The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 1, February 2025
https://doi.org/10.33022/ijcs.v14i1.4588

Digital Forensic Ethical Data Handling in Indonesia

Feby Thealma[1], Yova Ruldeviyani[2]
feby.thealma@ui.ac.id[1], yova@cs.ui.ac.id[2]
[1,2] Faculty of Computer Science, Universitas Indonesia, Jakarta

Article Information

Received : 27 Dec 2024
Revised : 22 Jan 2025
Accepted : 29 Jan 2025

Keywords

digital forensic, ethical data handling, private data protection

Abstract

Digital evidence in digital forensic investigations may contain sensitive information which includes private data, however none of the digital forensic standards used in Indonesia focuses on the ethical data handling aspect. Concerning the recent release of Indonesia's Private Data Protection law, this research aims to find clauses in the law that has not been addressed in the digital forensic standards. This research is conducted by correlating Indonesia's Private Data Protection law against digital forensic standards used in Indonesia to find how Indonesia's Private Data Protection law has been complied with the usage of digital forensic standards. As of now, only half of the existing digital forensic standards used in Indonesia has explicitly complied with Indonesia's Private Data Protection law and there are room for improvement to enhance digital forensic ethical data handling in Indonesia.

A. Introduction

Digital evidence in digital forensic investigation may contain sensitive personal and/or corporate data such as personal photographs, videos, business plans, email, medical documents, financial documents, music, movies, games and software and unrestricted access to the evidence poses a threat to the data owner's privacy [1]. Furthermore, when there is reason to suspect that some crime might have been committed using a computer, the investigators may also try to reconstruct the evidence so that it could be presented to a court of law [2].

Several guidelines such as Good Practice Guide for Digital Evidence (ACPO, 2012), Digital Evidence Handling from NIJ USA (Ashcroft, Daniels, & Hart, 2004), and ISO 27037 (BSN, 2014) are still referred to as the standard for digital forensic investigation guidance in Indonesian police [4]. SNI ISO/IEC 17025:2017 is also another standard that is used to standardize digital forensic laboratory in Indonesia [5]. However, neither of those standards focuses on the ethical data handling of private data in digital forensic investigation.

The two points mentioned above raises concern and question over how Indonesia's digital forensic practitioner has applied ethical data handling into their practice. Ethical data handling is a form of prevention for data misuse that may negatively affect people and organizations [6]. As the nature of digital forensic investigation is tightly related to law enforcement the disclosure of data misusage might not be made into public, the ethical data handling sets as a preventive measure deemed necessary in the field. Thus, the aim of this research is to find how Indonesia’s Private Data Protection law has been complied with the usage of digital forensic standards.

Unspecific to Indonesia, there has been some research about data privacy in digital forensic investigation specifically in India [1]. The survey results reveal a lack of professional ethics on the part of some investigators, a lack of legal support for lawyers about data privacy protection and confusion among the public regarding their data privacy rights [1]. Several other publications have also covered digital forensic investigation privacy concerns as future challenges in digital forensic. The issue has also been identified previously and defined privacy-protecting policies both from the user as well as investigator perspectives [2]. Devices used by user which are acquired in the investigation are not just descriptive of the primary user's life, but also of those associated with them in which all information contained can be considered as private information [3].

As of the writing of this document, there’s no research found related to digital forensic ethical data handling specific to Indonesia on several publication databases such as Scopus, IEEE Explore, and Springer Link. In regard to previous research conducted in other countries, this research aims to discover the compliance of data privacy law with existing digital forensic standards specifically in Indonesia. In case that the research found gaps between the law and the standard, the recommendations provided hopefully will be able to be an additional standard to the digital forensic practices in Indonesia.

This research is written in five chapters including Introduction of the research, Literature Review conducted as the research’s basis, Methodology on how the

research was performed, Results and Discussion discusses about the results obtained through the research, and Conclusions which answers the research questions raised in the beginning.

B. Literature Review

A. Digital Forensic Investigation

Digital forensics has become prevalent because law enforcement recognizes that modern day life includes a variety of digital devices that can be exploited for criminal activity, not just computer systems [7].

