Understanding and Communicating Data Protection Act 2018

Author: Akpovona Agbaire

Institution: University of Derby

Submitted in partial fulfilment of the requirements for the MSc in Cyber Security

Contents

Abstract

Privacy and data protection policies inform users how their data is retrieved, saved, processed, and shared between organisations. However, due to the length and complexity of the words used by organisations in these policies, users often do not read or comprehend most of the words used to form these policies. Hence, there was a need to develop a law to protect how personal data is used by organisations operating in a region. In the United Kingdom, this law is known as the Data Protection Act 2018. This research explores the Data Protection Act 2018 under the Data Protection and Privacy Laws of the United Kingdom of Great Britain and Northern Ireland for a hypothetical company based in the United Kingdom called ABX Limited. As the new CISO of this company, stating the importance of this law and how it affects the organisation, and its employees will also be addressed. Finally, we developed an awareness-raising campaign through training to ensure compliance by all relevant employees, which was backed up with an experiment to determine the effectiveness of the training conducted.

Introduction

Data privacy and protection are a major issue in the world we live in today, with the continuous advancement in IT. Everything we do today can be done from the comfort of our home, from our search enquiries to more confidential data like our health or financial data. Keeping this data private and protected has become imperative to ensure this information is not accessed or altered by unauthorised users, as this could be costly. Unauthorised users may try to gain access to personal data for financial gain or just for the fun of it at the expense of the owner of the information. It was evident that a framework adapting to the current realities should be implemented to ensure the safety of data while collecting and processing the data by organisations, businesses, and governments. The Data Protection Act 2018 was passed into law by the United Kingdom government to help address the issue of data protection and privacy and help individuals make informed decisions on how their data is used and what their rights are.

The Data Protection Act 2018 came into effect on the 25th of May 2018 in the United Kingdom as the new and improved version of the Data Protection Act 1998 (ICO, 2019). The Data Protection Act 2018 sits alongside and supplements the UK GDPR. (ICO, 2021) And is the UK's implementation of the General Data Protection Regulation. It regulates how enterprises, organisations, or the government use personal data. (UK.GOV, 2020). The Data Protection Act of 2018 aims to give people more control over their data and provide organisations with legal means of processing that data. (ICO, 2019). Personal information can therefore be defined as any information which can be used to directly identify a person or indirectly identify when combined with other information. (ICO, 2019). Any organisation making use of personal information must follow strict rules called the Data Protection Principles. (UK.GOV, 2020). These organisations must make sure that any information collected and or processed must:

1. Used in a fair, lawful and transparent way (UK.GOV, 2020).
2. Used for a specific and explicit purpose (UK.GOV, 2020).
3. Used in a way that is adequate, relevant, and limited to only what is necessary (UK.GOV, 2020)
4. Be accurate and up to date where necessary (UK.GOV, 2020).
5. Kept no longer than necessary (UK.GOV, 2020).
6. Managed in a secure manner, and protection against unlawful access or alteration (UK.GOV, 2020).

There is a stronger law for more sensitive information, for example, sex orientation, race, etc. And a separate safeguard for information relating to criminal convictions and offences (UK.GOV, 2020).

As the new CISO of ABX Retail Shop, with branches all over the UK, it is crucial that we comply with the Data Protection Act 2018, not just because it is a regulatory requirement, but because it could also save ABX from financial and reputational loss. It is worth of note here that ABX has been complying with the Data Protection Act 1998 but needs to comply with the new Data Protection Act of 2018 to ensure we follow technological advancements that made the 1998 act deficient.

Background Knowledge

The Data Protection Act 2018 is one of the many rules and legislation that serve to safeguard user privacy and data protection. Data Protection Act is a legal document which states how a business, organisation, or government collects, saves, and processes individuals' information (ICO, 2019). The retrieved data may include personal identifiable information called personal data.

