The Indonesian Journal of International Clinical Legal Education
Vol. 7 Issue 2 (2025) 203-234
DOI: https://doi.org/10.15294/ijicle.v7i2.21049
Available online since: June 30, 2025

The Indonesian Journal of International Clinical Legal Education
https://journal.unnes.ac.id/sju/index.php/iccle/index

Implementation of CNIL's Basic Logging Measures in Indonesia: A Juridical Study on Personal Data Protection

Tegar Islami Putra ✉
Faculty of Law, Universitas Negeri Semarang, Semarang, Indonesia

Nurul Fibrianti
Faculty of Law, Universitas Negeri Semarang, Semarang, Indonesia

Adinda Zeranica Putri Fakhis
Ahmad Ibrahim Kulliyyah of Laws, Faculty of Law,
International Islamic University Malaysia, Malaysia

✉ Corresponding email: tegarislami44@students.unnes.ac.id

Abstract

One of the efforts to realize preventive efforts to prevent all risks of personal data protection is to establish basic precaution logging as a personal data protection strategy that will serve as a guide for parties involved in personal data protection efforts. Indonesia, which has not formulated such a strategy, can make the provisions in France as a reference. The urgency of this research is that there is a mandate in Article 59 letter a of the Personal Data Protection Law in Indonesia for the Institution

to formulate and determine policies and strategies for Personal Data Protection as a guide. This research employs the Library Research method, also known as Legal Research, which focuses on analyzing primary and secondary legal materials based on literature. The results show that France already has an institution called CNIL which formulates basic precautions in logging operations to guide personal data protection strategies. As a result, there are 8 basic precautions in logging operations, which are to provide a logging system that can implement and learn by Indonesia, that are: keep these logs for a rolling period of between six months and one year; perform, for application logs, a record of the creation, consultation, sharing, modification, and deletion; inform users; protect the logging equipment and the logged information; ensure the proper functioning of the logging system; ensure that processors are contractually obliged; and actively analyze, in real time or in the short term.

Keywords

CNIL; Basic Precaution Logging; Indonesia; Personal Data Protection Strategy.

I. Introduction

The development of information and communication technology continues to take place and develop so fast that has become one of the triggers for the digitalization in the world, especially in Indonesia.[1] In

[1] Mahima Umaela Firdhausya et al., "The Urgency of Limiting The Utilization of Consumer IP Addresses By Companies as Personal Data Objects in The Study of Positive Law in Indonesia," *Law Research Review Quarterly* 10, no. 2 (2024): 393-410: 394.

Indonesia, the Internet Service Providers Association announced that the number of internet users in Indonesia in 2024 reach 221 million.[2] The prevalence of data breach, both domestically in Indonesia and international underscores the critical importance of integrating robust data protection measures into existing legal frameworks.[3] To guarantee the privacy rights of citizens, Indonesia has passed a regulation on personal data protection through Law No.27 of 2022 concerning Personal Data Protection that was passed by the President of Republic of Indonesia on October 17, 2022.[4] This legislative milestone coincided with a surge in incidents involving the unauthorized disclosure of personal data.[5] The concept of data protection and cyber security is a form of effort made to project user identity from various threats and legal access.[6]

The various parties involved in personal data protection efforts are described in Law No.27 of 2022 on Personal Data Protection. In general, the parties involved in personal data protection efforts, especially in Indonesia, are the government, personal data controller, personal data subject, and personal data protection institution. The role

---

2 Nurul Fibrianti et al., "Review of Child Consumer Protection in the Practice of Online Gambling Games Through the Gacha System," *The Indonesian Journal of International Clinical Legal Education* 6, no. 3 (2024): 427-452: 429.

3 Tegar Islami Putra and Nurul Fibrianti, "Threats and Legal Protection of Personal Data Combined in E-Commerce Transactions Based on Personal Data Protection Law in Indonesia," *Lambung Mangkurat Law Journal* 9, no. 1 (2024): 64–74: 65.

4 Tegar Islami Putra and Nurul Fibrianti, "Data Protection Impact Assessment Indicators in Protecting Consumer Personal Data on E-Commerce Platforms," *Legal Challenges in Overcoming the Digital Divide (Article in Press)* 6, no. 1 (2024): 111–150: 115.

5 Tegar Islami Putra, Akbar Jihadul Islam, and Abdullah Mufti Abdul Rahman, "Integrating Islamic Laws into Indonesian Data Protection Laws: An Analysis of Regulatory Landscape and Ethical Considerations," *Contemporary Issues on Interfaith Law & Society* 4, no. 1 (2024): 85–118: 95.

6 Tegar Islami Putra et al., "Critically Reveal The Dimensions of Damage From Unauthorized Use of Personal Data," *The Digest: Journal of Jurisprudence and Legisprudence* 5, no. 2 (2025): 231-262: 233.

of each party in personal data protection efforts has been explained in the law. One of the roles explicitly explained in the Law is what is carried out by the Personal Data Protection Agency as described in Article 59. In the Article in letter a, it explains that the Personal Data Protection Agency carries out the formulation and determination of policies and strategies for personal data protection which serve as guidelines for personal data subjects, personal data controllers, and personal data processors.