The key components of digital forensics investigation include:

1) Identification: recognizing an incident from indicators and determining its type. This is not explicitly within the field of forensics, but significant because it impacts other steps.

2) Preparation: preparing tools, techniques, search warrants, and monitoring authorizations and management support.

3) Approach strategy: dynamically formulating an approach based on potential impact on bystanders and the specific technology in question. The goal of the strategy should be to maximize the collection of untainted evidence while minimizing impact to the victim.

4) Preservation: isolate, secure and preserve the state of physical and digital evidence. This includes preventing people from using the digital device or allowing other electromagnetic devices to be used within an affected radius.

5) Collection: record the physical scene and duplicate digital evidence using standardized and accepted procedures.

6) Examination: in-depth systematic search of evidence relating to the suspected crime. This focuses on identifying and locating potential evidence, possibly within unconventional locations. Construct detailed documentation for analysis.

7) Analysis: determine significance, reconstruct fragments of data and draw conclusions based on evidence found. It may take several iterations of examination and analysis to support a crime theory. The distinction of analysis is that it may not require high technical skills to perform and thus more people can work on this case.

8) Presentation: summarize and provide explanation of conclusions. This should be written in a layperson's terms using abstracted terminology. All abstracted terminology should reference the specific details.

9) Returning evidence: ensuring physical and digital property is returned to proper owner as well as determining how and what criminal evidence must be removed [7].

B. Ethical Data Areas

Data handling ethics are concerned with how to procure, store, manage, use, and dispose of data in ways that are aligned with ethical principles. Handling data in an ethical manner is necessary to the long term success of any organization that wants to get value from its data [6].

There are three (3) ethical principles that may be adapted in Information Management which includes:

- Respect for Persons: This principle reflects the fundamental ethical requirement that people be treated in a way that respects their dignity and autonomy as human individuals. It also requires that in cases where people have 'diminished autonomy', extra care be taken to protect their dignity and rights.
- Beneficence: This principle has two elements: first, do not harm; second, maximize possible benefits and minimize possible harms.
- Justice: This principle considers the fair and equitable treatment of people [6].

C. *Indonesian Law on Personal Data Protection*

Referring to the first and third principle of ethical data [6], it is necessary to see how someone's rights of their own data and the consequences of breach enforced in one country. In this case, it'll be necessary to look at Indonesia's law.

Indonesia has released a law on private data protection on 17th October 2022 under Private Data Protection Law (Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi). This law regulates how private data whether specific or general should be protected throughout the processing of the subject's private data.

The law defines data processing that includes acquisition and collection; processing and analysis; storage; revision and renewal; presentation, announcement, transfer, dissemination, or revelation; and/or deletion or destruction. All the processes defined in the law are conducted within digital forensic investigation.

D. *Relation between Ethical Data Handling, Digital Forensic Process, and Indonesia's Data Protection Law*

Data handling ethics as defined are concerned with how to procure, store, manage, interpret, analyze / apply and dispose of data in ways that are aligned with ethical principles, including community responsibility [6]. Figure 1 represents the relation between ethical data handling, digital forensic processes, and Indonesia's data protection law.

DMBOK 2 Ethical Data Handling	Procure	Store	Manage	Interpret	Analyze / Apply	Dispose	-
UU No. 27 Tahun 2022 Perlindungan Data Pribadi	Acquisition & Collection	Storage		Processing & Analysis		Deletion / Destruction	Presentation
Reith, Mark & Carr, Clint & Gunsch, Gregg. (2003). **An Examination of Digital Forensic Models.**	Collection	Preservation		Examination	Analysis	Returning Evidence	Presentation

Figure 1. Relation between Ethical Data Handling, Digital Forensic Process, and Indonesia's Data Protection Law

Theoretical framework of how the theories and literatures used in this research can be seen on Figure 2.

