Critical Analysis of the Data Protection Act (DPA) 2018

Introduction

Currently an amended version of the Data Protection Act 2018 (DPA 2018) works alongside the UK General Data Protection Regulation (UK GDPR), found in UK domestic law. It focuses on granting individuals' rights over any of their personal information collected by companies. Such as, the right to erase, rectify and restrict processing / portability of the data.

Origin

The Access to Personal Files 1987 (APF 1987) and the Data protection Act 1984 (DPA 1984) together provided access for individuals to information relating to themselves maintained by certain authorities, as well as basic rules of registration for users of data. However, both were revised and superseded by the DPA 1998. 20 years later that act was replaced with the DPA 2018, due to multiple reasons.

One major reason was the DPA 1998 worked in tandem with the 1995 European Unions Data Protective Directive (1995 EU DPD). However, this was replaced by the GDPR in 2018. So, the DPA 1998 needed to be updated to continue cooperating with its new EU counterpart.

Another reason was an increase of major data breaches in the 21st century. All data breaches that follow are from **1. (Data Breaches, no date)** the underlined sentences are quoted from reference **1.** Examples are as follows:

- Wonga, (June 2018) 270,000 lives affected. Described as "one of the biggest" breaches of financial information in the UK, information stolen from the controversial lender included account numbers, sort codes and the last four digits of customers' card numbers.

- British Airways, (September 2018) 500,000 lives affected. Criminal hackers injected malicious code into British Airways' website, diverting traffic to a fraudulent replica site. Customers were then handing their information to fraudsters including login details, payment card information, address and travel booking information.

- Dixons Carphone, (July 2017) 10.2 million lives affected. Shares in Dixons Carphone plummeted by as much as 6% after approximately 10 million records containing personal data were compromised in what was described as the "biggest online data breach in UK history".

All of these non – trivial data breaches show security and law must be radically updated.

That is what pushed for the DPA 2018 to replace the DPA 1998. The increase of data breaches also shows the exponential advancement of technology as well as the internet as a platform increasing in number of users by the millions in a very short amount of time. The Government failed to keep up.

Due to the UK deciding to leave the EU in 2016, It was decided the GDPR would be retained in domestic law as UK GDPR in the EU (Withdrawal) Act 2018, sitting alongside an amended (1st January 2021) version of the DPA 2018. And as this essay is written, that is the current state of law.

KEY AIMS OF the DPA 2018

Main aims are as follows:

- increase the control individuals have over all of their personal data that is collected, processed and stored by any business.
- Make all businesses accountable /responsible for all sensitive information they hold

Together the DPA 2018 and the UK GDPR attempt to achieve this. There are key principles the Act and Regulation follow: from **2. (Data Protection Act 2018 Summary, 2014)** Are as follows (the underlined parts are quoted from **2.** Reference):

- Fair, lawful and transparent processing

All individuals must be aware of any processing the business performs. As well as following the law if any data is transferred to third parties. For example, stated in **3. (International transfers after the UK exit from the EU Implementation Period, 2021)** "… the UK GDPR restricts transfers of personal data to a separate organisation located outside of the UK…". So, if a UK based organisation wants to transfer data to an organisation that is located outside UK jurisdiction, they are denied to do such action, **3. "…** unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies**."** Meaning the receiving country must have their own data protection laws the UK deems adequate. All countries / territories that are covered by **3.**" adequacy regulations " have met the requirements the UK demand.

- Purpose limitation

If data is collected, the reason must be declared clearly beforehand and cannot alter during the process. **4. (Glossary Purpose limitation, 2022)** "personal data be collected for specified, explicit, and legitimate purposes". The process can only go as far as to reach the goal of the organisation and must be compatible with said purposes.

- Data minimisation

This limits that only data that is required to achieve the goal of the organisation to be processed / collected. **5. (Liz Burton-Hughes, 2018) "**Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". This is to minimise risk and damage to the individual if a successful data breach occurs within the organisation.

- Accuracy

Data that is processed / collected must be up to date and correct regarding to the individual it presumes to detail. This is so individuals can be correctly represented in the organisation and located / contacted if necessary. It is good practice to conduct effective procedures to check the accuracy of data **6. (Ico 2021)**.

