International Journal of Evaluation and Research in Education (IJERE)
Vol.3, No.3, September 2014, pp. 133~141
ISSN: 2252-8822

Data Protection Issues in Higher Education with Technological Advancements

Nigel McKelvey
School of Education, Queen's University, Belfast, Northern Ireland, UK.

Article Info

Article history:

Received April 25, 2014
Revised Jun 20, 2014
Accepted Aug 26, 2014

Keyword:

Data protection
Higher education
Technological
Advancements

ABSTRACT

Adhering to laws whilst working or studying in an educational establishment is often fraught with challenges. The Irish Data Protection Act 1988 (Amendment 2003) strives to protect the individual where their personal data is potentially being abused. The advancements in technologies have facilitated educational establishments by improving efficiencies and reducing costs. However, this paper will outline the salient features of the said Act and evaluate how well the law adapts with technologies such as cloud computing and biometrics. It will endeavour to align the law with these technologies and offer a critique of areas that are potentially lacking. Cases will be discussed where precedents have been set by the Irish Data Protection Commissioner and as a result, suggestions for a data protection policy for Higher Education will be proposed. Conclusions will draw upon research conducted and suggest whether the law, as it stands, it suitable with the technologies mentioned.

Corresponding Author:

Nigel McKelvey,
School of Education,
Queen's University, Belfast,
Northern Ireland.
Email: nmckelvey01@qub.ac.uk

1. INTRODUCTION

The Higher Education landscape has evolved considerably in recent years as technology has advanced [1]. Faster broadband connections and more efficient networking techniques have provided both educators and students with more options for teaching and learning. As a result of these new avenues of communication such as online discussions, Virtual Learning Environments (VLEs) and mobile technologies, it is imperative that data be protected through a policy that is maintained and implemented successfully. The Irish Data Protection Act 1988 was established for this reason and was amended in 2003 to bring it into line with the European Union Data Protection Directive 95/46/EC and all sections are in force with the exception of Section 4 (13) which refers to enforced subject access [2].

This paper will endeavour to highlight some of the salient features of the Irish Data Protection Act 1988 (Amendment Act 2003). A critical appraisal will also be conducted on how the amended act could be implemented in an Irish Higher Educational Institute in light of technological advances such as cloud computing and biometrics. Finally, a discussion will reference an existing policy in terms of how it protects those teaching and studying in Higher Education in Ireland. The discussion will also suggest provisions for inclusion in such a policy which are generalizable and applicable to all Institutes. The paper should serve to highlight the importance of adhering to Data Protection laws (not just because colleges are compelled to) but because other factors are also important such as the rights of the student and staff member, the potential loss of trust that could result by not adhering to it and the employability of students.

2. SALIENT FEATURES OF THE IRISH DATA PROTECTION ACT 1988 (AMENDMENT 2003)

The Irish Constitution endeavours to provide a number of fundamental rights. The Courts have analysed and interpreted these rights to also include certain unenumerated rights. Such human rights are not explicitly stated in the Constitution but are interpreted by the Courts as having meaning [3]. One unenumerated human right is the right to privacy. The EU Charter of Fundamental Rights: Article 8 [4] refers to the protection of personal data:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Determining policy that will consider these provisions can involve many aspects but it could be considered that an individual's right to information is at its core [5]. Having access to information facilitates transparency as well as accountability [5]. The right to information augurs positively for strengthening the knowledge of society but is only implementable (and enforceable) if protected by law. The Freedom of Information (Amendment) Act 2003 (FOI Act) endeavours to safeguard this right. Section 1(5) of the Data Protection Act 1988 and 2003 provides that:

(a) A right conferred by this Act shall not prejudice the exercise of a right conferred by the Freedom of Information Act 1997,
(b) The Commissioner and Information Commissioner shall, in the performance of their functions, co-operate with and provide assistance to each other.

Section 7(7) of the FOI Act imposes a duty on public bodies to assist people who request information or access to a record from a public body otherwise than under FOI [2].In light of this, Ireland has striven to balance the right to privacy and the right to information with the appointment of a Data Protection Commissioner (DPC). [6] suggests that rights cannot simply be integrated into society without the inclusion of measures to ensure that various institutions respond appropriately to different groups. This is arguably an important consideration in a society where technology has the potential to affect human rights and so the appointment of a Commissioner is necessary.