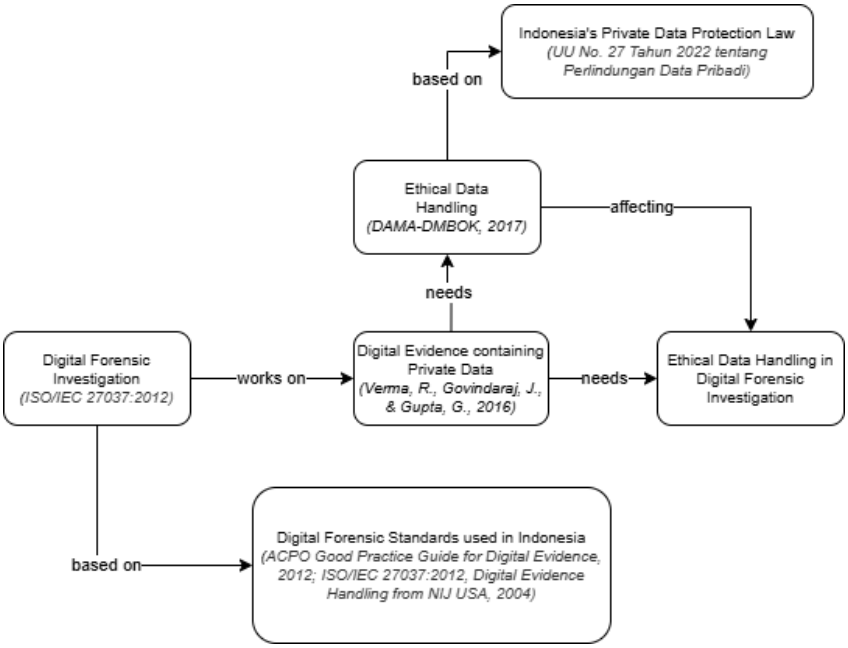

Figure 2. Theoretical Framework

C. Research Method

Figure 3 defines the diagram of methodology used in this research which are divided into three phases: Problem Identification, Literature Studies & Correlation Analysis, and Evaluation and Analysis.

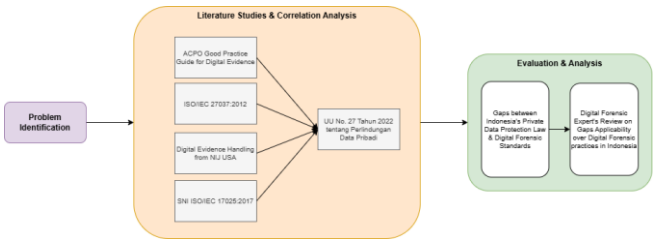

Figure 3. Research Methodology

i. Problem Identification

Problem researched was identified through studies upon Digital Forensic Investigations which may contain private data [1]. The private data contained in the digital evidence raises concerns upon data privacy of the private data subject and is related to ethical data handling which concerned with how to procure, store, manage, use, and dispose of data in ways that are aligned with ethical principles [6].

ii. Literature Studies & Correlation Analysis

All points related to rights and obligations in UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi is correlated with digital forensic standard practices such as Good Practice Guide for Digital Evidence (ACPO, 2012), Digital Evidence Handling from NIJ USA (Ashcroft, Daniels, & Hart, 2004), and ISO 27037 (BSN, 2014), NIST SP 800-86, etc. based on literature reviews.

Each points are taken into consideration and the context for each points are searched into other different standards. Once the same context was found, the points from both standards are compared and analyzed. If no other comparable point in different standards was found, the point was deemed unavailable in current digital forensic standards.

Through this process, the desired output is to be able to identify points in Indonesia's Private Data Protection law that has not been defined by existing digital forensic standards used in Indonesia.

iii. Evaluation & Analysis

In order to evaluate whether the output of this research is applicable in Indonesia's digital forensic investigation, a questionnaire to evaluate the result of correlations between the law and digital forensic standard performed is spread to Indonesia's digital forensic investigators in both private and public sectors. There were 7 investigators in total who had experiences working on multiple digital forensic cases in Indonesia for at least one year.

There's a total of 7 questions related to the data protection law and digital forensic standard identified beforehand. The questions asked in the questionnaire follows each point identified in the first process to ensure each point is applicable in Indonesia's digital forensic investigation.

D. Result and Discussion

1. Problem Identification

The private data contained in the digital evidence raises concerns upon data privacy as stated previously. Following the release of Indonesia's Private Data Protection law, this research identified how gaps might exist between the law and the digital forensic standard used in Indonesia. In the case that gaps exist between both, digital forensic investigator may be able to utilize the gap to perform data misusage.

