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

Data privacy principles of the GDPR:

1. Lawfulness, fairness and transparency:
   This principle enunciates that all personal data must be processed in a lawful and fair manner, which means establishing valid reasons for the collection and use of personal information, and not using data in a way that is harmful, unexpected, or deceptive. Also, one must be transparent, upfront, and honest with people about how their personal data is being used (NIBusinessInfo, 2019a) (ICO, 2021a)
2. Purpose limitation:
   According to the second principle, personal data must only be collected for a clear, explicit, and lawful reason, and this purpose must be documented clearly. (ICO, 2021b)
3. Data minimisation:
   In order to adhere to this principle, care must be taken to ensure that the data being processed is sufficient to justify the stated purpose, pertinent to the purpose, and confined to what is essential with the purpose. (ICO, 2021c)
4. Accuracy:
   This principle requires that the data being stored or processed is correct and periodically updated as and when required. If there is any incorrect data, necessary actions to either delete or rectify it should be taken accordingly. (ICO, 2021d)
5. Storage limitation:
   This principle states that personal information should not be kept for longer than necessary, and if it is being stored, proper justification should be present that aligns with public interests or research purposes. Appropriate time limits must be set after which the data not being used should be anonymized. (ICO, 2021e)
6. Integrity and confidentiality:
   This principle primarily focuses on data security, emphasising adequate security and confidentiality of personal data, like protection against illegal or illicit access to or use of personal data. It also mentions that suitable protective measures must be taken in case of unintentional loss or damage to the data. (ICO, 2021f)

Change required in US website for compatibility in the UK:

After looking at the current US website specifications, a suggested change to the website that would make it compatible with the GDPR requirements is a feature that allows the user to modify or update previously entered data. (itgovernance, 2018)
For example, if a user has moved to another country, they would need to update their address to the new one, and they should be able to access previously entered data and update the address. This feature has been suggested in order to comply with the accuracy principle of the GDPR, where it says that data must be kept up to date, and the user must have the option to do so. (GDPR, 2018a)

Two actions required in compliance with the GDPR Accountability principle:

In accordance with the accountability principle of the GDPR, one action that should be taken is that for all the personal data being processed, the approach taken should always prioritise privacy by making sure that processing is always minimal and ensuring that an individual can always monitor it. This is in line with the Data protection by design and default requirement of the Accountability principle. (ICO, 2021g)
Another action that should be taken is the setting up of an Impact Assessment, which assists in identifying and reducing a project's data security threats. This is because there is a high risk involved, and there is automated decision-making with significant effects in the implementation of the new features. (ICO, 2021h)

Issues and rectifications involved with individualised recommendations:

A possible GDPR related issue that could arise with the introduction of individual recommendations is that because the amount of data being cross referenced is so large, there could be a bias in the recommendations based on either the sex of a user or their place of residence. Also, there is a chance of a breach of privacy in case somehow the data is de-anonymised. (Milano, et al., 2020)
To address and rectify this issue, regular checks can be scheduled to monitor the functioning of the system, and a provision should be made where it is easy for any user to request human intervention or challenge a decision of the recommender system. This is in accordance with Article 22 of the GDPR. (GDPR, 2018b)

Discussing whether the deletion of personal data is sufficient or not for:

In line with the approach stipulated in the given scenario, the deletion of personal data will succeed in achieving anonymisation. And once data is truly anonymised, it doesn’t fall within the scope of the GDPR, thus making it a viable option. (UCL, 2019a) But at the same time, if personal data is deleted, then it fails to provide useful information for ratings and reviews, and hence is rendered useless for the intended purpose. To solve this conundrum, we make use of pseudonymisation, which is the processing of personal information such that it can no longer be associated with a particular data subject without the use of additional details, and these additional are stored elsewhere with limited access to it. (ICO, 2021i) This way, it stops direct identification of an individual, while also ensuring that the data falls within the scope of the GDPR, as mentioned in Recital 26. (privacy-regulation, 2018)

Incompatibility of a system generated avatar with the GDPR:

