ESARBICA JOURNAL

JOURNAL OF THE EASTERN

AND SOUTHERN AFRICA

REGIONAL BRANCH OF THE

INTERNATIONAL COUNCIL ON

ARCHIVES

Volume 39

2020

ISSN 2220-6442 (Print), ISSN 2220-6450 (Online)

https://dx.doi.org/10.4314/esarjo.v39i1.5

DATA PROTECTION LAW IN BOTSWANA: OPPORTUNITIES AND CHALLENGES FOR RECORDS MANAGEMENT

Tumelo Keakopa
University of Botswana
keakopa.tumelo@gmail.com

Olefhile Mosweu
University of Johannesburg, South Africa
olfmos@gmail.com

Received: 10 August 2020
Revised: 28 August 2020
Accepted: 23 December 2020

Abstract

Data protection legislation is concerned with the safeguarding of privacy rights of individuals in relation to the processing of personal data, regardless of media or format. The Government of Botswana enacted the Data Protection Act in 2018 for purposes of regulating personal data and to ensure the protection of individual privacy as it relates to personal data, and its maintenance. This paper investigates opportunities and challenges for records management, and recommends measures to be put in place in support of data protection, through proper records management practices. The study employed a desktop approach and data was collected using content analysis. The study found that opportunities such as improved retrieval and access to information, improved job opportunities for records management professionals and a conducive legislative framework are available. It also revealed that a lack of resources to drive the records management function, limitations in electronic document and records systems and a lack of freedom of information to regulate access to public information by members of the public is still a challenge. The study recommends the employment of qualified records management staff with capacity to manage records in the networked environment for purposes of designing and implementing records management programmes that can facilitate compliance with the requirements prescribed by the Data Protection Act.

Key words: Botswana, data protection, data; privacy, records management

Introduction

As a concept, the right to privacy has a long history. Its recognition can be traced back to 1890 when Samuel Warren and Louis Brandeis wrote an essay titled, *The Right to Privacy*, which was published by Harvard Law Review (Warren & Brandeis 1890). The authors called for the recognition of an individual's "right to be left alone" and advocated for this to be protected by law because it is a human right. Thus, the concept of a right to privacy is very well recognized but is still difficult to define. Privacy, as a part of human rights, identifies the protection of personal data as an important right. Attempts have been made to define 'privacy' but as yet, there is no universal definition for the concept (Lukács 2016). This is because the concept privacy is contextual. What is considered as privacy in particular societies and cultures may be viewed otherwise in other countries, thus leading to differing

needs for its protection (Fried 1968). For example, "opening a door without knocking might be considered a serious privacy violation in one culture and yet permitted in another" (Moore 2008:411). Thus practically, this calls for privacy to be reinterpreted in the light of the current era and be examined in the current context (Nissenbaum 1998).

Warren and Brandeis (1890) define privacy as the "the right to be left alone" while Pound and Freund (1971) define it in terms of an extension of personality or personhood. A more recent definition by Agre and Rotenberg (1998) says that privacy refers to the capacity to negotiate social relationships by controlling access to information about oneself. Building on the definition by Agre and Rotenberg (1998), it therefore follows that loss of control of information about oneself leads to erosion of privacy. Information about individual persons is disclosed and found in records created as they seek services and establish friendships (Pelteret & Ophoff 2016). Therefore, regulating personal information about individuals, and thus avoiding its use in violating privacy, calls for records of transactions documenting persons to be managed for as long as needed. Among others, records with personal information include health, educational and personnel records. According to Ngoepe, Mokoena and Ngulube (2010), records need to be properly connected as they form part of our identity as people. Records management, therefore, plays a role in the protection of the privacy of individuals.

Contextual background

Botswana, like other African countries such as Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Malawi, Morocco, Niger, Senegal, South Africa, Tunisia and Zambia, has enacted data protection legislation (Consumers International 2018). According to Deloitte (2017:6), the African Union (AU) adopted the AU Convention on cyber security and data protection in 2014 to provide a personal data protection framework for African countries and further encourage African countries to recognize the need for protection of personal information. It can, therefore, be concluded that more African countries will continue to introduce the data protection legislation in their respective nations. The right to privacy is a human right and privacy laws are passed as part of satisfying the United Nations' International Convention on Civil and Political Rights, under Article 17 which says that, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation" (United Nations 1976:177).