2. Literature Studies & Correlation Analysis

a. Private Data Subject's Rights

This area consists of eleven points starting from Point 5 until 15. Out of the eleven points, five points have been excluded because of Point 15 where it is stated that Point 8, 9, 10, 11, and 13 are excluded for law enforcement purposes. Thus, the analysis of the remaining points are as seen on Table I.

Table 1 Private Data Subject's Rights

Indonesia's Data Protection Law	**Existing Digital Forensic Standard**	**Analysis**
Point 5: Private Data Subject are entitled to information relating to clear identity, law enforcement basis, goals of request and usage of Private Data, and accountability of the Private Data requestor.	Point 4.1 and 6.1: laboratory legal aspect and review of request, tender, and contract [8].	Laboratory should have formal proof of existence and recognition as having formal proof of existence means the laboratory is permitted to conduct its' activity according to the laws [8].
Point 6: Private Data Subject's right to complete, update, and/or correct inaccurate data according to the goal of Private Data processing.	Principle 1 and 2.2.2: doctrine of the documentary evidence to prevent tampering of evidence [9].	Point 6 is inapplicable on digital forensic investigations as evidence produced is no more and no less now than when it was first taken into the possession of law enforcement [9].
Point 7: Private Data Subject's right to gain access to and obtain a copy of the Private Data.	All seized evidence should be sealed properly and secured thus limiting Private Data Subject access to the captured Private Data [10].	There are two interests in Point 7 that need to be addressed. Access to evidence is limited during investigation and deemed inapplicable to digital forensic practice. However, obtaining a copy of the Private Data has not been addressed explicitly in existing digital forensic standard. Thus, point 7 is potentially applicable partially to obtaining copy of the Private Data.
Point 12: Private Data Subject is entitled to sue and receive compensation for violation of Private Data's processing according to the law	This point relates to the Private Data Processing Basis which will be covered in Obligation of Private Data Controller and Processor in Private Data Processing area.	

b. Private Data Processing

This area consists of three points starting from Point 16 until 18. Point 17 explicitly mentioned that the clause is excluded for law enforcement purposes. Thus, the analysis of the remaining points is as seen on Table 2.

Table 2 Private Data Processing

Indonesia's Data Protection Law	**Existing Digital Forensic Standard**	**Analysis**
Point 16: explains the scope of Private Data Processing in the law which includes Acquisition & Collection, Storage, Processing & Analysis, Deletion / Destruction, and Presentation.	Digital Forensics Model [7].	The scope in the law aligns with digital forensic model as seen previously on Figure 1.
Point 18: enables two or more Private Data Controller who processes the Private Data	Point 5.6: external products and services [8].	External parties' involvement in laboratory's activities should be able to support laboratory's activities accurately and according specified specifications [8].

c. Obligation of Private Data Controller and Processor in Private Data Processing

This area consists of thirty-six points starting from Point 19 until 54 and split into four parts according to the subjects. Exceptions related to law enforcement purposes are made for Point 30, 32, 36, 40, 41, 42, 43, 44, 45, and 46. Points that are made to explain the scope of the law have also been excluded from this research which includes Point 19. Thus, the analysis of the remaining points are as seen on Table 3.

