UNIVERSITY OF GHANA

DATA PROTECTION AND ELECTRONIC HUMAN RESOURCE SYSTEMS (E-HRS): A CASE STUDY OF VALLEY VIEW UNIVERSITY, OYIBI-GHANA

BY

JULIET YEBOAH ASANTE

10442142

THIS THESIS/DISSERTATION IS SUBMITTED TO THE UNIVERSITY OF GHANA, LEGON IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF MPHIL HUMAN RESOURCE DEGREE

AUGUST, 2016

DECLARATION

I do hereby declare that this work is the result of my own research and has not been presented by anyone for any academic award in this or any other university. All references used in the work have been fully acknowledged.

I bear sole responsibility for any shortcomings.

…… ……..

Juliet Yeboah Asante Date

(10442142)

DEDICATION

I dedicate this work to the Almighty God for giving me the strength, wisdom and knowledge to do it. I doubted if I could really make it but He has made it possible by showing He is still in control.

My next dedication goes to my dear mother, Millicent Atuobua Annor, whose efforts have brought me this far. Mama, I say ayekoo and God bless you.

Also, this work is being dedicated to my little angel, Eliette Yeboaa.

This work is again being dedicated to Emmanuel Odai Laryea, Believe Quarcoo, Dorcas Kyeiwa Asante and Albert Amankwah who supported me through diverse ways to ensure the success of this work.

CERTIFICATION

I hereby certify that this thesis was supervised in accordance with procedures laid down by the University.

…… ……

Dr. Olivia Anku-Tsede Date

(Supervisor)

ACKNOWLEDGEMENT

I am indebted to the Almighty God, who cannot be compensated for His gift of Wisdom, Intelligence, Knowledge and Understanding.

I register my overwhelming gratitude to my supervisor, Dr. (Mrs.) Olivia Anku-Tsede for her interest, patience, suggestions, total commitment and dedication during the supervision of this work.

Special thanks also go to all my respondents who have helped to make this research authentic. Without them I would not have arrived at my findings.

I again acknowledge the help and contributions of all the Staff in the OHRM Department of UGBS.

TABLE OF CONTENTS

Content **Page**

LIST OF TABLES

Table **Page**

LIST OF ABBREVIATIONS

DTA – Data Protection Act

E-HR – Electronic Human Resource

E-HRM – Electronic Human Resource Management

E-HRS - Electronic Human Resource Systems

ERP – Enterprise Resource Planning

HR – Human Resource(s)

SAP – Systems Applications and Products

VVU – Valley View University

Data Controller – the body that ensures that the personal data collected from individuals or organisations are secured.

Data Processor – One who collects data of another with the intention of rendering some services to the latter.

Data Subject – Any individual or organisation who provides personal data to another in order to receive some services.

HR staff – those staff whose work involves HR activities. They may work indirectly with the HR department.

Senior Staff – Employees who have spent five (5) years or more at VVU and are non HR staff.

ABSTRACT

The study sought to ascertain the extent to which Valley View University (VVU) has complied with the Data Protection Act (DPA) since the implementation of the E-HRS at the University. This case study sampled a total of thirty employees from diverse functional units of the University. The aim was to evaluate respondents' acceptability, knowledge and understanding of E-HRS issues relating to the DPA, security issues in the DPA and adherence to such security issues. Findings revealed that, most of the employees were aware of the existence of the E-HRS and that its implementation has ensured the safety of employee records. On E-HRS related issues, a significant majority admitted that the DPA provides strict guidelines for ensuring confidentiality of information on the E-HRS whereas few observed the Act sets modalities to be followed in unfortunate circumstances when data is processed by unauthorized persons. On security issues presented in the DPA, many remarked that data controllers are to adopt measures to prevent the loss of, damage to or unauthorized destruction and unlawful access to personal data. Data controllers have the obligation to notify the data protection commission in all instances of breach or suspicion of breach by third parties of confidential data. Finally, there is adherence to some security issues by the University and interestingly, a significant majority expressed optimism that their information is kept confidential hence they trust the professionalism of the HR. Immediate and regular training of the workforce on the use and benefits of E-HRS is strongly recommended. To strengthen confidence, forestall data and other HR function-related grievances, and to enhance the working knowledge of security issues presented in the Act, copies of the DPA must also be made available to staff and other employees of the University.

CHAPTER ONE

INTRODUCTION

1.0 Background of the Study

In today's 21st century, organisations have resorted to the use of technology in order to enhance the effective management of its human resources as a measure to sustain competitive advantage (Cowham, 2008). Electronic Human Resource Management Systems (E-HRS) encompass a set of interacting human resource aspects that are powered by software to integrate the human resource function and dwells on web-based technologies to enhance human resource management practices (Ruël & Bondarouk, 2004; Van der Velde, 2006). According to Voermans and Veldhoven (2007), the combination of the need to work more efficiently as well as the possibilities of getting access to current information and communication technology, have resulted in the swift development of Electronic Human Resource Management Systems that are expected to facilitate a more efficient and strategic way of working for HR professionals.

Electronic Human Resource Management Systems (E-HRS) are used to deliver training, manage the performance of employees as well as administer compensation and benefit systems (Gueutal & Stone, 2005; Strohmeier, 2007). E-HRS also enhances the efficiency of HR processes by reducing administrative costs and transaction times in the recruitment and selection process (Gueutal & Stone, 2005). For instance, most organisations in their quest to overcome the challenges coupled with the traditional way of processing resumes have resorted to scanning technology (Baker, Smart & DeTienne, 1998). Guffey (2007) opines that, the scanning software has the capability of scanning an incoming resume with Optical Character

Recognition (OCR) which looks for keywords to achieve a match between applicants' qualifications and job requirements.

More advanced scanning software enable recruiting staff to search for keywords, rank resumes based on the number of matches or "hits," and generate reports based on those "hits" (Guffey, 2007). Once resumes are scanned, then data can be stored in the database for six months to a year. This enables organisations to track their application history and know their turnover easily, enabling administration to take quicker decisions affecting their recruitment processes as well as know whether there is the need to develop the workforce they already have in meeting the requirement of work (Guffey, 2007).

In as much as Electronic Human Resource Management Systems (E-HRS) are important to the effective management of human resource, it is noteworthy to emphasize that, data protection of employees at the workplace cannot be disregarded. According to Victor (2013), data protection is the right to privacy that people have against possible unauthorized use of personal information by a data processor and that data protection ensures that the privacy of employees is duly protected to avoid the misuse of their personal data. Victor (2013) continues his argument by taking the stance that, data protection is expedient because it allows employees to know who and for what purposes their personal data are processed and can object to its improper use. He adds that, employees can ensure control over personal data by objecting to its usage once they have been obtained by a processor or a third party.

Data protection involves a range of new individual rights designed to protect consumers whose personal information is collected, processed, and stored by corporations and other entities, which establish a consumer's "right to be forgotten" (Victor, 2013). This means the

consumer's data collected at any point in time by organisations, should be done away with and not be reproduced without express permission of that owner or as ordered by law.

The Data Protection Act (DPA) is one influencing factor in the adoption of E-HRS. This is because there are issues that need to be addressed in the electronic format of documents that should still comply with human resource standards. The implementation of the DPA, in this electronic age however presents some inherent challenges that make it difficult to observe all the requirements of the Act. Sampson (2013) puts these requirements in eight (8) principles in which she states that the data controller has a statutory duty to ensure that personal data are:

1. Processed fairly and lawfully
2. Processed only for specified and lawful purpose(s)
3. Adequate, relevant and not excessive
4. Accurate and kept up-to-date
5. Not kept longer than necessary
6. Respectful of data subjects' rights
7. Kept secure by technical/organisational means
8. Transferred outside Ghana using required secured means

These principles can be summarized to affect the perception of people with regards to E-HRS, implementation of the DPA, compliance and how effective the law is.

In Ghana, the Data Protection Act, 2012, (Act 843) mandates the appointment of a Data Registrar whose duty is to ensure the privacy of individuals by applying the principles of accountability, lawfulness of processing, specification of purpose, compatibility of further processing with the purpose of collection, quality of information, openness, data security

safeguards and data subject participation. Notwithstanding the duty of the Data Registrar in ensuring privacy of individuals through the Data Protection Act, the significance of E-HRS in data processing of employees cannot be relegated to the background. In this regard, organisations are expected to act in the interest of its employees whose data they process by ensuring that it is in compliance with the Data Protection Act (Act 843).

Against this background, this study seeks to gain empirical evidence as to whether the implementation of E-HRS at Valley View University ensures data protection of employees by complying to the dictates of the Data Protection Act (Act 843).

1.1 Problem Statement

This study seeks to unearth how data protection of employees at the Valley View University (VVU) has been in compliance with the Data Protection Act since the implementation of Electronic Human Resource Management Systems (E-HRS) at the University.

The implementation and application of E-HRS over the last decade has been plausible because of the rapid development of the internet. Research suggests that the number of organisations adopting E-HRS and the depth of applications within organisations are continually increasing. For instance, academic interest in E-HRS has increased since HR-related journals have deliberated on special issues about the phenomenon (Townsend & Bennett, 2003; Viswesvaran, 2003; Stanton & Coovert, 2004, Crestone, 2005).

Anderson (2003); Lievens & Harris (2003); Welsh, Wanberg, Brown, & Simmering (2003), argue that, results of studies about E-HRS remain unclear since such researches stem from several disciplines and are scattered throughout numerous journals. However, literature on E-

HRS suggests that cost reduction, improving HR services as well as strategic orientation improvement are the three key goals of E-HRS (Rue¨l et al., 2004; Stanton & Coovert, 2004). It is also worth noting that, some scholars observed that these goals are not clearly defined in practice, and that E-HRS is mostly directed towards cost reductions and increased efficiency in HR services rather than aiming to improve strategic orientation of Human Resource Management (Gardner et al., 2003; Rue¨l et al. 2004; Ruta, 2005).

Other evidence suggests that, in many organisations, E-HRS led to radical redistribution of the work that HR managers used to do, and that many of the reporting-type activities, previously performed by HR professionals, can now be performed on-line by managers and employees (Rue¨l et al., 2004; Ruta, 2005). On their own desktops, line managers nowadays perform appraisals, evaluate employee costs, generate HR reports (turnover, absenteeism, etc.), process training requests and oversee competence management. Employees have access to everything they need to change and manage their personal files, plan their development, process financial documents and apply for new jobs (Roehling et al., 2005).

It is clear that few studies have looked at the issue of data protection in organisations so long as E-HRS has been implemented. In Ghana, the Data Protection Act was established by Parliament which authorizes the Data Protection Commission to protect the privacy of the individual and personal data by regulating the processing of personal information to provide the process to obtain, hold, use or disclose personal information and for related matters (DPA, 2012). According to the Act, the Data Protection Commission shall implement and monitor compliance with the provisions of the Act; make the administrative arrangements it considers appropriate for the discharge of its duties; investigate any complaint under the Act and

determine the manner the Commission considers fair; and keep and maintain the Data Protection Register (DPA, 2012). The establishment of a Data Protection Commission depicts the importance of ensuring confidentiality of personal data especially in the public domain. As technology increases and Human Resource Management continues to evolve, this may be seen as a proactive measure in ensuring information which may now be easily obtained and can be processed easily, is available to the right people and used for the right purposes.

The Data Protection Act further advances that a data processor or a person who processes personal data on behalf of a data controller shall process the data only with the prior knowledge or authorization of the data controller and treat the personal data which comes to the knowledge of the data processor or the other person as confidential. A data processor or a person who processes personal data on behalf of a data controller shall not disclose the data unless required by law or in the course of the discharge of a duty (DPA, 2012). With the knowledge of what this Act demands and requires, organisations must put up structures to ensure they are in compliance with the Act. Confidential treatment of all personal information that comes to the institution must be ensured. Within the organization, a data processor and/or controller should be identified, who can be tasked with ensuring the provisions of the Act with respect to personal information, are well enforced. Without such responsibility being defined for an individual, the Act may seem a vague policy with no clear-cut guidelines for the organization to enforce. At large, all employees should be given an orientation on the Act to make all keep in tune with its provisions.

Electronic Human Resource Management Systems (E-HRS) has been implemented at the Valley View University since 2014. Although its implementation has improved Human

Resource Management practices such as recruitment and selection, performance appraisal, as well as training and development, it is still unknown whether data protection of employees has been ensured or not.

1.2 Research Objectives

The principal aim of the study is to investigate the extent to which data protection has been ensured at the Valley View University (VVU) since the implementation of Electronic Human Resource Management Systems (E-HRS). Specifically, the study seeks to achieve following;

1. Determine the acceptability of E-HRS by employees of Valley View University.
2. Explore the knowledge and understanding of employees of Valley View University on E-HRS related issues and the entire Data Protection Act.
3. Investigate the extent of adherence to security issues in the Data Protection Act at Valley View University.
4. Examine further possible concerns and security issues the Data Protection Act presents to employees of Valley View University.

1.3 Research Questions

1. To what extent is E-HRS accepted by employees of Valley View University?
2. How do employees understand E-HRS related issues and the entire Data Protection Act?
3. To what extent do employees of Valley View University adhere to the security issues presented in the Data Protection Act?
4. Does the Data Protection Act present further concerns and security issues to the employees of Valley View University?

1.4 Significance of the Study

The significance of the study cuts across two spectrums namely; research and policy. In terms of research, the study seeks to add to the body of knowledge existing on Electronic Human Resource Management Systems and Data Protection among organisations. This is because the researcher observes that, there is paucity of research on issues regarding the efficiency of E-HRS and Data Protection in organisations. The findings will therefore contribute immensely by providing empirical evidence on issues concerning E-HRS and Data Protection from a Ghanaian perspective. With regard to policy, the study seeks to provide management of organisations much insight on issues concerning E-HRS and Data protection. In this regard, management would be better informed in coming up with policies that seek to enhance effective implementation of Electronic Human Resource Systems (E-HRS) and to also ensure the protection of employees through the adherence to the Data Protection Act.

