International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 2 Issue 9, September 2014

Personal Data Protection Acts: Concepts and Review

Mayas Aljibawi[1], Roslan Ismail[2]

[1]College of IT Universiti Tenaga Nasional, Kajang-Selangor-Malaysia
[2]College of IT Universiti Tenaga Nasional, Kajang-Selangor-Malaysia

Abstract: ***In today environment there is a lot of data about people have been collected, processed and stored. This creates a situation where people's information are freely distributed and makes individuals' data available to be disclosed easily without the person's permission. It is quite challenging for people to control and manage their information, especially for those who has less familiarity with how to use computer and internet privacy and secure all of their personal data. The PDP act is important to manage the using of employees personal data inside organizations environment to identify rules and responsibilities of employees and organization sides to protect the personal data. The main challenges that faces the PDP inside any organization is the weakness of understanding the PDP act and the wrong systematic implementations of PDP acts. The objective of this paper is to lend some understanding on the PDP acts. The paper recommends that the awareness of PDP acts is important and a leads to better understanding to override the problem of data disclosure.***

Keywords: Personal Data Protection, PDPA, Data Privacy, Security

1. Background

Privacy is the right of permission in which people manage themselves based on their visions [1]. On the other words, people have the rights to select or structure the manner that represent themselves to other people. Privacy is one of the biggest problems in this new electronic age [2]. The privacy of information systems is the permissions to view or hide the information and activities that represent the persons on information systems such as real names, job activities, personal images and videos. The privacy techniques are dynamic and changed rapidly depend on the information processing strategies and techniques i.e. techniques of collecting, retrieving and sharing information [3]. Therefore, the development of information processing techniques leads to new privacy ways and strategies. The known history of privacy stated in 1980 by [4] through the "Right to privacy" article, and the purpose of this article is to develop copyrights printing technology such as finger printing for books, magazines and newspapers. The Internet revolution adds other challenges to information privacy. However, the information processing and sharing come more easily and quickly. Therefore, the traditional laws cannot cover the internet information privacy efficiently [5].

2. Introduction

This paper intention is to highlight the status of Personal Data Protection Acts particularly by the academic and scientific research groups. It presents the review in parts: what is PDP, Data Privacy; privacy vs security, Advantages and implementations of; PDP in Universities, and Online data protection.

3. What is personal data protection

An Act to regulate the processing of personal data in commercial transactions and to provide for matters connected therewith and incidental thereto" [6]. Also, Personal Data Protection (PDP) is standard rules to define the employees or individuals personal data protection rights. However, Personal data refers to data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organization has or is likely to have access. The objective of the data protection rule to is control the collection, use and disclosure of personal data. The PDPA will guarantee a baseline standard of personal data protection, and all organizations will have to obey with the PDPA as well as the common law and other relevant laws that are applied. However, the personal data management activity from the time personal data is calm, used, saved and destroyed will be affected by this law and the process will be more complex.

4. Data Privacy

According to [7] there are two types of control for privacies which are:

1) Systems Controlling: this type represents the options and features of privacy that offered by systems to control the personal information, activities and behaviors; some of these features are mandatory while the others are optional.

Systems Controlling: this type represents the options and features of privacy that offered by systems to control the personal information, activities and behaviors; some of these features are mandatory while the others are optional.

Nowadays, the communications channels increase rapidly between governments, organizations and people. The importance of managing the relations and connections between humans grow up to save the people and organizations rights based on a standard law. Thus, the privacies in many countries formulated as written rights and laws. However, the increasing in people and organizations communications has many challenges such as cultures, freedom of speech and behaviors differences. The privacy laws and rights in any countries manage the communications between organizations or the people that live in this country.

The privacy laws concerns about four main types of privacy which are; personal, information and organizational [8].
The data privacy can be classified into three parts:

A. Personal privacy

The personal privacy represents the rights of persons to protect their physical elements such as cars, clothes and money; any try to stole, damage or search in the personal or physical elements identified as theft, and the countries have the rights to punish the aggressor based on the laws penalties [9]. The personal privacy is defined as the rights of a person to protect his/her things that reflect the physical elements like stole money from electronic banks accounts.