Data Protection Act 218 is the UK law that governs the processing of personal data (UK.GOV, 2020). It is the UK's implementation of the General Data Protection Regulation (GDPR) which came into effect on the 25th of May 2018 to reflect the UK's departure from the European Union (ICO, 2019). It replaces the decade-old Data Protection Act 1998 and introduces new provisions to address the current state of data protection (ICO, 2019). The Act applies to organisations that process personal data in the UK, including businesses, charities and even government agencies (ICO, 2019).

Some of the key features which would be discussed next includes the requirement for organisations to obtain explicit consent from individuals before processing any of their personal data (ICO, 2020). It also provides individual with different rights on how their personal data is processed (ICO, 2020). Some of which includes right to rectify inaccurate data and right for individuals to have their personal data deleted as known as right to be forgotten just to mention a few (ICO, 2020).

Information Commissioner's Office (ICO) is responsible for regulating and enforcing Data Protection Act 2018 (ICO, 2019). They also have the power to imposes fines on organisations that breach the act and other enforcement actions such as conducting audits or issuing enforcement notices (ICO, 2019).

In concluding, Data Protection Act 2018 is a step in the right direction for data protection and privacy in the UK. By absorbing GDPR in the UK law and providing more provisions to reflect the UK's departure from the European Union, the act provides an inclusive framework for protecting individual's rights while allowing organisations to use personal data for legitimate purpose.

Analysis

The Data Protection Act 2018 became necessary to account for the inadequate Data Protection Act of 1998 passed over a decade ago to address today's internet and digital technologies, social media, and big data (ICO, 2019). The Data Protection Act 2018 is split into three different data protection regimes depending on the situation and function. They are general processing, law enforcement processing and finally intelligent service process. Firstly, we would investigate the rights of subjects.

The legal justifications for data processing are outlined in Article 6 of the UK GDPR (ICO, 2020). According to this law, at least one of these methods must be used to gather personal information. They include consent, contracts, legal requirements, compelling public interest, and legitimate interests (ICO, 2020). An individual's consent must be formally requested for a specified purpose, documented, and monitored (ICO, 2020). It must be concise and have a clear affirmative action. The organization's name, the name of the third-party data controller, why you

need the data, what you plan to do with it, and a statement that the data subject has the right to revoke their consent at any time (ICO, 2020).

Articles 13 and 14 of the UK GDPR give individuals the right to know how their data is used (ICO, 2020). This must be delivered to the person within a month, but no longer than a fair amount of time (ICO, 2020). Information given to a person shouldn't be information the person already possesses. There are few exceptions, such as where the information was obtained from a third party and delivering it would be impractical or take an excessive amount of work (ICO, 2020). However, there is an exception if obtaining or disclosing such personal information is necessary by law or if there is any professional secrecy. (ICO, 2020). There are additionally exclusions in cases where the disclosure will make the goal of the data processing impossible or severely impede it (ICO, 2020). Also, the language used to produce this information should be clear, plain, intelligent, and brief. It could be presented using a tiered approach, dashboards, just-in-time notices, iconography, and mobile and smart device features (ICO, 2020).

There is also a right to access called the Subject Access Request (SAR) (ICO, 2020). This request may be made orally, in writing, or even via the organization's official social media channels. ABX aims to treating a SAR request within a month of request and or final clarification on such request when multiple rights have been used for request or depending on the complexity of the request as required by law. A form of identification should be requested from the requester to verify the individual identify and an administrative fee may be charge on the individual. We will use reasonable efforts to locate and retrieve the requested information, but we may do irrational or excessive searches (ICO, 2020). The information shall be supplied on the individual preference. Also, a third party can request for SAR if it the information does not identify another individual or if the individual gives consent (ICO, 2020).

Under article 16 of UK GDPR, individuals have the right to rectify an inaccurate data (ICO, 2020). DPA 2018 states that personal data is inaccurate if it is incorrect or misleading as a matter of fact (ICO, 2020). All reasonable effort would be made to correct an inaccurate personal information, rectifying those that would affect the individual or others. All rectified personal data disclosed to others would be contacted and informed on this amendment unless proves impossible (ICO, 2020). In such a case, this would be communicated to the requester and a list of those recipients would be sent to the requester While inaccurate information might be easy to correct, opinions are not so much (ICO, 2020).