Plans to introduce privacy laws in Botswana go as far back as 2007 when the Maitlamo Policy, Botswana's national information and communications policy, was approved by the National Assembly (Government of Botswana 2007). The policy, commonly known as the Maitlamo Policy, recognized the need for new electronic legislation such as the electronic commerce, electronic signatures, the data protection law as well as the revision of existing electronic legislation such as the Cybercrime and Computer Related Crimes Act. The policy specifically provided for the development of the protection of personal privacy, which led to the Data Protection Act (DPA) finally being enacted in 2018 (Government of Botswana 2018).

Data protection law and records management

Good records management practice ensures that records are properly managed from creation through maintenance, use and disposal. A record, as defined by ISO 15489-1 (2016), is

information that is created, received, and maintained by an organization or individual as evidence of business transactions. Therefore, records management entails the management of records from the time they are created until they are disposed of. Respondents from a study by Whitman, McLeod and Hare (2001) assert that records management is an integral part of the functioning of any organisation and the ideal must be to control the life-cycle of records until they are destroyed or turned into archives. Any law that involves the creation, access, use, and dissemination of information in any way directly or indirectly impacts on the management of information or records management, the data protection law is no exception. In particular, records management as a form of information management entails the management of records throughout their life cycle from creation, through use, to final disposal either by destruction or archiving. According to Tagbotor, Adzido and Agbanu (2015), the primary function of records management is to facilitate the free flow of information through an organization and to ensure that information is available rapidly where and when it is needed. Performing this function needs an efficient, and effective records management programme. Section 4 of DPA highlights aspects of the records life cycle by stating that the information and data protection office is responsible for ensuring the right to the protection of personal data access, rectification, objection and cancellation of data (Government of Botswana 2018). A study by Tagbotor et al. (2015) argues that, in the absence of strong records management control systems and procedures, information can easily be disorganized, concealed, lost, stolen, destroyed or otherwise tampered with. In order to effectively protect and regulate access to information about individuals, the information should be properly managed from the time it is created to the time it is disposed of or deleted. This clearly implies that the data protection law directly impacts on the different aspects of records management, such as quick information retrieval and management, as such the right records management procedures should be followed when creating, accessing, rectifying and deleting personal data, in such a way that the privacy of data subjects is maintained. This is further supported by the ISO 15489-1 (2016), which defines records management as a field of management responsible for the efficient and systematic control of the creation, receipt, use and disposal of records. Key records management procedures such as the records management policy, the file classification system and the records retention and disposal schedules are developed and implemented to facilitate the organizing, retrieval, protection and disposal of records. Once these procedures are established and implemented, consistency and uniformity should be maintained to ensure that information is always accurate and only used and shared with those who are authorized to, and to delete the information following authorization thereunto.

Statement of the problem

Proper management of records promotes compliance with existing legislation. Thus in the conduct of business, organisations are legally obliged to create certain records and retain some for specified periods (Ngoepe 2008). Basically, properly implemented records management programmes are crucial in ensuring adherence to legal obligations. Despite the importance of records in the running of organisations, their management is more often than not neglected (Mnjama 2004; Ngoepe 2008; Ndenje-Sichalwe, Ngulube & Stillwell 2011). This study content analysed the DPA of Botswana to demonstrate that compliance with its provisions provide opportunities for the management of public sector records in Botswana, albeit with some challenges as outlined.

Methodology

This study used qualitative content analysis to identify opportunities and challenges for records management in the context of Botswana. It collected data from available literature, principally the Data Protection Act (DPA) of Botswana which was passed by Parliament of Botswana in 2018. Content from documentary sources in the form of texts and documents provide useful data about society, both historical and the present (Walliman 2011). An analysis of content from documents as a research method enables data collection through an evaluation of existing documents, both printed and digital (i.e. computer-based and internet-transmitted documents) (Bowen 2009). Ukwoma and Ngulube (2020) also used qualitative content analysis to study theory borrowing from library and information science research postgraduate research in Nigeria and South Africa.

Objectives of the study

The main purpose of this study was to analyse the Data Protection Act of Botswana in relation to public sector records management. The specific objectives were:

1. To identify and describe data protection legislation in Botswana.
2. To establish opportunities for records management arising from the enactment and implementation of the Data Protection Act of Botswana.
3. To find out which records management-related challenges are likely to be experienced in the public sector of Botswana.
4. To recommend measures to address anticipated challenges to records management brought about by the implementation of the Act.

