Case Study: 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]

The following paragraphs summarize the GDPR's data privacy principles, excluding the principle of accountability, as defined by the Information Commissioner's Office (ICO, 2019a)

- Lawfulness, Fairness and Transparency – Data collection and processing should be lawful to ensure that data owners are treated fairly when organization exercise their data privacy rights. Additionally, they must explain in plain language when, how and why they use personal data from the start.

- Purpose limitation - The organization should collect data for a specific purpose clearly defined in terms of how the organization will use the user data and the period during which the organization will retain the data until the objective is accomplished. If the organization intends to use the user's data for purposes other than those stated initially, they must inform the user before any activity.

- Data minimization - Data should be restricted, relevant, and adequate for the processing to reach the objective. Before compiling data, organization should ascertain the system is sufficient to guarantee that data is retained solely for the reason which it is collected.

- Accuracy - Data should be accurate and be verified to ensure that it is always maintained in an up-to-date state. To avoid outdated or erroneous information, Organization should rectify or delete it from the collection when data is not complete and expire.

- Storage limitation - Data is no longer required to use for any purposes should be deleted or anonymized. It will decrease the likelihood of becoming obsolete, excessive, inaccurate, or out of date, including minimizing the possibility that organization may utilize such data incorrectly to the damage of all stakeholders.

- Integrity and confidentiality (security) – Data should process and keep securely with appropriate technical and organizational measures in the dimension of confidentiality, integrity, and availability of systems. Organizations must consider risk analysis, corporate policies, and physical and technical protections to avoid unauthorized or unlawful processing.

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]

Following the purpose limitation, ACME should notify consumers that ACME may use their personal information to help target adverts to specific users (ICO, 2019b) and enable users to delete or update personal data submitted to ACME (GDPR, 2013). It is vital to notify consumers about the firm's intention of using their data for targeted marketing because data is the customer's property and should be acknowledged and consented to before any business purpose.

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.]

Action 1: ACME should adopt and implement data protection policies, conducting impact evaluations for uses of personal data posing a severe risk to the interests of an individual (ICO, 2020). The company can build a progressive protection strategy in an unforeseeable lousy event.

Action 2: Auditors must track all data to confirm that appropriate technological and organizational procedures are in place to meet the regulatory obligations. For instance, to guarantee that their system maintains confidentiality, integrity, and availability, including supporting documentation of process to demonstrate compliance (ICO, 2020).

Q4. Identify a GDPR related issue that the company may have with implementing the plan to provide individualized recommendations and suggest a way these could be addressed to allow this to proceed. [3 marks]

According to GDPR and the purpose limitation principle, that is collected for specific, valid reasons and not handled in a way that contradicts those objectives. Therefore, ACME needs to ask for permission from the users to obtain their consent for providing the recommendation system based on their data; the user has the right to withdraw approval at any time (European Parliament, 2016b).

To suggest a solution for the recommendation system, if a user withdraws consent or is unwilling to allow the system to use their personal data, the system should provide a recommendation system that treats them as a new user and pushes cars that are in high demand and have an excellent record of sales and promotions.

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]

I believe deleting the personal data could not be sufficient since some attributes from the rating or user comments may be associated with the user's data. For instance, a user's review may contain their personal or contact detail. The meaning of anonymous under UK GDPR, ACME must remove enough identifying features until they cannot identify. However, anonymization won't be adequate if you can re-identify that data refers to a specific person (ICO, 2019c).

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]

The way ACME generates the Avatar image would be incompatible with the GDPR's principles of lawfulness, fairness, and transparency since it would risk users' privacy. Additionally, taking advantage of this element violates the GDPR's purpose limitation principle (European Parliament, 2016a). ACME did not inform users that ACME may use their data for purposes other than those previously specified. In this scenario, ACME must explicitly disclose and provide a reasonable explanation additional purpose of collecting before implementing the new feature.

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]

I suggest the 'Identicons' technique used by GitHub for generating Avatar images by utilizing their user's ID hash. The algorithm traverses the hash and turns pixels on and off to determine color values to create an image avatar (Jason, 2013). This suggestion should be compatible with GDPR because the avatar picture will not touch any user's data, ensuring no possibility of data leakage.

Reference

European Parliament and of the Council, 2016a. *Principles relating to processing of personal data)* [Online] Available: https://www.legislation.gov.uk/eur/2016/679/article/5 [Accessed 8 Jan 2022].

European Parliament and of the Council, 2016b. *the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing* [Online] Available at: https://www.legislation.gov.uk/eur/2016/679/article/7. [Accessed 8 Jan 2022].

General Data Protection Regulation (GDPR), 2013. *Right to erasure ("right to be forgotten")*. [Online] Available at: https://gdpr-info.eu/art-17-gdpr/ [Accessed 8 Jan 2022].

Information Commissioner's Office (ICO), 2019a *The Principles*. [Online] Ico.org.uk. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/. [Accessed 8 Jan 2022].

Information Commissioner's Office (ICO), 2019b. *Right to be informed*. [Online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/ [Accessed 8 Jan 2022].

Information Commissioner's Office (ICO), 2019c. *What is personal data?* [Online] 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 8 Jan 2022].

Information Commissioner's Office (ICO), 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/ [Accessed 8 Jan 2022].

Long, J., 2013. *Identicons!* [Online] Available at: https://github.blog/2013-08-14-identicons/ [Accessed 11 Jan. 2022].