CM50266 Applied Data Science 2021-2022
Case Study 1 – Data Protection

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. [7 marks]

Criteria Q1.a. Has each principle been given, with sufficient description? One mark for each.

Principle (a): Lawfulness, fairness and transparency

Organisation's intent of data collection, its usage and any justified consequences on all users must be legal. Organisations must convey the background of who they are, their objectives of data collection and outline data usage processes beforehand, using uncomplicated terms and not mislead users purposely. (Principle (a): Lawfulness, fairness and transparency, 2022)

Principle (b): Purpose limitation

Organisation's privacy statement must be documented and presented to their users beforehand and should define the intent for data processing. Any update to the purpose of data usage must have a lawful basis or organisation must reobtain user consent or have a function set out in law for continued use of personal data for new purposes. (Principle (b): Purpose limitation, 2022)

Principle (c): Data minimisation

Personal data held should be adequate enough, be related and satisfy the organisation's intended purpose of collecting data. Organisation's responsibility lies in regularly identifying, deleting and always avoiding collecting excess data or details irrelevant to the purpose they initially stated or their users consented to. (Principle (c): Data minimisation, 2022)

Principle (d): Accuracy

It is the organisation's duty to keep data updated if required, rectify any inaccuracies identified in the data and ensure that the source of the data collected from organisation's own resources is accurate. Organisations should aim to identify challenges that undermine accuracy of personal data and ensure that a user's request to rectify incorrect data or erase incomplete data must be done without any delay. (Principle (d): Accuracy, 2022)

Principle (e): Storage limitation

Organisations should outline standard data retention periods justified for their purpose. Organisations must regularly review, delete or anonymise and not hold personal data longer than the data retention period and uphold users right to erasure after the retention period. (Principle (e): Storage limitation, 2022)

Principle (f): Integrity and confidentiality (security)

Organisations must ensure that the personal data is processed and held in a secure manner by having organisational policies that ensure confidentiality, integrity and availability at all times. Organisations must prevent unauthorized access, modification of personal data unknowingly or deliberately by implementing suitable levels of IT and physical security measures. (Principle (f): Integrity and confidentiality (security), 2022)

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. [3 marks]

Criteria Q2.a. Has a required change been given?

The website's UK version must get explicit user consent using an opt-in box on their website if they intend to use personal data to target advertisements and be GDPR compliant by using consent as a lawful basis for direct marketing. (Consent, 2022)

Criteria Q2.b. Has the reason for the change been given?

Providing only an opt-out means that all users are automatically signed up and their data is used for promotions without consent when they create an account.

Users can object to data usage or opt out only after it has been utilised by the website for a brief period between account creation and opt-out.

By using only opt-out, the website denies users the right to object the use of their data for marketing purposes when they create an account and GDPR UK clearly states that "consent must be unambiguous and involve a clear affirmative action (an opt-in)." to have consent as Lawful basis for processing personal data. (Consent,2022; The right to object to the use of your data, 2022)

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. [4 marks.]

Criteria Q3.a. Have two actions the company will need to take been given? One mark for each.

Action 1:

Data Protection Impact Assessment (DPIA):

Feature 1, the recommendation system will employ machine learning which GDPR classifies as innovative technology and Feature 2, the avatar generation system makes an automatic decision on how a user looks by processing their personal data, both of which fall under the "likely to result in high risk" processing category, therefore, DPIA must be done as per GDPR requirement. (Examples of processing 'likely to result in high risk', 2022; When do we need to do a DPIA?, 2022)

Action 2:

Data protection by design and default:

Since both of the new features rely on personal data processing, the features need to incorporate pseudonymisation and encryption of stored data, appropriate data retention policies for data minimisation and get user consent by ticking opt-in box on their website as part of design to protect the privacy of users. (Consent, 2022; Data protection by design and default, 2022)

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. [3 marks]

Criteria Q4.a. Has a relevant GDPR related issue with the proposed plan been identified?

Issue:

The recommendation system will also need to use cookies to track the user's interaction with the website for instance browser history, track how many recommendations the user actually clicked on, how much time they spend browsing each recommendation etc along with using personal data to generate individualised recommendations with good accuracy for each user.

GDPR UK classifies" cookie identifiers as a type of 'online identifier', meaning that in certain circumstances these will be personal data." (How do the cookie rules relate to the GDPR?, 2022)

Plan:

To be GDPR compliant, the website should do a cookie audit to determine what cookies would be essential for the recommendations and the website should get opt-in consent for use of cookies on their website. (How do we comply with the cookie rules?, 2022)

Criteria Q4.b. Has a viable suggestion been provided for how this issue could be addressed?

Website must use pop-ups or flash messages to list out the cookies they will use for the recommendations, marketing and other essential cookies and request consent for each type of cookie separately and store these preferences to show a suitable version of the website to the user.

The users should be given an option to set their cookie preferences and should explain the purpose, duration of cookies and a hyperlink to a document explaining the cookie policy in a clear, unambiguous and transparent way. (What are the rules on cookies and similar technologies?, 2022)

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. [4 marks]

Criteria Q5.a. See model answer for guidance of suitable explanations

Deleting personal details is insufficient as it does not truly anonymise the reviews, ratings and the user-defined screen-names since, there is a possibility that some personal details such as real name, age, sex, city of residence and email address might have been included by the user in their review and such a review in combination with their profile picture, IP address, cookies, browser history and screen name which might still be a user's real name can uniquely identify the individual.