Findings of the study

The findings of this study are organised into three themes as informed by the study objectives. The first to be presented relates to legislation that governs data protection in Botswana.

Legislation governing data protection in Botswana

The legislation governing data protection in Botswana is known as the Data Protection Act. It was enacted through an Act of Parliament in 2018 (Government of Botswana 2018). The objectives of the DPA are (1) to regulate the protection of personal data and ensure that the privacy of individuals in relation to their personal data is maintained, (2) to establish the information and data protection commission, and (3) to provide for all matters incidental thereto. The law is a form of privacy law that protects the right of individuals with regard to information about them (Olinger, Britz & Oliver 2007). Many of the privacy laws drafted so far seek to protect the individual against the potential information exploitation by powerful role players in possession of such personal information. In addition, Adamski (2012) asserts that the free flow of information is essential for the economic and political system, and government accountability. However, the protection of information should not only consider the economic interests of its proprietor or holder, but at the same time must preserve the interests of those who are concerned with the contents of information – an aspect resulting in new issues of privacy protection. Furthermore, Adamski (2012) states that the underlying idea of protection of personal data is to make it possible for the individual to exercise control over one's own data that is collected and used by others. In summary, the main objective of

the data protection law is to protect the rights and privacy of individuals with regard to their personal information.

Section 4 of the DPA provides for the establishment of the Information and Data Protection Commission (IDPC) body, which will be a public office responsible for ensuring the effective application of and compliance with the act (Government of Botswana 2018). The right to the protection of personal data, access, rectification, objection and cancellation of data is provided for in the legislation. The act defines personal data as information relating to an individual or identifiable individual, which individual can be identified directly or indirectly, in particular by reference to an identification number, to one or more factors specific to an individual's physical, physiological, mental, economic, cultural or social identity. One of the key terms in the act is the term 'data subject' which is defined as an individual who is the subject of personal information and this same term will be adopted and used throughout this paper. The DPA is the equivalent of the United Kingdom's Data Protection Act (GOV.UK 2018), which regulates how individual personal information is used by organisations, businesses and government. The Data Protection Act of 2018 is the UK's implementation of the General Data Protection Regulation (GDPR) which was issued by the European Union. According to Diaz (2016:216), "the aim of the GDPR is to improve the level of data protection for natural persons whose personal data is processed by automated means, or not, and to increase opportunities for trade and free movement in a single digital market, in particular, by reducing red tape." The IDPC as a body would administer the Act and monitor compliance with the provisions of the DPA.

The IDPC has a huge responsibility of regulating and ensuring the protection of personal data privacy and, as such, the DPA outlines some of the key positions and responsibilities of officers who will work for the common goal already identified. Section 4 of the data protection act gives the functions of the power of the commission as the following:

- Ensure the effective application of and compliance with this act, in particular, to the right to protect personal data, access, rectification, objection and cancellation of such data.
- The commission shall ensure compliance with the provisions of the Statistics Act, with regard to the collection of statistical data and statistical secrecy
- Provide guidance and instructions on appropriate security measures to ensure the security of personal data.
- Conduct research and studies, and promote educational activities relating to protection of personal data.
- Receive reports and claims from a data subject or his or her representative in regard to a violation of this Act, and to take such remedial action as is necessary.
- Investigate complaints from data subjects and respond to queries of such complaints.

In addition, section 2 of DPA also states the responsibilities of the staff of IDPC as follows:

- Commissioner: The commissioner of the information and data protection commission appointed under section 6
- Data Controller: A person who alone or jointly with others, determines the purpose and means of which personal data is to be processed, regardless of whether or not such data is processed by such person or an agent on behalf of the person
- Data Processor: The person who processes data on behalf of the data controller

- Data Protection Representative: A person who is appointed by the data controller, which person shall independently ensure that personal data is processed in a correct and lawful manner

The commissioner will be the overall overseer of the commission, working closely with the data controller, data processor, data protection representative and other staff of the commission.

Opportunities for records management

The enactment of the Data Protection Act brings to the fore a number of opportunities for the archives and records management in Botswana. These are presented in the next section.

