Addressing concern can bring trust and transparency to the customers group.

   (ii) There are limited ways companies and retailers can secure customer data.

   iii) Collecting extra data is a wastage of time and data handling costs also go up.

   (iv) The data is always used under some process protocols as planned by the company.

   (v) Employee levels-based exposure of data cannot help in protecting data

3.14 LET US SUM UP

In this age of the advancement in information technology, retailers collect many types of data at many touch points of sales. It has become a general practice that customers are asked at least mobile number which has lot of data points related to the area customer is coming from, frequency of purchases, purchase mix, etc. helping the retailers to make availability of such products at any point of time based on frequency. While collecting data, it is absolutely necessary that the retailers follow some ethical considerations. All such data gives valuable information about the customers which further helps in building special marketing campaigns. It also helps merchandising team to build minimum quantity based on frequency and speed in purchasing specific products within the category.

Customers these days are concerned about their data. There had been many instances where their data is made available to other businesses. It is difficult to question who has done it. Considering data privacy issues, customers generally avoid sharing too much of information about themselves unless they feel necessary to give to avail the services. It is the responsibility of a business to keep the data with utmost security. Consent is considered as the main factor in the consumer privacy and data protection in retail. Consent is a first step in ethical data collection and privacy, as it gives customers individual autonomy and their right to control their personal information. Confidentiality is a prime point in building ethical practices in consumer privacy and data protection in retail. Many countries have different rules and regulations to control data privacy issues and confidentiality. Every company which is exposed to customer data collection must have clear cut responsibility and accountability of managing customer data judiciously. The General Data Protection Regulation (GDPR) is legislation that updated and unified data privacy laws across the European Union (EU). GDPR was approved by the European Parliament on April 14, 2016 and went into effect on May 25, 2018. GDPR replaces the EU Data Protection Directive of 1995.GDPR has not been implemented till now in India.

Data compilation and then making the data ready based on some parameters is a key which company does when they have enough data to understand. Some data over a period reach to a garbage level; beyond that, data is not to be stored further and companies should work on deleting the data. Data access and control is a process related action point for any company which has collected customer data. It is an obligation of the company to ensure that all the customer data is managed well.There are many third parties involved in the retail business. Thus, there are various types of risks if data is leaked to a third party. There are various methods to mitigate these risks.

3.15 KEY WORDS

Above the line (ATL) marketing : Above the line marketing includes mass marketing strategies which are largely untargeted and are

focused on building the brand, such as TV, Radio, Print media, etc.

Anonymization : The action of blocking identifying information for the data, authorship, etc.

Below the line (BTL) marketing : Below the line marketing includes direct marketing strategies directed to specific target groups and focused on conversions rather than building the brand, such as direct mail (e-mail, text messages), sponsorship, etc.

General Data Protection Regulation (GDPR) : Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Loyalty card : A swipe card issued by a supermarket or chain store to a customer.

Merchandise mix : The combination of goods that a business decides to sell in order to increase its profits.

Moral obligation : An action to be done out of certain principles.

Profiling : Listing of personal characteristics or behaviour patterns about a person.

Promotional campaign : A planned set of activities to popularize certain product(s).

Public domain : Any literary work or invention which does not have any copyright and can be reused freely.

.**Vulnerable** : Susceptible to being attacked, damaged, or hurt.

3.16 ANSWERS TO CHECK YOUR PROGRESS

A 5. (i) True; (ii) True; (iii) False; (iv) True; (v) False

B 5. (i) True; (ii) False; (iii) True; (iv) True; (v) False

3.17 TERMINAL QUESTIONS

1. Define cyber security?
2. Explain critical factors responsible for transparency in data management?
3. What are customers' top concerns on data consent to companies?

4. Which rule in GDPR you liked the most? Highlight top 2 which you like the most?

5. Why is confidentiality of data required?

REFERENCES

https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/an-ethical-approach-to-data-privacy-protection

https://research-compliance.umich.edu/data-security-guidelines

https://resources.data.gov/assets/documents/fds-data-ethics-framework.pdf

https://www.ukcybersecuritycouncil.org.uk/ethics/ethics-scenarios