1.5 Scope and Organisation of the Study

The study seeks to unearth how Valley View University has complied with the Data Protection Act since the implementation of E-HRS. The study is however limited in scope to Valley View University thus, the generalization of the findings needs to be trodden with caution. The study is organized in five chapters. The first chapter focused on the background of the study, the research problem, the research objectives, and research questions, significance of the study, the scope and organisation of the study. The second chapter comprises the review of literature on both the theoretical and empirical works in relation to E-HRS and Data Protection. Chapter three of the study constitutes a detailed method of how the study was conducted which includes the research design, population, sample and sampling techniques, instrumentation, data, ethical considerations and data analysis. Chapter four deals

with the results and follows with a discussion of the findings. The final chapter presents the summary, conclusions and recommendations of the study, as well as directions for further studies.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter reviews literature including the theoretical foundations of the study. It explores the overview of E-HRS, the functions and advantages of E-HRS, and the structure of E-HR Systems. It also examines the factors affecting the adoption and implementation of E-HRS. The chapter further explores the data protection laws in certain parts of the world in comparison to the Data Protection Act of Ghana, among others.

2.1 An Overview of Electronic Human Resource System (E-HRS)

The knowledge-intensifying process of this current economy as well as the rise in organisational networks, with their greater dependency on qualified and committed employees, requires a form of HRM that meets the demands and needs of the management and the employees. The rapid development of the Internet during the last decade has also boosted the implementation and application of Electronic Human Resource Management. Surveys of HR consultants suggest that both the number of organisations adopting E-HRM and the depth of applications within the organisations are continually increasing (Swaroop, 2012).

2.2 Definition of E-HRS

The term e-HR was first used in the 1990's and refers to conducting Human Resource Management transactions using the internet or an intranet (Lengnick-Hall & Moritz, 2003). This internet based transactions aim at making information readily accessible to managers and employees anytime and anywhere. Currently, an e-HR system may include enterprise resource

planning software (ERP), HR service centers, interactive voice response, manager and employee portals and web applications. Therefore, a modern e-HR system permits employees to control their own personal information by updating records and making decisions, and allows managers to access information and data, conduct analyses, make decisions and interconnect with others, without consulting the HR department.

According to Zafar (2012), in today's technological organisational environment, the need for Electronic Human Resource Systems (E-HRS) has become imperative to meet the HR challenges of the 21st century. Hence, organisations have increasingly been introducing web-based applications for HR purposes, and these are frequently labeled as Electronic Human Resource Systems (E-HRS) (Swaroop, 2012). This definition by Swaroop emphasizes the web-based nature of the HR systems.

Dusmanescu and Bradic-Martinovic (2011) also provide a vivid explanation of the structure of E-HRS and define them as, systems of databases that allow users to store and track all types of data that are related to human capital in the company. This definition lays an emphasis on the database nature of the HR systems. In operationalizing the definitions of E-HRS for the purpose of any study, there should be an observation of the fact that, as posited by Kavanagh and Morgan (2009), E-HRS includes systems and processes that connect the function of HRM and information technology.

2.3 Evolution of E-HRS

Kavanagh and Morgan (2009) argue that, in order for HRM to be effective, it must be in the position to enhance competitive advantage through the provision of adequate and updated information of current employees and prospective employees who are found in the labour

market. They continue their argument by saying that, the Information Technology (IT) evolution to a greater extent has improved the technique of collecting employee data through the development and implementation of E-HRS among organisations. E-HRS therefore includes systems and processes that connect the function of HRM and information technology. It is being augmented that, organisations often choose to introduce this information system after the successful implementation of ERP (Enterprise Resource Planning) and CRM (Customer Relationship Management) solutions, aiming to improve the processes associated with making decisions about employees. In this regard, information technology has enabled the broad implementation of E-HRS applications and helps companies to improve efficiency in general by increasing the efficiency of HRM (Nuasair & Parsa, 2007). However, some experts of E-HRS point out that, the modern HR function is not merely reduced to administrative procedures in the processes of recruitment, organizing the employees, regulating their rights and obligations, but also has a major role in creating corporate culture (Vujovic, 2005).

Other researchers in the 1980's indicated that apart from daily and operational information, E-HRS has the ability to supply strategic information management of the company and that, data collected within the E-HRS provide a mechanism for management decision support. Therefore, with appropriate E-HRS, companies are able to provide calculations that will have consequences for the entire business. These calculations include the following: health care costs per employee, turnover rates and costs, the time required to fill in the appropriate position, return on invested capital in HR and increase in the value of human capital (De Sanctis, 1986).

Numerous studies have offered evidence supporting the recognition of the role of E-HRS in support of strategic decision making. For this reason, there has been a dramatic increase in the use of E-HRS in companies over time. For instance, Lower and Mohrman (2001) reported that the use of E-HRS is in constant increase over the years. Obviously, the use of E-HRS solutions raised sustainable development, even in those companies where HR management does not have a strategic role. Vujovic (2005) further argues that modern business requires intensive use of knowledge based on a multidisciplinary approach, while education should provide the acquisition of new skills, such as finding relevant information, encouraging creative thinking, effective communication, teamwork etc.

Employees were regarded and accepted as human capital from the period of 1945-1960 (Hendrickson, 2003). However, that did not lead to the substantial changes in the functioning of the E-HRS (at that time information systems had existed and operated without the use of modern information technology). In the next twenty years (1960-80) HR departments had become an integral part of the core activities in the company. During this period, computers (mainly mainframe) provided a new dimension in collecting, storing and processing HR information. At that time HR departments had become one of the most important users of computers in companies. Despite that, E-HRS were only useful in transactional information processing. Hendrickson (2003) continues that the new period started in the last twenty years of the 20th century when computers became available to many users (with commercial use of the Internet) and when companies started to use HR information for strategic management. Management started to rely on E-HRS in the decision making process about human capital, even in small and medium enterprises. In this regard, E-HRS became an integrated system with the objective to provide information for decision making on human resources. The base

of their functioning are databases that are used for collecting, storing, searching and controlling data on employees and other data related to human resources. Typical E-HRS includes personal information about employees, information on income, information on various types of training, the most diverse reports etc. (Hendrickson, 2003).

E-HRS are developed based on the needs of HR departments or company management. Changes that have taken place in the role of HR in the company also reflect in the development of E-HRS. According to Dainty, Loosemore and Lingard (2003), the role of HR had three stages: the phase of personnel or staff management, the phase of HRM and the phase of strategic HRM. The phase of personnel or staff management was focused on various forms of services in the HR departments. Those departments had to collect and store personal data (records) of each employee, handle their salaries, benefits, vacations among others. In the next phase, when it became clear that the importance of HR is greater, personnel management became HRM. Since then, its function developed and became a very important function of management and hence an important indicator for competitive advantage. The last stage introduced a strategic component in HRM which can be defined as the development and implementation of human strategies that are integrated within a company's strategy ensuring that the culture, values and company's structure together with the quality, motivation and commitment of employees fully contribute to achievement of the company's objectives. In this stage, the level of integration in the processes of HRM is much higher, than in the previous stages (Dainty, Loosemore & Lingard, 2003).

Following the above, Hendrickson (2003) explained that the E-HRS achieved new dimensions with the development of computer networks. By then, only trained employees, mainly from

the HR departments could perform operations in separated computers or in mainframes, through a local network of terminals. However, the sudden expansion of networks and falling prices of computers enabled everyone to become part of the system, no matter where they are. Under the new conditions each employee can use the E-HRS but their level of use is determined by their need and permissions granted. With network expansion, structure of the E-HRS becomes significantly more complex, and new problems appear, primarily related to security and privacy of information about employees.

E-HRS, like other information systems must be flexible and adaptable to changes. They have to follow the development of the organisation in order to satisfy all existing and new needs. On the other hand, if the company does not follow trends in the field of information and communication technology, it can have problems with effective E-HRS (obsolete or unfit to the company needs). Consequently, it affects the overall business, especially in large enterprises with complex organisational structure (Hendrickson, 2003).

2.4 Forms of E-HRS

Two forms/levels of e-HR have been identified (Lengnick-Hall & Moritz, 2003; Walker, 2001), depending on the primary focus of e-HR. The first type has to do with publishing of information and it involves a one-way communication from the company to employees or managers. The intranet is used as the primary information delivery medium in this type of E-HRS. The second type has to do with the automation of transactions with integration of workflow. In this type of E-HRS, paperwork is completely replaced by an electronic input. In this regard, both intranets and extranets are used and they frequently combine several distinct application programmes.

2.5 The Structure of E-HRS

Dusmanescu and Bradic-Martinovic (2011) provide a vivid explanation of the structure of E-HRS as well as the different modules that make up an E-HRS and also the importance of the modules to the effective management of employee data. According to them, E-HRS applications are systems of databases that allow users to store and track all types of data that are related to human capital in the company. It is necessary to pay attention to the fact that in practice, a company can buy partial software solutions, which only partially cover the needs of HRM (for example, just a collection of basic information about employees and payroll). According to Dusmanescu et al (2011), these systems cannot be classified as E-HRS because under the term of systems, complex and comprehensive software with all integrated functions for HRM are implied. To the scholars, only properly implemented systems that permeate the entire company will have maximum positive impact. In fact, these are systems that are used to collect, store, manipulate, analyze, retrieve and disseminate HR information

Dusmanescu and Bradic-Martinovic (2011) further observed that individual E-HRS software solutions differ according to the need of the company that developed a specific application. The solutions offered by software companies can be generally divided into three groups. The first group represents modules for HRM as part of ERP systems (for instance SAP HRMS, as one of the biggest module of SAP R/36 system). The second group represents the integral software solutions which merge different modules for computerization of HRM, i.e. integral E-HRS. The third group includes partial software packages that cover only one function. This group of software is a much simpler and relatively cheap solution for small companies that do not require all modules or solutions for those companies which consider it necessary to automate and improve only certain segments of HR. Regardless of the group to which they

belong, all of these solutions are the parts, i.e. modules that are integrated into the E-HRS in one company. In most cases, E-HRS contain all or most of the following modules:

The first module, according to Dusmanescu and Bradic-Martinovic (2011) is the collection and monitoring of applications for employment or online recruiting, which is an application that allows candidates to apply for a certain position in the company, but also for HR department to collect and process the received applications. In this module of E-HRS the using of computer systems and networks are very important, especially because of online accesses to the system. Online collection of application has become a standard in developed countries. After collecting applications, the company accesses to the next level using the E-HRS module. This includes support for the following activities: generating reports with statistics about labour market in the country, monitoring of interviews and the score assigned by the staff responsible for their evaluation, monitoring of job descriptions, keeping internal statistics on employees, auto-tracking and analysis of profiles of candidates, creating a list of e-mails, making online remarks etc.

The next module is record keeping of all personal data and it is an application which has a database with data of all employees. It is very important for each company to have these data, and in most cases data must be standardized. For instance, if a company needs information on whether an employee has a certificate for particular type of work and if the company has 7000 employees, only a search of standardized records can be effective. This module usually includes data for regular and emergency contact with the employee, data on all previously received wages (wage history), data on absenteeism from work, trainings and certificates, estimates the characteristics of employees, information on possible disciplinary action,

injuries at work, and data that companies can define by itself, unless they are part of a standard software package. In addition to these data, it is possible to store scanned documents (education diplomas, birth certificates, judgments, etc.)

Furthermore, the payroll module automates the pay process by collecting data on employee time and attendance, calculating various deductions and taxes, and generating periodic pay cheques and employee tax reports. According to Dusmanescu and his colleague, this module is often not fully part of the E-HRS, because it is heavily integrated into the system for financial management of the company. However, the financial management system cannot work without necessary input of the payroll data on time spent at work, absences, performances or regulatory compliances (Dusmanescu & Bradic-Martinovic, 2011). In addition to the payroll module, benefits administration provides administration of employee participation in various forms of benefits. All employees must be aware of their rights and obligations. The most important activities are included not only in pension plans, buying life insurance policies, but also in the distribution of shares of the company or division of profits. Dusmanescu et al (2011) remarked that the primary function of this module is to monitor all benefit programs and to notice any potential deficiencies. The advantage of online access is very important in this module. The fastest and cheapest way to maintain the beneficiary database is ability of online access to the data by the employees.

Thereafter, the training module and learning management systems provides a system for organisations to administer and track employee training and development efforts. Companies can buy this module on the software market as a separate solution. The most important functions of this module are tracking the education level of employees, their qualifications

and / or skills. It allows storing and displaying various types of courses, books, staff or materials that are suitable for web learning. Online learning and testing of employees is a remarkable savings in time and money, and provides a high flexibility on the part of employees (Dusmanescu & Bradic-Martinovic, 2011).

Besides, Dusmanescu et al (2011) emphasized that performance management is very important for each company because continuous monitoring and evaluation are essential when a company makes conclusions about effectiveness of E-HRS. It is also important to realize whether the objectives are met and which segment should improve. The goal of this process is not criticism but insight in potential updates and upgrades of the system. This module contains features for monitoring system performances, which provides valuable information for the management of the company (Dusmanescu & Bradic-Martinovic, 2011).

After performance has been managed, employees need to take control of their own affairs, with HRM support. Employee Self-Service in modern environment is a module based on web technology which allows employees, together with professionals in HR department to manage the employee's database. With the right permission they can access their data with read-only or change status. Depending on the exact solutions data access can be provided within Intranet (safety is increased) or through the Internet (in which case the company has greater availability of data). These applications are usually used with standard Internet browsers, such as Internet Explorer or Firefox (Dusmanescu & Bradic-Martinovic, 2011).

In addition to these modules which cover the basic functions of any E-HRS, there are still a number of solutions. These include modules with corporate documents such as instructions for the various programs for employees, HR planning module which include the analysis of

previous employment policy, documents about employee's database development, assessment tasks and jobs and the implementation of various satisfaction survey of employees in the company. Selection of software solution depends on the company's management and its decision. This situation also involves the possibility of internal development, acquisition of complete solutions (outsourcing) or renting the resources, i.e. cloud computing. Regardless of the choice, management must assess their needs and thus choose a software solution that will have the highest level of utilization. It is equally wrong to choose software that has too many options, which will never be used or does not possess the necessary options. Decision on E-HRS choice must be taken as a strategic decision.

2.6 Functions of E-HRS

E-HRS can have an impact on every area of HRM. The functions of E-HRS as identified in literature include: HR planning; acquiring HR (recruitment and selection); HR evaluation (performance appraisal); communication; rewarding HR (performance appraisal, compensation and benefits); and developing HR (training and development, career management) (Ensher *et al*., 2002).