Job opportunities for records management staff

The DPA provides for the establishment of the IDPC with key responsibilities particularly for records management, and these include:

a. Providing guidance and instructions on appropriate measures to ensure the security of personal data. In a computerized environment, this will be a shared role for records managers and IT personnel.
b. Providing information to persons on their rights connected to the processing of personal data.
c. Monitoring and adopting any authorisation for the trans-border flow of personal data, and facilitating international cooperation on the protection of personal data.
d. Creating and maintaining a public register for all data controllers

The responsibilities of the IDPC are specific to records management and as such will require the staff in charge to be qualified records management professionals or at least have basic knowledge of and experience in good records management practices. The first opportunity created by the establishment of the commission is the possible creation of more job opportunities for records management professionals. The commissioner in charge of the commission is directly appointed by the minister and as such the public office will be recognized at a high level as well as the importance of records management.

Enhancement of the profile of records management profession

Data protection enjoys attention from even the highest of authorities. In the context of Botswana, the DPA prescribes procedures regulating access personal information (Government of Botswana 2018). The mere fact that there is a need for procedures to be in place is a positive development for records management as a function in the public service of Botswana. Procedures regulating the management of personal information can help improve the management of records containing personal information. Shepherd and Yeo (2003) indicate that records managers have an obligation to understand the legislative and regulatory environment as these affect the way records should be managed. Since it is a legal requirement to have procedures in place to regulate the handling of personal information under the DPA, this becomes a development which would positively assist public records management in Botswana. The provision to have a procedures manual compels ministries and departments in Botswana to assume a systematic and organised approach to the management of public records (Mampe & Kalusopa 2012).

One of the challenges for records managers has been that the records management function is placed low in the organizational structures and as such it becomes difficult to enforce records management procedures because records management is not recognized or taken seriously. With the introduction of the data protection legislation and commission office at a high level sorely in charge of proper records management, it is an opportunity for records management to be recognized at a higher level and provide an opportunity to refresh records management policies and procedures relating to the safe stewardship of data. This in turn has the potential to influence other government departments to elevate the records management function in their respective departments.

Information access and retrieval

Records management allows for information to be stored properly following a records classification that is categorized according to the specific functions or activities of an organization. Quick and easy retrieval of information can only be achieved through good records management practices. Whether the information is manual or electronic, quick retrieval of records requires a proper, well-functioning classification system as it is a retrieval tool for records. When information is stored properly, access and retrieval becomes easy. Access to personal data forms the basis of the DPA because it is this information that is monitored and regulated, and as such should be available for access whenever it is required.

Section 30 of the DPA prescribes that the data subject must be able to ask the data controller if he has any information on him or not; however, the data controller has the power to refuse to submit to the request of the data subject, but there has to be a reason for the refusal. The data subject is at liberty to challenge the refusal and can even have the data modified or deleted. In addition, section 10 gives the commissioner an entitlement to obtain from the data controller, on request in writing, access to personal data, and any information or documentation relating to the processing of personal data. At the time of the request, the act also gives the commissioner powers to specify the time in which a data controller must respond to that request. With poorly organised records, retrieval of records becomes difficult and meeting time frames to honour the request for personal data may be difficult to attain.

A study by Whitman et al. (2001) highlighted the importance of proper records management in information access by stating that any information access legislation is only as good as the quality of the records to which it provides access. Furthermore, it was stated that such rights are of little use if reliable records are not created in the first place, if they cannot be found when needed or if the arrangements for their eventual archiving or destruction are inadequate. Similarly, the data protection law gives individuals the right to access information about them, but the right is of no use if this information cannot be accessed or is not available when requested. Failure to avail this information may be due to poor records management, for example where the information was stored in the wrong folder, incomplete, incorrect or even deleted. It is evident that proper records management is essential for the provision of information access in the context of the DPA. This statement is further supported by Tagbotor et al. (2015) by asserting that productivity will be improved and costs reduced through easier access to records and less time spent looking for information. Good records management will not only facilitate information access but will also result in quick retrieval of information if the right procedures were followed when creating and storing the information. With quick access the commission will be effective in its operations. The importance and seriousness of availing information when required is further emphasized in the Act, which states that failure of the data controller to provide information when requested

is a violation of the Act and can be charged. Once the data commissioner office is set up in Botswana, records management policies and procedures should be prioritized to ensure that the office is able to deliver on its mandate of ensuring that data protection legislation is not breached in any way with regard to information access as a result of poor records management.

