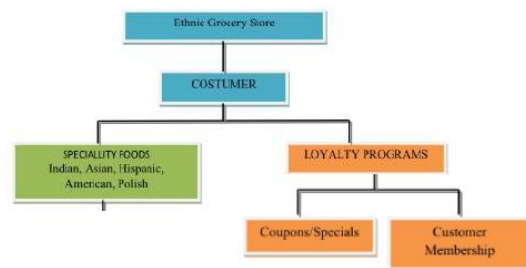


In this assignment, you will continue to develop your online grocery app by creating a privacy and security plan for your system. Use your mental models, concept models, organization, labels, metadata, taxonomies, and navigation structure to help you.

From the concept of my online grocery store, privacy concerns that customers will typically have includes unauthorized access to private information such as identity theft, address information, credit card information, password information, and personal identifying information. Other concerns are related to online shopping profiling that can be automatically processed to infer potentially more intrusive details about an individual, such as shopping behaviors, ethnic or racial origin, substance use, and personality.

- What personally identifying information, sensitive information, and traffic information does your system require and store?

With regard the type of identifying information, sensitive information and traffic information, my system will required are related to customer information such as name, address, credit card information, password, shopping history cart, membership information, rewards program enrollments.



- What data will you make available to third parties?

The information that I can make available to third parties will be related only to shopping cart products, and brands. According to the Data Protection Act, there are certain rules we need to follow when it comes to securing or protecting data. These rules apply to everything one does with personal data, except the case when one is entitled to an exemption.

- Personal Data must be processed lawfully and fairly.
- Personal data should be relevant, adequate and not excessive in relation to the purpose or purposes due to which they have been processed.
- Personal data must be obtained just for one or more than one specified and lawful reasons and must not be processed in any way that is not compatible with those reason/reasons.
- Personal data which is processed for any reason or reasons should not be kept for any time longer than required for that reason or reasons.

- Personal data should not be processed according to the rights of data subjects under this Act.
- The suitable technical, as well as organizational measures must be taken against any unauthorized processing or unlawful processing of personal data and also against any accidental destruction or loss of or damage of personal data.
- Personal data shall not be transferred to a territory or country outside the economic area of the data owner unless that region ensures the right level of protection for the freedom and rights of data subjects in relation to data's processing.

Data protection:

The protections that can be put in place to protect the privacy of the customers data should include the establishing strong passwords that can't be guessed by anyone; strong firewall to protect the network from undesirable network traffic; securing systems by using encryption during transactions to ensure no one can access unauthorized information; establishing backup protocol rules to avoid loss of data in case of a data security breach or corruption; and utilization of data monitor tools to prevent data leakage.

As we learned from this, there are two key aspects of collecting data: Privacy and Security. Where, information privacy deals with the ability to determine what data is of sensitive value and can't be shared with third parties. And data security refers to protective digital privacy measures that are applied to prevent unauthorized access to information and from data corruption. Consequently by protecting data, one also tends to achieve protection of privacy.