Section 2 (a) (iv) ofthe Irish Data Protection Action 1988 and Data Protection (Amendment) Act 2003 (DPA) refers to personal data as:

"'personal data' means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller"

As outlined in Section 11 of the DPA, one of the powers of the Commissioner is to prohibit overseas transfer of data [7]. It could be argued that the use of cloud computing contravenes Section 11 of the Act; however, the Commissioner has provided some guidance on how this obstacle can be overcome. A data controller (college or university) is not in breach of the DPA if the cloud services utilised reside within a country approved by the European Union Commission or is within the US 'Safe Harbour' [7]. Should the aforementioned not be the case, the data controller can still protect the data subject (staff and students) by using an EU-approved model contract which outlines data protection safeguards in accordance with EU standards. If an adequate contract cannot be established, there are nine alternative measures set out in Section 11 (4) of the DPA. The data controller need only provide evidence of having met one or more of the measures.

The alternative measures allow the transfer of data when necessary if [8]:

(a) Required or authorised by law
(b) The data subject gave consent
(c) Performance of a contract to which the data subject is party
(d) The contract is entered into at the request of the data subject
(e) Reasons of substantial public interest
(f) Obtaining legal advice
(g) Prevent injury/damage
(h) The data is an extract from the statutory public register
(i) Authorised by the Data Commissioner.

It is evident [7]-[10] that the data subject's consent can be used extensively by data controllers. The question arises however, as to the level of informed consent that exists. In an educational setting, if a student's grades are stored in a cloud paradigm, how aware are they of where that data resides. [7] refers to how the DPA outlines how data should be treated by stipulating that the data should be obtained and processed fairly, kept only for one or more specified and lawful purposes, processed only in ways compatible with the purposes for which it was given, kept safe and secure, kept accurate and up-to-date, adequate,

relevant and not excessive, that it is retained no longer than is necessary for the specified purpose or purposes and finally that a copy of an individual's personal data be provided to them, on request.

The evolution of technology has tested the scalability and robustness of current laws [11] and made adherence to data protection guidelines difficult. With cloud computing and biometrics often used in conjunction with each other [12], it is necessary to look at the security implications of utilising such technologies within an educational establishment and whether or not the DPA (as it exists) will continue to protect the data subject.

3. CLOUD COMPUTING IN EDUCATION

Technological advancements in Higher Education (HE) establishments have facilitated organisations in reducing the amount of storage required in order to maintain administrative records, e-mail data, student/staff records, relevant medical data, library resources, research information and admissions. It is for this reason that cloud services have been adopted but can often be implemented inappropriately [13]. The data maintained within HE environments can have varying degrees of sensitivity ranging from student/staff personal records to library contents. It is therefore the author's opinion that the sensitivity of this data be categorised and prioritised. This categorisation may help determine which cloud service should be established for each data category.

In the 'cloud', when a college (data controller) uses such a technology, they are utilising a service provider (data processor) to maintain the data on their behalf, in a data centre [2].

A client (college) can avail of various services within the cloud. If server space is all that is required then "Infrastructure as a Service" is sufficient, however, if server space plus an operating system is required then "Platform as a Service" is more appropriate. In addition to the cloud service(s) required, the cloud type is an important consideration. This jargon and technological obscurity can often lead to ambiguity and thus begs the question of what data protection issues might exist within said paradigm.

The obvious issues relate to the security of the cloud paradigm selected and the location of the data itself. It is important to consider the laws/guidance that pays particular attention to technological advancements in relation to data protection. The ePrivacy Regulations 2011 (S.I. 336 of 2011) deal with data protection for phone (mobile or other), electronic-mail, SMS and Internet usage. They give effect to the EU ePrivacy Directive 2002/58/EC (as amended by Directive 2006/24/EC and 2009/136/EC) [2].

