CM50266 CASE STUDY I – UK GDPR

Q1.

Excluding accountability, there are six principles which underpin the GDPR, labelled in article five of the act as **A**, **B**, **C**, **D**, **E**, and **F**[1]. They are as follows.

A – This principle requires any processing of personal data to be lawful, fair and transparent. This means that data subjects- individuals whose personal data is to be acquired, have a right to know what it is intended to be used for. Critically, data controllers should inform them of this information in a manner which can be easily comprehended.
B – This principle mandates that reasons and purposes for the collation and processing of personal data be specified, explicit and legitimate. The data controller should also be clear in its plans for how long the data is to be held for.
C –This principle maintains the requirement that no data be obtained beyond what is necessarily in fulfilling the original stated purpose of its processing by the data controller. This is known as 'data minimisation'[2]
D – This principle stipulates that data controllers fulfil a role in the maintenance of their data's accuracy. In this respect, where data is found to be inaccurate or incomplete, it must be rectified by the data controller, and when requested by the respective data subject, rectification must be performed within approximately one calendar month[3].
E – This principle ensures that data is not kept in perpetuity; it must only be kept for as long as is necessary to fulfil its originally stated purpose.
F – This principle requires that measures be taken by the data controller to maintain the security of the data they store. This might entail protecting data from potential hazards such as unauthorised access or accidental loss[4]. Measures they could take range from encryption to pseudonymisation.

Q2.

Regardless of an organisation's location, if it runs a website which obtains data on any British subject, they must comply with the rules set out in the UK GDPR.

Since ACME intend on acquiring personal information such as names and email-addresses on British users of their website, though based in the United States, ACME must abide by British data protection law. In spite of this, ACME is therefore obligated to notify users on its website that it will be using cookies.

---

[1] UK GDPR updated for Brexit, 2021
[2] Ibid (1)
[3] Guide to the UK General Data Protection Regulation (UK GDPR), 2018
[4] Principles, Guide to the UK General Data Protection Regulation (UK GDPR), 2018

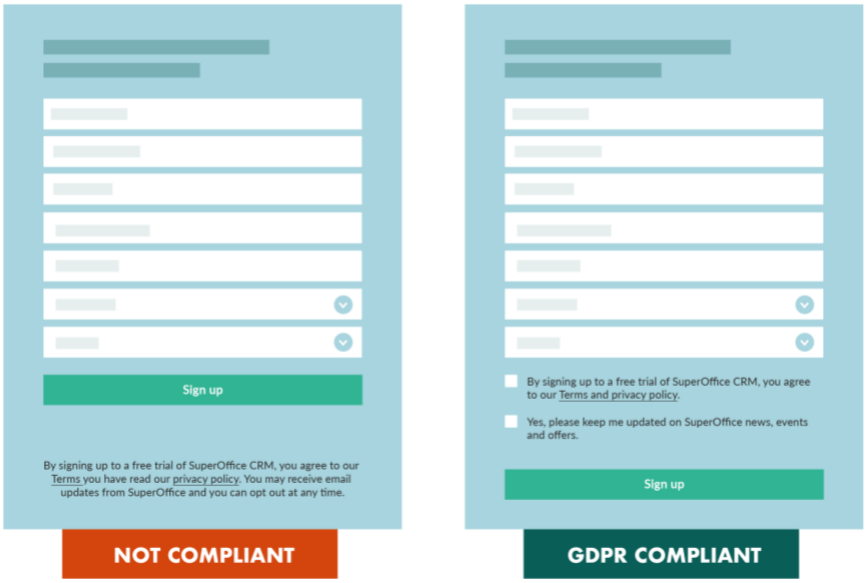

Figure 1: Comparison of cookie banner valid on separate sides of the Atlantic.

Further to this, it must also provide them with the option to opt out from giving their consent. This often comes in the form of a cookie alert consent banner, as can be seen in Figure.1[5].

Q3.

The accountability principle of the GDPR maintains that not only must ACME abide by the aforementioned six, but they must ensure, verify, and be able to demonstrate compliance with them.

The first feature integrates a new technology in the form of a recommender system. The second enables users to upload a profile image, which constitutes as biometric data- a form of personal data as stated by the act[6]. According to the ICO, initial action that should be taken when a new technology is used and when processing a new form of personal data is to conduct a data protection impact assessment (DPIA)[7]. Addressing the first feature, it will examine questions such as which types of data the recommender will use, how it will be used, how it will be stored, who has access to it, and how it will be protected. Similarly, for the second feature, the DPIA will address matters such as age checks on image uploads, where they will be stored, extending and updating existing privacy and data protection notices, processes for dealing with user requests for erasure and portability, and what to do in the event of a data breach.

[5] Lund, 2021
[6] Pg121
[7] Data protection impact assessments, 2018

A second action would be to ensure compliance by carrying out outcomes and processes formed in the DIPA. This means raising awareness within the company, training relevant members of staff, conduct audits of the data's management and recording everything in the process[8].

Q4.

