Study to the current protection of personal data in the educational sector in Indonesia

E Rosmaini¹, T F Kusumasari², M Lubis² and A R Lubis³

¹Universitas Sumatera Utara, Medan, 20155
²Telkom University, Jalan Telekomunikasi No. 1, Bandung, 40257
³Politeknik Negeri Medan, Jalan Almamater No. 1, Medan 20155

Email: muharmanlubis@telkomuniversity.ac.id

Abstract. This study examines how legal expert interpret UU ITE to protect personal data based on privacy principle by using content analysis. This act has importance in order to govern the process of collection, use, transfer, disclose and store personal data for profit or other commercial purposes. By recognizing both the right of individual for privacy and the need of organization to utilize the customer data, the Act, which was amended by Parliament at October, 27th 2016 have critical role for protection guideline in Indonesia. Increasingly, with the use of advanced technology, data protection became one of the main issues on various sectors, especially in the educational sector. Educational institutions require large amount of personal data to run their business process to support learning, teaching, research and administration process. It involves wide range of personal data from institution, agencies, colleges, lecturers, students and parents, which might consist of several sensitive and confidential data such as historical, health, financial, academic and experience background. Underestimating and ignoring these issues can lead to disaster such as blackmailing, stalking, bullying or improper use of personal data. In aggregation, they might deliver huge loss to institution either financially or trust. Thus, this study analyse the privacy principle of UU ITE through 21 coders from legal expert to obtain more understanding of appropriate approach to implement privacy policy in the educational sector.

1. Introduction
There is some changes in UU ITE for the purpose to prevent multi interpretation, to add new right, to decrease criminal threat, to execute the verdict of constitutional court, to synchronize with procedural law, to strengthen the role of investigators and government. The improvement by parliament to meet people’s demands should well appreciated. Currently, privacy has obtained substantial concern from educational institution with regards to students' and staff' personal data information in aligning with the government's initiative for a paperless-based administration and information management. Besides that, there are many activities in school and university that involve storing, collecting, transferring and manipulating student and staff data for the purpose of certification, examination, information sharing, etc. Unfortunately, most of individuals do not consider privacy as the necessary matter; when the government collect personal information for certain people, many people will mentioned that they are not worried by said that I have got nothing to hide. Then they will declare that only if you are doing something wrong should you worry and then you have no right to keep it private, which undervalue the right of people to be left alone [1].
In terms of legislation, since April 2016, 108 countries have applied national data protection laws. Ninety-five of these laws, among others, enacted in Singapore, Malaysia and the Philippines are regulations that specifically and comprehensively govern the individual data protection of its citizens except in Indonesia that still use several laws to cater the needs. Although UU ITE has been enacted to protect privacy in general but to provide fundamental law on privacy right and to improve the interaction and communication with other nation economically, Indonesia must have one codified Act on Personal Data Protection [2]. Privacy as individual right has been protected by government fundamentally but not absolute, mostly based on specific context such as information, physical, opinion, group, territorial, communication, association, identity determination and property [3]. Meanwhile, certain privacy aspects has been implemented in various Acts [4] such as UU No. 7/1971 (Basic Provision in Archiving) or UU No. 36/1999 (Telecommunication), which discuss several aspects such as public, access, security, confidential and safety. However, due to the rapid advancement of technology, the current law often not effective to control and regulate personal data protection. This study has objective to analyze specific verse in UU ITE to identify the role of regulation in providing privacy principle for the purpose of developing effective guideline in educational institution.

2. Principle of PDP ACT

Several international convention acknowledge and declare privacy as essential human right to be protected such as article 12 of UDHR, article 21 of ASEAN HRD, article 16 of Arab Charter HR, article of article 14 of UNCMW, article 16 of the UNCRC, article 17 of ICCPR, article 4 of the African Union Principles on FE, article 8 of European Convention on HR, article 11 of American Convention of HR; all of them mentioned the importance of privacy. The development of protection measures of personal data based on UU ITE in the online context should accommodates several principles [5, 6, 17] such as:

2.1. General Principle

It sets out the rights and obligations of the data user when processing personal data by virtue of this principle, thus, the processing of personal can only be done for a lawful purpose directly related to data user’s activity. It also requires that the data processed must not be excessive (imagine if a bank requires from its customer to declare the history of his illnesses, a data which is not directly related and is likely excessive). UU ITE discussed the general principle under section I article 4 (electronic document), article 9 (electronic certificate) and article 12 (electronic signature). Meanwhile, section III explained the right and responsibilities under article 9 (complete information), article 11 (legal requirement), article 12 (security measures). However, the educational institution is recommended to develop guidelines that accommodate the using of social media platforms in specific activity of students either teaching learning, communication or sharing relevant information about their educational institution.