Policies and strategies for the protection of personal data in Indonesia need to be formulated immediately, this aims to be a guide for all parties involved in personal data protection efforts. This policy and strategy can later become a guide for all parties in every stage of personal data processing. As stipulated in Article 16 of Law No.27 of 2022, the processing of personal data includes acquisition and collection; processing and analysis; storage; correction and updating; display, announcement, transfer, dissemination, or disclosure; and/or erasure or destruction. In each of these processing stages, it is necessary to establish a personal data protection strategy to guide all parties to avoid all personal data protection risks that may lead to other crimes. These crimes can be in the form of phishing, ransomware, online fraud, site and e-mail hacking, skimming crime, illegal content crime, cyber espionage, data falsification, cyber terrorism, identity thief, and so on.[7]

From the first processing of personal data to the final stage of processing, preventive measures must be taken to prevent all personal data protection risks. Since the first processing of personal data, the French data protection authority (Commission Nationale Informatique et Libertés/CNIL) has formulated a guide on preparing for an incident since the processing of personal data is carried out. Meanwhile, in Indonesia, the guidelines regarding the personal data protection strategy

[7] Muhamad Naufal and Aulia Azmi, "Analisa Kasus Kebocoran Data Pada Bank Indonesia Dalam Sistem Perbankan," *Jurnal Multidisiplin Ilmu Akademik* 1, no. 6 (2024): 448-458: 452.

policy have not been approved until this research was written, including the guidelines for logging personal data operations. These guidelines will be formulated and stipulated by the personal data protection agency as stipulated in Article 59 letter a of Law Number 27 Year 2022.

This research aims to analyze basic precaution logging as regulated in France and implement it in Indonesian regulations as will be formulated and determined later by the Personal Data Protection Agency in the personal data protection strategy. This will later become a guide regarding basic precaution logging of personal data for all parties involved in the processing of personal data, namely personal data subjects, personal data controllers, and personal data processors.

Similar research has been conducted by Maharani as published in the journal Edunity Vol.3 (6) in 2024. This research discusses The Urgency of a Personal Data Protection Institution within the Framework of Digital World Resilience. The results show that public institutions cannot immediately solve the problem of personal data management in Indonesia. A specific foundation zeroed in on supervising the administration of individual information is required, working as a device to smother infringement of individual information security. In order to strengthen the government's role in implementing personal data protection, the PDP Law mandates the establishment of an institution that plays a role in implementing personal data protection as stipulated in Article 58 of the Law No.27 of 2022.[8]

Similar research has been conducted by Yolanda as published in the Indonesian Scientific journal Vol.8 (6) in 2023. One of the findings of the research resulted in the finding that provisions regarding the role of personal data protection institutions have been present in Law Number 27 of 2022, precisely in Chapter IX regarding institutions, which states that the institution for organizing personal data protection

[8] Dhea Yulia Maharani and Suparno, "The Urgency of Personal Data Protection Agencies on Sustaining The Resilience of The Digital World," *Edunity* 3, no. 6 (2024): 345-353: 349.

will be formed by the president and is responsible to the president, and there are also arrangements regarding the authority of this institution later. The absence of the institution's existence causes legal uncertainty that causes the values of certainty, justice and expediency to be blurred.[9]

Similar research has been conducted by Ayiliani as published in the Indonesian Journal of Legal Development Vol.6 (3) in 2024. This research specifically discusses the urgency of establishing a personal data supervisory institution as an effort to protect the law against cross-border personal data transfers. The results of this research on the personal data protection institution show that the crucial role held is the supervisory function and facilitates the submission of complaints related to alleged violations of Law Number 27 of 2022 both domestically and abroad.[10]

Based on several similar previous studies as mentioned above, there are still limited studies that analyze the personal data protection agency, especially in Indonesia. None of the above studies discuss the Indonesian personal data protection agency in formulating protection strategy by implementing French basic precaution logging operations. So that this research will basically have a great novelty for science regarding personal data protection agencies in Indonesia. This research is expected to be a reference for future research that discusses personal data protection in Indonesia and the world, especially regarding the institution that oversees personal data protection in Indonesia. Therefore, the researcher is interested in writing a research entitled Indonesian personal data protection agency in formulating protection strategy: French basic precaution logging operations implementation.

---

9 Erlyns Yolanda and Rugun Romaida Hutabarat, "Urgensi Lembaga Pelindungan Data Pribadi Di Indonesia Berdasarkan Asas Hukum Responsif," *Jurnal Ilmiah Indonesia* 13, no. 1 (2023): 4166-4182: 4168.

10 Fanisa Mayda Ayiliani et al., "Urgensi Pembentukan Lembaga Pengawas Data Pribadi Sebagai Upaya Pelindungan Hukum Terhadap Transfer Data Pribadi Lintas Negara," *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431-455: 431.

There are two main objectives that form the basis of this research which are fully related to the novelty of personal data protection. First, this research aims to reveal the basic concept of French basic precaution logging operations. Second, to examine the implementation of French basic precaution logging operations in Indonesian personal data protection strategy. The selection of France as a comparison is due to the existence of a personal data protection supervisory institution in France. In addition, France is one of the countries that implement the Euro Union General Data Protection Regulation which has become a reference for personal data protection regulations throughout the world. Based on the background of the problem as described above, this study draws the following problem formulations: (1) What is the legal basis for French and Indonesian Supervisory Authorities to Formulate a Personal Data Protection Strategy? (2) How is the juridical study of implementing the French Basic Precaution Logging Operations in Indonesia's Personal Data Protection Strategy?