For HR planning, E-HRS, particularly through the functions of employee and manager self-service applications, has brought substantial progress in terms of employee data updates, personnel changes and job requisitions. This means that, since employees are given the opportunity to update their personal data, the HR record-keeping gains higher accuracy and data quality (Zampetti & Adamson, 2001). The same goes for personnel changes and job requisitions that are submitted by managers to the HR through manager self-service applications.

In the acquisition of human resources, the practice of online recruitment is one of the most widely discussed functions of E-HRS. Online recruitment refers to posting vacancies on the corporate web site or on an online recruitment vendor's website, and allowing applicants to send their resumes electronically via e-mail or in some electronic format (Galanaki, 2002). It also includes the active search of the internet and the location of resumes. This possibility of online recruitment has been much debated as a unique way to recruit passive job seekers. Furthermore, online recruitment brings substantial benefits in terms of cost, time, candidate pool and quality of response.

To evaluate human resources, E-HRS allows the whole performance appraisal (PA) to be conducted on-line, on the corporate internet interface. This means that the manager and the employee are able to submit performance data directly to the HR department in electronic form. This practice reduces paperwork and if read receipts for both supervisor and supervised are used, it can impressively decrease time and cost for the HR department. The self-service application allows managers to immediately enter PA results and employees to manage their performance goals and results and plan their performance on their personal HR page. It can also provide managers with information on how to conduct a PA, the specific criteria and measurements of given positions and roles as well as examples and models of effective appraisals (Adamson & Zampetti, 2001).

The benefits of E-HRS use in terms of communication are substantial. In its simplest form, E-HRS includes the use of electronic mail for communication with the employee. The penetration rate of computer-mediated communication, mainly e-mail, is higher than 75 percent in corporate environments and e-mail has emerged as the communication medium of

choice (Bontis *et al*., 2003). Intranet and e-forums have also altered corporate communication, allowing easy access to all kinds of information that management wants to transmit to employees and also easing upward communication.

When it comes to rewarding human resources, employee self-service allows employees to submit electronically their preferences in terms of benefit selection, reducing the burden for the HR department. Experience has shown that after the implementation of a self-service employee benefits system, employees may still be calling with benefit questions, confused about their choices and unable to grasp a broader rewards perspective (Dietch, 2001). However, it is believed that web-delivered employee benefits, if properly implemented, entail considerable economies for the HR department. Moreover, manager self-service allows the manager to take on or confirm salary actions, salary changes, bonuses and stock management. The application usually notifies managers on the choice they need to make or verify rewards of their subordinates and asks them to insert their decision.

When it comes to developing human resources, using the internet in training and development is one of the mostly discussed aspects of E-HRS and probably the one with the most potential in terms of cost benefits. The internet can be used in training needs assessment, in pure e-learning activity and in career management. The e-mail and electronic forms on the intranet of the company or a restricted web site are used to gather information on training needs assessment, inducing benefits in terms of less paperwork, lower administration cost, shorter distribution and response time, and higher response rate (McClelland, 1994). E-learning includes any learning activity supported by information and communication technologies. It can take the form of either local intranet provision, delivered over a network of interconnected

computers, or of full access to internet and the World Wide Web, drawing upon a full range of multimedia or links to other sites and resources, downloadable streaming videos and communication systems (Sambrook, 2003). E-learning can offer a solution to training in remote or disadvantaged locations (Hirschman, 2001), as well as tailor-made learning that fits the particular needs of the learner but it can also create barriers to learning, due to lack of hardware, fear of technology and learner isolation.

2.7 Advantages of Using E-HRS

Companies, regardless of their size can recognize the benefits of E-HRS, and implement software packages, in order to improve the efficiency of the entire organisation. E-HRS advantages can be systematized according to (Kovach, *et. al*., 2002) as follows:

It increases competitiveness by improving the operational transactions in the HR department; it has the ability to implement a number of different operations related to HR; can shift the focus from the operational (transaction) HR information to strategic HR information; and include employees as an active part of the E-HRS as well as Re-engineering the entire HR department. However, Kovach *et al* (2002) and other authors such as Beadles *et al* (2005) observed that all E-HRS advantages can be grouped under three dimensions which include the benefits for the management, the benefits for the HR department and benefits for employees.

Benefits of E-HRS to the management include: Increase of overall decision making efficiency, cost reducing and better control of budget, business transparency, a clear business vision and a clear insight into the process of hiring and firing employees, at the aggregate level.

Benefits of E-HRS to the HR Department include the fact that the department can possess a single database of all employees in the company with all necessary information and opportunities for different reports. There is also ability to update databases in real time, on the basis of all changes, which is of extreme importance to regionally diversified companies; elimination of paper forms that are much slower and with much higher probability of errors. The following benefits also hold true: minimize errors caused by human factor; employees in HR department do not have to constantly refer to the instructions on working hours, because the application is configured according to existing guidelines, which have reduced delays and uncertainties; improved management system in accordance with the legislation; reduction or elimination of redundancy in the system; standardization of business processes; highly reliable data in the system, whether it is external or internal threats; increased employee satisfaction in HR department because the easiest and efficient execution of the tasks; ability to establish full control over internal migration of employees and the management of their talents and the ability to take preventive measures to avoid unpleasant situations in the company.

Benefits of E-HRS to Employees include: the possibility of independent access to data, which often means working in one software window; Saving time (for example, if the employee wishes a day off the simplest wait is to fill the online form available as an option of the E-HRS and wait for approval by superiors); automatic tracking and reminder to the business obligations and events; encouraging employees to make decisions and initiatives on the basis of information obtained in the E-HRS system (for example, workers can monitor the internal competition for jobs and thus to advance in your company); data availability all the time; reducing the time required for desired information, which are available in the system; the

ability to attend internal training courses via the web and the development of personal skills and knowledge and also, increasing staff morale.

Besides all these advantages, there are a few shortcomings that need to be mentioned. First is the need of additional training of employees to enable them use self-service modules. It often is a problem when employees are to use new features provided by a system instead of keeping up with the methods they previously used. Secondly, employees in the HR department must attend several trainings to be able to use modules and to exploit all the options it provides. This problem is given special attention in companies, because without competent software users the company can miss a large number of advantages.

The last problem is connected with the process of replacing the old system with the new one. If the company chooses another producer or provider, the problem of incompatible data may arise or there will be possible danger to the security of the database. Because of privacy issues, the replacement process can be much longer comparing to other types of software integration. Regardless of the shortcomings connected with the implementation of E-HRS, the benefits provided by these systems are dominant.

2.8 Theoretical Foundation for E-HRS Adoption

The diffusion of innovation theory developed by Rogers (1983) was the most appropriate theory for the adoption of E-HRS in an organisation because of its focus to explain the flow of information, ideas, practices, products and services within and across organisations. Nonetheless, subsequent research provided empirical support for compatibility, relative advantage and complexity (Tornatzky & Klein, 1982). On the other hand, in the IT literature, one of the most prominent frameworks of IT (technological innovation) impact includes three

stages of use: automation, information and transformation (Remenyi & Twite, 1991). This framework of IT impact is developmental in that each stage but must be developed for the technology to be accessed or exploited. For this study, both theoretical perspectives were combined to better understand the influence of various perceived attributes of innovations on the extent of use of E-HRS system and the impacts of this E-HRS system usage. There have also been numerous studies on innovation, spanning many disciplines and focusing on both organisational and individual levels.

In his diffusion of innovation theory, Rogers (1983) proposed that innovation adoption is a process of uncertainty reduction and information gathering. Information about the existence of the innovation as well as about its characteristics and features flows through the social system within which adopters are situated. Potential adopters engage in information-seeking behaviors to learn about the expected consequences of using the innovation; and an assessment and evaluation of this information determines adoption behavior. Thus, communication channels and information processing by potential adopters play a central role in Roger's theory. The innovation diffusion theory further expounds that an individual's decision to adopt or not adopt a particular innovation is influenced by five key perceptions about the characteristics of the innovation: relative advantage, compatibility, complexity, trialability and observability. A short description of each of the constructs is presented below.

Rogers (2003) reviews relative advantages of E-HRS where he defines relative advantage as the degree to which an innovation is perceived to be better than the idea it supersedes. It can also be viewed as the degree to which an innovation is perceived to bring added benefits to the user. Hence, it is often measured in terms of economic profitability, productivity improvement

and other benefits. The nature of the innovation determines which specific types of relative advantage it brings to the end user. The adoption of an innovation depends on whether the expected benefits of an innovation match the demand of potential adopters. In the technology acceptance model (TAM) by Davis (1989), this particular attribute is referred to as perceived usefulness. In general, the relative advantage of an innovation as perceived by members of a social system is positively related to its rate of adoption.

Rogers (2003) further outlines the compatibility of E-HRS as the degree to which an innovation is perceived as consistent with the existing values, past experiences and needs of potential adopters. An idea that is more compatible with the existing values and norms is less uncertain to the potential adopters and hence fits more closely to an innovation that can be easily accepted by potential adopters into part of their lifestyle. An innovation can be compatible or incompatible with socio-cultural values and beliefs; previously introduced ideas; or client needs for the innovation. Besides, in acknowledging E-HRS as a complex issue, Rogers (2003) explains complexity as the degree to which an innovation is perceived as relatively difficult to understand and use. Any new idea may be classified on the complexity simplicity continuum. Some innovations are clear in their meaning to potential adopters whereas others are not. In the TAM model, this attribute is referred to as perceived ease of use.

According to Rogers (1983), trialability is the degree to which an innovation may be experimented with on a limited basis. New ideas that can be tried on an installment plan are generally adopted more rapidly than innovations that are not divisible. Some innovations are more difficult to divide for trial than others. The personal trying out of innovation is a way to

give meaning to innovation, to find out how it works under one's own interpretation. This trial is a means to dispel uncertainty about adopting an innovation. Finally, Rogers described visibility or observability as the degree to which the results of an innovation are visible to others. The results of some ideas are easily observed and communicated to others, whereas some innovations are difficult to observe or to describe to others. Rogers (2003) argues that the more visible an innovation (and its benefits), the greater the likelihood of adoption, simply because the gains from adoption will be more easily recognized.

2.9 Factors that Affect the Implementation of E-HRS

According to Stone, Stone-Romero and Lukaszewski (2003), there are four different factors which affect the implementation of E-HRS in organisations. These factors outlined by the authors include: information flows, social interaction pattern, perceived control of individuals and system acceptance. The four factors are discussed further in detail in this section of the literature review.

Information Flows: According to the authors, the use of E-HRS may change information flows. For instance, they may increase the organisation's ability to access, collect, and disseminate information about such factors as the nature of job openings, and the KSAs of individuals. In addition, such systems may provide individuals with rapid access to information about job openings, and the capacity to apply for jobs online (Stone, Stone-Romero & Lukaszewski, 2003).

Social Interaction: E-HRS may also modify social interaction patterns in organisations. In particular, such systems often substitute electronic communications for face-to-face interactions. As a result, they decrease the likelihood that employees will interact on a face-to

face basis with supervisors and other organisational members. These and other changes in social interactions may negatively affect the attainment of both individual and organisational goals. One reason for this is that employees often use face-to-face communication for such purposes as clarifying the requirements of their roles and coordinating their actions with those of other organisational members. As a consequence, E-HRS may decrease the degree to which individuals understand role requirements and behave in accordance with them. In addition, to the degree that face-to-face interactions are curtailed, there may be negative effects on trust levels between supervisors and subordinates (Cardy & Miller, 2005).

Perceived Control: One of the major purposes of E-HRS is controlling the behavior of individuals by ensuring that employees behave in ways that promote the achievement of organisational goals. However, because such systems limit the freedom of individuals, their use may evoke reactance and resistance in individuals (Stone & Stone, 1990; Stone et al., 2003). For instance, individuals may resist computerized performance management systems that keep track of such variables as the number of keystrokes or the amount of time spent on tasks. One way of doing so is to engage in rigid bureaucratic behavior (e.g., behave in ways that make them look good to the control system) or provide inaccurate data to the system (Stone & Stone, 1990). Unfortunately, the same behavior may have dysfunctional consequences for both individuals and organisations.

System Acceptance: The acceptance of E-HRS will be joint function of the nature of the systems and the attitudes, intentions, and behaviors of individuals who use them which include job applicants, employees, management, HR personnel etc. (Gueutal & Stone, 2005;

Stone-Romero, 2005). In this regard, individuals are unlikely to use such systems in intended ways if their attitudes about them are negative.

2.10 Regulatory Impact Assessment Works Involved in Data Protection

From the reviewed literature so far, it is noticed that there are three regulatory impact assessment works involved in Data Protection. These are the Data Regulator (Commission), the Regulated Group (Organisation/Institution) and the Consumer (Employee/potential employee).

The law establishes the Commission and gives it functions. The data commission is the regulator of data protection in any country. The data commission serves as the body which ensures that all organisations, institutions and individual bodies comply with data protection laws in the country in which they operate. In this regard, the data commission plays an integral part in the implementation of data protection laws in countries because they are obligated by the constitution to ensure that organisations, institutions and other bodies are in full compliance to all the clauses in the Data Protection Laws and hence put the organisations in check especially in instances when they violate the data protection laws.

The regulated group in data protection refers to the organisations, institutions and other bodies who employ the services of others. In this regard, such organisations, institution or bodies may need to collect data of the person or other organisations they are dealing with. This group is called the Regulated group because their activities are controlled by the Commission to ensure they comply with the regulations regarding the data being collected, especially, its safety and confidentiality. The HR department of organisations does serve as the data processors as they collect personal information from employees and potential employees and

ensure that such information is kept in safety either manually or through a computerized system like the E-HRS. The HR department also takes data from corporate bodies the organisation deals with. Hence ensuring security and confidentiality of the data collected is of upmost importance.

The consumer in data protection refers to the employees, potential employees, or other organisation whose services are hired by another. Such bodies are consumers since they are usually those to release/provide their data to another (legally referred to as data subjects). They release/provide personal data for the purpose of getting some services. They are required to provide accurate information about themselves in order to enhance the efficiency of record keeping in their respective organisations. Employees are also important actors in data protection issues because they provide the relevant information to the organisations for proper record keeping.

2.11 Sample Data Protection Laws of the World

In this section of the literature review, data protection laws of 6 countries (Argentina, Canada, China, Egypt, Spain and the United Kingdom) are assessed with emphasis placed on the collection and processing of personal data as well as security issues presented. These countries were randomly selected to represent the multi-state continents of the world.