3.1. Security, Location and Written Contract

Like any other organisation, colleges must strive to be more economical and to lessen their carbon footprint [14]. As a result, the traditional modes of storing large volumes of data on expansive servers housed physically on campus is starting to become replaced by cloud technologies [14]. As the data controller has full responsibility for the security of the data under the DPA (Section 2C (3)) [15], it is crucial that the controller be assured that the cloud provider will only execute their instructions in relation to the personal data being stored. This assurance should come in the form of a written contract as stipulated by [2].

Cloud computing enables colleges to access a multitude of services on demand. Transparency and control of the data is important to a data controller such as a HE institution [9]. Cloud services diminish these capabilities and so confidence in the cloud services utilised is paramount. One of the DPA principles is that a data subject can request that data held on them be updated or indeed deleted [16]. Cloud providers can share disk space on servers with other clients and/or other cloud providers. If data is to be deleted by wiping a disk, then this may be an impossible task if another provider or client is using the same disk [16]. With regard to a HE environment, it would be assumed that data be deleted after a specified period of time, particularly in relation to student/staff personal records [17].

The data centres within the cloud often exist in multiple nations which could prove difficult under the DPA in Ireland as a result of Section 11. It is an important aspect to consider by the data controller. In a traditional college or university, data is backed up regularly and stored securely. Cloud services, on the other hand, are a single point of failure [9]. Should a student or staff member be updating or retrieving a record using the internet (via a cloud paradigm) and a loss of internet connectivity occurs, then data could become inaccessible and/or inaccurate. Such a scenario could contravene the DPA where data should be 'accessible and up-to-date' [7].

Cloud services might be considered an efficient and cost-effective way of dealing with registration and fee payments. It is important to note that organisations that process or transmit cardholder (student) data are required to be Payment Card Industry Data Security Standard (PCI DSS) compliant [18]. It may prove difficult for a college to assign liability over for PCI compliance to a cloud provider as the DPA places full responsibility for the data with the data controller (Section 2C(3)) [15]; [18]).This in turn raises questions

over the suitability of cloud technology for registration and fee payment processing in HE. The lack of specificity in the DPA in relation to payment card processing via a cloud paradigm is a potential cause for concern.

4. BIOMETRICS IN EDUCATION

With biometric data collection including techniques such as iris scanning, voice recognition, hand geometry, fingerprints and face recognition, it is important to review the current definition of personal data[10]. As the data derived by using biometric techniques is unique to each individual, a data subject can be "identified" as outlined by [15] and indeed the Acts. As mentioned earlier, one of the salient features of the Acts relates to how data collected should be "relevant and not excessive". Data stored in an educational establishment should not unveil sensitive information pertaining to an individual such as race [7]. It is the author's opinion that biometric data collected in a HE environment may in fact be "excessive" as per Section 2 (1)(c)(iii) of the Data Protection Act 1988 (Amendment 2003). Asking students for fingerprints and/or requesting iris scans may be deemed excessive in order to record attendance for example.

Schools and colleges are tasked with keeping accurate and auditable records. It is essential to store this information securely. Biometrics is a consideration where a data controller may decide to use fingerprint identification methods. The finger is scanned and unique points identified on the image. The points are then converted to binary numbers and the original fingerprint scan destroyed [19]. Finally, the binary numbers are encrypted to a series of digits which equate to the student's identification number. A college may decide to implement such a mechanism to help with practical issues such as college access, attendance, library facilities, laboratory admission, medical centre facilities and transportation (commuting between multiple campuses) [19]. It is the author's opinion that while biometrics serve to reduce overheads and costs over time, it is evident ([15], p243-244) that precedents set down by the DPC in relation to biometric attendance recording in Ireland, requires an additional 'opt out' system running alongside. This inevitably incurs additional costs for the college and may well defeat the purpose of a biometrics system. Colleges in Ireland who are currently (or are considering) storing biometric data about students to record attendance should pay particular attention to Section 2(B) of the Act as it specifies that data should only be collected where consent is explicitly given and secondly, that the collection of data is considered necessary processing for the performance of a function ([7], [8]). The Education (Welfare) Act 2000[1] requires that attendance records are kept but does not specify that biometric data is necessary (or acceptable) for this function to be achieved [2]. The DPA uses the word "necessary" in relation to the collection of data and the Irish Data Protection Commissioner has considered the collection of biometric data (for the purposes of recording attendance) as being 'not necessary' [2]. The clarification by the Commissioner is evident that the issue of deriving inferential sensitive data from biometrics is a potential privacy issue for data subjects.