Individuals have the right to have their personal data deleted under UK GDPR Article 17 (ICO, 2020). This is also called the right to be forgotten (ICO, 2020). This can be applied when the purpose of the data is no longer necessary or when the individual withdraws his consent (ICO, 2020). It could also be for legal reasons or if the information was collected lawfully. The right to be forgotten does not apply when exercising one's freedom of expression, adhering to a legal requirement, carrying out a task of public interest, archiving material for public interest, or asserting legal claims.

Individuals have the right to limit how their personal data is processed under UK GDPR Article 18 if they have a specific justification for doing so (ICO, 2020). This may be because of the content of information held or how the data was processed. If an individual has requested to rectification or object, they could also request for their data to restricted until the process is completed (ICO, 2020). This can be achieved by moving the information to another processing system or making them unavailable to users or temporarily removing published data from a website (ICO, 2020).

The request can be done verbally or in writing and should be corrected in a month while following all the mentioned procedures for refusing and why it could be refused (ICO, 2020).

Also, people are entitled to data portability, which entitles them to obtain a copy from one controller and transmit information to another (ICO, 2020). This needs to be presented in a machine-readable, organised format that is widely utilised. This personal data does not include anonymous data or information about another person, but do include mailing address and search history, among other things. Also, procedures for refusal and informing the individual should be followed here too.

Each person has the right to object to how their information is processed (ICO, 2020). For example, when ABX collects data for marketing and the individual objects to the processing of their information. Rather than erase the individual details, the customer details are placed in a suppression list to prevent them from getting marketing mail but available for any other business they might still be interested in doing with ABX. Again, procedures for refusal and informing the individual should be followed here too.

Right related to automated decision making (ICO, 2020). This gives individual right to consent or object for their information to be used for decision making (ICO, 2020).

Legal Principles of Data Protection Act

1) Lawfulness, Fairness, and Transparency

Lawfulness means to identify specific grounds for processing personal data. This is called lawful basis and they include consent, contract, legal obligation, vital interest, public tasks, and legitimate interest (ICO, 2019). Fairness means processing data how people would reasonably expect and not in a way that would adversely affect them. Fairness must cut across board because if ABX is fair to all but one, then ABX is considered unfair. Care must also be taken to ensure personal data is gotten from someone who is legally authorized to provide it (ICO, 2020). Sometimes, personal data could be used in such a way that could have a negative effect but what matters most is that it is justified legally. Transparency is being honest, open and clear from the starting from who ABX is, how and why ABX uses their personal data. None of these is less important, as an organisation is not lawful would likely be unfair and of course not transparent on how the individual personal data would be used.

2) Purpose Limitation

This has to do with clearly specifying the extent of the purpose of personal data processed (ICO, 2020). The personal data processed for a specific purpose should not be used for another except they are compatible with the original purpose, a new consent is gotten, or it is a legal requirement requiring or allowing the new processing (ICO, 2020).

3) Data Minimisation

Personal information must be pertinent, sufficient, and reasonable given the reason it was collected in the first place (ICO, 2020). The best way to achieve data minimisation is to state clearly why that data is necessary to achieve the desired goal. Personal data is

periodically reviewed to determine whether it is still adequate and relevant. When there is too much information, it is deleted, and when there is insufficient information, people are requested for more information. Opinions should be clearly defined as such as this is not necessarily inadequate or irrelevant just because the individual disagrees with the opinion.

4) Accuracy

Personal data must be always accurate and not misleading at any time (ICO, 2020). All necessary steps must be taken to ensure any inaccurate personal data is erased or rectified. Information from third party should be handled with care and source of such information should be included in records (ICO, 2020).

5) Storage Limitation

Personal data should not be kept longer than is necessary for the purpose for which it was processed (ICO, 2020). Although it could be stored for longer solely for archiving, scientific or historical or statistical purpose implemented using appropriate technical and organisational measures.