II. Method

This scientific research uses one of the grand method sections, namely Library Research which is based on literature or literature. Based on the subject of study and the type of problem that exists, of the 3 (three) types of grand methods mentioned above, this research will use the Library Research method. Regarding this kind of research, it is also commonly called "Legal Research".[11] This kind of legal research does not recognize field research (field research) because what is studied is legal material so that it can be said to be library based, focusing on

[11] Soerjono Soekanto and Sri Mamudji, *Penelitian Hukum Normatif Tinjauan Singkat* (Jakarta: Rajawali Press, 2006): 66.

reading and analysis and analysis of the primary and secondary materials.[12]

III. Legal Basis of French and Indonesia Supervisory Authority to Formulating Personal Data Protection Strategic

In 1978, the French Government enacted Law 78-17, the Law on Computers, Files and Freedoms, which guarantees the protection of personal data on computer media as a logical consequence of the SAFARI policy (Système Automatisé pour les Fichiers administratifs et le Répertoire des Individus)[13] and GAMIN (Gestion Automatiséee de la Médicine Infantile).[14]

To ensure the proper implementation of this law, the provisions of Chapter III provide for the existence of an independent administrative body called the National Commission on Informatics and Liberty (Commission Nationale Informatique et Libertés/CNIL). The CNIL was established on January 6, 1978. This institution is the 'backbone' of the pillars supporting the legal culture of the personal data protection in the EU member states. According to Chapter VII of the French Government enacted Law 78-17, the Law on Computers, Files and Freedoms, CNIL has two main tasks, namely: (i) to monitor the implementation of this law, and (ii) to sanction violators.[15]

---

12 Jhony Ibrahim, *Teori Dan Metodologi Penelitian Hukum Empiris* (Malang: Bayumedia Publishing, 2006): 98.

13 Henri Delahaie and Félix Paoletti, *Informatique et Libertés* (Paris: Editions La Découverte, 1987): 20.

14 Herbert Burkert, "Privacy/Data Protection: A German/European Perspective," in *Proceedings of 2nd Symposium of the Max Planck Project Group on the Law of Common Goods and the Computer Science and Telecommunications Board of the National Research Council* (Massachusets: Wood Hole, 1999): 50.

15 Wahyudi Djafar, *Perlindungan Data Pribadi Di Indonesia, Lembaga Studi Dan Advokasi Masyarakat (ELSAM)* (Jakarta Selatan: ELSAM, 2016): 21.

CNIL is responsible for overseeing and enforcing the implementation of the European Union General Data Protection Regulation (GDPR) in France. As part of this task, the CNIL may formulate a personal data protection strategy to ensure data processing is done to carry out some of the GDPR mandates. To support the data protection strategy, the CNIL is authorized to conduct investigations that may result in strategic recommendations, guidelines or guidelines to strengthen personal data protection in France. This is as contained in GDPR Article 57 paragraph 1 letter c:

> *"Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory to advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing."*

In addition, CNIL may also formulate a personal data protection strategy to ensure data processing is carried out to carry out the mandate of Recital 122 of the GDPR which reads:

> *"Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation. This should cover in particular the processing in the context of the activities of an establishment of the controller or processor on the territory of its own Member State, the processing of personal data carried out by public authorities or private bodies acting in the public interest, processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory. This should include handling complaints lodged by a data subject, conducting investigations on the application of this Regulation and promoting public awareness of the*

risks, rules, safeguards and rights in relation to the processing of personal data."

Whereas in Indonesia, there are slight differences. The personal data protection agency is one of the key factors in the implementation of privacy and data protection policies.[16] The design of the form, duties, and authority of the Personal Data Protection Supervisory Institution in Indonesia seems to imply that this Institution has a special position.[17] According to Jimly Ashiddiqie, such institutions are better known as statue auxiliary organs or auxiliary institutions. This term is defined as a State Institution that is supportive and independent.[18]

The regulation of the personal data protection institution itself has been regulated in several articles in Chapter IX of Law Number 27 Year 2022. However, this institution has not yet been established and does not have an official name. In Law Number 27 of 2022, the regulation of this institution can be found in Article 58, Article 59, and Article 60, namely:[19]

a) *Arrangements related to personal data protection institutions as in Article 58 of Law Number 27 Year 2022, explains the following:*
    (1) *The Government shall play a role in the implementation of Personal Data Protection in accordance with the provisions of this Law.*

---

16 Farah Naurah Khansa, "Penguatan Hukum Dan Urgensi Otoritas Pengawas Independen Dalam Pelindungan Data Pribadi Di Indonesia," *Jurnal Hukum Lex Generalis* 2, no. 8 (2021): 649-662: 657.

17 Gunawan Widjaja and Fransiska Milenia Cesarianti, "Urgensi Pembentukan Lembaga Pengawas Pelindungan Data Pribadi Di Indonesia Berdasarkan Pasal 58 Juncto Pasal 59 Dan Pasal 60 Undang – Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *SINERGI : Jurnal Riset Ilmiah* 1, no. 4 (2024): 234-242: 239.