In Argentina, data controllers may only collect and process personal data with the data subject's consent. Consent is not required if: the data is collected from a publicly accessible database, in the exercise of government duties, or as a result of a legal obligation, the database is limited to certain basic information, such as name, ID, tax ID, job, birthdate and address, the personal data derives from a scientific or professional contractual relationship and

is used only in such context, or the information is provided by financial institutions, provided that they were required to do so by a court, the Central Bank or a tax authority.

However, when collecting personal data, the data collector shall expressly and clearly inform data subjects of: the purpose for which the data is being collected, who may receive the data, the existence of a database, the identity of the data collector and its mailing address; the consequences of providing the data, of refusing to do so or of providing inaccurate information; and the data subject's access, rectification and suppression rights.

In addition, data contained in databases must be truthful, adequate, pertinent, and not excessive, be used exclusively for the purpose for which it was legally obtained and be deleted on completion of that purpose. Incomplete or partially or totally false data must be immediately amended or suppressed.

No person may be required to disclose personal sensitive data. Sensitive personal data may only be collected and processed in cases of public interest, as determined by law. Anonymized sensitive personal data may be collected for statistical or scientific purposes, so long as the data subjects are no longer identifiable. Data related to criminal history or background may only be collected by public authorities (DLA Piper Report, 2013).

With regards to security issues regarding data protection in Argentina, the data collector must take all technical and organisational measures necessary to ensure the security and confidentiality of personal data, so as to avoid its alteration, loss, or unauthorized access or treatment. Such measures must permit the data collector to detect intentional and unintentional breaches of information, whether the risks arise from human action or the technical means

used. It is prohibited to record personal data in databases which do not meet requirements of technical integrity and safety (DLA Piper Report, 2013).

In the case of Canada, the Canadian Privacy Statutes set out the overriding obligation that organisations only collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. Subject to certain limited exceptions prescribed in the Acts, consent is required for the collection, use and disclosure of personal information. Depending on the sensitivity of the personal information, consent may be opt-in or opt-out. Organisations must limit the collection of personal information to that which is necessary to fulfill the identified purposes and only retain such personal information for as long as necessary to fulfill the purposes for which it was collected.

Each of the Canadian Privacy Statutes have both notice and openness/transparency requirements. With respect to notice, organisations are generally required to identify the purposes for which personal information is collected at or before the time the information is collected. With respect to openness/transparency, generally Canadian Privacy Statutes require organisations make information about their personal information practices readily available. All Canadian Privacy Statutes contain obligations on organisations to ensure personal information in its records is accurate and complete, particularly where the information is used to make a decision about the individual to whom the information relates or if the information is likely to be disclosed to another organisation.

Each of the Canadian Privacy Statutes also provides individuals with (i) a right of access to personal information held by an organisation, subject to limited exceptions, and (ii) a right to correct inaccuracies in/update their personal information records.

Finally, organisations must have policies and practices in place that give effect to the requirements of the legislation and organisations must ensure that their employees are made aware of and trained with respect to such policies (DLA Piper Report, 2013).

When it comes to security issues in the protection of data in Canada, each of the Canadian Privacy Statutes contains safeguarding provisions designed to protect personal information. In essence, these provisions require organisations to take reasonable technical, physical and administrative measures to protect personal information against loss or theft, unauthorized access, disclosure, copying, use, modification or destruction. These laws do not generally mandate specific technical requirements for the safeguarding of personal information (DLA Piper Report, 2013).

In China however, provisions relating to personal data protection are found in various laws and regulations, but none of the provisions clearly define the scope of privacy rights. The main provisions are found in the General Principles of Civil Law and the Tort Liability Law, which define such rights as a right of reputation or right of privacy. A draft Personal Data Protection Law has been under review by the government for many years, but there is still no indication as to if and when such law will be passed. The Ministry of Information and Industry of China ("MIIT") has published draft guidelines called the Information Security Technology – Guide for Personal Information Protection ("Draft Guidelines").

On 28 December 2012, the decision on strengthening online information protection (the "Decision") was adopted by the Standing Committee of the National People's Congress (NPC). The purpose of the Decision is to protect internet information security, safeguard the

lawful rights and interests of citizens, legal entities or other organisations, and ensure national security and public interests (DLA Piper Report, 2013).

Under the Draft Guidelines, data controllers may collect and process personal data when the following conditions are met:

1. Laws and regulations explicitly authorize such collection or the data subject consents; and
2. The data controller has a specific, clear and reasonable purpose for doing so.

Before a data controller collects personal data, it should notify the data subject of the following: The purpose, the scope of use and collection methods related to the collecting of the personal data; the name, address and contact information of the data controller; the consequences of not providing the requested personal data; the rights of the data subject; and channels for submitting complaints. Data controllers are not allowed to collect personal data that has no direct relation with the stated purpose, and in particular data relating to race, religion, Deoxyribonucleic acid (DNA), fingerprints, physical condition or sex life. The data controller should process personal data for the stated purpose and within the scope that the data controller has notified to the data subject. The data controller should take measures to keep the collected personal data confidential during processing and storage of the data. If the data controller uses a third party to process the personal data, they should inform the data subject of this fact prior to collecting the data.

Under the decision, network service providers and other enterprises may collect and use citizen personal information when the following conditions are met: comply with the lawful,

reasonable, necessary principle; specify the purpose, method and scope regarding the collection and use of the citizen's personal information; the personal information subject consents; satisfy the requirements established by the laws, regulations and mutual agreement; and disclose the rules regarding collection and use (DLA Piper Report, 2013). However, under the Draft Guidelines, data controllers must take appropriate technical and organisational measures against unauthorized or unlawful processing and against accidental loss, destruction of, or damage to, personal data. The measures taken must ensure a level of security appropriate to the harm that may result from such unauthorized or unlawful processing, accidental loss, destruction or damage, and appropriate to the nature of the data (DLA Piper Report, 2013).

In Egypt, the country does not have a law which regulates protection of personal data. However, there are some piecemeal provisions in connection with data protection in different laws and regulations in Egypt. Constitutional principles concerning individuals' right to privacy under the Egyptian Constitution as well as general principles on compensation for unlawful acts under the Egyptian Civil Code govern the collection, use and processing of personal data. In addition, the Egyptian Penal Code no. 58/1937 imposes criminal punishment for unlawful collection of images or recordings for individuals in private places. Some other laws provide for protection and confidentiality on certain data, such as the Egyptian Labour Law no. 12/2003 (confidentiality of the employee's file information including punishment and assessment) and the Egyptian Banking Law no. 88/2003 (confidentiality of client and account information). Egyptian Civil Status Law no. 143/1994 provides for the confidentiality of citizens' civil status data. The Executive Regulations of Mortgage Finance Law no. 148/2001 issued by virtue of Cabinet Decree no. 1/2001 as amended by Prime Minister Decree no.

465/2005 has a similar clause which provides for the confidentiality of the data of the clients of mortgage finance companies. The Mentally Disordered Care Law no. 71/2009 has the same clause on confidentiality of the patient's data.

The New Constitution has been promulgated in December 2012 and has replaced all the previous Constitutional Declarations issued by the Armed Forces Supreme Council and the President of the Arab Republic of Egypt. Although the constitution has not defined data protection, it however refers to the legislative authority to regulate the communication of data in a manner that does not encroach upon the privacy of citizens, their rights and National Security (DLA Piper Report, 2013). According to the principles of the Egyptian Civil Code, the collection, use or processing of personal data is prohibited in case it violates the individual right to privacy and provided that such collection, use or processing constitutes a fault pursuant to the Egyptian Civil Code. A fault is defined by the judiciary as an act or omission that violates an obligation imposed by the law or assumed caution and care of the average man.

In fact, only data considered pertinent to the data subject's private life requires the consent of the data subject. The competent courts will determine whether specific data is considered pertinent to the private life of the data subject or not and whether the collection or processing of such data violates an obligation imposed by the law or assumed caution and care of the average man. Collecting data about the employee is required by law (Article 77 of the Egyptian Labour Law) which provides that each employer must keep a file for each employee, which is to contain their personal data. Only certain persons are authorized by the law to have access to such data (DLA Piper Report, 2013). With regard to security issues in data

protection, apart from client and account data in banks, personal data controllers are not required by law to take specific measures against unauthorized or unlawful processing, accidental loss or destruction of, or damage to, personal data. The data controllers will be held liable according to the average man standard if their acts or omissions cause the processing, loss, destruction or damage to such personal data and this in turn results in damage being caused to the data subject (DLA Piper Report, 2013).

In Spain however, data controllers may collect and process personal data when any of the following conditions are met: The first condition is that the data subject must give consent. After this, the data controller needs to process the data to enter into or carry out a contract or pre-contractual deal to which the data subject is a party so that the contract or deal can be maintained or executed. The third condition is that the data is collected from "public open sources" and the processing is necessary to satisfy a legitimate interest of the data controller or a third party receiving the data, provided that the constitutional basic rights of the data subject are preserved. Another condition is that the processing should protect the data controller's vital interests; or the processing is required by an enactment or to legitimately perform a public function in the public interest. As the fifth condition, where sensitive personal data is processed, one of the above conditions must be met plus one further condition from a separate list of more stringent conditions (explicit and written consent in the case of political, moral and religious beliefs and trade union membership or explicit consent from the data subject plus general interest grounds supported by a law, in the case of ethnic origin, health and sex life). Finally, whichever of the above conditions is relied upon, the data controller must provide the data subject with "fair processing information". This includes the existence of a database storing his/ her personal data, the identity and address of the data

controller, the purposes of processing, the consequences of supplying/refusing to supply the information, whether it is mandatory or not to supply the information requested, and how the data subject may exercise the rights of access, modification, cancellation and objection to the data (DLA Piper Report, 2013).

Moreover, with regard to security issues in data protection, data controllers and processors must take appropriate technical and organisational measures against unauthorized or unlawful access or processing and against accidental loss or destruction of, or damage to, personal data. The measures taken must ensure a level of security appropriate to the nature of the data. "Basic" security measures must be applied to all data, and include, inter alia, control of access to data by employees of the data controller. "Medium" security measures must be applied to data relating to financial services, public security, public tax matters or which may allow data controllers to profile a data subject in detail. These measures include, inter alia, the execution of privacy audits every two years and the appointment of a Head of Data Security. Databases containing sensitive information as well as data relating to gender violence, and police records) require "high" security measures, including, inter alia, tougher access control and data encryption when communicating the data (DLA Piper Report, 2013).

In the United Kingdom (UK), data controllers may collect and process personal data when any of the following conditions are met: Just like in Spain, the first condition is that the data subject must consent. Next, the data controller needs to process the data to enter into or carry out a contract to which the data subject is a party. As a third condition, the processing should satisfy the data controller's legal obligation. Fourthly, the processing should protect the data controller's vital interests and after that, the processing should have been required by an

enactment, the Crown or the government. Another condition is for the processing to be required to perform a public function in the public interest, or to administer justice; or the data controller has a legitimate reason for the processing, except if the processing would damage the data subject's rights, freedoms or other legitimate interests. The sixth is that where sensitive personal data is processed, one of the above conditions must be met plus one of a further list of more stringent conditions. Finally, whichever of the above conditions is relied upon, the data controller must provide the data subject with "fair processing information". This includes the identity of the data controller, the Purposes of processing and any other information needed under the circumstances to ensure that the processing is fair (DLA Piper Report, 2013).

However, with respect to security issues, data controllers must take appropriate technical and organisational measures against unauthorized or unlawful processing and against accidental loss or destruction of, or damage to, personal data. The measures taken must ensure a level of security appropriate to the harm that might result from such unauthorized or unlawful processing or accidental loss, destruction or damage as mentioned above, and appropriate to the nature of the data (DLA Piper Report, 2013).

2.12 Data Protection in Ghana

Ghana as a nation has limited literature when it comes to issues regarding data protection. The DPA, 2012, Act 843, is one of the few laws governing the country when it comes to issues related to data protection. The DPA, sections 17 through 31 covers the following areas: Privacy of the Individual, Consent, Justification and Objection, Collection of Personal Data, Collection of Data for Specific Purpose, Security Measures and Notification of Security

Compromises. Section 17 through 19 of the DPA talks of privacy of the individual whose data is being collected. It states that a person who is processing data should take into account the privacy of the individual by applying the principles of accountability. The data collector/processor should be able to indicate the purpose for which the data is being collected. Again, the data processor/collector should follow the laid down laws with regards to processing. The data being collected should be for the purpose for which it is specified. There should be compatibility of further processing with purpose of collection. The information being collected should not be just any information but must be of quality for its intended usage. The data collector should be opened to ensure the data subject knows the reason for which the data is being collected and the data subject must be opened enough to give the needed and required information. Thereafter, the data that has been collected must be securely safeguarded with both the data collector and data subject participating in the process. It is the duty of the data processor to ensure that the above principles have been followed.

Section 18 continues that a person who processes personal data shall ensure that the personal data is processed without infringing the privacy rights of the data subject. The data must go to where it is intended and also for its specified purpose. The personal data must be processed in a lawful manner without any offense against the data subject. The data should also be processed in a reasonable manner but not contrary to the legal procedures. It emphasizes that a data controller or processor shall in respect of foreign data subjects ensure that personal data is processed in compliance with data protection legislation of the foreign jurisdiction of that subject where personal data originating from that jurisdiction is sent to this country for processing. In cases of foreign subjects, knowledge of the foreign law should not be ignored.

This means that knowledge of both local and foreign laws are important aspects of the data processors duties.

Section 19 gives situations under which data may be processed. It states that personal data may only be processed if the purpose for which it is to be processed is necessary, relevant and not excessive. As far as protection of personal data is concerned, section 20 of the DPA expands on the consent, justification and objection required of a data processor. It states that all data must be processed with the prior consent of the data subject. Therefore, a person shall not process personal data without the prior consent of the data subject unless the purpose for which the personal data is processed is necessary for the purpose of a contract to which the data subject is a party. This pre suggests that once the data subject is a party to the contract there is the awareness that such data may be needed. Also, consent of the data subject may not be sought before processing data if the processing is authorized or required by law. The law will serve as the mandate for the data to be processed. When data is to be processed to protect a legitimate interest of the data subject, then the data subjects' consent may not be sought before the processing. In cases where it is necessary for the proper performance of a statutory duty or necessary to pursue the legitimate interest of the data controller or a third party to whom the data is supplied, the data subject's consent may again not be sought. Sub section (2) continues that unless otherwise provided by law, a data subject may object to the processing of personal data and sub section (3) adds that where a data subject objects to the processing of personal data, the person who processes the personal data shall stop the processing of the personal data.