Table 3 Private Data Processing

Indonesia's Data Protection Law	**Existing Digital Forensic Standard**	**Analysis**
Point 20, 21, 22, 23, 24: Private Data Processing Basis.	Point 20 explains about the Private Data Processing Basis. Out of six points considered Private Data Processing Basis, there are several points of interest for digital forensic investigations purposes especially for investigations in private sector. Digital forensic investigation in public sector for law enforcement should fulfill the basis of public service in clause E immediately. Meanwhile, investigations in the private sector should have another basis outside of public service basis. The first basis mentioned In Point"20 includes explicit legitimate agreement from Private Data Subject for one or more goals mentioned by Private Data Controller to Private Data Subject through written or recorded and electronic or non-electronic. This agreement is further explained in Point 21 and Point 22, and the consequence of failure to comply with is emphasized in Point 23 and 24. As the scope of Private Data Processing in the law started on Acquisition and Collection of data, this agreement should exist prior to digital forensics' Collection phase. Other basis mentioned in Point 20 includes law obligations to be fulfilled in case of private investigations are in touch directly with law enforcement, and/or fulfilment of agreement where Private Data are required, and/or fulfilment of Private Data Subject's vital interests' protection, and/or other legitimate interests.	
Point 25, 26: extends the agreement mentioned in Point 20 to the guardian of Private Data Subject in cases where Private Data of children and disabled are to be processed.	None	
Point 27: obligation of Private Data Controller to process Private Data in specific and limited, legitimate, and transparent.	Point 5.3.1: Relevance, Reliability, and Sufficiency. 5.3.2, 5.3.3, 5.3.4, and 5.3.5: Auditability, Repeatability, Reproducibility, and Justifiability [11]. Principle 3: audit record of all processes applied to digital evidence [9].	To display objectivity and evidence integrity in a court of law, it's necessary to show each process through which the evidence was obtained and preserved that a third party is able to repeat the same process and arrive at the same result as that presented to a court [9].
Point 28: obligation of Private Data Controller to process Private Data according to the processing goal.	Point 5.3.1: Relevance, Reliability, and Sufficiency [11].	Investigator should be able to demonstrate that evidence acquired is relevant to the investigation [11].
Point 29: accuracy, completeness and	Point 5.3.2, 5.3.3, 5.3.4, and 5.3.5: Auditability, Repeatability,	All recorded processes applied to digital

Indonesia's Data Protection Law	Existing Digital Forensic Standard	Analysis
consistency.	Reproducibility, and Justifiability [11].	evidence are capable of producing the same result regardless of the party performing the process [9].
Point 31: record of all processes conducted to process Private Data.	Principle 3: audit record of all processes applied to digital evidence [9].	
Point 34: high risk Private Data processing criteria in which one of the items included decision making that have legal consequences.	Digital forensic is used in law enforcements as devices that can be exploited for criminal activity has extended into digital devices [7].	
Point 35, 39: obligation of Private Data Controller to protect and ensure the safety of the processed Private Data which includes planning and implementation of technical and operational steps to protect Private Data and determining level of security for Private Data based on the nature and risk of the Private Data.	Point 5.3, 5.4: facilities & environment conditions and tools, Chapter 7: management system conditions which has also included risk and control management [8].	Laboratory should plan actions to mitigate risks, integrate those actions into management system and ensure actions are proportionate to the effect of investigation legitimacy [8].
Point 36: obligation of Private Data Controller to protect confidentiality of Private Data.	Point 3.2: Confidentiality [8].	Confidentiality in laboratory activity is everything that is related to information and laboratory's customers ownership rights confidentiality [8].
Point 37: obligation of Private Data Controller to supervise all parties involved in Private Data processing.	Point 3.1: Impartiality, Chapter 4: Structural Conditions, Chapter 5: Resources Conditions [8].	Laboratory activities should be performed with impartiality, structured, and managed to ensure laboratory's impartiality with commitment and responsibility [8].

Table 3 Private Data Processing

Indonesia's Data Protection Law	**Existing Digital Forensic Standard**	**Analysis**
Point 38: emphasizes the importance of legitimate processing of Private Data	This point would be complied with the fulfilment of all standards applied.	
Point 47: points responsibility of Private Data processing to Private Data Controller.	Point 3.7: investigators are the party responsible for developing appropriate strategies to process evidence [9].	Investigators are the party responsible for developing appropriate strategies to process evidence [9] thus putting investigators in Private Data Controller position.
Point 48: Private Data Controllers who are in form of legal entities that performs merger, separation, acquisition, consolidation, or dissolution are obligated to notify the Private Data Subject of the matter, including destruction and/or transfer of Private Data before and after the merger, separation, acquisition, consolidation, or dissolution	None	
Point 53, 54: obligation of both Private Data Controller and Private Data Processor to appoint a staff member to perform roles and responsibilities of Private Data Protection.	None	

Point 47 points the responsibility of Private Data processing to Private Data Controller. Going by the definition stated in Point 1 Clause 4 is the one who determines the goal and performs control of Private Data processing, this corresponds to digital forensic investigators who are involved in the investigation process as based on ACPO Good Practice Guide for Digital Evidence point 3.7 where it is mentioned that investigators are the party responsible for developing appropriate strategies to process evidence. In this case, the Private Data Controller and Private Data Processor mentioned in the law are within the same party and thus fulfill Point 51 and 52 about Private Data Processor's obligations.

i. Transfer of Private Data

This area consists of two points related to the transfer of private data inside and outside of Indonesia. The details of the statements can be found on Table 4.

