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.

Lawfulness, fairness and transparency (*The principles*, 2021) – organisations must make sure they are not breaking any laws, complying with GDPR and not hiding anything from the users. (OneTrust, 2021)

Purpose limitation – the organisation should only collect data with specific and legitimate purposes and only for that purpose. The processing to achieving the initial purposes in the public interest, scientific, historical research or statistical research shall not be considered as a violation. (*The principles*, 2021)

Data minimisation – The data collected should be adequate, relevant and limited only to the stated purposes and intentions (*The principles*, 2021). This means that only collecting the necessary amounts of data to fulfil the purposes. (Irwin, 2021)

Accuracy – All data collected must be accurate and be kept up to date if possible. There must be reasonable measurements and methods to deal with inaccurate data before they are processed. This must be done immediately without any delays. (*The principles*, 2021)

Storage limitation - the length of time on the stored personal data must be justified and must not be kept longer than necessary. Personal data may be kept for longer periods if the processed data are solely used to achieve purposes with the public interest, scientific, historical research, or statistical purposes, with the inclusion of relevant technical measurements to protect the rights and freedoms of individuals. (*The principles*, 2021)

Integrity and confidentiality (security) – make sure that there is an appropriate amount of security to protect personal data. This includes protection against unauthorised entries to the data, unlawful processing of the data and protection against losses of data, such as accidental damages or destructions. There must be appropriate technical and organisational measurements and steps to prevent these events from happening. (*The principles*, 2021)

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.

Instead of asking explicit permission, the company should implement a consent form for any users who use the website inside and outside of the UK with a clear, concise explanation of how their data is going to be used (Irwin, 2021). The reason for this is because their personal data is going to be used for target advertisement, and the company has to comply and follow the GDPR principles in the UK to make sure that they are lawful and transparent (*The principles*, 2021).

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.

For their first action, the company should heavily consider the amount of data that they need to take from the users and think about if the amount of data collected has fulfilled its purpose while limiting the data collected. (*The principles*, 2021). The other action is when the new features are implemented, the data should be kept up to date and be as accurate as possible, with the relevant technical and organisation measurements in place to safeguard the data (*The principles*, 2021).

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.

Individualised recommendations are based on personal information, and these recommendations require users' explicit consent since this is an example of profiling(*Rights related to automated decision making including profiling*, 2021). Profiling is the processing of their data to evaluate certain ideas about the user, and it is illegal to push recommendations without the consent of the individual. A suggestion to address this problem is that the company must make a consent form for individualising recommendations with the explanation of how it would work and provide a privacy statement when obtaining the data(*Rights related to automated decision making including profiling*, 2021).

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.

Although anonymised data is not subjected to UK GDPR (*What is personal data?*, 2021) and it would be sufficient to anonymise the data under the law, I believe it is still not sufficient to delete the data this way, as there are still risks of the data getting retraced back to the user's personal information (Imperva, 2021). It would be sufficient if the company implemented technical and organisational measures to anonymise to make the data more unidentifiable (*What is personal data?*, 2021) and define the length of time they would keep the data. The company should also give the option for the users to completely erase all of the information relating to this company as a choice to comply with the right to erasure in GDPR (*Right to erasure*, 2021).

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.

The avatar pictures are generated through personal information, which can be deciphered and leaked to the public. This is a violation of the integrity and confidentiality principle in the GDPR (*The principles*, 2021), as the company has the responsibility to protect and safeguard personal data after having the consent of the users (*The principles*, 2021).

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.

An alternative approach would be to randomly generate the avatar without any basis of personal or sensitive information and allow the user to customize their avatar images, similar to how Bitmoji works (PureVPN, 2021). Add any form of consent and permission if the user wishes to customize further. By using this method, it would prevent any leakage of personal data and comply with the GDPR integrity and confidentiality principle (*The principles*, 2021).

References

Imperva (2021) ‘What is Data Anonymization | Pros, Cons & Common Techniques | Imperva’, *Learning Center*. Available at: https://www.imperva.com/learn/data-security/anonymization/ (Accessed: 11 January 2022).

Irwin, L. (2021) *The GDPR: Understanding the 6 data protection principles*, *IT Governance Blog En*. Available at: https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles (Accessed: 10 January 2022).

OneTrust (2021) *Understanding the 7 Principles of the GDPR*, *OneTrust*. Available at: https://www.onetrust.com/blog/gdpr-principles/ (Accessed: 10 January 2022).

PureVPN (2021) *Is Bitmoji Safe? Addressing Myths about Trending Custom Emoji App*, *PUREVPN*. Available at: https://www.purevpn.com/internet-privacy/is-bitmoji-safe (Accessed: 11 January 2022).

Right to erasure (2021). ICO. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ (Accessed: 11 January 2022).

Rights related to automated decision making including profiling (2021). ICO. 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/ (Accessed: 11 January 2022).

The principles (2021). ICO. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ (Accessed: 10 January 2022).

What is personal data? (2021). ICO. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/ (Accessed: 11 January 2022).