CTEC1905 – Law Component Essay

Question 3

CRITICALLY DISCUSS THE DATA PROTECTION ACT 2018; WHAT IS ITS ORIGIN AND HOW EFFECTIVE IS IT? YOUR ANSWER SHOULD INCLUDE POSSIBLE SUGGESTIONS FOR IMPROVING THE EFFECTIVENESS OF THE ACT.

1 Introduction

The mishandling of data has always been a prevalent issue in the world's rapidly evolving, technological climate and it was not until the Council of Europe released **Convention 108**[1] in 1981, that there was a "binding international instrument … [governing] the collection and processing of personal data" *(Council of Europe, 2019)*. The UK, bound by *Chapter II, Article 4* of Convention 108, was required to enact **The Data Protection Act 1984** (DPA 1984) which applied the European legislation domestic law within the UK. Now 38 years on, there have been two successors to the DPA 1984, the **Data Protection Act 1998** (DPA 1998) and the **Data Protection Act 2018** (DPA 2018). The latter of these will be further discussed in this paper, its impact and efficacy will be examined, leading to suggestions being made for potential adjustments to the act.

[1] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

2 Background

Convention 108 was exceptionally forward thinking for the time, considering that Sir Tim Berners-Lee would not invent the worldwide web for another eight years *(McPherson, 2009)*. Global internet traffic has been growing exponentially and was reported by The World Bank *(2021)* to be 3 zettabytes (1×10^{21} bytes), which is an unfathomably vast amount. Not only does this 'Big Data'[2] come in vast quantities, but the speed at which it is created and processed, along with the variety of data collected, is what give companies the advantage over their competitors *(McAfee and Brynjolfsson, 2012)*.

In 2012, the European Commission started a four-year process *(Burn-Murdoch, 2013)* to update the **1995 Data Protection Directive** (1995 DPD), which was the authoritative document for data protection in Europe at the time, and on 14 April 2016, it was superseded the **General Data Protection Regulation 2016** (GDPR 2016). As a member of the EU at the time, the UK needed to amend its own regulations governing data processing to keep up to date with EU law, and the new DPA 2018 sought to improve upon the existing DPA 1998. While the DPA 2018 originally employed EU GDPR to define its framework, as consequence to the UK's withdrawal from the EU, the UK merged GDPR 2016 into domestic law as **UK GDPR** and amended the DPA 2018 as per UK Statutory Instrument No. 419[3] *(2019)*.

2.1 Principles

In *Chapter II, Article 5* of the UK GDPR, the six principles relating to data collection, processing, and storage are defined. It states that all personal data should be:

- "processed lawfully, fairly and in a transparent manner"
- "collected for specified, explicit and legitimate purposes"
- "adequate, relevant and limited to what is necessary"
- "accurate and, where necessary, kept up to date"
- "kept in a form which permits identification … for no longer than is necessary"
- "processed in a manner that ensures appropriate security of the personal data"

These principles lay the foundation of how the law views data protection and the framework by which to prosecute. In addition, *Article 6* provides information on 'special categories of personal data', prohibiting the processing of sensitive data including, but not limited to a person's race, religion, genetic data, or sexual orientation.

2.2 Data Subject Rights

Chapter III of the UK GDPR details the rights of those whose data is collected, further explained by the Information Commissioners Office (ICO) in their 'Guide to the General Data Protection Regulation' *(2019)*. The seven key rights[4] described are as follows:

- The **right to be informed** ensures that people are aware that their information is being collected and promotes transparency, explicitly outlined in the first principle.
- The **right of access** ensures that people have free[5] access to their personal data that has been collected via Subject Access Requests (SARs).

[2] Massive data sets, complex beyond the capabilities of standard software *(Snijders, Matzat, and Reips, 2012)*.
[3] The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019
[4] Further rights around automated data processing are outlined in *Article 22* of the UK GDPR including requirements for controllers to gain explicit consent before programmatically evaluating a subject's data.
[5] For most requests, this service must be free of charge unless multiple copies are requested, or requests become "unfounded or excessive" *(UK GDPR, 2016, Article 12(5)),* the controller can then refuse or charge for fulfilment.