B. Information privacy

The privacy of information is protecting the data and information that identify a person such as his/her personal job data, birth of dates, and religion. People have the rights to keep their data and information private. The privacy Acts define any attacking on people information as theft; there are four main types of information privacy which are [10], [11]:

1. Financial privacy.
2. Internet Privacy.
3. Medical Privacy.
4. Political privacy

C. Organization privacy

[12] Mentioned that this type of privacy is important for the organizations, groups and governments to keep their job secrets and information private against any attacks and thefts. Most of organization apply the strategy of categorize the privacy levels based on many variables such as secrets and information importance and ages of secrets and information. The secrets and information's that stored, acquired and retrieved using electronic and internet systems face challenges on security fields such as viruses and networks attacking.

5. Privacy and Security

There are many people and organizations who believe that security and privacy are the same. [13] mentioned that, there are many organizations that understand the differences between security and privacy. Therefore, they maintain two fully separated departments for security and privacy, and the employees and managers of each department are different and have their own visions and missions. According to [13] the following points clarify the differences between security and privacy:

1) Security is the technical implementation to achieve privacy. In the other words, privacy is encompassed by written laws and security becomes the technical application of these laws.
2) Security is process; privacy is results.
3) Privacy is the outcome of security strategies.

Privacy represents the rights of people to protect their data, and the penalties upon those that attack these rights [14]. Therefore, the privacy is the act that determines the information types and the penalties of attack theses information. On other hand, security is the techniques that the organizations and governments develop to ensure the effective systematic implementation of privacy.

The Personal Information Identifications (PII) of 10,000 students enrolled in Stanford University was attacked in 2005 [15]; the attackers stole, updated, and damaged many students' information, such as credit cards information and Social Security numbers. In 2005, the information of 380,000 students from different UK colleges and universities was attacked. The security measures of the university were applied and that the security procedures of the university were followed based on analysts' reports and recommendations [15]. There were two main problems with this case: (1) there was no standard basis or rules to determine the student's information protection rights, and (2) there were no clear penalties placed on attackers. The difference between privacy and security is clear. Thus, privacy represents the security contract, and in this contract the rights of people and the attacker's penalties are clear and understood. Figure 2.3 shows that security will become the freedom from risks people will enjoy when there are well controlled and managed privacies.

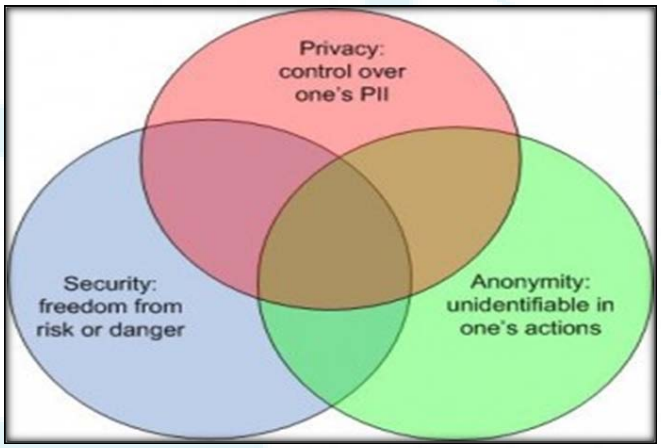

Figure 1: Interaction between Privacy and Security

6. Advantages and implementations

The purpose of PDPA is to manage the individuals and employees personal data efficiently. However, the huge increasing in the personal data volume lead to many challenges in the rights of collect, access and share the personal data in the organizations. Therefore, PDPA represents the standard rules that must follow to protect the personal data and protect the individual rights to keep these data private. There are many advantages of apply PDPA inside the organizations, and the following are the main advantages of PDPA [16], [17].

1. Individual's trust in the organizations.
2. Rights management.
3. Define responsibilities.
4. Define the penalties and post procedures.

There are many countries applies the PDPA in their communities, and these countries work hardly to maximize the performance of PDPA efficiency through enhance many variables such as people awareness. Table I summarizes some examples of PDPA development in various countries.