2.2. Notice and Choice Principle

It prescribes that when collecting personal data, data user shall properly notify the data subjects as to the purpose of that collection or processing, as well as the related rights of data subject with regards to those. This could refer to when the data subject is first asked to provide the information or when the data controller first collects the personal information while at the same time, the data subject has chance to decide either agree with the process or decline it. UU ITE mentioned the implementation of electronic certification and electronic system under section IV article 14 (notification to data subject), verse 15 (proper implementation) and verse 16 (minimum responsibilities). Thus, the educational institution should assure that obvious choice have been given to student and staff in regard to opt-in consent in conducting their primary activities such as submitting report, competition, performance indicator, etc.
2.3. Disclosure Principle
Another way of usage of personal data would be when due to several circumstances institution either school or university discloses personal data for their interest and benefit. Under section VI which lays out the disclosure principle, now prohibits such disclosure without the consent of the data subject, as well as this principle puts forward the restriction on disclosure of the personal data. Specifically, article 26 mentioned that data subject have right to file suit for damages under the provision of law. Meanwhile, the institution should provide clear understanding of several privacy attributes into their privacy policy such as retention, availability, integrity, accuracy, confidentiality, accessibility, operational, procedural and mechanical. Meanwhile, it is better for the educational institution to store personal data in isolated and protected location either physical and digital in which, it has been encrypted against possibility of attackers or illegal disclosure.

2.4. Security Principle
Under section III and IV of the Act, which embodies the security principle, the data controller must take practical steps to protect and safeguard personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. Indeed, where data processor is to be used, there must be sufficient guarantees regarding its security features and measures. On the other hand, section VII (prohibited action) under article 30 discussed in specific the list of actions involve accessing, obtaining or penetrate illegally without proper authority from data controller or data processor while under article 32 stated that modified, added, reduced, transmitted, break, deleted, transferred and hide illegally with intention, which lead confidential data to be accessed may be subjected to the punishment under section XI (criminal provisions) articles 46 and 48. Therefore, educational institution should create clear guidelines for physical and digital data by developing privacy policies and procedure to set reference to show relevant person on their roles of responsibility, set appropriate activity process of data use and determine the acceptable workflows.

2.5. Retention Principle
Regarding the period for retaining personal data, the section IV, which represents the retention principle, does not state the time frame allowed to store personal data but general criteria that instruct the data controller to destroy the data after all related business has ended. The development of guideline supposedly provide specific criteria in which terminate the right for data owner to store or use the data after the purpose for students or staff has been fulfilled except for reference only, so those data should be deleted permanently. Even though, the Act appears to make it optional but this principle can be aligned with general and notice principle that data controller dispose the data after the data no longer require to preserve the trust among them. It is better if the criteria specify the exact time for educational institution to keep data to make it clear for staffs after they change job or student after they graduate. The assessment should be done to consider the god and bad impact that might be influence the result in the educational institution such as certification, grading, health record, examination result, delinquency, parental fees paid, salary, reference, acknowledgement, award, gift, reunion, etc.to balance the right and responsibility by updating the terms and condition that allow relevant person decide for the own benefit.

2.6. Data Integrity Principle
Educational institution in Indonesia, which hold and use data should provide suitable approach to assure that the personal data is accurate, complete, not deceptive and recent to avoid loss to the data owner and improve everyday decision in the institution. Thus, designing the system for data protection should be integrated into daily routine such as removing duplication wherever possible, stop collecting data that the school does not need and centralise as much data as possible under management of information system. Under section IV mentioned the duty of data user to ensure the accuracy and completeness of the personal data they collect, also, data integrity that avoid manipulation and illegal access. It is crucial to train and raise awareness among all staff members and organize continual
professional development on data protection, at least once a year.

2.7. Access Principle
PDP law is encouraging for more accountability that expect data users to create specific procedure where data owners or relevant authorized person have privilege to access related personal data and be able to update the information in which they think suit directly or indirectly. Thus, the educational institution should conduct data audit that classify and categorize personal data that they hold through verification and validation to identify what data easily extract, manipulate or delete on a per-person basis or through permission data owners. Under section X article 43 set the process to investigate the violation in the form of illegal access by considering privacy, confidentiality, public service, data integrity and accuracy. The access to the personal data must be differentiated through the restriction or limitation by creating several roles or position to avoid data leaked out of responsibilities.