18 Jimly Asshiddiqie, *Perkembangan Dan Konsolidasi Lembaga Negara Pasca Reformasi* (Jakarta: Sinar Grafika, 2012): 7.

19 Widjaja, *Loc.Cit.*

(2) *The implementation of Personal Data Protection as referred to in paragraph (1) shall be carried out by an institution.*
(3) *The institution as referred to in paragraph (2) shall be stipulated by the President.*
(4) *The institution as referred to in paragraph (2) shall be responsible to the President.*
(5) *Further provisions regarding the institution as referred to in paragraph (2) shall be stipulated by Presidential Regulation.*

b) *The regulation regarding the institution for the protection of personal data as stipulated in Article 59 of Law Number 27 Year 2022 explains the matters carried out by the institution for the protection of personal data, namely:*
(1) *Formulation and stipulation of policies and strategies for Personal Data Protection that serve as guidelines for Personal Data Subjects, Personal Data Controllers, and Personal Data Processors.*
(2) *Supervision of the implementation of personal data protection.*
(3) *Administrative law enforcement against violations of Law Number 27 Year 2022.*
(4) *Facilitation of out-of-court dispute resolution.*

c) *Regulation on personal data protection institution as stipulated in Article 60 of Law Number 27 Year 2022 describes the authority of personal data protection institution, namely:*
(1) *To formulate and stipulate policies in the field of personal data protection.*
(2) *To supervise the compliance of personal data controller.*

(3) *To impose administrative sanctions for violations of Personal Data Protection committed by Personal Data Controller and/or Personal Data Processor.*

(4) *Assist law enforcement officials in handling allegations of Personal Data criminal offense as referred to in this Act.*

(5) *Cooperate with Personal Data Protection institutions of other countries in the context of resolving alleged cross-border violations of Personal Data Protection.*

(6) *To assess the fulfillment of requirements for transfer of Personal Data outside the jurisdiction of the Republic of Indonesia.*

(7) *To give orders in the context of follow-up of supervision results to the Personal Data Controller and/or Personal Data Processor.*

(8) *To publish the results of supervision implementation of Personal Data Protection in accordance with the provisions of laws and regulations.*

(9) *To receive complaints and/or reports regarding the alleged violation of Personal Data Protection:*

(10) *To examine and trace the complaints, reports, and/or the results of supervision on the alleged violation of the protection of personal data.*

(11) *To summon and present any Person and/or Public Body related to the alleged violation of the Protection of Personal Data.*

(12) *To request information, data, information, and documents from any Person and/or Public Entity related to the alleged violation of the Protection of Personal Data.*

(13) *To summon and present experts required in the examination and investigation related to the alleged violation of the Protection of Personal Data.*

(14) *To conduct examination and investigation on electronic system, facility, room, and/or place used by Personal Data Controller and/or Personal Data Processor, including obtaining access to data and/or appointing a third party.*
(15) *To request legal assistance to the prosecutor's office in the settlement of disputes over Personal Data Protection.*

Based on the juridical basis as stated above, it can be determined implicitly that the establishment of personal data protection strategy in France can be done by CNIL as the mandate of GDPR Article 57 paragraph 1 letter c. Whereas in Indonesia, it is clear that by the personal data protection institution in Indonesia, the establishment of personal data protection strategy is the mandate of Article 59 of Law Number 27 Year 2022.

IV. Juridical Study of Implementing The French Basic Precaution Logging Operations in Indonesia's Personal Data Protection Strategy

The CNIL published "Practice Guide for the Security of Personal Data" (Version 2024). One of the mentioned topics within the guidance are "Logging Operations" (Factsheet 16). The CNIL has already adopted recommendations on the adoption of logging measures. A logging system is an essential tool for personal data security, where it can be used to identify incidents or unauthorized access. In order to identify fraudulent access or misuse of personal data, or to define the origin of an incident, it is essential to record certain actions performed on IT systems. The records that are then collected are also useful evidence to demonstrate compliance. There are 8 basic precautions in logging operations, that are provide a logging system; keep these logs for a

rolling period of between six months and one year; perform, for application logs, a record of the creation, consultation, sharing, modification, and deletion; inform users; protect the logging equipment and the logged information; ensure the proper functioning of the logging system; ensure that processors are contractually obliged; and actively analyze, in real time or in the short term.

A. Provide A Logging System

The first precaution is providing a logging system. Provide a logging system for user activities, technical interventions, anomalies and security-related events. (i.e. recording system in log files). Logs provide important insight regarding the activity on a system or a network. With the help of logs, your security professionals can keep track of the activity on the systems and networks of your organization, notice unusual activity/ CNIL does not provide further explanation regarding these precautions. CNIL state that:

> "*Provide a logging system (i.e. recording system in log files) of users' business activities (application logs), technical interventions (including by administrators), anomalies and security-related events (technical or system logs).*"

Based on Savinov research state there are two types of records management system, post-Soviet system of records management and Western system of records management.[20] In the Western records management system, the movement of records is horizontal: they are received by the organization and sent to the executors without additional redirection to the head immediately. In the Post-Soviet records management system, the movement of records is not horizontal, but vertical, that is, according to the head-executor-head scheme.[21] In the end, it should be noted that records management at

---

20 Alexey Savinov, "Systems of Record Management," *InterConf* 73 (2021): 61-66: 62.

21 *Ibid.*

the international level is becoming more and more integrated, as there is exchange of practical and theoretical experience through various international conferences of a scientific and practical nature, online seminars.[22]

Whereas in the EU GDPR, this precautionary measure is regulated in Article 30 which states:

> "*Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.*"

The point of Provide a Logging System is in line with the mandate of Article 31 of Law Number 27 of 2022 which reads:

> *"The Personal Data Controller must record all Personal Data processing activities."*

B. Keep These Logs for A Rolling Period of Between Six Months and One Year

To meet data retention requirements, organizations might need to keep copies of log files for a longer period of time than the original log sources can support, which necessitates establishing log archival processes. Because of the volume of logs, it might be appropriate in some cases to reduce the logs by filtering out log entries that do not need to be archived.[23] The confidentiality and integrity of the archived logs also need to be protected. It is important to keep logs for a period of between six months and one year, unless there is a legal obligation or other specific need. Log files are an important source of digital forensic evidence because they

---

22 *Ibid.*

23 Karen Kent and Murugiah Souppaya, *Guide to Computer Security Log Management, NIST Special Publication*, 2006: 16.

usually connect events to points in time.[24] Whereas in the EU GDPR these precautions are not regulated with specific. However, the EU GDPR mandates that the data of data subjects for no longer than is necessary for the purposes for which the personal data are processed. This is as stipulated in Article 5 Paragraph 1 (e) which essentially states:

> "*Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.*"

Law No. 27 of 2022 does not specifically state that These Logs For A Rolling Period Of Between Six Months and One Year. Although, the point of Keep These Logs For A Rolling Period Of Between Six Months and One Year is in line with the mandate of Article 35 letter a of Law Number 27 Year 2022 which basically states:

> *"The Personal Data Controller shall develop and implement operational technical measures to protect Personal Data from interference with the processing of Personal Data contrary to the provisions of laws and regulations."*

C. Perform, For Application Logs, A Record of The Creation, Consultation, Sharing, Modification and Deletion

CNIL states that these precautions are to avoid duplication. The mandate states that these precautions:

> "*Perform, for application logs, a record of the creation, consultation, sharing, modification and deletion of the data by retaining the author's identifier, the date, time and nature of the operation as well as the reference of the data concerned (to avoid duplication).*"

---

[24] Dario Forte, "The Importance of Log Files in Security Incident Prevention," *Network Security* 7 (2009): 18–20:19.

In the EU GDPR, the provision on avoiding duplication is in line with the mandate of Article 5 Paragraph 1(c) relating to the principles relating to the processing of personal data which states:

> "*Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization').*"

Through the mandate in Article 5 Paragraph 1 (c), it can be identified to emphasize the recording of relevant and necessary data without duplicating data. Which refers to the use of unique references or identifiers to link log data with processed data without having to duplicate the information in its entirety.

The point Perform, For Application Logs, A Record of The Creation, Consultation, Sharing, Modification and Deletion is in line with the mandate of Article 31 of Law Number 27 of 2022 which basically states:

> *"The Controller of Personal Data is obliged to record all Personal Data processing activities."*

D. Inform Users

Inform Users as a basic precaution, CNIL state that:

> *''Inform users, e.g. when authenticating or accessing the system, of setting up the logging system, after informing and consulting the representative bodies of the staff."*

In the EU GDPR, this basic precaution is in line with the mandate of Article 12 Paragraph 1 which states:

> *"The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent,*

> *intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."*

The data subject has the right to obtain "a copy of the personal data undergoing processing". This copy must be provided free of charge. This right to access is intended to allow individuals to check whether the processing of their data is lawful.25 Users should be informed of the existence of the logging system, including the type of data recorded, the reason for recording, and how the data is used. This principle demands the delivery of information in a transparent, simple, and easy-to-understand manner to build trust with data subjects.

The inform users point is in line with the mandate of Article 21 paragraph (1) of Law Number 27 of 2022 which states:

> *"In the case of processing personal data based on consent, the personal data controller shall provide information regarding:*
> *a) The legality of the processing of personal data;*
> *b) The purpose of the processing of personal data;*
> *c) The type and relevance of the personal data to be processed;*
> *d) The retention period of documents containing personal data;*
> *e) Details of the information collected;*
> *f) Period of processing of personal data; and*
> *g) Rights of the subject of the personal data."*

25 I. van Ooijen and Helena U. Vrabec, "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective," *Journal of Consumer Policy* 42, no. 1 (2019): 91-107: 102.

E. Protect The Logging Equipment and The Logged Information

This basic precaution state by CNIL that:

> *"Protect the logging equipment and the logged information against unauthorized operations (e.g. by making them inaccessible to the individuals whose activity is logged), misuse by authorized accounts (e.g.: by setting up a use charter or specific alerts) and the crushing of logs generated by the concerned applications."*

In the EU GDPR, this basic precaution is in line with the mandate of Article 32 Paragraph 1 regarding security of processing, which states:

> *"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk."*

The word appropriate is key; it is natural to expect higher security standards from a large corporation handling sensitive data (e.g., a hospital or a bank) than from a small business with a small number of employees and customers.[26] The point of protecting the logging equipment and the logged information is in line with the mandate of Article 35 letters a and b of Law Number 27 of 2022 which basically states:

> "*The personal data controller shall protect and ensure the security of the personal data it processes, by:*

---

[26] Tina Marjanov et al., *Data Security on the Ground: Investigating Technical and Legal Requirements under the GDPR, Proceedings on Privacy Enhancing Technologies*, vol. 2023 (Association for Computing Machinery, 2023): 405.

a) The development and implementation of technical operational measures to protect personal data from interference with the processing of personal data contrary to the provisions of laws and regulations;
b) Determining the level of security of personal data taking into account the nature and risks of the personal data to be protected in the processing of personal data."