Table 4. Transfer of Private Data

Indonesia's Data Protection Law	Existing Digital Forensic Standard	Analysis
Point 55: enables Private Data Controller to transfer Private Data to another Private Data Controller in Indonesia by adhering to the Private Data Protection law.	None	
Point 56: enables Private Data Controller to transfer Private Data to another Private Data Controller outside of Indonesia as long as the receiving Private Data Controller's country has a similar or higher level of Private Data Protection.	None	

Point 55 enables Private Data Controller to transfer Private Data to another Private Data Controller in Indonesia by adhering to the Private Data Protection law. This clause has not been mentioned in any digital forensic standard practice used in this research.

Point 56 enables Private Data Controller to transfer Private Data to another Private Data Controller outside of Indonesia as long as the receiving Private Data Controller's country has a similar or higher level of Private Data Protection. If unfulfilled, the Private Data Controller should ensure there is decent and binding Private Data Protection in place. If also unfulfilled, Private Data Controller is obligated to receive agreement from Private Data Subject.

The summary of the correlation performed between Indonesia's Private Data Protection law and existing digital forensic standards used in Indonesia can be seen on Table 5.

Table 5. Summary of Correlation

Status	No. of Clauses	Items
Excluded due to law enforcement purposes	16	Point 8, 9, 10, 11, 13, 17, 30, 32, 36, 40, 41, 42, 43, 44, 45, and 46
Inapplicable due to contradiction with law enforcement purposes	1	Point 6
Partially applicable due to certain cases where there is contradiction with law enforcement purposes	1	Point 7
Has been addressed and aligns with existing digital forensic standard used in Indonesia	14	Point 5, 12, 16, 18, 27, 28, 29, 31, 34, 35, 36, 37, 38, 39
Has not been addressed in existing digital forensic standard used in Indonesia	12	Point 7, 20, 21, 22, 23, 24, 25, 26, 48, 53, 54, 56

The summary of correlation in Table 6 allows us to calculate the compliance rate of current digital forensic standards against Indonesia's Private Data Protection law by dividing number of clauses that has been addressed and aligns with existing digital forensic standard used in Indonesia (14) against the total of clauses that is not explicitly mentioned excluded for law enforcement purposes (28) which resulted in 0,5 or 50%.

Meanwhile, to find the irrelevancy between Indonesia's Private Data Protection law and digital forensic investigation it is possible to divide the number of clauses that is explicitly mentioned excluded for law enforcement (16) against the total of clauses that states rights and obligations related to Private Data Protection (44) which resulted in 0,36 or 36%. Which also means that the relevancy of Indonesia's Private Data Protection law and digital forensic investigation is about 64%.

The twelve clauses that need to be addressed in digital forensic ethical data handling are evaluated and those with same focuses are merged into one statement which results in six statements as seen on Table 6.

Table 6 Statements Needs to be Addressed Based on Correlation Performed

Code	Statement	Basis
S1	Private Data Subject has the right to access and obtain a copy of the Private Data collected unless restricted by law enforcement purposes.	Point 7
S2	Digital Forensic Investigator should be able to present investigation basis in form of explicit legitimate agreement from Private Data Subject for one or more goals mentioned by Private Data Controller to Private Data Subject through written or recorded and electronic or non-electronic and/or other legitimate interests fulfilment purposes before collection of evidence.	Point 20
S3	Investigation conducted with Private Data of children and/or disabled should include agreement from the Private Data Subject's guardian.	Point 25 & 26
S4	Digital Forensic Investigators who are in form of legal entities that performs merger, separation, acquisition, consolidation, or dissolution are obligated to notify the Private Data Subject of the matter, including destruction and/or transfer of Private Data before and after the merger, separation, acquisition, consolidation, or dissolution.	Point 48
S5	Digital Forensic Investigators to appoint a staff member to perform roles and responsibilities of Private Data Protection stated in the Private Data Protection law.	Point 53 & 54
S6	Digital Forensic Investigators are allowed to transfer Private Data to another Private Data Controller outside of Indonesia within the conditions stated in the Private Data Protection law.	Point 56

