CM50266 Applied Data Science 2020-2021

Case Study 1 – Data Protection

Q1.

The GDPR includes six data privacy principles that should be followed when handling personal data[1].

Firstly, we have **Lawfulness, Fairness and Transparency**, as personal data must always be processed lawfully, fairly, and the intent of the how the data will be used should always be transparent.

Furthermore, we have **Purpose Limitation** where the purpose of storing personal data should be clearly stated, providing that the explicit reasons are legitimate and keeping the data for as long as necessary.

Additionally, we have **Data Minimisation**, where the data must be used in a way that is adequate, relevant, and limited to what is needed for the processing purpose.

Further, we have **Accuracy**, data should be accurate and always up to date, taking measures in removing inaccurate or incomplete data but also making sure that individuals have the option on requesting data that are related to them to be rectified and erased.

Also, **Storage Limitation,** which describes that data should only be retained for as long as necessary considering their purpose of keeping, and securely deleting any data when are no longer needed.

Lastly, we have **Integrity and Confidentiality**, which also describes that data should always be kept secure by establishing appropriate security measures including preventing “unauthorised or unlawful processing” [1] or destruction or damage.

Q2.

The GDPR Accountability principle states that a company should be responsible and be able to demonstrate their ability of compliance with the other data protection principles. But there are many elements of Accountability that should also be established and correctly addressed in order for a company to fully comply with the rules. There are several actions the company will need to take for the implementation of the new features. Firstly, we have the action of **Transparency** [2] which describes, communicating information of individuals regarding their privacy program, procedures, and processes regarding the use of their personal data as well as potential risks. The company should clearly inform their users of how the addition of the new feature will use their private information. This communication engages the privacy regulations of the company regarding their privacy program. Furthermore, we have **Risk Assessment** [2] where the company should assess their privacy program regarding these newly added features as they should be able to able to mitigate any risks of individuals in case of data breach incidents. The addition of these features should in no way disrupt the security of the company so their policies should be updated and addressed.

Q3.

There are some key additions in the 2018 Data Protection Act that updates the previous 1998 DPA. These 3 additions are "**the right to erasure**", "**inclusions of exemptions of the Data Protection Act**" and "**being regulated in tandem with the GDPR**" [3].

The right to erasure introduced the right to individuals to have their personal data erased at their request but can only be applied under certain circumstances [4]. The consequence of this addition prevents the company from indefinitely keeping a user's data and using it for processing purposes.[5]

Additionally, the 2018 DPA includes the exemptions from particular provisions. In this case you may not have to follow all of the rights and obligations. Some of these exemptions include "the right to be informed, the right of access, dealing with other individual rights"[6] and more. The consequence is now the exemptions are much clearer for the people to know and understand making it stricter for the companies to follow and implement the rules accordingly.[3]

Finally, for the 3rd difference we have the inclusion of the GDPR which works in tandem with the DPA 2018. With the creation of the GDPR the Data Protection Act was updated and are intended to be used together [3]. This combination has a consequence that rules are applied not only for the citizens for the UK but also of the European Union. Thus, companies that use information from citizens of the European Union need to also abide by the rules of the GDPR.

Q4.

Automated decision making and profiling was an issue which was addressed in the 2018 GDPR which states "Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them." [7] Since the company wants to make movie recommendations to their user's by comparing the similarities of the profiles it directly addresses to this issue. For the company to allow it to proceed forward with the addition of this feature they need to clearly state their **intentions** of the new feature and they need to have the individual's **explicit consent** [8] .

Q5.

The GDPR contains the 'Right to Erasure' where each individual can ask for their personal data to be erased whilst still abiding to some restrictions [9] . It was believed that erasure meant the complete deletion of data but as it turns out with the process of data anonymization it is enough to deem that the data was 'erased' [10] given that in no way can the data be used to re-construct the identity of the user.

The issue is that the company wants to remove all personal data from the user trying to make their profiles 'Anonymous', but their ratings and review comments will still be present which are enough information to re-identify falling in the category of pseudonymization.

Although the company requests for consent to use their 'Anonymous' data it is just not true since their data are only Pseudonymous. This means that simply removing the personal data of the users but still keeping the ratings and reviews is not sufficient in following the GDPR rules.

Q6.

Allowing users to modify a generic avatar is a reasonable approach but, the issue is the automated construction of the initial face using provided information. It violates the principle of **Integrity and Confidentiality** as using the information they have provided can potentially be used to identify an individual. “GDPR only concerns with the processing of personal data that relates to a natural person that allows identification of an individual directly or indirectly via that information.” [10] . This avatar will be a direct link with the user which is a significant concern according to the GDPR.

Q7.

An approach to overcome this profiling issue is with the use of pre-defined collection of images [11] but with the addition of a unique system generated avatars. Instead of choosing a completely random image the user may choose something that relates better to them. This can be in the form of their favourite movie, show or genre. The avatar generator can then provide the user with a more personalized avatar but at the same time be general enough that it can never be used to re-identify them with just using the avatar as the piece of personal information, thus it correctly follows the rules of the GDPR.

References:

[1] Nibusinessinfo.co.uk. 2020. Data Protection Principles Under the GDPR | Nibusinessinfo.Co.Uk. [online] Available at: https://www.nibusinessinfo.co.uk/content/data-protection-principles-under-gdpr [Accessed 27 December 2020].

[2] The Central Role of Organisational Accountability in Data Protection. Informationpolicycentre.com. 2020. [online] Available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf [Accessed 27 December 2020] (pp. 7-8).

[3] En.wikipedia.org. 2020. Data Protection Act 2018. [online] Available at: https://en.wikipedia.org/wiki/Data_Protection_Act_2018 [Accessed 29 December 2020].

[4] Ico.org.uk. 2020. *Right To Erasure*. [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-erasure/#ib1 [Accessed 29 December 2020].

[5] Iapp.org. 2020. *How To Comply With The Right To Erasure (If You Haven't Already!)*. [online] Available at: https://iapp.org/news/a/how-to-comply-with-the-right-to-erasure-if-you-havent-already/ [Accessed 29 December 2020].

[6] Ico.org.uk. 2020. *Exemptions*. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ib2 [Accessed 29 December 2020].

[7] Ico.org.uk. 2020. Rights Related To Automated Decision Making Including Profiling. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/#ib3 [Accessed 28 December 2020].

[8] Ico.org.uk. 2020. Rights Related To Automated Decision Making Including Profiling. [online] Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/#ib4 [Accessed 28 December 2020].

[9] Ico.org.uk. 2020. Right To Erasure. [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-erasure/#ib2 [Accessed 28 December 2020].

[10] Data Privacy Manager. 2020. Pseudonymization According To The GDPR [Definitions And Examples] – Data Privacy Manager. [online] Available at: https://dataprivacymanager.net/pseudonymization-according-to-the-gdpr/ [Accessed 28 December 2020].

[11] Judin, J., 2020. Avatars, Identicons, And Hash Visualization. [online] Jussi Judin's weblog. Available at: https://barro.github.io/2018/02/avatars-identicons-and-hash-visualization/ [Accessed 28 December 2020].