In the brief, ACME suggest that they will use 'a similar profile of existing car ratings' when attempting to make recommendations to its users. There would be a clear issue if it were to incorporate user's sensitive data within the system to build such a profile. This is because it would be a definitive instance of profiling, the consequences of which may find ACME in direct breach of the GDPR. This can be prevented through pseudonymisation of user's data[9]- a process in which the data is restructured so that anything sensitive is stored separately from the rest, and only connected together through the use of a key. Alternatively, ACME could consider an item-to-item based collaborative filtering method instead, which would only explore the relationship between cars, not users, e.g., 'if you liked the Car X, you may also like Car X Sport', or 'trending items'[10].

Q5.

Under Article 17, data subjects have a right to request that their personal data be erased[11]. However, by definition, if data can no longer be 'related to an identified or identifiable living individual'- anonymised, then it is no longer personal and therefore not covered by the GDPR. Ambiguously though, no lucid definitions are provided within the act that state the exact meaning of anonymisation, or perhaps more frustratingly, erasure[12]. To seek clarity, one may look to Austria, where in late 2018 a comparable case over the right to erasure between a data subject and controller was tested in court. Here, the data subject contested that though the controller had deleted their personal information, they had breached the act for choosing to keep other held data, claiming it to be anonymised. However, because the controller had ascribed this other data to a randomly generated person, it was ruled that they had acted in compliance with the act. This is an example of a 'dummy customer connection'[13]. If we take the outcome of this case and consider further that ACME will seek consent for this continued processing of data, one could be fairly certain of its sufficiency to stay within the law.

[8] le Cat, n.d.
[9] Vas, 2021
[10] Item-to-Item Based Collaborative Filtering - GeeksforGeeks, 2020
[11] Right to erasure, 2018
[12] Marko and Riepan, 2019
[13] Ibid (11)

Q6.

Compliancy with the GDPR may fail should the system be complicit in profiling. This is largely dependent on what type of 'additional information previously provided by the user' ACME decides to incorporate. If any form of personal data is used, such as gender or age, then one could certainly consider it profiling. The Article 29 Working Party have suggested that automated processes like this could perpetuate existing stereotypes and social segregation[14].

Q7.

One solution would be to build the system so that it generates avatars completely randomly, where none of user's personal details are incorporated. Users could then still have the ability to adapt the avatar in the initial intended way e.g., changing hair/eye colour. It would then need to pseudonymise the images or use a third-party system to encrypt them. It could even use a third party to generate the actual avatars, by using for example, Jdenticon, who makes avatars as a visual representation of a hash value. This would enable users' privacy to remain intact[15].

Bibliography on the next page…

[14] Matheson, 2017
[15] Jdenticon - Open source identicon generator, n.d.

Bibliography:

- UK GDPR updated for Brexit, 2021. *Chapter 2 – Article 5*. [online] GDPR Advisor. Available at: <https://uk-gdpr.org/chapter-2-article-5/ > [Accessed January 2021].

- Ico.org.uk. 2018. *Guide to the UK General Data Protection Regulation (UK GDPR)*. [online] Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/> [Accessed January 2022].

- Ico.org.uk. 2018. *Guide to the UK General Data Protection Regulation (UK GDPR)*. [online] Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/> [Accessed January 2022].

- Marko, R. and Riepan, I., 2019. *Austrian GDPR-Tracker: Data Protection Authority On Erasure By Way Of Anonymization - Privacy - Austria*. [online] Mondaq.com. Available at: <https://www.mondaq.com/austria/data-protection/780272/austrian-gdpr-tracker-data-protection-authority-on-erasure-by-way-of-anonymization> [Accessed January 2022].

- Ico.org.uk. 2018. *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/> [Accessed January 2022].

- Vas, G., 2021. *How Recommendation Systems Comply with Privacy Regulations-Yusp*. [online] Yusp. Available at: <https://www.yusp.com/blog-posts/recommendation-systems-comply-with-privacy-regulations/> [Accessed January 2022].

- GeeksforGeeks. 2020. *Item-to-Item Based Collaborative Filtering - GeeksforGeeks*. [online] Available at: <https://www.geeksforgeeks.org/item-to-item-based-collaborative-filtering/> [Accessed January 2022].

- Lund, J., 2021. *GDPR: What is It and How Does it Impact My Business?*. [online] Superoffice.com. Available at: <https://www.superoffice.com/blog/gdpr/> [Accessed January 2022].

- Matheson, L., 2017. *WP29 releases guidelines on profiling under the GDPR*. [online] Iapp.org. Available at: <https://iapp.org/news/a/wp29-releases-guidelines-on-profiling-under-the-gdpr/> [Accessed January 2022].

- Ico.org.uk. 2018. *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 January 2022].

- Jdenticon.com. n.d. *Jdenticon - Open source identicon generator*. [online] Available at: <https://jdenticon.com/> [Accessed January 2022].
- le Cat, S., n.d. *GDPR-Accountability principle | Deloitte Switzerland*. [online] Deloitte Switzerland. Available at: <https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-accountability-principle.html> [Accessed January 2022].

Fig.1:

Lund, J., 2021. *GDPR: What is It and How Does it Impact My Business?*. [online] Superoffice.com. Available at: <https://www.superoffice.com/blog/gdpr/> [Accessed January 2022].