Obtaining and processing biometric data fairly and in accordance with Section 2(1)(a) of the Act assumes that the student (data subject) has given consent for the data to be collected. It could be assumed that students in a college would be aged eighteen or over. However, it is often the case [20] that a first year student is aged seventeen[2]. In this instance, it is also necessary for the college to gain parental/guardian consent, otherwise a breach of the Act is possible [21].

In order to maintain and uphold transparency, the data collector (college) should make themselves known to the data subject, provide reasons for the processing of the data and identify any third parties to whom the biometric data is being shared [7]. Adhering to all three guidelines is necessary in order to comply with Section 2D of the DPA. The compliance is more prevalent where the biometric data is stored in a cloud paradigm where the data subject (and indeed the data controller) may not know the exact location of the data.

Data retained should be accurate and up-to-date [16]. Manual (and often electronic) records can be easily edited and updated as required. Section 2(1)(b) of the Act can be difficult to implement in relation to biometric data. Where a data subject (student) goes through physical or physiological changes, the biometric data would, as a result, be inaccurate. Such changes may include scarring due to burns, eye damage or amputations. Colleges should strive to implement a policy or procedure that can accommodate these changes without contravening Section 2(1)(c)(iii) where gaining data in an invasive (or excessive) way may breach the Act. This could potentially affect an individual's human right to privacy under the Irish Constitution. It is the author's opinion that challenges such as these are not articulated clearly in the Acts and leave ambiguity as a result.

[1] A child <18 years of age

[2] 2294 seventeen year old fulltime undergraduate students registered on the 1st January 2013 across all HEA-funded Institutions.

5. DATA PROTECTIONC ASE LAW ANALYSIS

[2] documented a case (number 12) from 2007 where employees at a company contacted the Commissioner as they felt that their personal data was being compromised by the proposed introduction of a biometrics system to record time and attendance. The employer had sought and gained consent from all employees and had provided information and training sessions. It was suggested that the technological move was based on an abuse of their existing system of recording attendance. The new system required finger print data to be stored that would be encrypted and allow employees to enter a PIN in order to record their attendance. The employees felt this was in breach of the DPA under proportionality, accuracy/security of personal data and fair obtaining. It was made known that those who did not wish to interact with the new system, were not forced to by their employer. After consideration, the DPC decided, that the employees involved should use the new PIN system, but without the requirement to provide biometric data. It was concluded that no breach of the Act had taken place as the aggrieved employees were not forced to use the biometrics system against their wishes.

This was an interesting case as no breach had taken place, but the employees were still not required to comply with the employer's new biometric system. This 'opt out' approach to biometrics was also upheld in the Boran Plastic Packaging Ltd. case as discussed by [15] (p243-244). The potential security implications of biometric data are of concern and the excessive nature of the data appears to be unsupported in relation to attendance recording. This precedence in recording attendance was also upheld by the office of the DPC when a large secondary school in 2010 attempted to apply a biometric system for all students to record attendance (Case 12) in 2010 [2].The Commissioner decided that an 'opt out' option be available and that evidence of informed written consent be kept for all students using the system. Colleges might well face opposition in implementing such a system for said purposes. Delhi University is facing contempt as a result of failing to introduce a biometrics system to record their lecturing staffs' attendance as a result of a court order by the Delhi High Court [22]. Staff are blocking the proposed system and are threatening strike action as a result. Within such institutions, biometric data may be deemed appropriate for particular staff to gain access to high risk laboratories where dangerous chemicals are stored or where medical records are kept [23]. It is the author's opinion that the requirement to have a parallel 'opt out' system in place would only serve to increase overheads in the long run.

Cloud computing can be used as a mechanism to exchange or share information [24]. In the United Kingdom in 2011, Durham University were in breach of the DPA after sharing training material online which made personal data about trainees available [25]. The advantages of cloud computing were lost by misguided users who did not receive sufficient training in the area of data protection [25]. Simply anonymising the training manuals could have protected the data subjects and averted the breach. The investigating officer concluded that such organisations should adhere to a comprehensive training programme in data protection.