F. Ensure The Proper Functioning of The Logging System

This basic precaution state by CNIL that:

"Ensure the proper functioning of the logging system by integrating the equipment into a monitoring tool and regularly checking the presence of exploitable logs."

In the EU GDPR, this basic precaution corresponds to the provision of resilience of Processing Systems as mandated by Article 32 Paragraph 1 (b) which states:

"*Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.*"

To ensure the proper functioning of the logging system also need the robust security to implement. There are some practical/technical points of view to ensure data security on the ground by evaluating existing industry standards (e.g., ISO-family),

practices (e.g., Privacy by Design Privacy Policy) and existing technologies (e.g., smart phones, blockchain, Internet-of-Things).[27]

The point of protect ensure the proper functioning of the logging system is in line with the mandate of Article 35 letter a of Number 27 of 2022 which basically states:

> *"The personal data controller is obliged to protect and ensure the security of the personal data it processes, by preparing and implementing operational technical measures to protect personal data from interference with personal data processing that is contrary to the provisions of laws and regulations."'*

G. Ensure That Processors Are Contractually Obliged

This basic precaution state by CNIL that:

> *"Ensure that processors are contractually obliged to implement logging in accordance with these recommendations and to notify as soon as possible of any anomaly or security incident to the controller."*

In the EU GDPR, this basic precaution is in line with the mandate of Article 28 Section 3 on security of processing, which mentions a Data Protection Agreement (DPA):

> *"Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller."*

DPA is a "legally binding contract that states the rights and obligations of each party concerning the protection of personal

[27] Marjanov. *et. al.*

data."[28] Specifically, under Article 28 of the GDPR, there are eight topics that must be addressed in a DPA: (1) the processor agrees to process personal data only on written instructions of the controller; (2) confidentiality is required for all parties coming into contact with the data; (3) appropriate technical and organizational measures are utilized to protect the security of the data; (4) the processor will not subcontract to another processor, unless instructed to do so in writing by the controller, in which case another DPA will be required to be signed with the subcontractor; (5) the data processor will aid the controller in upholding the controller's obligations under the GDPR; (6) the processor will help the controller maintain GDPR compliance with regard to Article 32 and Article 36 of the GDPR (regarding the security of processing and consultation with data protection authority before undertaking high-risk processing); (7) the processor will agree to delete all personal data upon the termination of services or return the data to the controller; and (8) the processor must allow the controller to conduct an audit and will provide whatever information is necessary to prove compliance.[29]

The point of protecting ensure the proper functioning of the logging system is in line with the mandate of Article 51 paragraph (1) and paragraph (3) of Number 27 of 2022. Article 51 paragraph (1) states:

> *"In the event that the Personal Data Controller appoints a Personal Data Processor, the Personal Data Processor shall be obliged to carry out the processing of Personal Data based on the order of the Personal Data Controller."*

---

[28] Aska Fujimori-Smith, "Analysis of Global Data Privacy Regulations and How Transnational Companies Are Impacted," *Santa Clara High Technology Law Journal* 40, no. 1 (2024): 91-114: 102.

[29] *Ibid.*

Meanwhile, Article 51 paragraph (3) of Law Number 27 Year 2022 states:

> *"The processing of Personal Data as referred to in paragraph (1) is included in the responsibility of the Controller of Personal Data."*

The point of protect ensure the proper functioning of the logging system is basically also in line with the definition of the personal data processor itself as mandated by Article 1 point 5 of Law Number 27 Year 2022 which states:

> *"Personal Data Processor is any person, public body, and international organization acting individually or jointly in the processing of Personal Data on behalf of the Personal Data Controller."*

H. Actively Analyze, in Real Time or in The Short Term

The term real-time system signifies the requirement for IT systems to process events as they occur and within a specified time interval. This time interval is typically in order of milli-, micro- or even nano-seconds, depending on the system in question. Real-time systems are often said to be the systems in which timeliness is essential to correctness.[30] This basic precaution also state by CNIL that:

> *"Actively analyze, in real time or in the short term, the logs collected to be able to detect the occurrence of an incident."*

In EU GDPR, this basic precaution is in line with mandate in Article 32 Paragraph 1 d about Regular Testing, Assessing, and Evaluating Security Measures, states that:

---

[30] Z. Milosevic et al., "Real-Time Analytics," in *Big Data* (Elsevier, 2016), 39-61: 42.

"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing."

This is important to consider, with an example being a Data Protection Impact Assessment (DPIA). The importance of DPIAs has grown in recent years and fines for non-compliance or malpractice are not uncommon. For instance, in 2022, two Belgian airports received fines due to the inadequate quality of their DPIA processes, while in 2023, a Dutch financial services provider was fined for failing to appropriately conduct a DPIA before processing special categories of personal data on a large scale Similarly, in January 2024, the Danish Data Protection Authority fined a controller operating a secure document platform for failure to conduct a DPIA.[31]

The point of actively analyze, in real time or in the short term is basically in line with the mandate of Article 34 paragraph (1) and Article 35 letter a of Law Number 27 of 2022. Article 34 paragraph (1) of Law Number 27 of 2022 states:

> *"The Personal Data Controller shall conduct a Personal Data Protection impact assessment in the event that the processing of Personal Data poses a high potential risk to the Personal Data Subject."*

[31] Kevin Werbach, "What Could Possibly Go Wrong?," *Technology and Regulation,* 2019, 309-329: 314.