Information accuracy and evidence

The International Organisation for Standardization (ISO) for records management ISO 15489-1 (20), which provides guidance on managing records, states that a record should have characteristics of authenticity, reliability, integrity, and usability in order to be used for accountability purposes. It is, therefore, important for a record to be an accurate true representation of a business transaction which can be used to provide evidence of the business transaction as well as legal evidence in cases of litigation. The DPA recognizes the importance of information accuracy because it requires that all information recorded and processed about individuals should be accurate and, if need be, it provides a provision for the information to be rectified. Section 30(1) of the Act gives the data subject the right to challenge personal data relating to him or her by submitting a complaint in accordance with section 42(1), and if the challenge is successful, have the personal data deleted, rectified, completed or amended, whichever is required. This evidently shows the importance and need for the Commission to ensure that information about individuals is always correct and accurate. The data controller has a responsibility to ensure that information collected/captured is accurate. The data protection law provides for the data subject to request information and have it rectified if it is incorrect or inaccurate. When information is inaccurate, it may be evidence of poor records capturing. Furthermore, in cases of litigation as a result of breach of the DPA, the Data Commission Act will be required to provide information that will be used as evidence and this will rely on proper records management practices. For the information and data protection commission to fully realize and deliver on its mandate, it will be dependent on accurate and reliable records management. The implementation of a records management programme guided by ISO 15489-1 (2016) would ensure that data generated in the conduct of organisational processes possess the characteristics of an authoritative record as being record authenticity, integrity, usability and reliability.

Accountability

Record management is crucial to all organizations. Unless records are managed efficiently, it is not possible to account for what has happened in the past or to make decisions about the future. ISO 15489-1 (2016) explains accountability in records management as a principle that individuals, organisations and the community are responsible for their actions and may be required to explain them to others. Accountability can be achieved through good records management practices that accurately capture what was communicated, what action was taken, who took the action, and when the action was taken. Records are a vital corporate asset and are required to provide evidence of actions and decisions (Tagbotor et al. 2015). According to Cowling (2003), evidence of past action is the basis of all forms of accountability; it is captured as records. For records to retain their value as evidence, they need to be preserved and managed. Accountability is a key factor in the DPA. According to section 8 of the DPA (2008), before assuming their duties, the key staff of the commission take an oath of secrecy before the Minister to carry out their duties with equity and impartiality in accordance with the Act. The importance of accountability is also highlighted on several sections that state that where there is a breach of the provisions of the Act,

investigations shall be carried out. Section 10(4) states that where the commissioner made a request and obtained sufficient information to conclude that the procession of data is unlawful, the commissioner may prohibit the data controller from processing personal data. It is evident from the provisions of the act cited above that those in charge of managing personal information will be held accountable if there is any evidence of breach of the act. Failure to manage records properly has been a contributory factor in the lack of accountability as, without records, there can be no accountability. This is an opportunity for records management as the law compels public organisations to implement proper records management practices which would comply with the provisions of DPA. This assertion takes into consideration that although records are a strategic resource, their management is often neglected (Mnjama 2004; Ngoepe 2008; Ndenje-Sichalwe et al. 2011).

Retention and disposition schedules

Section 14(h) of the DPA states that personal data is not kept for a period longer than is necessary, having regard for the purposes for which it is processed and personal data is processed in accordance with good practice. Section 32(1)(a) of the DPA also states that the controller, a data processor or a person acting under authorization of the data controller or the data processor, shall, in order to safeguard the security of personal data, take appropriate technical and organizational security measures necessary to protect personal data from neglect or unauthorized destruction. This section emphasizes that personal data should only be deleted after the purpose for which is was created has been realized, unless otherwise stated. In the records management practice, a tool known as a records retention and disposition schedule is developed, approved and used to ensure that records are disposed properly following the right procedure and authorization from senior management. The commission will have to enforce the development and implementation of a retention schedule to ensure that personal information is not kept longer than necessary and that the destruction of personal data is always authorized following an approved retention schedule. In cases where personal data destruction is authorized, a record to show evidence of the destruction will be required and this can only be achieved through effective records management.