- Data retention periods

This principle focuses on limited time periods of how long the organisation can store personal information of an individual. The duration of storing the data must be only for as long as required to complete the organisations' goal. The duration must be made clear and precise to the individual the sensitive data represents. **7. (James Hutchinson, 2018)** "However, akin to the principle under the 1998 Act, if you anonymise the data, you can keep it for as long as you like.". Rules such as this benefit both parties, it protects the individual in case of a successful data breach. And the organisation can use this information for surveys and statistical analysis of its clients. Showing the DPA 2018, when possible, tries to find a reasonable middle ground to protect the individual and still allow the company to benefit.

- Data security

If the organisation wants to store / process sensitive information they must **8. (Pinsent Masons, 2005) "**put in place adequate technical and organisational measure to safeguard personal data…**"** Many of the principles stand to limit the damage if a data breach occurs, however this one focuses on avoiding one altogether. Now this has been put in place, companies can take responsibility of damage to individuals if substantial measures were not met. This principle also holds organisations responsible for any third parties they transfer data to, to comply with sufficient data security.

- Accountability

This is the sort of guilt clause of the GDPR. Organisations must prove they have sufficient protective measures. This can also include providing privacy policies and records of their processing activities.

Examples of Offences Addressed by the Act

So, using the principles just mentioned, offences have been recognised and detailed in the DPA 2018. Offences are a breach of law; an illegal act. Many of the criminal offences build on or update parts of the DPA 1998. There are also different types of offences. There were suggestions that some offences under the DPA may have the consequence of imprisonment, however **9. (Kingsley Napley, 2018) "**the act preservers the status quo ante of financial penalties only.**"**. However, they can impose an unlimited fine, and no current guidance as to how severe the fine should be, apart from the accused ability to pay. The Information Commissioner's Office (ICO) are responsible of imposing the fines.

All underlined statements are quoted from **9.**

Access and Disclosure Offences

- Section 170 (builds upon the s.55 DPA 1998) describes the offence of illegally obtaining personal data. More specifically without the consent of the data controller. This can be knowingly or recklessly. An example was at the Heart of England NHS foundation trust. **10.(Roger Sahota, no date) "**…employee pleaded guilty to unlawfully accessing personal records for 14 individuals and was sentenced to a fine of £1000**"**
- Section 184 (builds on s.56 DPA 1998) This is an act that focuses on anti-discrimination. It makes it illegal for organisations to request a record to health, conviction or cautions, or statuary functions when it comes to deciding to employ the individual or providing services.

Investigation Offences

- Section 144 (replicates s.47 (2) DPA 1998) criminalises providing incorrect statements responding to an ICO information notice.

New offences

- Section 171 re-identifying personal data that has been redacted to conceal personal data. Ceases organisations to potentially cheat the data retention periods, while deleting data at their legal expiry date, then rebuild the data and store unnecessary personal data then breaking the data minimisation and purpose limitation principle.

- Section 173 – It is illegal to conceal / alter information that should have been provided in response to a data subject access requestion.

There have been several major fines dished out in the 21st century.

One was to a pharmacy in London, who left 500,000 documents or sensitive information in unlocked containers, who was fined £275,000 and 3 months to increase data protection procedures **11. (Hutsix, no data)**.

Another was Facebook itself. In 2015 Facebook was fined the maximum possible fine at that time (£500,000). However, if it was fined after the GDPR was introduced, it could have been 4% of Facebooks revenue in 2018 (£1.7 billion) **11.**

Possible Improvements

One weak spot I noticed when researching how the severity of fines are decided was there is no general premise to follow. Only a very vague foundation on taking into account the chance of the accused ability to pay the fine. Even then this does not have to be followed. No rule of law states any guidelines must be observed. This is a worry to say the least. This could lead to two separate organisations or individuals committing the identical crimes at identical magnitude and having different consequences. Potential unethical and discriminatory accusations could be pointed to the legal system. But also, from a legal perspective, vague and unclear laws are disliked in the courts by the very lawyers, attorneys and judges. Since it opens the law to interpretations, personal opinion and, inevitably, disagreements on the very foundation of what the law actually states. If we expect people to follow and obey the laws of this country, our courts must remain consistent to be taken seriously.

