**Answers**

1. A large supermarket chain has recently updated its Privacy Policy in line with the new Data Protection Act (2018). The store operates an online shopping and delivery service, and shoppers using this service are issued with a Loyalty Card which they may also use in store to obtain discounts on selected items.

(a) State **two** items of personal data about holders’ shopping behaviour that the company might hold. [2]

Data about online purchases, for example what a customer bought, when and where, how much it cost

Data about devices used / browsing behaviour

Details of emails and texts that they send to you and whether you open them / whether they got a response

(allow any other reasonable answers)

(b) Explain **three** requirements of the Data Protection Act (2018) which the company needs to consider. [6]

(Up to two marks for each of the points below or any other relevant point)

* The company must state the purpose which it is using to collect data (1) such as consent / legitimate interests (1) so that it is clear to customers why they are processing data (1)
* The company must ensure that data is accurate (1) by performing verification when users join the scheme (1) / by letting users update their details (1)
* The company needs to store the data securely (1) by using encryption / firewalls / locked rooms (1) so that data breaches are unlikely to happen (1)
* The data must only be processed for the given purpose (1) and must be processed lawfully / so that customer’s privacy is respected (1)
* If the company has gained the data by consent (1) then it will need to allow the customer the ability to remove their consent (1) and delete the data (1)
* The company will need to employ one or more people (1) to deal with subject access requests (1) so that the customer can be shown/sent all the data that the company has on them (1)

(c) Discuss the impact that this legislation has on the organisation and customers. [6]

**Impact on the organisation:**

* It must appoint a Data Controller whose job is to ensure compliance
* It must write and publish its privacy policy which informs customers what data it holds, why, and how they can inspect it
* It must be careful that the legislation is adhered to, and put in place security measures to protect data, keep it accurate and up to date
* Encryption will need to be used for data and access to servers will need to be restricted
* Staff will need to be trained to show what they can/can’t do with the data and how it is protected

**Impact on individuals**

* It builds trust in the company through transparency
* Customers can hold the company to account if their data is stolen
* They can find out exactly what data is held about them
* Customers can withdraw their consent to having their personal data stored (if it was gained by consent)
* Customers can make a data subject request and see the data held about them by the company

|  |  |  |
| --- | --- | --- |
| * L | Mark | Descriptor (award up to 6 marks) |
|  | 0 | No rewardable material |
| Level 1 | 1–2 | Demonstrates isolated elements of knowledge and understanding, with major gaps or omissions  Few of the points made will be relevant to the context in the question  Limited discussion which contains generic assertions rather than considering how the legislation impacts both organisations and customers. |
| Level 2 | 3–4 | Demonstrates some accurate knowledge and understanding, with only minor gaps or omissions  Some of the points made will be relevant to the context in the question, but the link will not always be clear  Displays a partially developed discussion which considers some of the techniques and some consideration of how the legislation impacts both organisations and customers. |
| Level 3 | 5–6 | Demonstrates mostly accurate and detailed knowledge and understanding  Most of the points made will be relevant to the context in the question, and there will be clear links  Displays a well-developed and logical discussion which clearly considers how the legislation impacts both organisations and customers. |

(d) An employee of the company finds customer details from the database. They then use these to commit fraud by taking out loans from the customer.

(i) State the law covers their unauthorised access to a computer with an intent to commit further offences. [1]

Computer Misuse Act (1990)

(ii) State the penaties which may be applied to the employee. [1]

(up to five years) imprisonment / fine / lose job

2. (a) Describe the purpose of a code of practice for the protection of data produced by   
the Information Commissioner’s Office. [2]

It helps organisations

* Apply the GDPR/Data Protection Act effectively
* Demonstrate their compliance
* Implement their own privacy policy and other data protection act documents more easily

(b) State **two** advantages to an organisation of having a code of practice . [2]

Any two of:

* Be more transparent and accountable - enabling businesses or individuals to distinguish which processing activities, products, and services meet GDPR data protection requirements and they can trust with their personal data
* Give them a competitive advantage
* Create effective safeguards to mitigate the risk around data processing and the rights and freedoms of individuals
* Improve standards by establishing best practice
* Reduce the likelihood of enforcement action
* Demonstrate that they have appropriate safeguards to transfer data to countries outside the EU
* Reduce the risk of a fine
* Show staff what behaviours are acceptable or not acceptable (specific examples one mark each)

See <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/>

[Total 20 marks]