d. Evaluation and Analysis

The questionnaire contains six (6) statements identified previously where respondents choose whether they agree or not with its' applicability in Indonesia's

digital forensic practices. The questionnaire received a total of six (6) responses with the details on Table 7.

Table 7 Questionnaire Responses

Statement Code	No. of Responses	
	Yes	***No***
S1	4	2
S2	5	1
S3	5	1
S4	4	2
S5	5	1
S6	3	3

A follow-up interview with several respondents is conducted for statements with more than 1 disagreeing response. Through the interview, it is uncovered that there are concerns regarding several statements as respondents deemed the statement unapplicable as it contradicts evidence handling procedure in Indonesia.

On the first statement, several respondents expressed concern as evidence is not supposed to be accessed by people without any role and/or rights in the investigation. However, upon further research, it is found that seized evidence is allowed to be lent to the evidence owner or parties with the right to borrow within permission of the investigator's supervisor [12]. Thus, the part of the statement that mentioned 'unless restricted by law enforcement purposes' should be proper in this case.

On the fourth statement, the concern expressed by respondent is related to investigation within public sector or investigation performed by the police. Respondent mentioned that it is possible for Private Data Subject to be unknowingly investigated in investigations conducted by the police. However, this clause has been addressed to in the correlation phase and the phrasing of the statement should be changed into a more specific phrase.

The concern expressed for the last statement is related to cases where the suspect is wanted internationally, the Private Data transfer should be addressed according to bilateral or international law. Thus, it is important to address the statement to fit this condition as well.

The result of the research shows that only 50% of the clauses have been addressed explicitly in existing digital forensics standards.

For the first statement, it is advisable to add limitation of restrictions as judged by the law enforcement. This is due to the statute of interventions that may take place at the earliest stage as deemed necessary by the law enforcement member before any harm was done [13]. The second statement should be able to be added to consideration especially considering how consent is required for the collection, use, or disclosure of personal information under the GDPR [14] and Indonesia's Private Data Protection law. As children in Indonesia have become more active in social media and the rising trend of cybercrime surrounding it [15],

it became important to include protection for the legal awareness regarding personal data on each child [16] as stated in the third statement.

The market is seeing a rising trend of acquisition and merger of Indonesian companies even if the rate of acquisition and merger conducted by Indonesian companies can be seen as fewer than other foreign countries [17]. Thus, the protection of private data being held by entities who undergo structural changes such as mergers and acquisition is stated in the fourth statement.

The fifth statement talks about a designated Data Protection Officer in the digital forensic investigation. A Data Protection Officer should be someone who has expert knowledge of data protection law and practices and the ability to fulfil the tasks [18]. This role is relevant to the digital forensic area as the role is required for core activities which involve processing special categories of data or criminal convictions or offences data on a large scale [18].

Jurisdiction in cybercrimes is a tricky issue when certain acts are legal in the state where they are initiated and may be illegal in other states [19]. In 2020, Taiwanese law enforcement investigated a high-profile case of European criminals who hacked into a Taiwanese financial institution by collaborating with different branches of law enforcement involved in the investigations [20]. In such cases, the sixth statement should be applicable in which the investigation involved multiple law enforcements, and the suspect is originated from another country.

E. Conclusion

Digital forensics investigations are used by law enforcement to investigate a variety of digital devices that can be exploited for criminal activity. 36% Indonesia's Private Data Protection law clauses that states rights and obligations related to Private Data Processing is explicitly mentioned to be excluded for law enforcement purposes which brings down the relevancy of the law to digital forensic investigations to 64%.