A possible reason for why a system generated avatar could be incompatible with the GDPR is that the avatar could contain features of a specific race, ethnic type, or location of the user, since the avatar is constructed using some of the personal data of the user. (Hill, 2012) This makes it possible for anyone to infer the race or location of another user, just by looking at similarity and features of the avatar, thus violating the privacy rights of a user as stated in the sixth principle of the GDPR. (GDPR, 2018c)

Alternative approach to make a system generated avatar compatible with the GDPR:

Since the use of a system generated avatar from personal data is incompatible with the GDPR, one solution to this problem is that after the avatar is created, the user must select whether they are satisfied with the avatar, and if not, they should have an option to modify it or even choose a blank one. (NIBusinessInfo, n.d. b)
This approach ensures that every system generated avatar is the outcome of the user’s personal choice, thus upholding the GDPR’s privacy as stated in Article 25 and Recital 72 of the GDPR. It also meets the requirement of giving the user the option to modify, update or even delete data as requested, as formulated in the GDPR. (GDPR, 2018d)

References

GDPR, 2018a. *Article 16 GDPR.* [Online]
Available at: https://gdpr.eu/article-16-right-to-rectification/
[Accessed 10 January 2022].

GDPR, 2018b. *Article 22 GDPR.* [Online]
Available at: https://gdpr.eu/article-22-automated-individual-decision-making/
[Accessed 10 January 2022].

GDPR, 2018c. *Recital 75 GDPR.* [Online]
Available at: https://gdpr.eu/Recital-75-Risks-to-the-rights-and-freedoms-of-natural-persons/
[Accessed 11 January 2022].

GDPR, 2018d. *Recital 72 GDPR.* [Online]
Available at: https://gdpr.eu/recital-72-guidance-of-the-european-data-protection-board-regarding-profiling/
[Accessed 11 January 2022].

Hill, D. W., 2012. Avatar Ethics: Beyond Images and Signs. *Journal for Cultural Research,* 17BEC1092(1), pp. 69-84.

ICO, 2021a. *Principle (a): Lawfulness, fairness and transparency.* [Online]
Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/
[Accessed 9 January 2022].

ICO, 2021b. *Principle (b): Purpose limitation.* [Online]
Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/
[Accessed 9 January 2022].

ICO, 2021c. *Principle (c): Data minimisation.* [Online]
Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/
[Accessed 10 January 2022].

ICO, 2021d. *Principle (d): Accuracy.* [Online]
Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/
[Accessed 10 January 2022].

ICO, 2021e. *Principle (e): Storage limitation.* [Online]
Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/
[Accessed 9 January 2022].

ICO, 2021f. *Principle (f): Integrity and confidentiality (security).* [Online]
Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/integrity-and-confidentiality-security/
[Accessed 9 January 2022].

ICO, 2021g. *Data protection by design and default.* [Online]
Available at: 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 10 January 2022].

ICO, 2021h. *Data protection impact assessments.* [Online]
Available at: 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 10 January 2022].

ICO, 2021i. *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 11 January 2022].

itgovernance, 2018. *The EU GDPR (General Data Protection Regulation) – Overview.* [Online]
Available at: https://www.itgovernance.eu/en-ie/eu-general-data-protection-regulation-gdpr-ie
[Accessed 9 January 2022].

Milano, S., Taddeo, M. & Floridi, L., 2020. Recommender systems and their ethical challenges. *Springer.*

NIBusinessInfo, 2019a. *UK General Data Protection Regulation.* [Online]
Available at: https://www.nibusinessinfo.co.uk/content/data-protection-principles-under-uk-gdpr
[Accessed 9 January 2022].

NIBusinessInfo, n.d. b. *Security principle under the UK GDPR.* [Online]
Available at: https://www.nibusinessinfo.co.uk/content/security-principle-under-uk-gdpr
[Accessed 11 January 2019b].

privacy-regulation, 2018. *Recital 26 GDPR.* [Online]
Available at: https://www.privacy-regulation.eu/en/recital-26-GDPR.htm
[Accessed 11 January 2022].

UCL, 2019a. *Anonymisation and Pseudonymisation.* [Online]
Available at: https://www.ucl.ac.uk/data-protection/guidance-staff-students-and-researchers/practical-data-protection-guidance-notices/anonymisation-and
[Accessed 11 January 2022].