The need for electronic document and records management systems

Section 32(2) prescribes that the data controller, a data processor or a person acting under authorization of the data controller shall ensure an appropriate level of security by taking into account technical development of processing personal data, and the cost of implementing security measures. Enforcing the required security of personal data required by the DPA and facilitating quick retrieval of information when needed will in some instances require the commission to develop and implement an electronic records management system (EDRMS) to manage the electronic information. An EDRMS is an electronic system or process managed with the assistance of computers and software, implemented with functionalities to manage both electronic documents and electronic records within an organization (International Records Management Trust 2009). The system is important because it will facilitate compliance with the DPA by improving security through strict access control, quick retrieval and traceability of records, especially electronic records.

Use of information for archival purposes

The DPA of 2018 recognizes the importance of archives and their use in research and cultural heritage. Section 24(1) of the act states that sensitive data may be processed for research,

scientific and statistics purposes, provided that the processing is compatible with specified, explicitly stated and legitimate purposes, but the data controller should ensure that there are appropriate security safeguards in place. Even though the Act states that personal data has to be collected for a specific, explicit and legitimate purpose and cannot be used for other purposes beyond that, it provides an exception and allows for information to be used and processed for scientific research, archiving or statistical purposes with or without the consent of the data subject. The DPA makes an exception when information is used for research purposes. This is evidence that it recognizes the value of archives.

Challenges for records management

Although the DPA presents a lot of opportunities for records management, it also presents some challenges for information and records management. If some of the challenges are not addressed, the information and data protection commission office will be ineffective and in some cases result in government losing a lot of money due to breach; for example, failure to respond to requests by data subjects due to missing information as a result of poor record keeping practices. Failure to comply with this law will see those in charge of managing information being prosecuted and fined if they do not respond to requests or comply with the DPA. Therefore, proper records management will be critical and, if good principles are followed, there will be even more opportunities for the records management profession. A study by Tagbotor et al. (2015) supports this by arguing that in the absence of strong records management control systems, records can easily be disorganized, concealed, lost, stolen, destroyed or otherwise tampered with. Similarly, the findings of the study by Whitman et al. (2001) asserted that effective records management was identified as a precondition for managing the implications of freedom of information and data. Regulating the protection of personal data and ensuring that the objectives of the information commission are achieved in practice will be dependent on good records management practices.

The project by Whitman et al. (2001) also raised broader perspectives among interviewees other than tensions associated with the rights of individuals under both acts. Respondents expressed that the data protection legislation would sanction the destruction of records rather than preserve their value as historical archives. This is because the data protection law states that once the purpose for which the data about individuals is completed, the information should be deleted. In contradiction, the law requires that when data subjects or the commissioner requests personal information, it should be available and accessible. In response to this perceived problem, one interviewee from a study by Whitman et al. (2001) suggested that the privacy of data subjects could be ensured by means of long retention periods and associated rules of access while preserving the records for the future. Maintaining a balance between deleting information when the purpose for which it was created has been achieved and availing the information in the future when it is needed, especially for evidence purposes, will be a major challenge for records officers in charge of managing the information. Developing and approving retention schedules will be critical for ensuring that records are only deleted after the approved retention period. However, the law should also provide a provision for stating that once the data subject has authorized deletion of information, they will not be allowed to request the information in the future. For this provision to be effective, it will require records professionals to ensure that evidence confirming that data subjects authorized destruction of their information is managed and preserved to provide evidence of records disposal in the future. The importance of records management cannot be over-emphasized when it comes to producing evidence during litigation. Failure to do so may result in organizations losing court cases that could otherwise

be easily won by producing evidence in the form of authentic, complete records. For example, in cases where the data subject authorized deletion of their information and later comes back to request it, and records officers fail to produce evidence showing that indeed the record deletion was authorized, the commission office will be liable and may face litigation if data subjects decide to exercise their rights to sue.