Section 21 of the DPA deals with the collection of personal data. The section states that a person shall collect personal data directly from the data subject. However, personal data may be collected indirectly where the data is contained in a public record; which presumes that that data is already in the public domain. Where the data subject has deliberately made the data public, such data could also be collected indirectly without contacting the data subject. There are also cases where the data subject has consented to the collection of the information from another source, in such instance the data could be collected indirectly. The collection of the data from another source is not likely to prejudice a legitimate interest of the data subject and where the collection of the data from another source is necessary for the prevention, detection, investigation, prosecution or punishment of an offence or breach of law it could be collected indirectly. Data may again be collected indirectly for the enforcement of a law which imposes a pecuniary penalty; for the enforcement of a law which concerns revenue collection; for the conduct of proceedings before any court or tribunal that have commenced or are reasonably contemplated; for the protection of national security or for the protection of the interest of a responsible or third party to whom the information is supplied. Also where compliance would prejudice a lawful purpose for the collection or where compliance is not reasonably practicable, data could be collected indirectly.

Section 22 through 24 of the DPA states the requirements for collecting data for a specific purpose. It states that a data controller who collects personal data shall collect the data for a purpose which is specific. The data collector must always know the purpose for which data is being collected to enable specific collection. The purpose should also be explicitly defined and it should be lawful. Data being collected must be related to the functions or activity of the person. The sections continue that data subject is to be made aware of the purpose for

collection and must not be kept in the dark. Hence, a data controller/collector shall take the necessary steps to ensure that the data subject is aware of the exact purpose for the data being collected.

Furthermore, for the retention of records a data controller who records personal data shall not retain the personal data for a period longer than is necessary to achieve the purpose for which the data was collected and processed unless the retention of the record is required or authorized by law. Data should be discarded as soon as it intended need is over. The retention of the record is reasonably necessary for a lawful purpose related to a function or activity, the retention of the record is required by virtue of a contract between the parties to the contract or the data subject consents to the retention of the record. Further, Section 24 explains that the law does not apply to records of personal data retained for historical, statistical or research purposes. It continues that a person who retains records for historical, statistical or research purposes shall ensure that the records that contain the personal data are adequately protected against access or use for unauthorized purposes. Personal data in a record should therefore be separated from historical, statistical or research records.

Indeed, a person who uses a record of the personal data of a data subject to make a decision about the data subject shall retain the record for a period required or prescribed by law or a code of conduct. In cases where there is no law or code of conduct that provides for the retention period, then the record should be retained for a period which will afford the data subject an opportunity to request access to the record. Section 24 further statuses that a data controller shall destroy or delete a record of personal data or de-identify the record at the expiry of the retention period. There should be a complete destruction or deletion of a record

of personal data which shall be done in a manner that prevents its reconstruction in an intelligible form of any kind.

Section 28 through 30 also address security measures in data protection. These sections define whose responsibility it is to ensure that security measures are put in place. The sections indicate that a data controller is responsible for taking the necessary steps to secure the integrity of personal data in the possession or control of a person through the adoption of appropriate, reasonable, technical and organisational measures. The data controller must ensure these measures are in place to prevent loss of, damage to, or unauthorized destruction and unlawful access to or unauthorized processing of personal data. To ensure this is effective, the data controller shall take the necessary and reasonable measures to identify foreseeable internal and external risks to personal data under that person's possession or control. The data controller again establishes and maintains appropriate safeguards against the identified tasks. Once such measures are in place, the data controller regularly verifies that the safeguards are effectively implemented and ensures that the safeguards are continually updated in response to new risks or deficiencies. It is the responsibility of the data controller to observe and study generally accepted information security practices and procedure, and specific industry or professional rules and regulations.

Data is usually processed by a data controller but there are instances where data is processed by an authorized person. In the case where data is processed by an authorized person a data processor or a person who processes personal data on behalf of a data controller shall process the data only with the prior knowledge or authorization of the data controller, and treat the personal data which comes to the knowledge of the data processor or the other person as

confidential. The person processing data on behalf of another must ensure that the data processor has a prior knowledge of the issue. A data processor or a person who processes personal data on behalf of a data controller shall not disclose the data unless required by law, or in the course of the discharge of a duty. Confidentiality is the objective of data protection.

The data processor also has the obligation of complying with security measures in the DPA. It is the duty of the data controller whose work is to ensure compliance of the law, that the data processor acts in accordance with Section 30 of the Act which indicates that, a data controller shall ensure that a data processor who processes personal data for the data controller, establishes and complies with the security measures specified by this Act. From section 30 of the DPA, it is made clear that the data processor work for and on behalf of the data controller. Thus, the processing of personal data for a data controller by a data processor shall be governed by a written contract. In this wise, a contract between a data controller and a data processor shall require the data processor to establish and maintain the confidentiality and security measures necessary to ensure the integrity of the personal data. Section 30 of the DPA continues that where a data processor is not residing in this country, the data controller shall ensure that the data processor complies with the relevant laws of this country. This means the data processor would have to learn and understand what the law says in this country.

Section 31 of the DPA finally deals with the notification of security compromises. The section emphasizes that where there are reasonable grounds to believe that the personal data of a data subject has been accessed or acquired by an unauthorized person, the data controller or a third party who processes data under the authority of the data controller shall notify the

Commission and the data subject. This is because such bodies would be the first to be legally held responsible in the case of a compromised data of a data subject. The notification shall be made as soon as reasonably practicable after the discovery of the unauthorized access or acquisition of the data.

The data controller shall then take the necessary steps to ensure the restoration of the integrity of the information system and also inform the data subject of the issue at stake. Where the security agencies or the commission inform the data controller that the notification will obstruct a criminal investigation the data controller will have to delay notification to the data subject. Where there is breach of security to personal data, the notification to a data subject shall be communicated by registered mail to the last known residential or postal address of the data subject. Also, electronic mail would have to be sent to the last known electronic mail address of the data subject, then there shall be placement in a prominent position on the website of the responsible party. There would also be publication in the media or any other manner that the commission may direct. All these are to ensure that the data subject gets to know what is at stake. A notification shall provide sufficient information to allow the data subject to take protective measures against the consequences of unauthorized access or acquisition of the data. Only the needed and important information is to be posted through any of the means that would be used.

Section 31 of the DPA carries on that the information shall include, if known to the data controller, the identity of the unauthorized person who may have access or acquired the personal data. The data controller must give the full known identity of the unauthorized person. Should the commission have grounds to believe that publicity would protect a data

subject who is affected by the unauthorized access or acquisition of data, the commission reserves the right to direct the data to publicize in the specified manner.

2.13 Comparison of Data Protection Laws of Ghana and Other Countries

Comparing the data protection laws from other parts of the world including Argentina, Canada, China, U.K, Egypt and Spain to that of Ghana, it is observed that all these countries have legislations which govern data protection. Such a feature is similar to Ghana, where the Data Protection Act was instituted by an Act of Parliament in the year 2012. Despite the existence of these legislations, there are some differences in the kind of legislations that confer data protection in these countries. In China for instance, data protection laws and regulations were not clearly defined in the scope of privacy rights as main provision were only found in the principles of civil law and the Tort liability law. However, data protection laws in China are established in what they call the "Draft Guidelines" which was adopted in the year 2012 with the ultimate purpose of protecting internet information security, safeguard the lawful rights and interest of the citizenry and also make it incumbent on the part of legal entities and other organisations to ensure national security and public interests. In the case of Egypt, the country does not have a law which actually regulates the protection of personal data of citizens. However, Egypt makes use of constitutional principles which concerns the individual right to privacy which are under the Egyptian constitution and the Egyptian Civil Code.

Moreover, it is observed similar to Ghanaian data protection laws, all these other countries are very particular about the way and manner data is collected and processed. The similarity in the collection and processing dwells on the fact that, the data processor shall only collect relevant

information from persons after seeking their consent. Another similarity dwells on the premise that, data collection and processing is done by authorized persons who are supposed to ensure that data gathered is kept confidential and used for the purpose it is intended to be used for. However, some of the countries are different in terms of collection and processing of information. For instance, in the case of Canada, emphasis is placed on the sensitivity of the data to be processed. Thus, according to the Canadian Privacy Statutes, consent may be given for the collection and processing of data based on the sensitivity of the information to be given and that, the individual may decide to provide the information or not. Further, the Canadian data collection and processing is guided by the concepts of notices and transparency which are not found in the data collection and processing of the other countries including Ghana. In Canada, organisations are supposed to identify the purpose for which personal information is collected at or before the time the information is collected and that begets the notice concept. On the other hand, the Canadian Privacy Statutes obligates organisations to make information about their personal information management practices available to its regulators.

Finally, with regard to security issues, it is observed that the data protection laws of all the countries are similar to that of Ghana as they all stress that, data processors must ensure that data in their custody are not lost, damaged or unlawfully accessed by a third party. The security issues further stressed that data must not be lost or damaged due to human error or a technical problem from the system through which the data is stored.

CHAPTER THREE

METHODOLOGY

3.0 Introduction

This section outlines the method used in carrying out the study. It presents a description of the approaches and techniques that were used in assessing the implications of data protection and electronic human resource systems in human resource development at the Valley View University. The chapter covers the research design, population, sample and sampling techniques, instruments for data collection and data analysis.

3.1 Research Design

This study employed the case study approach, which employed qualitative methodology. The case study design was thus adopted in organizing the subjects for study. According to Baxter and Jack (2008) a case study provides an opportunity for the researcher to gain a deeper sense of the problem under study in order to facilitate an in-depth description, understanding and explanation of the phenomenon under study. A case study design should be considered when the focus of the study is to answer 'how' and 'why' questions of the phenomenon under study (Yin, 2009). According to Gerring (2004), a descriptive case study design is used when the researcher intends to describe the characteristics of the phenomenon in a particular context. The descriptive case study is therefore justified on the grounds that, the study seeks to give a detail description of how Electronic Human Resource Management Systems (E-HRS) are used in tertiary institutions, with particular focus on Valley View University. The study further seeks to make descriptive deductions on how Data Protection has been enhanced in the usage of E-HRS at the University. The choice of a descriptive design therefore provides an in-depth analysis of E-HRS and Data Protection by describing responses in logical and

qualitative manner. Pope and Mays (1995) emphasizes that, the goal of qualitative research is to develop concepts which help to understand social phenomena in accepted settings, giving due emphasis to the meanings, experiences, and views of all participants.

3.2 Population

The study population consists of all employees at Valley View University. The sampling frame consists of all major departments and functional units of the University. Thus, senior staff employees as well as all other permanent but not contract nor National Service personnel formed the study population. These senior staff employees have spent more years in the institution and could give required and needed information about their experiences on the implementation of E-HRS at the University. On the other hand, other category of employees especially those from HR department who have played active role in the implementation of the E-HRS and may have much information about the system were also included. It must be noted however that, since the workforce consists of both part-time and full-time employees, it was appropriate to recruit the study participants accordingly. The study was therefore narrowed and restricted to Valley View and not any other university because, the school was not only deemed to fully enroll on the E-HRS but essentially have an exploratory and tentative understanding of the phenomenon.

The researcher decided on a private university since it was anticipated that a private institution would be devoid of the stringent bureaucracies that are often prevalent in the public institutions. The Valley View University being the first accredited private university in Ghana started the implementation of E-HRS in August, 2014, just prior to the onset of this study. As a new comer to this electronic system, the University was selected by the researcher to gain

further insights into the system at the primary stage of its implementation. It was also the intention of the researcher to capture any unforeseen events which might occur in the implementation of the system during the course of this research study.

3.3 Sample and Sampling Techniques

Fraenkel and Wallen (2002) opined that there is no clear-cut answer to the question on a sample size. In their opinion, the best answer lies in the sample which can be as large as the researcher can rely on to obtain the needed data with affordable time and energy. They therefore recommend that researchers should endeavor to obtain a sample size that they can reasonably have and handle. Dwelling on the recommendation of Fraenkel and Wallen (2002), a sample of thirty (30) respondents were drawn from various departments and functional units to participate in the study. This involves an equal number of both senior (employees who have been in the university for five years and more) and junior staff (employees who have spent less than five years in the university) of the university. In drawing the sample, the non-probability purposive and convenience sampling techniques were used in the selection of the study respondents. Thus, although opportunity was limited to only employees expected to have the needed information, room was provided for only those available and willing to participate in the study. Thus, not all employees were given a known and equal chance to participate in the study.

3.4 Instrumentation

The instrument for data collection was structured interviews. The idea for using interviews was to obtain an in-depth, useful and relevant data, which answers the study objectives and the study questions. Since structured interview permits greater flexibility and limit

subjectivity and bias, it was adopted to allow the respondents to give answers in their own possible way. The guide was developed through existing studies and some existing indexes with peer reviews and discussions with the supervisor. The study measured the understanding and knowledge of employees on the data protection under the electronic human resource systems at Valley View University. The data was grouped under four main sections reflecting the study aims and objectives. This included acceptability of E-HRS by employees of Valley View University, knowledge and understanding of Valley View University employees on E-HRS related issues and the entire Data Protection Act, extent of adherence to security issues in the Data Protection Act at Valley View University and possible concerns and security issues the Data Protection Act presents to employees of Valley View University. The responses gained from the respondents were tape recorded and transcribed for analysis.

3.5 Data

Primary data was used for this study. The primary sources of data comprised information directly and orally gathered from the study participants at the Valley View University through interviews. During the process, the researcher was focused in the administration in order to achieve the set objectives of the study. To encourage participation, the items were concise and clear and took not more than 10 minutes for the respondents to answer the questions.

3.6 Ethical Considerations

Data collected from various respondents are deemed to be sensitive organisational data and as such was not made public against the wishes of respondents. Knowing that the study itself is about data protection, all efforts were made to keep the data confidential. Thus, ethics of anonymity and confidentiality were upheld with the collected data treated as aggregate and not units of analysis. Further, participation was strictly voluntary with no participant coerced

since the researcher was obliged to respect the right, dignity, and beliefs of the participating individuals. Besides, they were provided detailed information on the possible costs and benefits associated with their participation. Thus, consent of the participants was sought before they were enrolled onto the study. Finally, the ethics of beneficence was upheld. The principle requires the research to maximize possible benefits and minimize potential harms that might occur in the course of the investigation. The principle further requires the study to be useful to both participants and the society. Thus, the study was used as an advocacy tool to create interest and public awareness on the relevance of data protection under the electronic human resource systems and to suggest interventional measures to address some inherent consequences.