6) Integrity and confidentiality (Security)

Personal data should be handled in secure manner to ensure the integrity and confidentiality is maintained by taking appropriate security measures be it accidental or unauthorized access to personal data, accidented or unauthorized loss, erasing or modification (ICO, 2020).

Discussion

Responsibilities of Employees

We have looked at the Data Protection Act 2018, its purpose and how its compliments with UK GDPR. It would be fair to ask why we are providing this information to you and how it affects you as a staff of ABX Ltd. This is what we shall discuss next. Security is everyone's business and we all must work together to ensure we maintain the protection and privacy of all data managed by this organisation. Staffs are encouraged to report to their line managers and the data protection team, if they find any lost or disposed data believe to contain personal data of any kind (University of Bath, 2018). This also includes data that may have stolen, accidentally lost, or inadvertently disclosed. While ABX limits personal data given to designated individual to limit exposal, it the responsibility of that individual to manage that data securely (University of Bath, 2018). It is also the responsibilities of staffs to provide accurate information from the start and report any rectification request to ensure any updated or inaccurate data is corrected promptly (University of Bath, 2018). This includes sales record, staff records and so on. ABX would conduct periodic training of its employees, and all are charged to be abreast with the laid down policies and procedures to prevent any data loss or theft of confidential information. For any staff who handles personal data as part of their day-to-day activities, they should ensure they process these data in accordance with the Data Protection Act 2018 which starts with having a valid lawful basis being the foundation of the law and all other laws that it entails. While ABX data protection team aims to provide a comprehensive report on the law in a concise and easy to understand format, staffs are encouraged to seek further clarification when in doubt on ways to handle new or existing form of data. It is also imperative to follow the guideline for encrypting personal data when shared with a colleague for privacy issue as has been sent on the encryption policy sent to all staffs' mail and can also be found on our intranet page for reference. It is also the responsibilities of all staffs to pass on any enforced right request to the Data Protection Team as so as possible as to get a time response to the request. There are cases when ABX might refuse to comply to a request. In such a case, the reason for not complying, their right to make a complain to ICO and their ability to seek to enforce the request through the court would be informed to the requester. ABX can also refuse to comply if the request is excessive or manifest to be unfounded. ABX has set up a retention policy to hold customers information for a year after their last activity as this would help the organisation so send marketing mails and help the individual make a purchase quickly when they fancy any item. This is also done as a legal requirement.

Human Aspect of Security

While ABX has provided a robust framework to ensure there is minimal security vulnerabilities, it is imperative all employees follow laid down procedures in ensuring the safe use of ABX asset to prevent any data breach. Some of the framework employed by ABX includes stating everyone's responsibilities at a strategic and operational level as regards data protection activities with a clear flow of information (ICO, 2021). Though we have a Data Protection Officer, but we all have a role to play in achieving data protection compliance (ICO, 2021). Appropriate reporting channel has been communicated earlier on with operations roles being defined, setting up an oversight group with a follow up on regular operational meeting (ICO, 2021). ABX has laid down procedures and policies on individual rights requests, transparency and records of processing and lawful

basis. Contract and data sharing policies are also in place as well as risks and data protection impact assessment, record management and security, breach responses and monitoring with a continuous and periodic, training and awareness campaign (ICO, 2021). Humans serve as the last line of defence in ensuring the privacy and security of an organisation. Staffs should protect their personal data by avoiding sharing personally identifiable information or leaking ABX data accidentally or otherwise (University of Bath, 2016). For example, a simple harmless picture taken in the office could be show important that can be used by unauthorized users and such could cause great harm. Staffs should avoid pop up, unknown emails, attachment, and links as this could be a phishing mail (University of Bath, 2016). Staffs must use strong password following the required length and complexity and enable two factor authentication (University of Bath, 2016). This would make it difficult for unauthorized users to gain access to confidential data. Only connect to secured WIFI and enable virtual private network for those that work remotely (University of Bath, 2016). Firewall and antivirus protection has already been enabled by ABX team on staff workstation. By no mean, should it be disabled. While working remotely, ensure firewall and antivirus protection are enabled too (University of Bath, 2016). Staffs should promptly install software updates from authorized sources (University of Bath, 2016). Staffs should also talk to Data Protection Team or IT staffs to get any clarification or enquiries. Staffs should also swift alert Data Protection Team and IT when there is security issue even if it is just suspicion of breach. ABX would continue to do online and offline training to ensure all staffs are aware of on latest update as regards data protection and other security update. Staffs should embrace the educational and training as this would be go a long way in securing the organisation and staff's data.