- The **right to rectification** ensures that people can rectify any inaccurate information discovered in the result of a SAR.
- The **right to erasure** ensures that people can, in certain cases, request that their data be erased permanently.
- The **right to restrict processing** ensures that people can, in certain cases, request that their data is restricted from being processed.
- The **right to data portability** ensures that people can reuse their personal data across services and commonly used data formats are employed for open data.
- The **right to object** ensures that people can, in certain cases, stop processing of their data and, in all cases, allow direct marketing to be denied use of that data.

The outlining of the rights of the data subject is instrumental in protecting people against the misuse of their data; any violation of those rights, or deviation from the data protection principles, will enable the Commissioner to enforce regulation and levy fines as below.

2.3 Enforcement

In *Part 6* of the DPA 2018, the rules regarding enforcement of the UK GDPR are outlined giving instruction regarding the Commissioner's handling of legislation infringements. There are four types of notice that the Commissioner has available to promote secure data use:

- **Information notices** require responsible persons to yield information that the Commissioner may use to conduct their role or investigate potential data misuse.
- **Assessment notices** require responsible persons to allow the Commissioner to evaluate whether data protection legislation has been, and currently is being, consistently upheld. Giving the Commissioner access to premises and equipment, accessible information, and permission to observe the processing of personal data.
- **Enforcement notices** require controllers and processors to rectify any contraventions of legislation discovered by the Commissioner, such as failure to comply with the data protection principles or violating data subject rights. This can extend to prohibiting a person from processing in a specified manner or entirely.
- **Penalty notices** require persons or 'undertakings'[6] to pay the Commissioner a fine, either alongside and enforcement notice[7], or upon failure to comply with one of the previously mentioned notices. The 'higher maximum amount' that can be imposed is outlined in *Section 157* as the higher of £17,500,000 or in the case of an undertaking 4% of the undertaking's turnover in the prior fiscal year.

The above notices, alongside the principles of data protection, and rights of the data subject make up the core of how the DPA 2018 aims to prevent data mishandling and, from here, the success of these aims will be drawn into question, establishing how the statute has affected the UK and notable cases where the regulations have had to be enforced.

[6] "A body corporate or partnership, or … an unincorporated association carrying on a trade or business, with or without a view to profit." *(Companies Act 2006, Part 38 Section 1161)*

[7] In *Part 6* of the DPA 2018, *subsection 1* of *Section 159* (Penalty notices), refers to failures detailed in *Section 149* (Enforcement notices), so they are often served together.

3 Discussion

In terms of the success of the DPA 2018, and how much of a positive impact it has had on data protection within the UK, there must be an evaluation made concerning the preventative nature of the existing regulations, as well as the proportionality of the penalty given to the offender. The quote "Men are not hang'd [*sic*] for stealing Horses, but that Horses may not be stolen" *(Savile 1750, p. 114)*, when applied to the realm of data protection, provokes the question: does the legislation itself prevent data misuse or do solely the convictions of others encourage conformity?

Consider the following three cases involving large data breaches in the UK:

3.1 TalkTalk Telecom Group PLC, 2015

The ICO received a report of a data leak from TalkTalk on 22 October 2015, which resulted in the largest ever fine at the time of £400,000, due to neglection towards prevention of the unlawful use of personal data *(ICO, 2016)*. The BBC *(2016)* reported 156,959 affected customers with 15,656 of them having their bank account number and sort code stolen. Given that this breach was due to a SQL injection attack *(ICO, 2016)*, an extensively recognised type of cyber-attack, it can be assumed a tort of negligence. This implies that the DPA 1998, serving as the basis for their admonishment, was less than preventative of malpractice regarding personal data. TalkTalk *(2014, p. 3)* reported their revenue to be £1,727m, which puts the fine at a surface-scratching 0.02%, further demonstrating the lack of firm dissuasion afforded by the legislation. Upon its repeal, the maximum penalties outlined in the DPA 1998 were increased drastically by the DPA 2018, but the question still stands: will higher fines and new legislation prevent future infringements, or will it take cases of higher fines to ensure secure data handling? This being the first of three examples indicates toward the contrary.