3. Personal Data Practice in Educational Institution
In the last years, organizations have become more decentralized and often deal with unexpected situations whereby, increasingly, with greater interaction of physical and digital aspects but lack of security mechanism. Meanwhile, use outsourcing or part time staff to conduct several internal activities becomes a common practice to reduce costs and increase the performance. On the other hand, it has strong implication on the data protection requirements of organization and policy compliance, which personal data are often disclosed to an external supplier over whom the organization may not have direct control [8]. As a result, the system have difficulty to evaluate whether the objective has been met or the improvement should be made. Hassan [5] explained that the academic activities of educational institution are basically involves the education process (teaching & learning), research works and additional services. In conducting education activities, the various online materials are often stored in separate database according to respective department and transmitted electronically for certain purpose periodically. The most popular reason on why people reluctance to complete online registration form on the website is that there is no information available about how the data will be used (62%) and they do not trust the data collector (60%) [10]. In Canada, a survey showed that 85% of respondents received unsolicited ads, 74% expressed their concerns on misappropriate service and 82% believed they should get their approval before sending any type of ads. Meanwhile, 61% assumed that all types of telemarketing should be rejected despite the possibility they are leaving out on a good opportunity [7]. In educational sector, personal data has been used in various activities, not limited for the academic purpose only, in fact it has been displayed in the blog or social network for the purpose of promotion or communication. The data user usually maintains the data extracted from research with labelling as confidential and secret to assure specific objective that might be protected under intellectual property law. Thus, the data management requires strict security measure to assure personal data could not be disclose to unauthorized person, in which educational institution should be more proactive to assist relevant process upon request from the data subject. Importantly, the strategy need to be synergized between social and ethics approach to develop the level of understanding in the environment that in which using technology approach to prove the capability to do the in encountering cybercrime or preventing violation [9].

4. Research Methodology
The use of content analysis has to address prior questions on the origin of the available texts, what they mean and to whom, how they mediate between antecedent and consequent condition, and ultimately, whether they enable the analysts to select valid answer to questions concerning their contexts or not [12]. Percent agreement measure uses the point-by-point reliability or moment-by-moment reliability based on proportion of all observation occasion for which the two observers agree regarding whether or not target behavior occurred [13]. There is never 100% certainty about research results, even when statistical significance is achieved [14].

4
There is 63 out of 210 of

| C1  | C2  | C3  | C4  | C5  | C6  | C7  | C8  | C9  | C10 |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| .301| .007| .195| .102| .018| .15 | .231| .178| .009| .001|
| .057| .125| -.031| -.042| -.034| .075| .075| .187| .055| -.003|
| .023| .389| .009| .024| .018| .019| .019| .046| .047| -.004|
| .214| .081| .018| .016| .015| .017| .018| .036| -0.3| .023|
| .058| .012| .086| .005| .024| .024| .009| .019| .046| .074| .055|
| .647| .367| .218| .122| .155| .032| .111| .163| 0 | 0.002|

Table 1. Pairwise Percent Agreement (Orange) & Cohen Cappa (Blue) of UU ITE

When kappa values are below 0.60, the confidence intervals about the obtained kappa are sufficiently wide that one can surmise that about half the data may be incorrect [15]. Both percent agreement and kappa have strengths and limitations. The percent agreement statistic is easily calculated and directly interpretable [15]. The highest score for the percent agreement is 90.32% (coder1 & coder16), followed by 80.65% (coder5 & coder4) and 77.42% (coder16 & coder2). Meanwhile, the lowest score is 2.15% (coder9 & coder16) followed by 3.23% (coder10 and coder16) and the same value for both coder9 and coder10 over coder2 with 3.27%. There is 63 out of 210 of percent agreement, which has score above 40% with the exception of both closed-limit score of 39.79% (coder7 & coder14, coder18 & coder21). Therefore, the low average score occurred because three type of coding rules combined. It can also be interpreted as general picture on the quality of the
current regulation has weak support based on coders’ perspective and has no clarity in the context of PDP. It can be concluded that there is the range of 9.68%, 19.35% and 22.58% of the amount of data, which misrepresents the research data or incorrect data. The highest score in Cohen’s kappa is 0.763 (coder4 & coder5), was followed by 0.647 (coder1 & coder16) and 0.472 (coder12 & coder17). For its reliability, it means that 24%, 35% and 53% of the data being analysed are erroneous. In the end, there is 21 out of 210 value of kappa, which below zero value – one have an exact zero, while there is three values in the percent agreement, which has score below 5% as the boundaries. Meanwhile, there is 23 out of 210 kappa value, which above 0.2 as the boundaries to be considered as the depiction of moderate level agreement among coders, though in the average, the agreement level was low. Despite the lack of agreement between coder, this act has the vital role as the basis for the direction of PDP in Indonesia in which the development of privacy policy can consider other perspectives to increase the concern on privacy [11].