The solution is a more precise guidebook should be created. Since the variables can alter with each different offence, the guidebook must directly take into account of details of each individual case. Such as

- Number of people who were affected, there is a major difference between 12 people (like the NHS employer **10.**) and millions of people (like Dixons Carphone **1.**) The higher the number of affected people, the increased severity of the punishment.
- Does the organisation / individual have past charges of failing to implement adequate protection for people's sensitive info? Depending on the past charges, perhaps the fine should increase in amount if the accused has a history. However, if this is the first time of a data breach, the punishment should be reduced. this will need to depend heavily on other factors.
- Is the accused an organisation or an individual? Or perhaps a better metric is the size of the workforce you are accusing. A recognised difference between a sole trader and a major company like Facebook. Perhaps big companies should be held to a higher standard, due to increase funds, increased workforce so the fine should consider the structure of the accused.
- Lastly, the severity of the data that was leaked. For example, sexual orientation, though still personal, is not as severe when leaked compared to your bank details or home address.

Another potential improvement is extending section 184. Section 184 (that I have mentioned previously) is a DPA 2018 Access and Disclosure Offence. It focuses on criminalising unfair discrimination. I agree what personal data it already covers, which is health, conviction or cautions, or statuary functions. I believe more categories of personal info should be added. Such as: Gender, sexual orientation, nationality, race (skin colour), religion, political views, age. However, I am in favour of exceptions in special circumstances, such as if you are employing for a political campaign, you would want employees to have similar political views. Or if the work you are offering is highly physically taxing, age and health will be essential to know for the individuals personal safety.

Conclusion

In conclusion, the DPA 2018 covers majority / most significant of the digital landscape with minor weaknesses and small possibility of exploits. The Act successfully gives more power to the individual over their own personal data, while still allowing organisations to operate in fair amount of freedom.

REFERENCES

1. It governance (No date) Data Breaches. Available at: https://www.itgovernance.co.uk/data-breaches?promo_name=megamenu-dataprivacy&promo_id=info-databreaches (accessed 27 April 2022)
2. Liz Burton-Hughes (2014) Data Protection Act 2018 Summary. Available at: https://www.highspeedtraining.co.uk/hub/data-protection-act-summary/ (accessed 27 April 2022)
3. Ico (2021) International transfers after the UK exit from the EU Implementation Period (GDPR). Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/ (accessed 28 April 2022)
4. Thomas Reuters (2022) Glossary Purpose limitation. Available at: https://uk.practicallaw.thomsonreuters.com/Glossary/UKPracticalLaw/I1a11102e5ea511e89bf199c0ee06c731?transitionType=Default&contextData=(sc.Default)&firstPage=true (accessed 28 April 2022)

5. Liz Burton-Hughes (2018) Key Principles of the Data Protection Act 2018. Available at: https://www.highspeedtraining.co.uk/hub/data-protection-act-key-principles/ (accessed 28 April 2022)
6. Ico (2021) Principle (d): Accuracy. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/ (accessed 28 April 2022)
7. James Hutchinson (2018) Document Retention under the GDPR and the Data Protection Act 2018 December 2018. Available at: https://www.lexology.com/library/detail.aspx?g=c6d51a82-28a0-458b-94da-f7ef1b77c5cb (accessed 29 April 2022)
8. Pinsent Masons (2005) Data Protection. Available at: https://www.pinsentmasons.com/out-law/guides/data-protection (accessed 29 April 2022)
9. Kingsley Napley (2018) The Data Protection Act 2018: new criminal offences for data breaches. Available at: https://www.kingsleynapley.co.uk/insights/blogs/data-protection-blog/the-data-protection-act-2018-new-criminal-offences-for-data-breaches (accessed 29 April 2022)
10. Roger Sahota (No date) Data Protection Act 2018. Available at: https://www.bsblaw.co.uk/data-protection-act-2018-law-and-sentencing
11. Hutsix (No date) Data Protection Act Punishment. Principles, GDPR and Failure to Comply. Available at: https://www.hutsix.io/what-is-the-punishment-for-breaking-the-data-protection-act/