Since the reviews are visible to other users of the site, there is a risk of identification of a natural person by any user with access to such reviews. (What is personal data?, 2022)

When the user deletes their account, consent for using their personal data is withdrawn and therefore, GDPR rules such as user consent and data minimisation, as the website is holding extra details about an existing user without deleting it still apply to the reviews and ratings since they have not been anonymised properly. (How should we obtain, record and manage consent?, 2022; Principle (c): Data minimisation, 2022; Principle (e): Storage limitation, 2022)

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. [3 marks]

Criteria Q6.a. Has a valid reason why the proposed plan may not be appropriate been provided?

The system generates avatar based on personal details like real name, age, sex, city of residence that has a good chance of resembling the user, for instance the avatar's hairstyle could be according to sex or could be white, black or grey based on age and use user's location to display racial or ethnic origin similar to majority of people in the user's location. (What is personal data?, 2022)

The avatar may resemble real user and reveal their personal details and is not compliant with GDPR's Data Protection by design and default which requires data processing to protect personal and special category data. (Data protection by design and default, 2022)

The system also violates purpose limitation and data minimisation as the personal data processed to generate avatar was initially collected with the intention of scoring and reviewing cars and also because the avatar images generated are extra details being stored that irrelevant for reviewing and scoring cars. (Principle (c): Data minimisation, 2022, Principle (b): Purpose limitation, 2022)

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]

Criteria Q7.a. Has a viable alternative solution been provided?

The system can generate non-human looking cartoons based on a predefined set of geometric shapes for head, eyes, nose etc, avoid colours that depict skin tones, be gender neutral by avoiding hair styles and accessories.

A unique avatar for every user can be generated by combining different non-skin tone colours, geometric shapes for the face, eyes, nose etc, with different facial expressions and coloured backgrounds.

The system will then randomise and generate an avatar by picking a unique combination of geometric facial features and colours for facial features and backgrounds for every user.

Criteria Q7.b. Has an explanation of why this is an appropriate solution been provided?

The new alternative will be GDPR compliant by not processing personal data to generate avatar and by using non-human like geometric shapes, skin tones and being genderless protects user's personal data from getting leaked.

It will make it difficult to identify or resemble a natural person solely based on their avatar or in combination with other personal data, hence the avatar will be pseudonymised and be GDPR compliant according to the Data Protection by design which requires safeguards for rights of data subjects. (Data protection by design and default, 2022)

Unique combinations of avatars can be generated by using coloured background, coloured facial features and facial expressions for instance, popular websites like Reddit and Discord generate combinations of alien cartoons as default avatars which would never resemble a real human and require minimal/no processing of personal data.

References:

Criteria Q1.b. Has an appropriate reference been provided for the principles?

Anon, 2022. *Principle (d): Accuracy*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/ [Accessed 14 Jan. 2022].

Anon, 2022. *Principle (c): Data minimisation*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/ [Accessed 14 Jan. 2022].

Anon, 2022. *Principle (f): Integrity and confidentiality (security)*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/integrity-and-confidentiality-security/ [Accessed 14 Jan. 2022].

Anon, 2022. *Principle (a): Lawfulness, fairness and transparency*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/ [Accessed 14 Jan. 2022].

Anon, 2022. *Principle (b): Purpose limitation*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ [Accessed 14 Jan. 2022].

Anon, 2022. *Principle (e): Storage limitation*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/ [Accessed 14 Jan. 2022].

Criteria Q2.c. Has a suitable reference been given for the required action?

Anon, 2022. *Consent*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ [Accessed 14 Jan. 2022].

Anon, 2022. *The right to object to the use of your data*. [online] Ico.org.uk. Available from: https://ico.org.uk/your-data-matters/the-right-to-object-to-the-use-of-your-data/ [Accessed 14 Jan. 2022].

Criteria Q3.b. Have suitable references been given for each action? One mark each.

Anon, 2022. *Consent*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ [Accessed 14 Jan. 2022].

Anon, 2022. *Data protection by design and default*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ [Accessed 14 Jan. 2022].

Anon, 2022. *Examples of processing ‘likely to result in high risk’*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/ [Accessed 14 Jan. 2022].

Anon, 2022. *When do we need to do a DPIA?*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/ [Accessed 14 Jan. 2022].

Criteria Q4.c. Has a suitable reference for the issue and its resolution been provided?

Anon, 2022. *How do the cookie rules relate to the GDPR?*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-the-cookie-rules-relate-to-the-gdpr/ [Accessed 14 Jan. 2022].

Anon, 2022. *How do we comply with the cookie rules?*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/ [Accessed 14 Jan. 2022].

Anon, 2022. *What are the rules on cookies and similar technologies?*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/what-are-the-rules-on-cookies-and-similar-technologies/ [Accessed 14 Jan. 2022].

Criteria Q5.b. Has a suitable reference that assists in understanding the explanation been given?

Anon, 2022. *How should we obtain, record and manage consent?*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/how-should-we-obtain-record-and-manage-consent/ [Accessed 14 Jan. 2022].

Anon, 2022. *Principle (c): Data minimisation*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/ [Accessed 14 Jan. 2022].

Anon, 2022. *Principle (e): Storage limitation*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/ [Accessed 14 Jan. 2022].

Anon, 2022. *What is personal data?*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/?q=anon [Accessed 14 Jan. 2022].

Criteria Q6.b. Has a referenced been provided that assists in the understanding of the reason?

Anon, 2022. *Data protection by design and default*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ [Accessed 14 Jan. 2022].

Anon, 2022. *Principle (c): Data minimisation*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/ [Accessed 14 Jan. 2022].

Anon, 2022. *Principle (b): Purpose limitation*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ [Accessed 14 Jan. 2022].

Anon, 2022. *What is personal data?*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/ [Accessed 14 Jan. 2022].

Criteria Q7.c Has a reference been provided that assists in assessing the validity of the solution?

Anon, 2022. *Data protection by design and default*. [online] Ico.org.uk. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/?q=pse [Accessed 14 Jan. 2022].