However, it needs to be noted that in cases where digital forensic investigations are performed privately and not in relation to law enforcement purposes, the clauses that have been excluded in this research must be adhered to.

Among the clauses in the law that are not explicitly mentioned excluded for law enforcement purposes, only 50% of the clauses have been addressed explicitly in digital forensics standards. This means that there are still room for ethical data handling practices to be improved in Indonesia's digital forensics investigation.

The clauses that have not been addressed in digital forensic standards used in Indonesia are summed up into six different statements that is evaluated by Indonesian digital forensic investigators for its' applicability to digital forensic practices in Indonesia. The evaluation of the statements resulted in concerns as there needs to be more context to the statement for different cases. Future studies should aim to enhance digital forensic ethical data handling in Indonesia to raise the rate of compliance to the law.

F. References

[1] Verma, R., Govindaraj, J., & Gupta, G. (2016). Data privacy perceptions about digital forensic investigations in India. In *Advances in Digital Forensics XII: 12th IFIP WG 11.9 International Conference, New Delhi, January 4-6, 2016, Revised Selected Papers 12* (pp. 25-45). Springer International Publishing.

[2] *Srinivasan, S. (2006, November). Security and privacy in the computer forensics context. In 2006 International Conference on Communication Technology (pp. 1-3). IEEE.*

[3] Horsman, G. (2022). Defining principles for preserving privacy in digital forensic examinations. *Forensic Science International: Digital Investigation*, *40*, 301350.

[4] Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2020). The framework to support the digital evidence handling: A case study of procedures for the management of evidence in Indonesia. *Journal of Cases on Information Technology (JCIT)*, *22*(3), 51-71.

[5] Badan Standarisasi Nasional (BSN). Pentingnya Forensik Digital Sesuai SNI ISO/IEC 17025:2017. https://www.bsn.go.id/main/berita/detail/11148/pentingnya-forensik-digital-sesuai-sni-isoiec-170252017, 2020, retrieved June 15, 2023.

[6] International, D. (2017). *DAMA-DMBOK: Data management body of knowledge*. Technics Publications, LLC.

[7] BSN. (2018). Persyaratan umum kompetensi laboratorium pengujian dan atau laboratorium kalibrasi dalam ISO/IEC 17025:2017.

[8] ACPO (Association of Chief Police Officers). (2012). ACPO good practice guide for digital evidence.

[9] Standard Operasional Prosedur Penyitaan Bareskrim Polri.

[10] ISO/IEC 27037:2012 - Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence.

[11] Peraturan Kapolri No. 10 Tahun 2010 tentang Tata Cara Pengelolaan Barang Bukti di Lingkungan Kepolisian Negara Republik Indonesia

[12] Shavell, S. (1993). The optimal structure of law enforcement. *The Journal of Law and Economics*, *36*(1, Part 2), 255-287.

[13] Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019, November). (Un) informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 acm sigsac conference on computer and communications security* (pp. 973-990).

[14] Tiwari, S., Rai, S. K., & Sisodia, V. (2023). Rising cybercrime on social media during covid pandemic and its impact on digital marketing. *Academy of Marketing Studies Journal*, *27*(S4).

[15] Sari, R. K., Purwoleksono, D. E., & Paripurna, A. (2023). The Legal Certainty On Children's Personal Data: Realizing Legal Protection On Social Media. *Syiah Kuala Law Journal*, *7*(2), 130-140.

[16] Tarigan, J., Claresta, A., & Hatane, S. E. (2018). Analysis of merger & acquisition motives in Indonesian listed companies through financial performance perspective. *Kinerja*, *22*(1), 95-112.

[17] Lambert, P. (2016). *The Data Protection Officer: Profession, Rules, and Role*. CRC Press.
[18] Brenner, S. W., & Koops, B. J. (2004). Approaches to cybercrime jurisdiction. *J. High Tech. L.*, *4*, 1.
[19] Wang, S. Y. K., Hsieh, M. L., Chang, C. K. M., Jiang, P. S., & Dallier, D. J. (2021). Collaboration between law enforcement agencies in combating cybercrime: implications of a taiwanese case study about ATM hacking. *International journal of offender therapy and comparative criminology*, *65*(4), 390-408.