5. Conclusion
To maintain the enforcement of personal data protection, educational institution is encouraged to create the periodical auditory, proper compliance and privacy impact assessment towards the implementation of the policy. Thus, the policy should measure the attribute of the process, data subject behavior and characteristics. Educational institution must ensure that all component; the system consisted of human, technology, task and structure; culture and policy aligned with relevant and related personal data protection act. It will determine whether the effort to protect the personal data will be effective or not in supporting the learning and teaching activities. The intention of having security policy was not to persuade users but to convince them, by letting the users reflect, on their own terms, on why information security is important and on how to react in certain circumstances [16].

References
[1] Solove D J 2011 Why Privacy Matters even if you have nothing to hide The Chronicle of Higher Education The Chronicle Review May 15th
[2] Latumahina R E 2014 Aspek Hukum Perlindungan Data Pribadi di Dunia Maya Jurnal Gema Aktualita Vol 3 2
[3] Budhijanto D 2003 The Present and Future of Communication and Information Privacy in Indonesia Jurnal Hukum Internasional University Padjadjaran Vol 2 2 pp 140
[4] Makarim E 2005 Pengantar Hukum Telematika (Suatu Kompilasi Kajian) Jakarta: Raja Grafindo Persada
[5] Hassan K M 2011 Personal Data Protection in the Business of Higher Education: Malaysian Law International Conference on Sociality and Economics Development. IPEDR Vol 10 (IACSIT Press, Singapore) pp 53-57
[6] Zulhuda S and Delpisheh M 2011 Personal Data "Up in the Air" International Conference on Social Science and Humanity IPEDR Vol 5 (IACSIT Press, Singapore) pp V1-300-V1303
[7] Sarabdeen J 2008 Laws on Right to Privacy in Mobile Marketing WSEAS TRANSACTION on Business and Economic Vol 5 ISSN: 1109-9526 5 pp.280-290.
[8] Zannone N, Petkov M and Etalle S 2010 Towards Data Protection Compliance Proceedings of the 5th International Conference on Security and Cryptography (SECRYPT) pp 213-216
[9] Lubis M and Maulana F A 2010 Information and Electronic Transaction Law Effectiveness (UU-ITE) in Indonesia IEEE ICT4M pp C-13-19
[10] Noor R, Elena and Jawalitha 2003 Security and Privacy Issues as Barriers to E-Commerce Growth: A Consumer Perspective Proceedings the International Business Information Management Conference (Cairo December 16-18) p 114
[11] Lubis M, Kartiwi M and Zulhuda S 2017 Privacy and Personal Data Protection in Electronic Voting: Factors and Measures Telkomnika March vol. 15(1) pp 512-521
[12] Krippendorff K 2004 Content Analysis: An Introduction to its Methodology London, England: Sage Publication

[13] Birkimer J C and Brown J H 1979 Back to Basics: percentage agreement measures are adequate, but there are easier ways *Journal of Applied Behavior Analysis* 12(4) pp 535-543

[14] Marusteri M and Bacarea V 2010 Comparing groups for statistical differences: how to choose the right statistical test? *The Journal of Croatian Society of Medical Biochemistry and Laboratory Medicine* 20(1) pp 15-32

[15] McHugh M L 2012 Interrater Reliability: the Kappa Statistic *The Journal of Croatian Society of Medical Biochemistry and Laboratory Medicine* 22(3) pp 276-282

[16] Ahlan A, Lubis M and Lubis A R 2015 Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures *Procedia Computer Science* 72 361–373

[17] governorsagenda 2017 Data Protection law to be strengthened in 2018: Impact on Schools https://governorsagenda.co.uk/2017/04/18/data-protection-law-to-be-strengthened-in-2018-impact-on-schools/