Table 1: PDPA's implementations in various countries

Country	*PDPA Producing*	*Comments*
European	1998	There are 8 rules to respect the family privacy such as correspondences.
U.K	1998	U.K data protection penalties of personal data attacking are the strongest penalties in the world.
U.S.A	1965	The oldest data protection law and the only law that designed based on historical and theoretical research in many privacy fields.
Canada	1998	Include special and clear data protection rules for electronic applications
Australian	1998	Contain very well definition and classification for individual's personal data.

7. Personal data protection in university

Each university keep large amount of personal records about the students and that leads to a concerning about the protection of data. Staff and employees in addition to their work are responsible for the safety of that data. It's important to prevent illegal access to or review of students' information and data in the regular work. In this context, lots of rules and regulation has been made to prevent these breaches. Despite this, the rules still not obeyed. An example for this breaches happened in Hamburg University, when the university hospital lost the patient's records due to huge access rights established to 5,800 employees that can access to patient records by using the internet from many German hospital. Another example from Hamburg also, in 2010, a fine of €200,000 against Hamburger Sparkasse, a savings and loans company, has been forced by the Hamburg data protection authority (DPA), due to using neuromarketing methods without customer approval [18]. The disclosure of banks account data represented a serious breach of the BDSG [19]. Data protection breaches will not happened without employees. That's why the employees are responsible for implementation the PDPA regulation.

Many universities has applies the personal data protection acts to their rules and regulations. Ulster university [20] develops a framework based on UK 1998 Act of data protection to ensure that the employees satisfaction on data privacy. The framework of Ulster depends on analyzing the collected data from the university employees using questionnaire method. The main objective of the developed framework is to balance between the government data protections act and the university services efficiency. The developed framework of Ulster maximizes the awareness of using the employees' personal data protection through organize and define the procedures and rules of process and use the personal data of employees and clarify these procedures for employees' to identify their personal data protection rights. Another example is Hertfordshire University [21], their data protection team adopt the UK 1998 acts of data protection to determine the personal data authentications and usability in the university activities. The university team classifies the personal data of employees as four main types:

1. General information such as name, phone number and email.
2. Sensitive personal data such as health data,
3. Assessment information such as next of keen information and,
4. Financial information such as salaries.

The main objective of information classifications is to follow the UK 1998 data protection act classifications and determine the university activities and services based on the employees' information types. Therefore, each service has its own security and privacy procedures based on the used personal information of employees. Instead of the systematic procedures to protect the personal data of employees, [21] produce data protection guidelines and recommendations to clarify the rights and penalties of personal data usages which maximize the employees' awareness of personal data protection.

Data Protection Office of Heriot Watt University [22] explained that employees and students personal data and information that used by the university system need to protect and keep private. The data protection Act of university based in country privacy rules is necessary to protect the employees and students rights. The data protection group of Heriot Watt University adapt the European 1998 Act of data protection as basement of university systems design to determine the data and information permissions, authorization to maximize the data protecting performance. The data protection group of Heriot Watt University mentioned that the systems programming, settings and tools should reflect the data protection acts to be compatible with county laws to define the rights and penalties of data privacy issues; there are four important things need to clarify to ensure the efficiency of university services and high data protection performance which are:

1. Know what information the University holds and processes about them and why.
2. Know how to gain access to it.
3. Know how to keep it up to date.
4. Know what the University is doing to comply with its obligations under the 1998 Act.

Thus, there are 3 main sides control the performance data protection;

1. Staff and students awareness and responsibilities to protect their data.
2. The country should provide responsible data protection acts and support the university to execute the acts penalties formally.
3. Apply the acts rules and contents through privacy settings and security applications of university systems.

The main aim of the personal data protection projects in the universities is to maximize the awareness of employees' and students skills and knowledge of personal data protection processing and using. Thus, the universities adapt the personal data protection acts in their countries to reflect it on the systematic procedures in the universities environments which maximize the performance of data protection procedures and clarify these procedure and processes for employees' to allow them to protect their personal information effectively.