3.2 British Airways PLC, 2020

After a cyber-attack resulting in unauthorized access of over 420,000 customer and employee records including the payment details of 244,000 customers, British Airways (BA) were fined a substantial £20m, the highest penalty to date *(ICO, 2020a)*. This fine was initially £183m but considering the effects of COVID-19, it was reduced *(The Guardian, 2020)*. While the original fine seems far more severe than the TalkTalk breach, and even the enforced £20m penalty, it remains a trivial 1.4% of the £13,290m of revenue that BA *(2019 p.6)* reported the year earlier, and the data compromised was far more extensive than the TalkTalk breach. Although the DPA 2018 declares that the maximum fine can be up to 4% of a company's turnover, as previously stated, that seems a small amount when the personal data of customers are being openly exposed.

3.3 Marriott International Inc., 2020

With an estimated impact of 339 million guest records being unlawfully processed, Marriott became subject of a £18.4m failure to put effective measures into place to protect the personal data that it was processing *(ICO, 2020b)*. Being only 0.09% of their annual revenue *(Marriott, 2019 p. 24)* it is dubious as to whether the effort required to maintain such unwieldy data sets is worth the investment if the cost is negligible in comparison. Furthermore, the only tangible impact there seems to be is the societal repudiation that comes from having a data breach tied to the company's name which no doubt is looked upon poorly by stake holders.

The Department for Digital, Culture, Media & Sport *(2018)*, on the impact of increased fines, stated that the DPA 2018 grants an array of remedial measures which aim to ensure that fines are a fallback

if corrective action is not made. Given that the main goal of the DPA 2018 is preventing malpractice regarding data protection, there still seems to be refinements needed in enforcing how personal data should be processed.

While *Article 83* of the UK GDPR outlines the relevant considerations made when determining the penalty amount, the legislation could improve the proportionality of the response by, for example, extending it to be based on the duration between incidents and disclosure and the number of records affected by the breach. Unless the amount of the fine is high enough to wound a business, where it would be righteous to do so on account of an infraction of the law, there will be no incentive to refrain from neglecting any issues with data processing. A better deterrent would be limiting the ability of an offender to process data for a period proportional to the severity of their infringement which is touched upon in *Part 6*, *Section 150*, *subsection 3* of the DPA 2018.

The ICO could commission the release of data collection protocols used in a company's infrastructure that enable them to gather personal data in a homogenous fashion. In 2017 the nine largest banks in the UK were ordered by the Competition and Markets Authority to create application programming interfaces that follow direct specifications ensuring consistent communication between banks *(OBIE, 2021; CMA 2021)*, similarly, companies could be given technical specifications on how to collect data securely and the protocol could go as far as to require collectors of data to relay metadata about data processing actions to the ICO for automated monitoring.

4 Conclusion

In summary, the DPA 2018 is a marked improvement on the DPA 1998; increased fines will always pose a threat to negligent or malicious wrong doers and the social implications of causing distress and harm to millions of people are not to be understated. There will be another DPA in the years to come that will have further developments but for now, with an increase in penalty, the DPA 2018 ensures controllers and processors to act in a responsible and respectful nature when working with the personal information of others.

