Case Study 1 – Data Protection

Q. Excluding Accountability, what are the data privacy principles of the GDPR?

A. The GDPR consists of six core principles (excluding Accountability) which are 'Integrity and confidentiality', 'Lawfulness, fairness and transparency', 'Purpose limitation', 'Data minimisation', 'Accuracy' and 'Storage limitation'. To briefly summarise, the principle of 'Integrity and confidentiality' demands that personal data be secure against unauthorised use and accidental damage/ loss through appropriate technical means. 'Lawfulness, fairness and transparency' requires that personal data is used lawfully, fairly and transparently relative to the individual. The principle of 'Purpose limitation' necessitates that personal data should only be processed if relevant to the purpose or other compatible purposes and explicitly not be processed if incompatible with such purpose. Similarly, 'Data minimisation' requires that personal data only be processed if it supports and has a rational link to the purpose, and using the minimum information required to achieve such purpose. The GDPR mandates that personal data be accurate and maintained, ensuring that measures are taken to rectify inaccurate data if otherwise through the principle of 'Accuracy'. The remaining principle of 'Storage limitation' requires that personal data must not be kept for longer than necessary in fulfilling the required purpose, unless kept in the public interest of archiving, or research/ statistical purposes.

Q. 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.

A. To account for its targeted advertising system, the company should update the website's cookie policy since there is no general cookie law in the US, ensuring that users clearly informed and have the option to give consent. This can be done through implementing a cookie banner which informs the individual of what data is collected and why, also explaining that the data is shared with a third-party. This banner should give the user to opt in or out of cookie usage. This is necessary for the website to comply with GDPR's principle of 'Lawfulness, fairness and transparency' as the cookies process personal data in order to selectively target users with advertisements.

Q. 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.

A. The company must take measures in complying with GDPR by demonstrating its responsibility in deploying appropriate measures to meet the Accountability principle's requirements. Such measures include maintaining documentation which clearly states processing purpose(s) and records processing activities. The company plans to introduce a feature which recommends cars based on users sharing similar profiles of existing car reviews. Therefore, it is imperative that users can access documentation explaining the decisions in recommending cars based on their profile, and such automated decisions should have the capability of being reviewed. In addition, these individuals must have the right to be informed about what data is shared and who it is shared with.

The company plans to also introduce another new feature that allows users to either upload a small image or be assigned an avatar, constructed from the personal additional information of the user that has previously been provided to the company. Essentially, this feature involves profiling and automated decision-making to generate an avatar. However, this can potentially discriminate against users by stereotyping features based on their personal data. This can be a violation of the 'Lawfulness, fairness and transparency principle' if personal data is used to infer/predict a user's appearance, which may not be accurate or fair. Since the company plans on using a model to make possibly significant decisions in a solely automated way, the company must first seek the user's explicit consent or have substantial public interest in the feature. Furthermore, the inference of special category data using personal data is intentional, so it is treated as special category data regardless of if the inferences are correct. Thus, the company should ensure that they comply with articles 9 and 10 of the GDPR. To demonstrate compliance with GDPR, the company should carry out a DPIA (Data Protection Impact Assessment) since there is high risk in processing special category data. In addition, the company should make documentation detailing all automated profiling decisions in the case a user requests to know how such decisions are made.

Q. 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.

A. Assuming the individualised recommendations are solely automated, in an unlikely event, it is possible that a recommendation could be offensive to the user based on stereotyping a particular group of people. For example, users from minority groups being recommended low budget cars can portray the company as prejudiced. To avoid this, the company can hire workers to review the automated decisions ensuring that such issues do not occur and does not violate the 'Lawfulness, fairness and transparency' principle.
To avoid this, users should be given the option to reject personalised recommendations in which case, they should be able to filter results based on user specified search inputs.

Q. 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 held about the user. It plans to seek permission to do this. Is the deleting of personal data sufficient to achieve this?

A. Yes, provided that the company has requested consent (and informed any others they have shared the data with about the erasure), and that there is no possibility of reversing the anonymisation process since the data is deleted, the deletion of personal data should be sufficient to achieve the above. It is imperative that all the personal data is deleted from all systems including backup systems if the company wants to anonymise the data. Given the data is fully anonymised, it is not subject to the restrictions of the GDPR as personal data is. As the data has undergone appropriate anonymisation, the remaining data can be used to provide ratings and review comments.

Q. Other than the 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.

A. As described in the previous answer referring to this feature, the data can be considered special category data as personal data is used with the intent to infer special category data. Besides the lack of explicit consent, the feature fails to meet the alternate conditions for processing special category data listed in article 9 of the GDPR. The processing of the data is not: for employment, social security, vital interests, made public by the data subject, legal claims, health care, in substantial public interest or for archiving for statistical purposes so the conditions of processing the special category data are not met. Therefore, the feature is incompatible with the GDPR.

Q. 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.

A. To comply with GDPR, the avatars could be randomly generated without a basis so no personal data or special category data would influence the outcome of the solely automated decision. The avatar should be generated from carefully curated sets of options that doesn't raise any issues of discrimination or prejudice and should not resemble any group of individuals. Using this method, the avatars would minimise the possibility of leaking any personal identification information and no one should be able to make accurate inferences of the user's personal details based on their avatar. Hypothetically, there still may exist a small possibility of identifying an individual so certain factors must be considered to assess the possibility of identification. The company should consider the trade-off for the costs and time required to identify a user as well as the availability of technology at the time to determine if it is a likely risk. The company should account for all perspectives of why someone would want to identify an individual, e.g., the individual being investigated may be a high-profile figure or a user investigating may be a stalker. The actions the company takes in assessing and preparing for methods of identifying users should be documented to demonstrate compliance with GDPR.

Bibliography

1. Information Commissioner's Office, 2018. *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 8 January 2022].

2. Iubenda, n.d. *Cookies and the GDPR: What's Really Required?* [Online]. Available from: https://www.iubenda.com/en/help/5525-cookies-gdpr-requirements [Accessed 9 January 2022].

3. Information Commissioner's Office, 2018. *Lawfulness, fairness and transparency* [Online]. 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 9 January 2022].

4. Information Commissioner's Office, 2018. *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 9 January 2022].

5. GDPR Informer, 2018. *How does the GDPR affect profiling?* [Online]. Available from: https://gdprinformer.com/gdpr-articles/gdpr-affect-profiling [Accessed 10 January 2022].

6. Intersoft Consulting, n.d. *Art. 9 – Processing of special categories of personal data* [Online]. Available from: https://gdpr-info.eu/art-9-gdpr/ [Accessed 10 January 2022].

7. Information Commissioner's Office, 2018. *What is automated individual decision making and profiling?* [Online]. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-*making*-and-profiling/#id4 [Accessed 9 January 2022].

8. Intersoft Consulting, n.d. *Recital 71 – Profiling* [Online]. Available from: https://gdpr-info.eu/recitals/no-71/ [Accessed on 10 January 2022].

9. Data Protection Commission, 2021. *Anonymisation and Pseudonymisation* [Online]. Available from: https://www.dataprotection.ie/en/dpc-guidance/anonymisation-pseudonymisation [Accessed 10 January 2022].

10. European Commission, 2018. *Do we always have to delete personal data if a person asks?* [Online]. Available from: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/do-we-always-have-delete-personal-data-if-person-asks_en [Accessed 10 January 2022].

11. Information Commissioner's Office, 2018. *Special category data* [Online]. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/ [Accessed 11 January 2022].

12. Information Commissioner's Office, 2018. *Can we identify an individual indirectly from the information we have (together with other information)?* [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/can-we-identify-an-individual-indirectly/ [Accessed 11 January 2022].