3.7 Data Analysis

The descriptive and thematic analyses were employed in analyzing the data obtained for the study. The techniques ensured the central and major themes were pulled from each unit of analysis and further used as aggregates using frequency distribution, mean scores and percentages in determining the proportion of respondents portraying various responses on the subject. These provided detailed and in-depth understanding of the variables. Facts were gathered from the interactions and observations were used in supporting the analyses based on which conclusions and recommendations are made. Tables, charts and graphs were used for graphical representation of facts and to ensure easy understanding of the analysis. The demographic characteristics measured constituted variables such as gender, marital status, current position, tenure (number of years spent in working at the university), etc.

3.8 Profile of Valley View University

Valley View University was established in 1979 by the West African Union Mission of Seventh-day Adventists (now Ghana Union Conference). In 1997 it was absorbed into the Adventist University system operated by the Africa-Indian Ocean Division (WAD) of Seventh-day Adventist with headquarters in Abidjan, Cote d'Ivoire. The Ghana Union Conference of Seventh-day Adventists (organized in 2000) serves as the local manager of the University. The University was initially called the Adventist Missionary College and was located at Bekwai-Ashanti. It was transferred to Adentan near Accra in 1983 where it operated in rented facilities until it was relocated to its present site near Oyibi (Mile 19 on the Accra-Dodowa Road) in 1989 and was renamed Valley View College. The Adventist Accrediting Association (AAA) has, since 1983, been evaluating and reviewing the accreditation status of the institution. In 1995, the university was affiliated to Griggs University in Silver Springs, Maryland, USA. This allowed the university to offer four-year bachelor's degrees in Theology and Religious Studies. The National Accreditation Board (Ghana) granted it national accreditation in 1997 thus allowing the university to award her own degrees. Thus, Valley View University became the first private institution in Ghana to be granted national accreditation. The university serves students from all over the world. It admits qualified students regardless of their religious background, provided such students accept the Christian principles and lifestyles of the university (Valley View University, 1997).

CHAPTER FOUR

RESULTS AND DISCUSSION OF FINDINGS

4.0 Introduction

This chapter presents the results and findings of the study. The first section presents the biographical sketch analysis whereas the second presents the descriptive outcome and analysis. This section includes the discussion where the main findings are discussed in the context of the literature. It further explores which findings are consistent with prior literature and which are inconsistent, adducing possible reasons accounting for such occurrences. In all, four study aims and objectives are discussed.

4.1 Demographic Profile of Respondents

This section deals with demographic characteristics of the sampled respondents. It presents information on the gender, age, marital status, academic qualification, department and employment status of respondents. It further deduces descriptive meaning with respect to how such characteristics account for variation in responses and associated meaning in understanding data protection under the electronic human resource systems in tertiary institutions.

Table 4.1.1: Demographic features of respondents

Variable		Frequency	Percent (%)
Gender	Male	13	43.33
	Female	17	56.67
	Total	30	100
Age	25 – 30	8	26.67
	31 – 35	4	13.33
	36 – 45	14	46.67
	Above 45	4	13.33
	Total	30	100
Marital Status	Single	11	36.67
	Married	19	63.33
	Total	30	100
Functional Units	Theology and Missions	2	6.67
	Computer Science	3	10.00
	Business Administration	8	26.67
	Nursing	2	6.67
	Human Resource	15	50.00
	Total	30	100
Level of Education	Graduates	20	66.67
	Postgraduates	10	33.33
	Total	30	100
Employment Status			
	Fulltime	22	73.33
	Part-time	8	26.67
	Total	30	100

Source: Field Data (2015)

From Table 4.1.1, majority of the respondents were females constituting 17 (56.67%) whereas males formed the minority comprising of 13 (43.33%) of the sample. With respect to age, it could be deduced that majority of the respondents 14 (46.67%) were between the age range of

36-45. A total of 8 (26.67%) were between the age range of 25-30 whereas a minimal 4 (13.33%) were each represented in the age groups of 31-35 and 46-55yrs. Thus, it may be concluded that most of the employees belong to the middle age group of 36-45yrs. It is further observed that majority of the respondents constituting 19 (63.33%) were married whereas the other 11 (36.67%) were single or unmarried. Thus, consistent with expectations, we can conclude that majority of the employees have been married. With respect to departments and functional domains, findings indicated that half of the respondents 15 (50%) were from the Human Resource department, 8 (26.67%) were from Business Administration (Accounting, Finance, Marketing), a total of 3 (10%) of the participants were sampled from the department of Computer Science whilst 2 (6.67%) were each from Nursing as well as Theology and Missions department. It is worthy to note that since the HR is responsible for managing data of employees, the study purposively sampled larger participants for the purposes of the depth and needed information. From Table 4.1.1, most of the respondents 20 (66.67%) were Graduates who have attained Master's degree in diverse educational disciplines whereas the other 10 (33.33%) have also attained other postgraduate qualifications beyond Master's degrees. Thus, twice as much of the postgraduate holders represented Master's degree qualifications in the total sample. Finally, it could be inferred from the Table that majority of the respondents constituting 22 (73.33%) were in full time employment whereas the other 8 (26.67%) of the respondents were part time employees of Valley View University. Thus, consistent with expectations most of the employees have been working with the organisation on full time basis.

4.2 Descriptive and Item Analyses

This section presents the descriptive and item analysis of the study. It presents the quantitative findings in frequencies and percentages whereas the qualitative data is presented using content analysis where central themes and ideas are pulled in quotes and italicizes. In all, four main study aims and objectives are discussed.

Table 4.2.1: Acceptability of Electronic Human Resource Systems

Acceptability of E-HRS	**Frequency**	**%**
Existence of E-HRS at VVU		
Respondents who accept	30	100
Respondents who do not accept	0	0
Total	30	100
General Opinion about the Implementation of E-HRS at VVU		
Smooth Implementation	10	33.33
Implementation with some difficulty	20	66.67
Total	30	100
Respondents who accept that the process was rolled out in phases with final implementation occurring after operational certification	30	100
Respondents against the same view	0	0
Total	30	100
How implementation of E-HRS has Ensured Protection of Clients' Data		
Implementation has ensured protection of client's data as the manual storage of files have been done away with	8	26.67
Implementation has ensured that employee data can only be accessed by the appropriate people.	6	20

Implementation has ensured that employee data is stored centrally in one safe location with access being granted to only the authorized officials.	6	20
Employee records are safe with the E-HRS	10	33.33
Total	30	100

Source: Field Data, 2015

Findings revealed that all the respondents (100%) were duly aware of the existence of Electronic Human Resource Systems (E-HRS) at Valley View University. With regard to the implementation however, 20 of the respondents representing 66.67% claimed that the implementation of E-HRS at the University was done with some difficulty. A total of 10 respondents, representing 33.33% attested that the implementation of the E-HRS was done with no hitches. In fact, all of the respondents (100%) admitted that the process was rolled out in phases with final implementation occurring after operational certification.

To further interrogate the extent to which the implementation of the E-HRS has ensured the protection of clients' data at the University, 8 of the respondents (26.67%) declared that the implementation of the E-HRS has ensured protection of clients' data. For them, the manual system of filing has been abolished hence not anyone could have access to the administrator part of the system, but only each employees level of access. Also, 6 of the respondents (20%) claimed that the implementation of the E-HRS has ensured that employee data can only be accessed by appropriate personnel. 6 of the respondents also representing 20% admitted that the implementation of the E-HRS has ensured central data storage in a database that can only be assessed by authorized personnel. Finally, the remaining the remaining 10 respondents, representing 33.33% were confident that employee records are safe with the E-HRS.

Knowledge and Understanding of Issues Presented in the DPA

Table 4.2.2: Knowledge about Data Protection Law

What is the Data Protection Act About	Frequency	%
Have no idea	4	13.33
The Act exists to safeguard data stored and processed in Ghana	11	36.67
The Act provides standard principles to be complied with	7	23.33
The Act was passed to bring some legal framework into the administration, processing and storage of data across the nation	5	16.67
The Act protects the privacy of the individual and personal data by regulating the processing of personal information	3	10
Total	30	100
Issues in Data Protection Presented that are Related to E-HRS		
Have no idea	4	13.33
It sets modalities to be followed in the unfortunate event where data is processed by unauthorized people on the E-HRS.	3	10
It sets timelines for the retention of records in the E-HR system	5	16.67
The DPA provides strict guidelines for the protection of the confidentiality of information on the E-HRS.	14	46.67
It prohibits the sale of information held on the E-HR System.	4	13.33
Total	30	100

Source: Field Data, 2015

Responses from Table 4.2.2 sought to explore employee knowledge on Data Protection Law in Ghana. It was not surprising to note that when respondents were asked of their knowledge about any data protection laws in Ghana, 4 (13.33%) of the respondents had no idea of the Data Protection Act. The remaining 26 (86.67%) seemed to have some knowledge about Data Protection Act as well as the issues presented in the Data Protection Act in Ghana. Out of the 26 respondents, a total of 11 (36.67%) intimated that the Act exists to safeguard data stored

and processed in Ghana, 7 (23.33%) believed the Act provides standard principles to be complied with by all who process personal information both within and outside the country. Whereas 5 (16.67%) were of the view that the Act was passed to bring some legal framework into the administration, processing and storage of data across the nation, an insignificant 3 (10%) on the contrary averred that the Act protects the privacy of the individual and personal data by regulating the processing of personal information. Indeed, respondents attested that because E-HRS is branded more as an HR system, other employees at the university do not interfere in anything related to the system.

Moreover, on issues in the Data Protection Presented that are related to E-HRS, as demonstrated in Table 4.2.2, 4 respondents (13.33%) had no idea of such issues. 3 (10%) of the respondents observed that the Act sets modalities to be followed in the unfortunate event where data is processed by unauthorized people on the E-HRS, 5 (16.67%) of the respondents indicated that the Act sets timelines for the retention of records in the E-HR system. Whereas an insignificant 4 (13.33%) of the respondents thought the Act prohibits the sale of information held on the E-HR System, a significant majority of 14 respondents representing 45.67% admitted that the DPA provides strict guidelines for the protection of the confidentiality of information on the E-HRS.

Table 4.2.3: Security Issues in the Data Protection Act

Responses	Freq.	%
Have no idea	4	13.33
The Act empowers the Data Protection Commission to enforce its statues by serving enforcement notices and fines to all non-compliant organisations thus reinforcing the need for absolute security of E-HRS systems.	4	13.33
Data providers must be informed of the purpose of the collection of their data and can either object or consent to the use of their data	3	10
Data controllers must adopt appropriate reasonable, technical and organisational measures to prevent the loss of, damage to, or unauthorized destruction and unlawful access of personal data.	11	36.67
It obligates all data controllers to notify the Data Protection Commission in all instances of breach or suspicion of breach by third parties of confidential data	5	16.67
A data controller is obligated by the law to take all necessary steps to secure the integrity of personal data in his possession or control.	3	10
Total	30	100

Source: Field Data, 2015

Table 4.2.3 presents data on the awareness of respondents on security issues presented in the Data Protection Act. From the Table, 4 (13.33%) of the respondents had no idea of the security issues in the Data Protection Act. This reflects the presentation in the previous paragraph as such respondents were not even aware of the Act, hence the issues presented in it. A significant 11 (36.67%) of the respondents underscored that one of the key security issues presented in the Data Protection Act was that data controllers are supposed to adopt appropriate, reasonable, technical and organisational measures to prevent the loss of, damage to or unauthorized destruction and unlawful access of personal data. 4 respondents (13.33%) knew the security issues presented in the E-HRS deals with empowering the Data Protection

Commission to enforce its statues by serving enforcement notices and fines to all non-compliant organisations thus reinforcing the need for absolute security of E-HRS systems. Besides, 5 respondents (16.67%) claimed that the security issues presented in the Data Protection Act gives obligation to all data controllers to notify the data protection commission in all instances of breach or suspicion of breach by third parties of confidential data. Interestingly, whilst 3 respondents (10%) claimed that, data providers must be duly informed of the purpose of the collection of their data and can either object or consent to the use of their data, the other 3 respondents (10%) claimed that, as a security measure in the Data Protection Act, the data controller is obligated by law to take all necessary procedures to secure the integrity of personal data that is in his possession or control.

Table 4.2.4: Further Security Concerns

Responses	Frequency	%
Adherence to Security Issues at VVU		
Yes	12	40
No, not all the issues	8	26.67
To some extent	6	20
Not Aware	4	13.33
Total	30	100
Issues presented in the Act		
Confidentiality of personal data	26	86.67
Not aware of any security issues	4	13.33
Total	30	100

Source: Field Data, 2015

With regard to adherence to security issues by Valley View University, Table 4.2.4 provides further security concerns. From the table 12 of the respondents representing (40%) attested that the university adhered to security issues presented in the Data Protection Act. Besides, whilst a significant 8 respondents representing (26.67%) claimed that there are still some security issues the university does not adhere to, a total of 6 respondents (20%) also shared similarly opinion that the University does not in fuller extent adhere to all security issues presented in the Data Protection Act. On the contrary, some respondents accounting for 4 (13.33%) seems to have no knowledge of security issues in the DPA. Regarding the concerns pertaining to the adherence of security issues in the Act, a significant 26 (86.67%) of the

respondents expressed optimism that their information is kept confidential by the Human Resource unit of the University and that they trust in their professionalism. However, 4 (13.33%) of the respondents could not indicate if they were aware of the security issues but based their confidence on trust.

4.3 Discussion of Findings

The study sought to discover issues related to Data Protection and Electronic Human Resource Management Systems (E-HRS) among employees of the Valley View University. The study specifically sought to ascertain the acceptability of E-HRS by employees of Valley View University, the Knowledge and Understanding of Valley View University employees on E-HRS related issues and the entire Data Protection Act, the extent of adherence to security issues in the Data Protection Act at Valley View University and possible concerns and security issues the Data Protection Act presents to employees of Valley View University.