5 References

1. Council of Europe (2019) Details of Treaty 108. Available at: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108 (Accessed: 26 April 2022)
2. Council of Europe *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981, CETS 108. Available at: https://rm.coe.int/1680078b37 (Accessed: 28 April 2022)
3. McPherson, Stephanie Sammartino (2009). *Tim Berners-Lee: Inventor of the World Wide Web*. Minneapolis: Twenty-First Century Books
4. The World Bank (2021) Crossing Borders. Available at: https://wdr2021.worldbank.org/stories/crossing-borders (Accessed: 27 April 2022)
5. McAfee, A and Brynjolfsson E. (2012) 'Big Data: The Management Revolution', *Harvard Business Review,* 90(10), pp. 60-68
6. Burn-Murdoch, J. (2013) 'Europe deadlocked over data protection reform', *The Guardian*, 12 August. Available at: https://www.theguardian.com/news/datablog/2013/aug/12/europe-data-protection-directive-eu (Accessed: 28 April 2022)
7. *The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019* (SI 2019/419) Available at: https://www.legislation.gov.uk/uksi/2019/419/contents (Accessed: 28 April 2022)
8. '*Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*' (2016) *Official Journal* L119 Available at: https://www.legislation.gov.uk/eur/2016/679/contents (Accessed: 28 April 2022)
9. ICO (2019) *Individual Rights* Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/ (Accessed: 27 April 2022)
10. Snijders C., Matzat U., and Reips U. (2012) '"Big Data": Big Gaps of Knowledge in the Field of Internet Science', *International Journal of Internet Science*, 7(1), pp. 1-5
11. Data Protection Act 2018 c. 12 Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents (Accessed: 27 April 2022)
12. Companies Act 2006 c. 46 Available at: https://www.legislation.gov.uk/ukpga/2006/46/section/1161 (Accessed: 27 April 2022)
13. Savile G. (1750) A Character of King Charles the Second and Political, Moral and Miscellaneous Thoughts and Reflections. London: J. and R. Tonson
14. ICO (2016) 'TalkTalk cyber attack – how the ICO's investigation unfolded' 2 November. Available at: https://ico.org.uk/about-the-ico/news-and-events/talktalk-cyber-attack-how-the-ico-investigation-unfolded (Accessed: 28 April 2022)
15. BBC (2020) 'TalkTalk hack 'affected 157,000 customers'', *BBC News*, 6 November. Available at: https://www.bbc.co.uk/news/business-34743185 (Accessed: 28 April 2022)
16. TalkTalk Telecom Group PLC (2014) Annual Report 2014. Available at: https://www.talktalkgroup.com/dam/jcr:9cdfcf7c-e7d9-4fb3-994d-2b9deade9cc0/4%20TalkTalk%20Annual%20Report%202014.pdf (Accessed: 29 April 2022)
17. ICO (2020a) 'ICO fines British Airways £20m for data breach affecting more than 400,000 customers' 16 October. Available at: https://aico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers (Accessed: 27 April 2022)

18. Topham G. (2020) 'BA fined record £20m for customer data breach', *The Guardian*, 16 October. Available at: https://www.theguardian.com/business/2020/oct/16/ba-fined-record-20m-for-customer-data-breach (Accessed: 28 April 2022)
19. British Airways PLC (2019) Annual Report and Accounts 2019. Available at: https://www.iair-group.com/~/media/Files/I/IAG/documents/British%20Airways%20Plc%20Annual%20Report%20and%20Accounts%202019.pdf (Accessed: 29 April 2022)
20. ICO (2020b) 'ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure' 30 October. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure (Accessed: 27 April 2022)
21. Marriott International Ltd. (2019) 2019 Annual Report. Available at: https://marriott.gcs-web.com/static-files/178683c9-c9d9-47b0-b115-726588f43130#:~:text=In%202019%2C%20gross%20fee%20revenue,strong%20existing%20premium%20to%20competitors (Accessed: 29 April 2022)
22. DCMS (2018) *Data Protection Act 2018 Factsheet – The Information Commissioner and Enforcement (Sections 114-181)* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711238/2018-05-23_Factsheet_5_-_Information_Commissioner.pdf (Accessed: 29 April 2022)
23. Open Banking Implementation Entity (2021) Regulatory. Available at: https://www.openbanking.org.uk/regulatory (Accessed: 29 April 2022)
24. Competition & Markets Authority (2021) Update on Open Banking. 5 November Available at: https://www.gov.uk/government/publications/update-governance-of-open-banking/update-on-open-banking (Accessed: 29 April 2022)