Lack of adequate resources

For the information and data protection commission public office to be effective in delivering its mandate of ensuring the effective application and compliance with the Act, particularly the protection of personal data access, rectification, objection and cancellation, qualified records professionals and records management tools must be available. Should the office be understaffed or lack proper policies and procedures in the management of information, it will be difficult to deliver on its mandate. In their study, Olinger et al., Britz and Olivier (2007) argue that there are low levels of enforcement, compliance and awareness with respect to the national regimes. Bygrave (2004:345) asserts that Germany has one of the most powerful data protection laws in Europe, but also acknowledges one of its weaknesses as the federal data commissioner's lack of competence to issue legally binding orders. The study also suggested that privacy legislation in most European countries displayed a similar weakness of low levels of enforcement, compliance and awareness. and concluded that privacy agencies in Europe have been found, in general, to be under-resourced, leading to under-resourcing of enforcement efforts (Bygrave 2004). If employees do not have guidelines in the form of records management policies and procedures that will guide them in how to operate and are not trained in how to use filing systems, productivity cannot be improved (Tagbotor et al. 2015).

Lack of freedom of information (FOI) legislation

The data protection legislation and freedom of information legislation go hand in hand. While the DPA protects the privacy of information and the right of individuals to access information about them, FOI facilitates easy access to this information (Whitman et al. 2001). Whitman et al. (2001) opine that although the data protection legislation established a right of access to information held on individuals as 'data subjects', FOI provides rights of access to all information held by public authorities. Sebina (2005) adds that the FOI legislation is expected to facilitate access to information while records management is expected to create, manage and make the information available for access.

Limitations in the management of electronic personal data

The DPA has a provision for trans-border flow of information which is defined in the Act as the international flow of personal data which can either be transmitted by electronic or other forms of transmission, including satellite. The use of ICT systems to process and manage data will present new challenges for information management. Data processed using computer systems is more vulnerable to data manipulation, interception and erasing of proprieties that constitute a major concern of computer security, and the criminal law provisions on computer crime Adamski (2012). Furthermore, section 14(f) of the DPA (2018) states that a data controller shall ensure that personal data is protected by reasonable security safeguards against risks such as loss, unauthorized access, destruction, use, modification or disclosure. However, data protection on the internet is an even more complex issue. Sensitive personal data can be communicated from sites located in countries without any privacy legislation

where they can be accessed from all over the world by a simple mouse click (Adamski 2012). Records professionals in charge of the management of personal data in the electronic environment will face challenges because of the vulnerabilities and challenges that come with the flow of information on the internet across borders. Another challenge that might lead to violation of the Act is that once personal information is computerized, it is vulnerable to long-term storage because it may be in many different locations even though it might have been properly deleted following authorized destruction.

Conclusion and recommendations

Perusal of the DPA shows that it provides for the protection of the privacy of individuals by regulating and managing the creation, use, processing, sharing and deletion of the personal information. To properly manage the cycle of personal information from creation to disposition, good records management practice is a necessity. The findings from this study presented a lot of opportunities for records management in the public sector of Botswana. Some of the opportunities include job opportunities for records management, improved accountability, the need to implement an EDRMS and proper records retention and disposal. These opportunities outweigh the challenges such as inadequate resource provision for records management, a lack of FOI legislation and limitations in the management of electronic personal data. The DPA thus presents an opportunity for public sector organisations to lobby for support for proper records management that is resourced as it is handy in helping to comply with the provisions of the DPA in relation to upholding the privacy of personal information.
In view of the findings of this study, the following recommendations are made to mitigate against records management challenges in the context of the implementation of the DPA:

- The processing of personal data should be limited to their usage such that once the purpose for which it was collected has been satisfied, it should be disposed of appropriately.
- Records management professionals should be capacitated to manage records, especially in the networked environment to cope with personal data management in the electronic age.
- Public sector organisations are encouraged to implement EDRMSs as they are designed to regulate access and protect records. The system is important because it will facilitate compliance with the DPA by improving security through strict access control, quick retrieval and traceability of records, especially electronic records.
- The Government of Botswana, through the Botswana National Archives and Records Services, should lobby for the elevation of records management as function to a more senior role so that it can influence records management activities effectively in government.
- More records management professionals, even qualified ones, should be employed to spearhead records management programmes that can assist with compliance with the requirements of the DPA.
- The Government of Botswana is encouraged to enact FOI legislation in order to legally provide for access to information by individuals or members of the public.

© ESARBICA ISSN 2220-6442 | ESARBICA Journal, Vol. 39, 2020

References

Agre, P.E. & Rotenberg, M. 1998. Technology and privacy: the new landscape. *Harvard Journal of Law and Technology* 11(3): 871-880.