8. Online Data Protection

Online social services have increased rapidly and the user of social networks has expanded [23]. Thus, one of the most important issues of online social services is providing personal data privacy. As analyzed by [23], the personal data protection criteria in the privacy policies of 60 sites that provide social services; the main objective of his study was to analyze whether the social services sites have systematic procedures in place to ensure personal data protection based on their privacy policies, and to enhance the technical processes of these organizations to maximize the performance of personal data protection within social networks. Moreover, [23] classified the privacy features of these privacy policies as main privacy features and warning features, and compared the privacy settings of the social networks systems. The researchers found that there are many social sites that do not have clear privacy policies; there was a large gap between the privacy policies and the systematic applications. For example, many sites used third party applications and links to complete their services. It was determined that many collected data forms were insecure and there were static identifier variables to collect personal information.

As studied by [24], they found that 22% of 1360 social networks collect personal information from their users without providing alerts about data privacy; the researchers mentioned that the privacy alerts and notices maximize the users' awareness of personal data protection and initiate trust channels between users' and online sites.

In 2005 [25] founded that 30% of surveyed social network users had no awareness of using privacy tools and settings of online social sites to protect their personal information. In 2007 [26] surveyed the employees of 300 corporations in the European Union to analyze the personal skills and behaviors of users of personal data protection. The researcher's results showed that 66% of respondents provide real personal information to unknown services, such as third party applications, and the employees create online account passwords that relate with their real personal data and information, which minimizes the efficiency of online personal data protection. In 2011 [27] found that most problems associated with personal data protection are due to the weakness of the users' skills when using the privacy settings provided by online services. In 2007 [28] found in their survey research that American teens put a variety of information on their profiles, but the most common items are their first names (82%) and pictures of themselves (79%). In addition, 66% include pictures of friends, 61% include the name of their cities or towns, and 29% post their last names and include videos. [29] Found comparable results in Belgium, except that they found a higher amount of posted videos (37%) and last names (46%).

In 2012 [30] focuses on protecting the personal data of children that use online services; the main study problem they encountered was that children have not enough experiences and skills to protect their data privacy. Thus, the children may bring many risks to their families and themselves by providing personal information through online services. The main objective of [30] is to produce personal data protection procedures to help parents support their children's data privacy; the researchers analyzed the behaviors and interests of children using online services by surveying European children between 6-17 years; the data analysis showed that the children use online services for many purposes, such as online games, education, watching video clips, and for social communications. They also found that children use the Internet from many places, such as home, schools and libraries.

Moreover, it has been found that Internet availability allows children to use online services anywhere and anytime, and the problem of verifying age on online services allows children to accesses any service as an adult [30]. Thus, parents represent the most effective method in which to manage and control their children's online activities in order to protect their children's personal data and ensure that their children are following the online services' privacy policies.

According to the research discussed above, there are two main aspects of online data privacy:

1-Users' awareness of privacy, which represents the users' skills and knowledge to manage their online activities in order to protect their personal data from being breached and prevent the online services from using and processing the personal data of users without known and responsible procedures.
2-The systematic procedures of online services that are needed to protect the users' personal data, which represents the country's privacy acts that the online services belong to.

9. Conclusion

Personal data protection act is the standard rule to define the employee's or individual's personal data protection rights. Therefore, individuals have the right to protect their personal data privacy based upon PDPA. Many countries, like the UK and USA, implemented this acts to manage and control the huge volume of gathered information and information disclosed. This paper briefly reviewed the PDPA issues and the privacy and security aspect as well as the PDPA implementations. The most effecting factor on the PDP among the individuals or organization's employees is the awareness. Awareness will give a good understanding about the PDPA and help people to understand their rights and the penalties from breaching the rules.