While Article 35 letter a of Law Number 27 Year 2022 states in essence:

> "*The Personal Data Controller shall protect and ensure the security of the Personal Data it processes, by preparing and implementing operational technical measures to protect personal data from interference with the processing of personal data contrary to the provisions of laws and regulations.*"

It should be noted, every strategy that will be implemented in the logging operation as described above is carried out in accordance with the principles of Personal Data Protection as stipulated in Article 16 paragraph (2), which includes:

a) *Personal data collection is limited and specific, legally valid, and transparent;*
b) *Processing of personal data is carried out in accordance with its purpose;*
c) *Processing of personal data is carried out by guaranteeing the rights of the Personal Data Subject;*
d) *The processing of personal data shall be accurate, complete, not misleading, up-to-date and accountable;*
e) *The processing of personal data is carried out by protecting the security of personal data from unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction, and/or erasure of personal data;*
f) *Processing of personal data is carried out by informing the purposes and activities of processing, as well as the failure of Personal Data Protection;*
g) *Personal Data shall be destroyed and/or erased after the retention period has expired or based on the request of the Personal Data Subject, unless otherwise provided by laws and regulations; and*

h) *Processing of Personal Data is carried out responsibly and can be clearly proven.*

Based on the juridical and comparative study of the implementation of *Basic Precaution Logging Operations* by CNIL in France and its relevance to the strategic needs of personal data protection in Indonesia, it is recommended that the personal data protection institution to be established under Articles 58 to 60 of Law Number 27 of 2022 immediately formulate technical guidelines for personal data protection strategies, particularly regarding logging operations. This strategy should incorporate eight basic principles as implemented in France, namely: providing a logging system, keeping these logs for a rolling period of between six months and one year, performing records of creation, consultation, sharing, modification, and deletion of personal data, informing users, protecting the logging equipment and the logged information, ensuring the proper functioning of the logging system, ensuring that processors are contractually obliged, and actively analyzing in real time or in the short term. Implementing these principles will strengthen the national data security system and provide legal certainty in the practice of personal data protection in Indonesia, while promoting accountable, transparent, and human rights-based data governance.

V. Conclusion

France and Indonesia differ significantly in terms of their supervisory authorities for personal data protection, both in their designation and legal foundation. In Indonesia, this supervisory authority is called CNIL with the legal basis of the 1978 Law on Computers, Files and Freedoms. Meanwhile, in Indonesia, this institution has not yet been established and does not have an official name. The absence of an official supervisory authority in Indonesia may delay the implementation of robust personal data protection measures, as seen in the established

framework in France, where CNIL plays a crucial role in ensuring compliance with the GDPR. However, its juridical arrangements have been determined in Law Number 27 of 2022. the establishment of personal data protection strategy in France can be done by CNIL as the mandate of GDPR Article 57 paragraph 1 letter c. Whereas in Indonesia, it is clear that by the personal data protection institution in Indonesia, the establishment of personal data protection strategy is the mandate of Article 59 of Law Number 27 Year 2022. In terms of Basic Precaution Logging Operations as one of the Personal Data Protection Strategies, it can implement what is applied in France in the Practice Guide for the Security of Personal Data published by CNIL. There are 8 basic precautions in logging operations, namely providing a logging system; storing these logs for a rolling period of between six months and one year; performing, for application logs, records of creation, consultation, sharing, modification, and deletion; notifying users; protecting logging equipment and logged information; ensuring the proper functioning of the logging system; ensuring that processors are contractually obligated; and actively analyzing, in real time or in the short term. As a recommendation, the eight basic principles as implemented in France can be adopted as part of Indonesia's personal data protection strategy to strengthen preventive measures and ensure legal certainty. These principles will serve as a practical guideline for all parties involved in data processing, supporting secure, transparent, and accountable data governance.

VI. References

Asshiddiqie, Jimly. *Perkembangan Dan Konsolidasi Lembaga Negara Pasca Reformasi*. Jakarta: Sinar Grafika, 2012.

Ayiliani, Fanisa Mayda, Elfia Farida, Magister Hukum, Fakultas Hukum, Universitas Diponegoro, Fakultas Hukum, and

Universitas Diponegoro. "Urgensi Pembentukan Lembaga Pengawas Data Pribadi Sebagai Upaya Pelindungan Hukum Terhadap Transfer Data Pribadi Lintas Negara." *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431-455: 431.

Burkert, Herbert. "Privacy/Data Protection: A German/European Perspective." In *Proceedings of 2nd Symposium of the Max Planck Project Group on the Law of Common Goods and the Computer Science and Telecommunications Board of the National Research Council*, 50. Massachusets: Wood Hole, 1999.

Delahaie, Henri, and Félix Paoletti. *Informatique et Libertés*. Paris: Editions La Découverte, 1987.

Djafar, Wahyudi. *Perlindungan Data Pribadi Di Indonesia. Lembaga Studi Dan Advokasi Masyarakat (ELSAM)*. Jakarta Selatan: ELSAM, 2016.

