CASE STUDY

Q1. Excluding accountability, what are the data privacy principles of the GDPR? You should provide a brief one or two sentence explanation for each, in your own words, not just a heading.
Ans: The seven principles are:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

1. Personal data must be processed lawfully, fairly, and in a transparent manner:
It states that organisations need to make sure their data collection practices don't break the law and that they aren't hiding anything from data subjects. They need to remain transparent about the type of data they are collecting and the reason they are collecting it for.

2. Personal data must be processed for specified, explicit, and legitimate purposes:
It states that it should be clearly specified as to why someone's personal data is being collected and how it is intended to be used. The data cannot be collected for another, 'incompatible', or unlawful purpose.

3. Personal data must be adequate, relevant, and not excessive:
Only the required bare minimum data must be collected. Any data that isn't immediately relevant to the specified purpose or is more information than required should not be collected.

4. Personal data must be accurate and up to date:
Any information held must be factually accurate and updated where necessary.

5. Personal data shouldn't be kept any longer than is necessary:
This storage limitation principle states that the data shouldn't be kept any longer than needed. If the data is collected for a purpose that's time-limited then the information should not be retained beyond that point.

6. Personal data must be processed securely
The personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

Reference: Irwin, L. (2019). *The GDPR: Understanding the 6 data protection principles*. [online] IT Governance Blog. Available at: https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles

Q2. Identify a change to the way the current US website works that the company will need to make to be compatible with the GDPR when it launches the UK version, and why this is necessary.
Ans: A change that needs to be made from how the current US website works to be compatible with the GDPR when it launches the UK version is that expilict consent has to be taken from the customer regarding the data that is being collected and used. It must be clearly stated what type of data is being collected and why and until when is it used for.
b)This is necessary to be compatible with the Data protection law(GDPR).

Reference: www.cookiebot.com. (n.d.). *GDPR in the USA | GDPR compliance in US | GDPR and PII*. [online] Available at: https://www.cookiebot.com/en/gdpr-usa/

Q3. Indicate two actions the company will need to take in relation to the implementation of the new features described above, because of the GDPR Accountability principle.
Ans: Accountability states that that you must be able to demonstrate your compliance. Hence, two of the many actions that the organisation can take since they are collecting data from the individuals with their consent are:
1.to adopt and implement data protection policies and maintain documentation of all processing activities, and
2.implement appropriate security measures and carry out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests.

Reference for 1:
ico.org.uk. (2020). *Accountability and governance*. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/.

Reference for 2:
ico.org.uk. (2020). *Accountability and governance*. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/.

Q4. Identify a GDPR related issue that the company may have with implementing the plan to provide individualised recommendations and suggest a way these could be addressed to allow this to proceed.
It violates the data minimisation principle of GDPR.
Ans: If the company wants to provide individualised recommendations it requires a lot of personal data of the user and it contradicts with the data minimisation principle.
b)The solution for this problem is, it should clearly let the user know that it is collecting data for providing individualised recommendations and should let the user to opt-out of recommendations if he is not interested.

Reference- What is data Minimisation? (no date) Experian.co.uk. Available at: https://www.experian.co.uk/business/glossary/data-minimisation/

Q5. When a user decides to close their account on the website, the company is required to delete their data. In order to continue to provide the useful ratings and review comments to other users, the company would like to turn this data into anonymous data by disconnecting it from the personal details (name, city, etc.) held about the user. It plans to seek permission to do this. Is the deleting of the personal data sufficient to achieve this? Explain why it is/is not sufficient.
Ans: Yes, turning the data into anonymous data (given it deleted all of the personal data and makes it non-identifiable) is sufficient.
b) Once data is truly anonymised and individuals are no longer identifiable, the data will not fall within the scope of the GDPR

Reference: ico.org.uk. (2020). *Accountability and governance*. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

Q6. Other than a lack of consent, suggest a reason that allowing the system to generate the avatar image in the way described would not be compatible with the GDPR.
Ans: Generating avatar image in the way described is not compatible with GDPR because the data subject would be identifiable from the avatar image(for eg: color, sex, etc) hence leaking the personal details indirectly.

Reference: The Chino.io Blog. (2018). *What is anonymous data according to GDPR?* [online] Available at: https://www.chino.io/blog/what-is-anonymous-data-according-to-gdpr/

Q7. Indicate an alternative approach that could be employed to provide a unique system generated avatar image for each user that would be compatible with the GDPR and would not leak any of the user details. And explain why this would be compatible. [4 marks]

Ans: The system can generate a random avatar without using any of the personal details and optionally the customer also can be given the option to customize it themselves.

b)This would be compatible with the GDPR because generating random avatar without the use of any personal data is not under the scope of GDPR.

Reference: ico.org.uk. (2021). *Rights related to automated decision making including profiling*. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/#ib3