With the issue of data protection prevalent in cloud computing [7], it is important to examine legal cases which have analysed such issues. In 2010, the case of Italy *v* Google [26] where some Google executives uploaded videos which breached Italy's DPA is of interest. The process involved a cloud paradigm where data was not processed on Italian servers and the discussions pertaining to the video's content was not uploaded in Italy but the organisation had a marketing cloud service operating within the country [26]. The Courts claimed jurisdiction based on 'context' issues. As the cloud service was based in Italy and formed part of the company's overall business, even though the video itself was not running on Italian servers, the Courts found Google to be in breach [26]. It is the author's opinion that this case signifies the importance of both data and service location. With the upload not taking place in Italy it was assumed that no litigation would be possible but the case demonstrates that the courts can claim jurisdiction when it comes to the location of the data (or service) itself.

6. RIGHTS OF THE DATA SUBJECT

Within colleges, students and staff all have the right to gain access to the data stored on them under Section 4 of the DPA regardless of age. Although it is worth noting that students in HE under 18 years of age must have parental/guardian consent given for their data to be stored. The data subjects also have a right to have the data updated and/or deleted [8]. It is only with consent that a data controller can store data about an individual.

There is an exception to this provision however within HE institutions. Section 4(6) of the DPA makes the point that students cannot request access to their examination scripts, with the exception of medical examinations [15]. Section 4(6)(a) of the DPA, provides a right 'to request the results of an examination at which a person was a candidate 60 days after the date of the first publication of the results of the examination' [21]. The same does not necessarily apply to scripts that were submitted for an exam. Access to such material would have to be analysed as to whether it could be considered 'personal data'[21].

Where the exam comprises of questions and a student needs to recall the subject material taught as part of academic modules, it is the position of the DPC that the right of access under Section 4 of the DPA does not apply to that material [21]. However, scoring/marking tables which accompany such material, if they exist, would be subject to consideration for release where an individual makes a request for them under Section 4 of the DPA [21].

[21] outlined how the Commissioner had previously considered a complaint from an individual in relation to the failure by a professional body to furnish him with a copy of his examination scripts further to an access request. The examination in question involved reproducing model answers from a text book. Accordingly, the Commissioner considered that the examination scripts in the case did not constitute personal data within the meaning of the DPA and that there was no substantive breach of the Acts. The individual lodged a Circuit Court Appeal against the Commissioner's opinion that there was no basis to investigate the matter. While the matter was decided on a jurisdictional point in favour of the Commissioner, the Court noted that the exam scripts in question were not personal data within the meaning of Section 1 of the DPA and therefore the requester was not entitled to copies of his exam scripts. The individual appealed the decision of the Circuit Court to the High Court. Again, the High Court found in favour of the Commissioner on a jurisdictional point. However, the Court considered all of the issues involved and noted that, had the Court jurisdiction to hear the appeal, it would have upheld the finding of the Commissioner that the exam scripts in question did not constitute personal data within the meaning of the Acts. With courses now being delivered online in greater numbers [27] and less of a focus on end of term examinations, students are being provided feedback and grades on continuous assessment through Virtual Learning Environments (VLEs). If a module is being assessed online, it is possible to breach the DPA should the results/feedback be inadvertently made public. Such an issue could occur by clicking the wrong checkbox. It is therefore important for staff to be mindful in protecting their students' data using this forum. A related issue is where the data subject has the right against automated decisions being made (via a computer based system) that affects the individual [15]. From a teaching perspective, a VLE facilitates automated assignment marking and grade allocation/weighting. Section 6B (i) of the DPA, however, has a provision which does not allow a decision making process which is solely conducted using automated methods about an individual, that produces legal effects, to take place [15]. Colleges should be mindful of this fact and ensure informed consent has been received from students in relation to any modules which may adopt such a grading approach with assignments and to that end, their admissions policy. However, Examination Board guidelines usually contain a specific provision/requirement that would ensure a student's progress is reviewed by at least one human and is not therefore an automated decision. Personal data held at a HE institution can be requested by third parties. Section 28 of the Student Support Act 2011 supports the Data Protection Acts [29]. It makes a provision whereby a data controller may be obliged to provide personal data stored about a student to a local authority, a Minister or an awarding body where the processing is for a relevant purpose. Such purposes might include the processing of grants or offences against the State [29]. It would be prudent for a college or university to fully inform students of this process upon registration and obtain consent.