It is observed that, even though E-HRS had been implemented at Valley View University, many although aware, were however ignorant about how the E-HRS works. It was also found especially among the senior staff that many could not determine the issues in the data protection law which were related to the Electronic Human Resource Systems. Further, many portrayed relatively less knowledge and awareness about the security issues presented in the Data Protection Act. However, it was interestingly discovered that many of the employees were optimistic that their data were kept confidential because of the trust they had in the HR of the university. Further investigations revealed that most of the employees especially from the HR department knew of the Data Protection Act and the issues presented in it. The employees were also aware of the issues related to the E-HRS. The results indicated that

employees from the HR department were much abreast with the security issues presented in the Data Protection Act and also attested that, Valley View University adhered to the security issues presented in the Data Protection Act.

4.3.1 Objective 1: Acceptability of E-HRS by Employees of Valley View University

Findings revealed that all the respondents were duly aware of the existence of Electronic Human Resource Systems (E-HRS) at Valley View University. With regard to the implementation however, 66.67% of the respondents for instance claimed that the implementation of E-HRS at the University was done with some difficulty whilst 33.33% attested that the implementation of the E-HRS was done with no hitches. All the respondents (100%) admitted that the process was rolled out in phases with final implementation occurring after operational certification. In essence, the acceptability of the E-HRS was largely found to be in congruence with literature. According to Zafar (2010), the technological organisational environment of today has made the use of E-HRS imperative to meet the HR challenges of the 21st Century.

In support to the findings, an employee observed;

> *"From my point of view, E-HRS was implemented smoothly in the university because the implementation had various phases which prepared the entire university community for the acceptance of the E-HRS as a better way of enhancing human resource development at the institution."*

Conversely, another employee remarked;

> *"I can testify that, the implementation of the E-HRS has enhanced my work positively as HR personnel. Before the implementation of the E-HRS, the processing and storage of information was done manually in files and it made work very difficult over here. But since the implementation of E-HRS, our*

> *workload especially in terms of processing and storage of employee data has been greatly minimized."*

This revelation affirms the findings of De Sanctis (1986) who addresses the issue of effectiveness and efficiency of staff in the E-HRS environment. According to him, apart from daily and operational information, E-HRS does not only have the capacity to supply strategic information to management but data collected within the E-HRS provides a mechanism for management decision support. De Sanctis (1986) further observed that, with suitable E-HRS, organisations are able to provide indicators including; health care costs per employee, turnover rates and costs, the time required to fill in the appropriate position, return on invested capital in HR and increase in the value of human capital, etc., that may have consequences for the entire business.

For instance, one of the respondents remarked;

> "*Well, for me I don't understand anything about that system. I only know that the HR people have been using it. But for someone like me, I don't have much insight about the entire system."*

> "*As I said earlier, that system is for the HR people and for me, as I sit here I don't know whether my information in that system is protected or not."*

This confirms the assertion of Swaroop (2012) and Hendrickson (2003) that the HR department has become the most important users of computers, hence, E-HRS in the century. Accordingly, Swaroop (2012) underscored that organisations have increasingly been introducing web-based Human Resource Systems (E-HRS) applications for HR purposes. He further mentioned that the rapid development of the internet during the last decade has not only boosted the implementation and application of Electronic Human Resource Management

but empirical findings suggest that both the number of organisations adopting E-HRM and the depth of applications within the organisations are continually increasing. Swaroop (2012) adds that organisations are adopting the use of E-HRS for HR purposes and as a result, surveys of HR consultants suggest that both the number of organisations and the depth of application of E-HRS within organisations are continually increasing. Dwelling on the literature, it could however be explained that, Valley View University which is the premier private university in Ghana has undergone rigorous expansion especially with regards to the variety of programmes that the school is currently offering. The university is also in the spree of expanding to other regions such as Ashanti and Brong-Ahafo which makes the work of the HR quite challenging hence the adoption of the E-HRS in the school.

4.3.2 Objective 2: Employees' Knowledge of E-HRS Related Issues and the Entire Data Protection Act

In seeking to understand the knowledge of employees on the Data Protection Law in Ghana, 26 (86.67%) of the respondents expressed some appreciable knowledge about the Act. The remaining 4 respondents (13.33%) however expressed pessimism about the existence of any data protection laws in Ghana. They seemed not to have much knowledge about the Data Protection Act as well as the issues presented in the Data Protection Act in Ghana. A total of 11 (36.67%) of the respondents intimated that the Act exists to safeguard data stored and processed in Ghana, 7 (23.335) of the respondents believed the Act provides standard principles to be complied with by all who process personal information both within and outside the country. In fact, most of the respondents attested that because E-HRS is branded more as an HR system, other employees at the university do not interfere in anything related to the system. On E-HRS related issues, 3 (10%) of the respondents for instance observed that

the Act sets modalities to be followed in the unfortunate event where data is being processed by unauthorized people on the E-HRS whilst 5 (16.670%) of the respondents indicated that the Act sets timelines for the retention of records in the E-HR system. A significant 14 (46.67%) of the respondents nonetheless admitted that the DPA provides strict guidelines for the protection of the confidentiality of information on the E-HRS.

Data Protection is a very important element in Human Resource Management. In Ghana, the Data Protection Act (Act 843) serves as a guideline to data regulators to apply the principles of accountability, lawfulness of processing, specification of purpose, compatibility of further processing with purpose of collection, quality of information, openness, data security safeguards and data subject participation (DPA, 2012; Act 843, Section 17). In this regard, while implementing E-HRS at Valley View University, it is incumbent on the HR department to provide employees an insight about Data Protection issues. However, the findings of the study proved otherwise, in the context that, staff at Valley View University are ignorant of the Data Protection Act. A respondent for instance intimated;

> "*Hmm, I have no idea about data protection laws in Ghana, in fact it could be because much awareness has not been created on it as compared to something like the Labour Act.*"

Another respondent opined that;

> *"Well, I have heard about the Data Protection Act, but I don't have much detail about the content of the Act."*

> *"I know about the Data Protection Act and I understand that, it contains the principles and standards which are supposed to be complied with by anyone*

entrusted with the authority to process information of employees in an organisation."

It is important to know that these remarks are contained in sections 22 through 24, which also addresses the requirement for collecting data for a specific purposes as well as sections 17 through 31 which indicate that consent of individuals or organisations should be given before their data is collected. The study speculates that employees of VVU do not give their personal data because they know of the law, but because it has become a norm. This gives the indication that because of the higher level of ignorance among the staff on issues related to Data Protection, when their data are being abused in any way, they may not have the potency to address their grievances. This shows a huge lapse in the implementation of the E-HRS at Valley View University.

According to Ensher et al (2002), the Electronic Human Resource Systems perform five key functions which include Human Resource Planning, Recruitment and Selection, Performance Appraisal, Compensation as well as Training and Development. In performing these functions by the HR through the use of E-HRS, personal information of employees is supposed to be protected. Thus, personal information of employees must not be made available to a third party without the consent of the employee. From the researcher's perspective, the use of the E-HRS must be able to ensure a higher level of confidentiality by constantly ensuring that, updated information into the E-HRS system are not released under any circumstance to a third party without the consent of the employee. In essence, two different employees revealed;

"We the staff from other departments do not interfere in any way with that system for the HR people."

> *"I do know that, the Data Protection Act is key in ensuring confidentiality of information processed in the E-HRS. That is to say that, if employee data is processed into the E-HRS, only authorized personnel are supposed to have access to the employee's data. No unauthorized person should ever be given access to employee's data without the consent of the employee."*

However, it is observed that staff of Valley View University are not aware that the issue of confidentiality which is key component of the Data Protection Act (DPA 2012; Act 843, sections 18, 19 & 20) is supposed to be given key precedence in the implementation of the Electronic Human Resource Systems (E-HRS) at the university. It could however be fairly argued that there is a huge loophole in the implementation of the E-HRS at the university. This revelation validates the findings of Lengnick-Hall and Moritz (2003) who averred that E-HRS permits employees to control their own personal information by updating records and making decisions, and allows managers to access information and data, conduct analyses, make decisions and interconnect with others, without consulting the HR department. However, the study reveals that senior staff use the system without knowing they are part of the users.

4.3.3 Objective 3: Adherence to Security Issues in the Data Protection Act at Valley View University.

In exploring the extent of adherence to security issues in the Data Protection Act, 4 (13.33%) of respondents had no idea of the security issues hence, the extent of adherence. A significant 11 (36.67%) of the respondents remarked that data controllers are supposed to adopt appropriate, reasonable, technical and organisational measures to prevent the loss of, damage to or unauthorized destruction and unlawful access of personal data. 4 (13.33%) of the respondents for instance expressed some considerable understanding of security issues

presented in the E-HRS that deal with empowering the Data Protection Commission to enforce its statues by serving enforcement notices and fines to all non-compliant organisations thus reinforcing the need for absolute security of E-HRS systems. Among others, 5 (16.67%) of the sampled workers affirmed that the security issues presented in the Data Protection Act gives obligation to all data controllers to notify the data protection commission in all instances of breach or suspicion of breach by third parties of confidential data. Moreover, in reference to the adherence to security issues, 12 (40%) of the respondents attested that the university adhered to security issues presented in the Data Protection Act. Besides, whilst a significant 8 (26.67%) of the respondents asserted that there are still some security issues the university does not adhere to, 4 (13.33%) on the contrary seems to have no knowledge of security issues in the DPA. When further asked about how the university ensured adherence to the security issues presented in the Data Protection Act, the respondents attested that, the university ensures that only authorized staff is given the administrative access to the E-HRS. However, minority of the respondents who claimed that the university did not adhere to all the security issues in the Data Protection Act explained that, there is the need for the university to become accountable to the staff in the use of their data in order to remove doubts concerning the security of their E-HRS.

It is imperative to note that the security issues in the Data Protection Act specifically upholds that, a data controller shall take the necessary steps to secure the integrity of personal data in the possession or control of a person through the adoption of appropriate, reasonable, technical and organisational measures to prevent loss of, damage to, or unauthorized destruction; and unlawful access to or unauthorized processing of personal data (DPA, 2012; Act 843, Section 28). However, findings revealed that employees of Valley View University

are not aware of such an important element in the Data Protection Act. It could however be fairly argued that, because staff are not aware of the security issues in the Data Protection Act, there is the higher tendency that, they will not be able to put the HR on its toes appropriately especially with regards to issues related to the protection of their personal data in the E-HRS.

A senior employee for instance indicated;

> *"Well, for security issues, I know that as a lecturer every information about me which is in the hands of the HR should not be disclosed to another person without my consent."*

This assertion support sections 17 through 31 of the Act. Moreover, it was found that, staff could only trust and hope that the HR was keeping their personal information confidential in the E-HRS. It is however vehemently argued that, dwelling on the importance of Data Protection Issues and E-HRS, employees are not supposed to be hopeful. This is because, the Data Protection Act clearly specifies that, the data controller is responsible for the processing of the personal information of employees. The data controller must further ensure that personal information of employees is not damaged or experience any kind of loss in anyway. These are issues that employees must be made aware of in order to put the HR on its toes in strict adherence to the security issues of the Data Protection Act (843).

In a related development, a senior employee remarked;

> *"In this university, the HR people are professionals and based on their high level of integrity, we believe that information about us which is on their system will be kept confidential."*

This assertion supports Nuasair and Parsa (2007) and Vujovic (2005) who buttressed the professionalism of HR personal in order to gain competitive advantage. To Nuasair and his colleague, information technology has enabled the broad implementation of E-HRS applications and helps companies to improve efficiency in general by increasing the efficiency of HRM. Vujovic (2005) further avowed that some E-HRS experts underscored the modern function of HR not merely reduced to traditional administrative procedures in the processes of recruitment, regulating their rights and obligations, etc., but also has an essential role in creating corporate culture.

In furtherance, a respondent emphasized;

> *"It is incumbent on the data controllers to ensure that the necessary measures are put in place to safeguard that employee data is not lost or damaged or assessed by a third party without the consent of the client or employee."*

This remarkable understanding is based on sections 28 to 30 of the Data Protection Act. Meanwhile, in enhancing security, another respondent emphasized;

> *"The security of employee data will be well enhanced if the data commission is much effective by ensuring that organisations which do not comply with the security issues of the Data Protection Act are sanctioned accordingly."*

The findings can further be discussed in relation to the diffusion innovation theory proposed by Rogers (1983). Specifically, the findings of the study are discussed in line with three components of the theory namely; relative advantage, compatibility and complexity. According to Rogers (1983), the adoption of a system is dependent on the perceived benefits that it will bring on its user and this is what he termed as relative advantage. However, applying this principle to the findings of the study, the researcher argues that, the

implementation of E-HRS at the Valley View University was adopted because of the perceived benefits that it seeks to bring in the effective management of its human resources especially in the context of data processing and storage.

On the other hand, with regard to compatibility, Rogers (1983) defines it as the degree to which an innovation is perceived to be consistent with existing values and past experiences and needs of its potential adopters. However, in relating the concept of compatibility to the findings of the study, the researcher augments that, there is a discrepancy between senior staff members and the HR staff. The ignorance of the senior staff could be explained based on the premise that, the E-HRS as a system is not in congruence with their values and past experiences. Thus the E-HRS is very new to them because they have not had any kind of encounters with such a system in their career as staff. However, it is possible that, the HR staff of the institution will be much abreast with the system because probably, they might have fore knowledge about the system and are likely to appreciate it more if they are able to practically use it in their work as HR professionals.

On the issue of complexity, Rogers (2003) defines it as the degree to which an innovation is perceived as difficult to understand and use. From the researchers' perspective, it is reasonable to argue that, the senior staff of the university are not committed to learning how the E-HRS works because of the preconceived idea about its complexity. However, the HR staff do understand how the system work because they are not perceiving the E-HRS as complex system but rather, they consider it as a system which has come to aid them in their delivery as HR professionals.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

This chapter provides the summary of the findings, the conclusion and key recommendations. The summary offers highlights of major findings whilst the conclusion provides detailed discussions where inferences and other extrapolations are drawn for industry and research.

