Case Study 1 – Data Protection

Note: References at the end of the document.

Question 1

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.

(a) Lawfulness, fairness and transparency (ICO, 2021a)
Data must be processed in a manner that is considered lawful (The DPO Centre LTD, 2021) such as with subject consent or public interest. Data processing must also be *fair*, without adverse effects on the subject, as well as *transparent*, with the data controller being clear about their intent and being able to prove how the data is being used.

(b) Purpose limitation (ICO, 2021a)
Data can be collected only for “specified, explicit and legitimate purposes”.
The purpose of data collection should be well-defined to the subject prior to collection and documented. After data collection, the data may *only* be used for that pre-stated purpose.

(c) Data minimisation (ICO, 2021a)
The amount of data collected should be limited to only what is absolutely necessary for the intended use. No additional data that is not directly required should be collected.

(d) Accuracy (ICO, 2021a)
Data that is collected and stored should be accurate and up to date. If this is not the case, it is the controller’s responsibility to correct, update, or erase the data.

(e) Storage limitation (ICO, 2021a)
Subject data should not be kept for longer than is absolutely necessary for the stated purpose. If kept for longer, it must be purely for archiving purposes in the public interest, or in the interest of scientific/historical/statistical research purposes, and stored in a way that follows GDPR guidelines.

(f) Integrity and confidentiality (security) (ICO, 2021a)
Subject data must be kept secure from internal and external threats at all times.
Data must not be processed without an authorised and lawful purpose and must be protected against any kind of loss, destruction or damage.

Question 2

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.

Change

When the user signs up, the company should ask for explicit permission to use their data to help target advertising to the user.

Reason

Even though it gives the user the option to opt-out, it is initially not fully transparent with the user about how their data would be used (breaks principle (a) (ICO, 2021a)) and the data would be used for a purpose other than the specified one (breaks principle (b) (ICO, 2021a)).

Question 3

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.

Measure 1 — Records of Processing Activities (ROPA)
The first action that the company will need to take is to implement a Record of Processing Activities (ROPA) (ICO, 2021d).
This record should include all activities involving the processing of data in similar profiles and the use of data for the generation of avatar images.

Measure 2 — Data Protection Impact Assessments (DPIAs)
The second action that the company will need to take is the enactment of Data Protection Impact Assessments (DPIAs) (ICO, 2021e).
DPIAs should be used to identify, document, and minimise data protection risks. It is especially needed when sensitive data is involved such as the personal data in the two new features that the company needs to implement.

Question 4

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.

Issue

An issue the company may have with implementing the first feature is that it has not asked for explicit permission from the user to use their profile of existing car ratings (subject data) to find similar profiles and make recommendations.

This breaks GDPR principle (a) because processing is not lawful and transparent, and principle (b) because the data is used for a purpose that was not previously stated (ICO, 2021a).

Solution

The company could address the issue by asking the user for permission to use their data for individualised recommendations when the user signs up.

This would not break any GDPR principles (ICO, 2021a).

Question 5

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.

Answer

Deleting the personal details is *not* sufficient to do this.
This is because the user can potentially still be identified from their review comments (which may include car owned, location, sex etc.), so the data is not completely anonymous and still falls under the category of *personal data* (ICO, 2021c) that has to abide by the GDPR UK principles.

Question 6

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.

Answer

Allowing the system to generate the avatar image would not be compatible with GDPR UK principle (f): Integrity and confidentiality (ICO, 2021a).

This is because the avatar image is displayed in the comments and provides other users with personal information about the commenter (e.g. sex or age), thus not providing appropriate security of the data and confidentiality.

Question 7

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.

Approach 1: Do not use subject data

Generate a random avatar image that is unique for each user and does not use any of the user details. This could use a pool of a large number of features that are combined to create a person's avatar face.

This is compatible with the GDPR because the principles do not apply when there is no user data involved (ICO, 2021a).

Approach 2: Ask for consent

Ask the user for explicit permission to use personal data to generate a unique avatar image. Also, provide a reason why the generation of this image is necessary.

This would make it compatible with the GDPR (ICO, 2021a) because

a. There would be lawfulness, fairness, and transparency (principle a)
b. The purpose would be explicitly stated (principle b)
c. There is no additional data collected that is unnecessary (principle c)
d. Data will be accurate since it is provided by the user and the user can change it (principle d)
e. (Storage limitation does not apply here)
f. Subject data would not be "leaked" since consent has been given.

NB: (Optional) See next page for notes on this.

——

<u>**Other approaches that do NOT work with justification:**</u>

Approach 3: Car Avatar Images

The users have given explicit consent for their car review comments to be shared with site visitors.

If the avatar images are generated using these reviews and comments (e.g. avatar images of cars) then they would be compatible with the GDPR since consent has been given, and would be unique for each user.

NO because of “purpose limitation” (b). It has not been explicitly stated that the data will be used for generation of avatar images.

——

Approach 4: Hidden Images

Keep generated avatar images hidden from site visitors and give the user the option to make them public.

(NO because it does not guarantee a unique avatar image for each user which is what the question asks for since some users won’t necessarily to have a *unique* one)

——

NB: (Optional) See next page for references.

References

Information Commissioner's Office (ICO), 2021a. *The principles* [Online]. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ [Accessed 07 January 2022].

Information Commissioner's Office (ICO), 2021b. *Accountability and Governance* [Online]. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/ [Accessed 07 January 2022].

Information Commissioner's Office (ICO), 2021c. *What is personal data?* [Online]. Available from: 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/#pd4 [Accessed 07 January 2022].

Information Commissioner's Office (ICO), 2021d. *Records of processing and lawful basis* [Online]. Available from: https://ico.org.uk/for-organisations/accountability-framework/records-of-processing-and-lawful-basis/ [Accessed 07 January 2022].

Information Commissioner's Office (ICO), 2021e. *Data protection impact assessments* [Online]. 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-impact-assessments/ [Accessed 07 January 2022].

The DPO Centre LTD, 2021. *Article 6 EU GDPR "Lawfulness of processing"* [Online]. Available from: https://www.dpocentre.com/resources/gdpr/article-6/ [Accessed 07 January 2022].