Awareness Raising Campaign

An awareness raising campaign strategies would be developed to reinforce the importance of Data Protection Act 2018 to ABX employees using mixed method. ABX would be focusing on training its employees which is one of the ways to manage risk as prescribed by ICO (ICO, 2020). Using a scientific methodology, we would set a hypothesis as "training increases the awareness of DPA 2018 on ABX employees". A control and trial group would then be created in the same branch in the same working department. The independent variable would be the training while the dependant variable awareness level of ABX employees on DPA 2018. This can be achieved by conducting a pre-training and post-training survey for the control and trial group. The result of pre-survey and post survey of both groups would be analysed to check the efficacy of the training done. The survey would not only provide insight on staff willingness to comply after being trained on DPA 2018, but it would also provide statistic on the awareness and knowledge growth among ABX employees.

It should be noted here that training should be done in such a way that it is not perceive as hard work or boring, but it should interactive and visually engaging (Ipsos MORI, 2020). It should also be done on a self-pace approach and on the job training for best result (Ipsos MORI, 2020).

On the flip side, some barriers to training could the constant evolution of cyber security, varying quality of accredited vendor, trainings are mostly theoretical and not business oriented among others (Ipsos MORI, 2020).

Security Briefing Outline

A security briefing would be developed for the management team stating Data Protection Act 2018 as the legislation in view. It would also contain the why it is important and the consequence for not complying. It would further contain the awareness and compliance level for staffs before and after the awareness campaign and how effective the campaign was. Finally rounding up with follow up audit to reduce or maintain the awareness and compliance level for non-complying old staffs or untrained new staffs.

Conclusion

In this work, we conducted a thorough research into the Data Protection Act of 2018 by the UK government to tackle the issues associated with present realities of IT and its infrastructure which the Data Protection Act of 1998 could not address. We further stated how and where it complements the UK GDPR and where it defers from the EU GDPR as the latter is no longer in use in the UK due to Brexit. The articles of the Data Protection Act 2018 were analysed and the responsibilities and important roles of staffs in ensuring the privacy and protection of data in the organisation. We rounded up with the content of a security briefing which would be given to the management team.

In future work, I will explore other legislation for ABX Limited to ensure ABX is up to date in all its dealings to prevent any financial or reputational loss.

References

ICO, 2019. *An overview of the Data Protection Act 2018*. [Online]
Available at: https://ico.org.uk/media/for-organisations/documents/2614158/ico-introduction-to-the-data-protection-bill.pdf
[Accessed 25 March 2023].

ICO, 2020. *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 25 March 2023].

ICO, 2021. *About the DPA 2018*. [Online]
Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-dpa-2018/about-the-dpa-2018/
[Accessed 5 March 2023].

ICO, 2021. *Accountability Framework*. [Online]
Available at: https://ico.org.uk/for-organisations/accountability-framework/
[Accessed 02 May 2023].

Ipsos MORI, 2020. Cyber Security Skills in the UK Labour Market 2020. March, pp. 44-46.

UK.GOV, 2020. *Data Protection*. [Online]
Available at: https://www.gov.uk/data-protection
[Accessed 25 March 2023].

University of Bath, 2016. *University of Bath Electronic Information Systems Security Policy*. [Online]
Available at: https://www.bath.ac.uk/corporate-information/university-of-bath-electronic-information-systems-security-policy/
[Accessed 02 May 2023].

University of Bath, 2018. *Data Protection Policy*. [Online]
Available at: https://www.bath.ac.uk/corporate-information/data-protection-policy/
[Accessed 28 March 2023].