Bowen, G.A. 2009. Document analysis as a qualitative research method. Available at: http://ngsuniversity.com/pluginfile.php/134/mod_resource/content/1/DocumentAnalysis.pdf (Accessed 15 August 2019).

Bygrave, A.L. 2004. Privacy protection in a global context – a comparative overview. Scandinavian *Studies in Law* 47: 319-348.

Consumers International. 2018. The state of data protection rules around the world. Available at: https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf (Accessed 15 August 2019).

Deloitte. 2017. *Privacy is paramount: personal data protection in Africa*. Johannesburg: Deloitte Touche Tohmatsu Limited.

Díaz, E.D. 2016. The new European Union General Regulation on Data Protection and the legal consequences for institutions. *Church, Communication and Culture* 1(1): 206-239.

Freund, P.A. 1971. Privacy: One concept or many? In Roland Pennock and John W. Chapman (eds) Privacy *Nomos XIII*. New York: Atherton Press.

Fried, C. 1968. Privacy. *Yale Law Journal* 77: 475-493.

Government of Botswana. 2007. *National Information and Communication Technology Policy*. Gaborone: Government Printer.

GOV.UK. 2018. Data protection. Available at: https://www.gov.uk/data-protection (Accessed 15 August 2019).

International Records Management Trust. 2009. *Glossary of terms: training in electronic records management*. London.

Lukács, A. 2016. What is privacy? The history and definition of privacy. Available at: http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf (Accessed 9 August 2019).

Mampe, G. & Kalusopa, T. 2012. Records management and service delivery: the case of Department of Corporate Services in the Ministry of Health in Botswana. *Journal of the South African Society of Archivists* 45: 1-23.

Mnjama, N. 2004. Records and information: the neglected resource. *ESARBICA Journal* 23: 33-44.

Moore, A. 2008. Defining privacy. *Journal of Social Philosophy* 39(3): 411-428.

Ndenje-Sichalwe, S., Ngulube, P. & Stillwell, C. 2011. Managing records as a strategic resource in the government ministries of Tanzania. *Information Development* 27(4): 264-279.

Ngoepe, M. 2008. An exploration of records management trends in the South African public sector: a case study of the department of provincial and local government. MINF Dissertation, University of South Africa, Pretoria.

Ngoepe, M., Mokoena, L. & Ngulube, P. 2010. Security, privacy and ethics in electronic records management in the South African public sector. *ESARBICA Journal* 29: 36-66.

Nissenbaum, H. 1998. Protecting privacy in an information age: the problem of privacy in public. *Law and Philosophy* 17(5-6): 559-596.

Olinger, H.N., Britz, J.J., & Olivier, M.S.2007. Western Privacy and/or Ubuntu? Some Critical Comments on the Influences in the Forthcoming Data Privacy Bill in South Africa. *International Information & Library Review* 39: 31-43.

Pelteret, M. & Ophoff, J. 2016. A review of information privacy and its importance to consumers and organizations. *Informing Science: The International Journal of an Emerging Transdiscipline* 19: 277-301.

Sebina, P. 2005. Access to information: the role of freedom of information legislation and constitutional guarantees. *ESARBICA Journal* 24: 43-57.

Shepherd, E. & Yeo, G. 2003. *Managing records: a handbook of principles and practice*. London: Facet Publishing.

Tagbotor, D.P., Adzido, R.Y.A. & Agbanu, P.G. 2015. Analysis of records management and organisational performance. *International Journal of Academic Research in Accounting, Finance and Management Sciences* 5(2): 1-16.

Ukwoma, S.C. & Ngulube, P. 2020. To borrow or not to borrow is the question? Theory borrowing in library information science postgraduate research in Nigeria and South Africa. *International Information & Library Review*. DOI: 10.1080/10572317.2020.1790261

United Nations. 1976. International Covenant on Civil and Political Rights. Available at: https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf (Accessed 15 August 2019).

Walliman, N. 2011. *Research methods: the basics*. New York: Routledge.

Warren, S.D. & Brandeis, L.D. 1890. The right to privacy. *Harvard Law Review* 4(5): 193-220.

Whitman, J., McLeod, J. & Hare, C. 2001. BIAP: balancing information access and privacy. *Journal of the Society of Archivist* 22(2): 254-274.