References

[1] National Library of New Zealand Cataloguing-in-Publication Data (NZLC). (2009). Invasion of privacy: penalties and remedies: review of the law of privacy: stage 3. (Issues paper 14), New Zealand Law Commission, ISBN 978-1-877316-67-8.
[2] Sager.M. (2000). What I've Learned: Andy Grove. Chairman of Intel, 63, Santa Clara, California. Retrieved from: www.esquire.com.
[3] EUROPEAN COMMISSION. (2010) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. Brussels, COM (2010) 609 final.
[4] William.D & White.A, (2002). The Impact of Computer Security Regulation on American Companies, 8 Tex. Wesleyan L. Rev. 505;
[5] Madden, M., 2012. Privacy management on social media sites. Project of Pew Research Center.
[6] LAWS OF MALAYSIA, Act 709, PERSONAL DATA PROTECTION ACT 2010.
[7] Motorola, I., 2010. The User Role in Information Security, US: Motorola, Inc.
[8] Schuler, D., 1994. Social Computing. Social Computing special edition of the Communications of the ACM, 37(1).
[9] CMOD. (2008). Protecting the confidentiality of Personal Data. Guidance Note. Department of Finance. Ireland Government.
[10] Lin, Tom C. W., (2009). Undressing the CEO: Disclosing Private, Material Matters of Public Company Executives. 11 University of Pennsylvania Journal of Business Law 383. Available at SSRN: http://ssrn.com/abstract=2040940.
[11] Lin, Tom C. W., (2012). Executive Trade Secrets 87 Notre Dame Law Review 911. Available at SSRN: http://ssrn.com/abstract=2047462.
[12] Solove, Daniel J., Rotenberg, Marc, Schwartz, Paul M.. (2006). Privacy, Information, and Technology, Aspen Publ. pp. 9-11.
[13] Kosta, E. a. D. J., (2008). Searching the man behind the tag: privacy implications of RFID technology. International Journal of Intellectual Property Management (IJIPM), Issue Special Issue on: "Identity, Privacy and New Technologies".
[14] Cranor L., G. P. a. A. M., 2006. User Interfaces for Privacy Agents. CM Transactions on Computer-Human Interaction, 13(2).
[15] Anderson.A. (2005). Effective Management of Information Security and Privacy. Educause Quarterly Vol(1).
[16] William.D & White.A, (2002). The Impact of Computer Security Regulation on American Companies, 8 Tex. Wesleyan L. Rev. 505;
[17] Zaidi.K, (2003). Harmonizing U.S.-EU Online Privacy Law: Toward a U.S. Comprehensive Regime For the Protection of Personal Data, 12 Mich.St. J. Int'l L. 169
[18] Foth, M., C. Schusterschitz, et al. (2012). "Technology acceptance as an influencing factor of hospital employees' compliance with data-protection standards in Germany." Journal of Public Health **20**(3): 253-268.
[19] Tan, S. (2012). "Privacy Scofflaws Beware: Increasing Fines in the United Kingdom and Europe."
[20] ULSTER. (2012). DATA PROTECTION POLICY Framework. UNIVERSITY OF ULSTER. UK. Founded online: www.ulster.ac.uk (dataprotection/data_protection_policy.pdf)
[21] Hertfordshire. (2012). General Policy Statement GPS4: Data Protection Policy. University of Hertfordshire .Higher Education Corporation. UK founded online: sitem.herts.ac.uk/secreg/upr/pdf/IM08-Data%20Protection-v05.0.pdf
[22] Brown.D. (1999). DATA PROTECTION ACT 1998 THE UNIVERSITY'S DATA PROTECTION POLICY. Data Protection Office. Heriot Watt University.
[23] Kuzma.J. (2011). Empirical Study of Privacy Issues among Social Networking Sites. University of Worcester, UK.
[24] Birnhack.M and Elkin-Koren.N. (2011). Does Law Matter Online? Empirical Evidence on Privacy Law Compliance.
[25] Gross.R. (2005). Information Revelation and Privacy in Online Social Networks (The Facebook case). roceedings of the 2005 ACM workshop on Privacy in the electronic society.
[26] Herley.F. (2007). A large-scale study of Web password habits. USA, Sixteenth International Conference on the World Wide Web.
[27] Livingstone.S. (2011). Risks and Safety on the Internet: The Perspective of European Children. London, LSE: EU Kids Online.
[28] Madden.A. (2007). Teens, Privacy & Online Social Networks, USA: PEW Project.
[29] Paulussen.S. (2010). Adolescents' New Media Literacy in Flanders (Belgium). Observatorio, 4(4).
[30] OECD. (2012). the Protection of Children Online: Recommendation of the OECD COUNCIL. Report retrieved from: www.oecd.org