7. A DATA PROTECTION POLICY IN AN EDUCATIONAL SETTING

A data protection policy for a college should aim to explain the purpose of the DPA. The policy should be an opportunity for the college to articulate its commitment to data protection so that it might instil confidence amongst staff and students. The document might outline the principles of the data protection legislation and highlight where responsibilities lie. In accordance with the DPA, the data controller should be clearly identified. In addition, where cloud technologies and/or biometric systems are in use, the technologies used to process the data should be explained.

It would be prudent for the policy to outline procedures and guidelines for students and staff alike. A section of the document might stipulate the data subjects' rights, the exceptions to any rights of access to data and guidelines for staff on the disclosure of student data to third parties. The latter is particularly pertinent in HE where lecturing staff are often contacted by potential employers to give references for students. Staff giving references can be problematic and deserve detailed guidelines which are outside the scope of this paper. As outlined in Appendix A, a section on how to protect personal computers when processing institute data is important. Guidance on encryption techniques as well as suitable firewall installations and appropriate passwords would be of benefit. So as to guide students (and indeed staff), it is important that the role of the Data Protection Commissioner be explained and contact details provided. To compliment this, it is the author's opinion that a dedicated college Data Protection Officer be established and identified. Having a staff member dedicated to the role of data protection as more new technologies are introduced is important. The officer would review the policy in light of technological and/or legislative changes.

A data protection policy within HE should go beyond just policy and incorporate practice. A college might strive to be context-aware and offer students and staff awareness initiatives as well as training schemes where staff might earn a data protection award [29],[30]. With industry experience an important credential for any graduating student [31], an extra credits initiative, equivalent to the staff certificate, would aid students in gaining invaluable knowledge and skills.

8. EDUCATION ABOUT LAW

The Data Protection Acts Section 2 (A) outlines the following provision [7]:

(2) A: the data controller or data processor shall take all reasonable steps to ensure that —

(a) Persons employed by him or her, and

(b) other persons at the place of work concerned, are aware of and comply with the relevant security measures aforesaid.

The use of the term "reasonable steps" may result in ambiguity. With the protection of personal data, it is the author's opinion, that defined steps should be followed by data processors so that those affected are fully aware of their rights and obligations. With technological advancements edging forward, it would be prudent for colleges to educate their staff and students accordingly [32].

When a student logs in to a network, they are (most likely), agreeing to an Acceptable Usage Policy (AUP) but are they aware of its contents and any potential implications. The AUP warns students (and staff) not to expect privacy on college laptops/machines [33]. Similarly, when a lecturer uses Dropbox, email or a flash drive to update a spreadsheet containing student grades at home, are they aware that they are inadvertently making a copy of private data (student grades, names, student number) on a non-approved personal machine. The lecturer's home machine may not have adequate security software installed which could facilitate student data being hacked. Dropbox also uses a cloud provider to store its data and until recently it did not conform to the US Safe Harbour initiative [34].

[35] alludes that a lack of education about law is impacting on the administrators' ability, in educational settings, to make legally-sound decisions. Ensuring that their rights and the rights of the students are protected is important.

9. CONCLUSIONS

Protecting data relating to students and educators is an important and often difficult undertaking. Whether the data pertains to grades, attendance records, medical records, admissions, finance, research, or biometrics, the law in Ireland exists to protect both the data controller and the data subjects. Technology in the form of cloud computing has facilitated a more economical and efficient campus administration. The same however cannot be said for biometrics if the technology cannot be implemented in its entirety without requiring the additional overheads of an obligatory opt-out system running in parallel. Such technologies have raised questions around the location of data, its security, transparency and purpose. While the DPA has made strides towards adapting to cloud and biometrics, it has remained steadfast in its resilience in protecting the individual. Nevertheless, technology is continuing to evolve and will continue to be adopted by HE establishments.