5.1 Summary of Findings

This study sought to uncover the Data Protection and Electronic Human Resource Systems (E-HRS) issues of the Valley View University. The study however revealed that, staff of the University were duly aware of the existence of the E-HRS at the Valley View University. However, despite the existence of the E-HRS at the school, it was obvious that many employees do not have much insight about how the system works. Findings further revealed that most of the employees could not determine whether the implementation of the E-HRS at the school ensured data protection or not. With regard to knowledge of staff about the data protection law, it was discovered that many of the respondents were quite familiar with the Data Protection Act and the issues presented in it. Those who were unfamiliar with the Act attributed it to lack of awareness creation at the university. It was also revealed that many of the respondents were not aware of issues presented in the Data Protection Act that were related to the E-HRS. The study further showed that not all respondents were aware of the security issues presented in the Data Protection Act. However, with regard to adherence to security issues by Valley View University, the respondents were only hopeful that their data will be kept confidential through the use of the E-HRS.

On the other hand, whilst some were of the view that the implementation of the E-HRS was done smoothly, a few of them disagreed with such assertion. Many of the HR professionals emphasized that the implementation of the E-HRS has enhanced their work as professionals since the processing and storage of employee data have become easier and more secured. The HR professionals were not only aware of the Data Protection Act as the law which governs the way and manner personal information is supposed to be processed and stored in Ghana, but also some of the issues related to E-HRS. Those responses gave the impression that the key issues in the Data Protection Act that were presented in the E-HRS had to do with the confidentiality of employee data because, only authorized persons had access to employee data. Essentially, the security identified by the employees also had to do with ensuring the privacy and confidentiality of employee data. It was however not surprising that most of the employees remarked that Valley View University to a large extent adhered to security issues in the Data Protection Act because they ensured that only authorized persons had access to the E-HRS where the employee data are stored.

5.2 Conclusion

Improvement in technology and the increasing pace of life generally demands work processes to be improved and made more convenient and user-friendly for both employees and clients of the organization. The implementation of E-HRS at Valley View University is therefore an important step towards this direction, though it is coupled with loopholes which need to be addressed. From the researcher's perspective, awareness of employees about data protection and E-HRS issues are very instrumental in the implementation process. This is because it is only the foreknowledge of the employees about issues in the Data Protection Act, most especially the security issues that can make them put the data controllers on their toes. The

Act defines a data controller as a person who collects personal data for a purpose which is specific, explicitly defined, and lawful and is related to the functions of the person. The Human Resource Manager of the organization can be identified as such a person. Thus, knowledge of employees about the data security issues will make the data controllers feel obliged to adhere to the security issues in the Data Protection Act as they manage employee's data through the E-HRS.

5.3 Recommendations

Based on the findings, the researcher recommends the following:

First, the HR department of Valley View University must organize training for employees on how the Electronic Human Resource Systems (E-HRS) is used and its benefits to both the HR staff and employees as well. As most employees are aware of the system but are ignorant of how it works, the training session should aim at exposing employees to how the system operates. This will provide much insight to employees, for them to appreciate the usefulness of E-HRS in the performance of HR functions in the university. This education should not be limited to a particular group. Senior staff should be encouraged to participate so they can learn and be abreast with the issues in the Data Protection Act related to E-HRS.

Second, copies of the Data Protection Act must be made available to all employees of the university. It should not be assumed that they are aware of what is in the Act. Further, employees must be encouraged to read the Data Protection Act as it will enhance their knowledge on the issues presented in the Act, most especially the security issues. This is most important because, as employees get to know of the issues in the Data Protection Act, the HR

department will be put on their toes as employees could voice out their grievances because of the insight gained. Knowledge should not be limited to only employees of the HR department.

Last, the researcher recommends that, security issues regarding data protection should be well applied by the HR department as it uses the E-HRS in the performance of its HR functions. In this way, employees will gain much confidence in the HR and the system they are using to enhance their work (E-HRS).

5.4 Directions for Future Research

This study was concerned with Data Protection and Electronic Human Resource Systems issues at Valley View University. The study was able to access the acceptability of the system, knowledge of staff on Data Protection, Issues in the Data Protection that were related to E-HRS, Security issues in the Data Protection as well as Adherence to Security Issues in the Data Protection Act. However, future researchers can evaluate the attitude of employees towards the implementation of the E-HRS at Valley View University. Future researchers can also ascertain the effectiveness of the E-HRS in the eyes of the employees by finding out whether the E-HRS has been effective in remuneration and compensation, performance appraisal, training and development and other important HR functions.

REFERENCES

Adamson, L. & Zampetti, R. (2001), *Web-based manager self-service: adding value to the work*, in Walker, A. (Ed.), Web-Based Human Resources, McGraw-Hill, New York, NY, 24-35.

Anderson, N. (2003). Applicant and recruiter reactions to new technology in selection: A critical review and agenda for future research. *International Journal of Selection and Assessment*, 11 (2/3), 121-136.

Baker, W.H., DeTienne, K. & Smart, K. L. (1998). How Fortune 500 companies are using electronic resume management systems. *Business Communication Quarterly*, 61 (3), 8-19.

Baxter, P. & Jack, S. (2008). Qualitative case study methodology: Study design and Implementation for novice researchers. *The Qualitative Report*, 13 (4), 544-559.

Beadles, A., Lowery, C. & Johns, K. (2005). The Impact of Human Resource Information Systems: An Explarotary Study in the Public Sector. *Communications of the IMMA*, 5 (5).

Bontis, N., Fearon, M. & Hishon, M. (2003). The e-flow audit: an evaluation of knowledge flow within and outside a high-tech firm, *Journal of Knowledge Management*, 7 (1), 6-19.

Cardy, R. L., & Miller, J. S. (2005). *E-HRS and performance management: A consideration of positive potential and the dark side.* San Francisco: Jossey- Bass.

Cowham, C. (2008). The effect of individual factors on the transfer of human resource management knowledge in Chinese subsidiaries, the perspective of Chinese HR manager. *Journal of Technology Management in China*, 3 (2).

Crestone, C. (2005). *The Cedar Crestone. Workforce technologies and service delivery approaches survey*, 8th Annual Edition.

Data Protection Act 2012, (Act 843).

Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology, *MIS Quarterly*, 13 (3), 319-40.

De Sanctis, G. (1986). Human Resource Information Systems- A Current Assessment, *MIS Quarterly*, 10 (1).

Dietch, J. (2001). *Web-delivered employee benefits. From 'Why?' to 'Wow!'*, in Walker, A. (Ed.), Web-Based Human Resources, McGraw-Hill, New York, NY, 36-51.

DLA Piper Report (2013). Data Protection Laws of the World.

Ensher, E.A., Nielson, T.R. & Grant-Vallone, E. (2002). Tales from the hiring line: effects of the internet and technology on HR processes, *Organisational Dynamics*, 31 (3), 224-244.

Fraenkel, H. & Wallen, T. (2002). *How to design and evaluate research in education*. Boston: McGraw Hill Higher Education.

Galanaki, E. (2002). The decision to recruit online: a descriptive study, *Career Development International*, 7 (4), 243-251.

Gardner, D., Lepak, D.P. & Bartol, K.M. (2003). Virtual HR: The impact of information technology on the human resource professional. *Journal of Vocational Behaviour*. 63 (2), 159-179.

Gerring, J. (2004). What is a case study and what is it good for? *American Political Science Review*, 98 (2), 341-354.

Gueutal, H.G., & Stone, D.L. (Eds.). (2005). *The brave new world of eHR: Human resources management in the digital age San Francisco*, CA: Jossey-Bass.

Guffey, M.E. (2007). *Essentials of Business Communication*, 7th ed., Thomson South-Western, Mason, OH.

Hendrickson, A. (2003). Human Resource Information Systems: Backbone technology of contemporary human resources. *Journal of Labour Research*, XXIV (3).

Hirschman, C. (2001). Alternatives to business trips can pay off, available at: Workforce.com (accessed 23rd February, 2015).

Kavanagh, M. J. & Mohan, T. (2009). *Human Resource Management – Basics, Applications and Future Directions*. Sage.

Kovach, K. A., Hughes, A. A., Fagan, P. & Maggitti, P.G. (2002). Administrative and Strategic Advantages of HRIS. *Employment Relations Today*, 29 (2).

Lengnick-Hall, M. L. & Moritz, S. (2003). The impact of e-HR on the HRM function. *Journal of Labor Research*, 24 (3), 365-79.

Lievens, F. & Harris, M.M. (2003). Research on Internet recruiting and testing: Current status and future directions. *International Review of Industrial and Organisational Psychology*, 18, 131-165.

May, N. & Pope, C. (1995). Rigour and Qualitative Research. BMJ: *British Medical Journal.*

McClelland, S.B. (1994). Training needs assessment data-gathering methods: Part 1, survey questionnaires, *Journal of European Industrial Training*, 18 (1), 22-26.

Nuasair, K.K. & Parsa, H.G. (2007). Critical Factors in Implementing HRIS in Restaurant Chains, *Advances in Hospitality and Leisure*, Vol. 3.

Roehling, M.V., Boswell, W.R., Caligiuri, P., Feldman, D., Graham, M.E., Guthrie, J.P., Morishima, M. & Tansky, J.W. (2005). The future of HR management: research needs and directions. *Human Resource Management*, 44 (2), 207-212.

Rogers, E.M. (1983), *Diffusion of Innovations*, 3rd ed., The Free Press, New York, NY.

Rogers, E.M. (2003), *Diffusion of innovations*, 5th ed., The Free Press, New York, NY.

Ruël, H. J. M., Bondarouk, T. & Looise, J. C. (2004). E-HRM: Innovation or irritation. An explorative empirical study in five large companies on web-based HRM. *Management Review*, 15 (3), 364 −381.

Ruel, H.J.M., Bandarouk, T.V. & Van der Velde M. (2006). The contribution of e-HRM to HRM effectiveness. Results from a quantitative study in a Dutch ministry. *Employee Relation* 29 (3), 280-291.

Ruta, C.D. (2005). The application of change management theory to HR portal implementation in subsidiaries of multinational corporations. *Human Resource Management*, 44 (1), 35−53.

Sambrook, S.E. (2003). E-learning in small organisations, *Education & Training*, 45 (8/9), 506-516.

Sampson D., (2013). Data Protection Act: Privacy & Security in the Information Age, Presentation at Yaoundé Conference, 2013. Available at http://www.cto.int. Date Accessed [Monday, October 13, 2014].

Stanton, J. M. & Coovert, M.D. (2004). Turbulent waters: The intersection of information technology and human resources. *Human Resource Management*, 43 (2), 121−125.

Stone, D. L., Stone-Romero, E. F., & Lukaszewski, K. (2003). *The functional and dysfunctional consequences of human resource information technology for organisations and their employees.* Greenwich, CT: JAI Press.

Stone, E. F., & Stone, D. L. (1990). *Privacy in organisations: Theoretical issues, research findings, and protection strategies*. Greenwich, CT: JAI Press.

Stone-Romero, E. F. (2005). *The effects of eHR system characteristics and culture on system acceptance and effectiveness.* San Francisco: Jossey Bass.

Strohmeier, S. (2007). Research in e-HRM: Review and implications. Human Resource Management Review 17 (2007) 19–37.

Swaroop, K.R. (2012). E-HRM and how IT will reduce the cost in organisation, *Journal of Marketing & Management Review* 1 (4), 133-139.

Tornatzky, L.G. & Klein, K.J. (1982). Innovation characteristics and innovation adoption implementation: a meta-analysis of findings. *IEEE Transaction on Engineering Management*, 29 (1), 28-43.

Townsend, A.M. & Bennett, J.T. (2003). Human resources and information technology. *Journal of Labor Research*, 24 (3), 361−363.

Victor, J. M. (2013). The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy, *the Yale Law Journal*, 123:513.

Viswesvaran, C. (2003). Introduction to special issue: Role of technology in shaping the future of staffing and assessment. *International Journal of Selection and Assessment*, 11 (2/3), 107−112.

Voermans, M. & van Veldhoven, M., (2007). Attitude towards E-HRM: an empirical study at Philips, *Personnel Review*, 36 (6), 887-902.

Welsh, E., Wanberg, C., Brown, K. & Simmering, M. (2003). E-learning: Emerging uses, empirical results and future directions, *International Journal of Training and Development*, 7 (4), 245-258.

www.vvu.edu.gh.com, retrieved on 20th February, 2015.

Yin, R. K. (2009). Case study research: Design and methods (4ed.). Los Angeles, CA: Sage.

Zafar, J. (2012). An Analysis of E-Human Resource Management Practices: A Case Study of State Bank of Pakistan, *European Journal of Social Sciences*. 15 (1).

Zampetti, R. & Adamson, L. (2001). Web-based employee self-service: a win-win proposition for organisations and employees, in Walker, A. (Ed.), Web-Based Human Resources, McGraw-Hill, New York, NY, 15-23.

APPENDIX B: SAMPLE INTERVIEW GUIDE

UNIVERSITY OF GHANA BUSINESS SCHOOL
UNIVERSITY OF GHANA
LEGON

Introduction

Dear Sir/Madam,

I am a student of University of Ghana Business School pursuing a Master of Philosophy Programme in Business Administration. As part of requirements for the completion of the programme, I am writing a thesis on the topic "Data Protection and Electronic Human Resource Systems: A Case Study of Valley View University, Ghana. I am therefore seeking your consent for an interview on issues regarding data protection and electronic human resource systems in this institution. I would be much grateful if you could provide me with the necessary assistance for the study.

Thank You.

Bio-Data of Interviewee

Gender: Age:

Marital Status: Academic Qualification:

Department: Areas of Specialty:

Employment Status: Part Time / Full Time:

INTERVIEW QUESTIONS

1. Does Valley View University have any Electronic Human Resource Systems (E-HRS)?
2. What is your general opinion about the implementation of Electronic Human Resource Systems (E-HRS) at the Valley View University?
3. In your opinion, in what ways has the implementation of E-HRS at this institution ensured the protection of employee data?
4. Do you know of any data protection laws in Ghana?
5. What is the Data Protection Act About?
6. What are some of the key issues presented in the Data Protection Act?
7. What are some of the issues in the Data Protection Act that are related to E-HRS?
8. In what ways has your knowledge about the Data Protection Act impacted on you as an employee of Valley View University?
9. What are some of the security issues presented in the Data Protection Act?
10. Do you think the law has sufficient provisions to protect employee data?
11. Does Valley View University adhere to the security issues presented in the Act as it implements E-HRS?

11a. If yes, how does the university ensure adherence to the security issues presented in the Data Protection Act as it implements E-HRS?

11b. If no, what are the hindrances that prevent the university from adhering to the security issues presented in the Data Protection Act as it implements E-HRS?