The Irish DPA and the EU Directive 95/46 that required it, place the onus of responsibility for data protection on the data controller [36]. However, in the case of cloud services, the provider could be considered a data processor [36]. This becomes difficult to interpret when a cloud provider may often determine how the data is processed and also the extent to which the data is processed [36]. An example might be a cloud provider deciding what kind of database data is stored within and indeed how the data is backed up. The client (college) might find themselves in a difficult position if their role (under the DPA) cannot be clearly defined. It is the author's opinion that a clearer definition of both a data controller and data processor is required in the context of cloud computing. In order to continue protecting data controllers and data subjects, it is also suggested that the DPA further clarify particular subsections pertaining to the processing of payment cards (when paying fees) using a cloud paradigm, the physical deletion of data from a shared disk in the cloud, the updating of biometric data following physiological changes and the exception to a right of access to examination scripts when conducted entirely online.

[32] refers to how public trust in professionals is essential for society to function safely and effectively and also argues that students graduating should be taught the importance of data protection in an attempt to advance knowledge and promote compliance. Training staff and students alike is a worthwhile endeavour. It is therefore the author's opinion that the proper implementation and adherence to the principles enshrined within a comprehensive data protection policy should form part of the curriculum in HE.

In light of the privacy concerns raised above, HE Institutions should revise their data protection policies to specifically instruct academics not to upload any personal data belonging to students to cloud services e.g. Dropbox and to cater for potential introduction of biometric systems. This study proposes that these guidelines are applicable to all HE Institutes in Ireland.

ACKNOWLEDGEMENTS

The author would like to acknowledge the support and guidance of Prof. Laura Lundy, School of Education, Queen's University, Belfast.

REFERENCES

[1] Trustwave, "Data Security Program for Higher Education", 2013. Available: https://www.trustwave.com/downloads/Trustwave-Higher-Ed-Data-Security.pdf. Last accessed 8th December 2013.
[2] Office of the Data Protection Commissioner, "Data Protection", 2013. Available: http://www.dataprotection.ie/ViewDoc.asp?fn=%2Fdocuments%2Flegal%2FLawOnDP.htm&CatID=7&m=l. Last accessed 8th December 2013.
[3] Keane, R., "Judges as Lawmakers: The Irish Experience", Paper delivered at the National University of Ireland Galway Law Society, 2004.
[4] EU, "Charter of Fundamental Rights of the European Union", 2010. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF. Last accessed 8th December 2013.
[5] Chakraborty, S., "Right to Information and its Realization: Role of Higher Education in India", *Calcutta Law Times*, pp. 2, 2010.
[6] Paré, M., "Inclusion of Students with Disabilities in the Age of Technology: The Need for Human Rights Guidance", *Education Law Journal*, vol/issue: 22(1), pp. 39-61, 2012.
[7] Carey, P., "Data Protection - A Practical Guide to Irish and EU Law", Dublin: Round Hall, 2010.
[8] Data Protection Commissioner (DPC), "Data Protection Acts 1988 and 2003 - A guide for data controllers", Ireland: Brunswick Press Ltd, 2009.
[9] Nicholson, J., "Cloud Computing's Top Issues for Higher Education", 2009. Available: http://www.universitybusiness.com/article/cloud-computings-top-issues-higher-education. Last accessed 28th December 2013.
[10] Cehic, M. and Quigley, M., "Ethical Issues Associated with Biometric Technologies", Managing Modern OrganisationsThrough Information Technology, Proceedings of the 2005 Information Resources Management Association International Conference, pp. 540-543, 2005.
[11] Rotenberg, M., "Preserving Privacy in the Information Society", *UNESCO Infoethics*, 1998.
[12] Sussman, A., "Biometrics and Cloud Computing", Biometrics Consortium Conference, 2012.
[13] Intel, "Protecting Healthcare Data in the Cloud: GNAX Health and Intel", 2011. Available: http://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/gnax-health-and-intel-protect-healthcare-data-in-the-cloud-brief.pdf. Last accessed 30th December 2013.
[14] Hignite, K., "Low-Carbon Computing", National Association of College and University Business Officers (NACUBO): EDUCAUSE, 2009.
[15] Lambert, P., "Data Protection Law in Ireland - Sources and Issues", Dublin: Clarus Press, 2013.
[16] Smith, R., "Head In", *Law Society Gazette*, vol/issue: 104(10), pp. 24-27, 2010.
[17] University College Dublin (UCD), "UCD Records Management and Freedom of Information", 2003. Available: http://www.ucd.ie/foi/recordk/coll_ret.html. Last accessed 17th February 2014.
[18] Blackwell, C. and Gahan, M., "PCI DSS compliance - meeting the demands", *Data Protection Ireland Journal*, vol/issue: 2(6), pp. 10-13, 2009.
[19] Identi Metrics (IDM), "Biometric Student Identification: Practical Solutions for Accountability & Security in Schools", *identi Metrics*, 2009.
[20] Higher Education Authority (HEA), "New Entrants by Institution, Gender and Age", 2013. Available: http://www.hea.ie/sites/default/files/ft_ug_new_entrants_2012-13_by_age.xlsx. Last accessed 3rd January 2014.
[21] Fennell, S., "Data Subjects and Examinations", info@dataprotection.ie, 2014. Last accessed 9th January 2014.
[22] Garg, A., "Biometric attendance on cards, DU tells Delhi high court", 2013. Available: http://www.hindustantimes.com/India-news/NewDelhi/DU-faces-contempt-notice-for-not-starting-biometric-attendance/Article1-1048716.aspx. Last accessed 14th February 2014.
[23] Jerdan, T., and Callahan, M., "Privacy Impact Assessment for the Biometrics Access Control System at the Transportation Security Lab", U.S. Department of Homeland Security, 2011.
[24] McKelvey, N. and Houston-Callaghan, E., "The Capabilities and Vulnerabilities of the Cloud", *International Journal of Engineering and Technology*, vol/issue: 2(6), pp. 1062-1075, 2012.
[25] ICO, "University published personal data in online training manual", 2012. Available: http://www.ico.org.uk/news/latest_news/2012/university-published-personal-data-in-online-training-manual-01032012. Last accessed 9th January 2014.

[26] Harris, A., "The Legal Standing of Data in a Cloud", *Dissertation*, - Dublin Institute of Technology, 2012.
[27] Allen, E., and Seaman, J., "Learning on demand. Online education in the United States, 2009", Needham: Sloan Center for Online Education, 2010.
[28] Irish Statute Book, "Student Support Act 2011", 2011. Available: http://www.irishstatutebook.ie/pdf/2011/en.act.2011.0004.pdf. Last accessed 4th January 2014.
[29] Law Society of Ireland, "Certificate in Data Protection Practice", 2014. Available: http://www.lawsociety.ie/S14-Certificate-in-Data-Protection-Practice.aspx. Last accessed 6th January 2014.
[30] PDP, "PDP Training", 2014. Available: http://www.pdp.ie/training/. Last accessed 6th January 2014.
[31] Tomlinson, M., "Graduate Employability and Student Attitudes and Orientations to the Labour Market", .*Journal of Education and Work*, vol/issue: 20(4), pp. 285-304, 2007.
[32] Naughton, M., Callanan, I., Guerandel, A. and Malone, K., "Medical students' knowledge of data protection legislation". *Clinical Governance*, vol/issue: 17(1), pp. 28-38, 2012.
[33] Kotyk, J., "What is a Reasonable Expectation of Privacy in the Information Contained on a Workplace Computer?", *Education Law Journal*, vol/issue: 22(2), pp. 223-229, 2013.
[34] Reeves, C., "Dropbox amends privacy policy to conform to international Safe Harbor Laws", 2012. Available: http://www.westhost.com/blog/2012/02/29/dropbox-amends-privacy-policy-to-conform-to-international-safe-harbor-laws/. Last accessed 3rd January 2014.
[35] Findlay, N., "In-School Administrators' Knowledge of Education Law", *Education Law Journal*, vol/issue: 17(2), pp. 177-202, 2007.
[36] Hustinx, P., "Data Protection and Cloud Computing under EU law", Third European Cyber Security Awareness Day - European Parliament, 2010.