Fibrianti, Nurul, Tri Andari Dahlan, Rahayu Fery Anitasari, Niken Diah Paramita, and Tegar Islami Putra. "Review of Child Consumer Protection in the Practice of Online Gambling Games Through the Gacha System." *The Indonesian Journal of International Clinical Legal Education* 6, no. 3 (2024): 427-452: 429. https://doi.org/doi.org/10.15294/ijicle.v6i3.13198.

Firdhausya, Mahima Umaela, Muhammad Hilmi Naufal Aflah, Anisa Tussaleha, Tegar Islami Putra, and Eko Mukminto. "The Urgency of Limiting The Utilization of Consumer IP Addresses By Companies as Personal Data Objects in The Study of Positive Law in Indonesia." *Law Research Review Quarterly* 10, no. 2 (2024): 393-410: 394.

Forte, Dario. "The Importance of Log Files in Security Incident Prevention." *Network Security* 7 (2009): 18–20:19.

Fujimori-Smith, Aska. "Analysis of Global Data Privacy Regulations

and How Transnational Companies Are Impacted." *Santa Clara High Technology Law Journal* 40, no. 1 (2024): 91-114: 102.

Ibrahim, Jhony. *Teori Dan Metodologi Penelitian Hukum Empiris*. Malang: Bayumedia Publishing, 2006.

Kent, Karen, and Murugiah Souppaya. *Guide to Computer Security Log Management*. *NIST Special Publication*, 2006.

Khansa, Farah Naurah. "Penguatan Hukum Dan Urgensi Otoritas Pengawas Independen Dalam Pelindungan Data Pribadi Di Indonesia." *Jurnal Hukum Lex Generalis* 2, no. 8 (2021): 649-662: 657. https://doi.org/10.56370/jhlg.v2i8.114.

Maharani, Dhea Yulia, and Suparno. "The Urgency of Personal Data Protection Agencies on Sustaining The Resilience of The Digital World." *Edunity* 3, no. 6 (2024): 345-353: 349.

Marjanov, Tina, Maria Konstantinou, Magdalena Jóźwiak, and Dayana Spagnuelo. *Data Security on the Ground: Investigating Technical and Legal Requirements under the GDPR*. *Proceedings on Privacy Enhancing Technologies*. Vol. 2023. Association for Computing Machinery, 2023. https://doi.org/10.56553/popets-2023-0088.

Milosevic, Z., W. Chen, A. Berry, and F.A. Rabhi. "Real-Time Analytics." In *Big Data*, 39-61: 42. Elsevier, 2016. https://doi.org/10.1016/B978-0-12-805394-2.00002-7.

Naufal, Muhamad, and Aulia Azmi. "Analisa Kasus Kebocoran Data Pada Bank Indonesia Dalam Sistem Perbankan." *Jurnal Multidisiplin Ilmu Akademik* 1, no. 6 (2024): 448-458: 452.

Ooijen, I. van, and Helena U. Vrabec. "Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective." *Journal of Consumer Policy* 42, no. 1 (2019): 91-107: 102. https://doi.org/10.1007/s10603-018-9399-

7.

Putra, Tegar Islami, and Nurul Fibrianti. "Data Protection Impact Assessment Indicators in Protecting Consumer Personal Data on E-Commerce Platforms." *Legal Challenges in Overcoming the Digital Divide (Article in Press)* 6, no. 1 (2024): 111–50. https://doi.org/doi.org/10.15294/ijicle.v5i3.72001.

———. "Threats and Legal Protection of Personal Data Combined in E-Commerce Transactions Based on Personal Data Protection Law in Indonesia." *Lambung Mangkurat Law Journal* 9, no. 1 (2024): 64–74. https://doi.org/10.32801/lamlaj.v9i1.438.

Putra, Tegar Islami, Nurul Fibrianti, Adinda Zeranica Putri Fakhis, and Mohammad Raziq Fakhrullah. "Critically Reveal The Dimensions of Damage From Unauthorized Use of Personal Data." *The Digest: Journal of Jurisprudence and Legisprudence* 5, no. 2 (2025): 231-262: 233. https://doi.org/doi.org/10.15294/digest.v5i2.19941.

Putra, Tegar Islami, Akbar Jihadul Islam, and Abdullah Mufti Abdul Rahman. "Integrating Islamic Laws into Indonesian Data Protection Laws: An Analysis of Regulatory Landscape and Ethical Considerations." *Contemporary Issues on Interfaith Law & Society* 4, no. 1 (2024): 85–118. https://doi.org/doi.org/10.15294/ciils.v3i1.78690.

Savinov, Aliaksei. "Systems of Record Management." *InterConf* 73 (2021): 61-66: 62.

Soekanto, Soerjono, and Sri Mamudji. *Penelitian Hukum Normatif Tinjauan Singkat*. Jakarta: Rajawali Press, 2006.

Werbach, Kevin. "What Could Possibly Go Wrong?" *Technology and Regulation*, 2019, 309-329: 314. https://doi.org/doi.org/10.26116/techreg.2024.022.

Widjaja, Gunawan, and Fransiska Milenia Cesarianti. "Urgensi Pembentukan Lembaga Pengawas Pelindungan Data Pribadi Di Indonesia Berdasarkan Pasal 58 Juncto Pasal 59 Dan Pasal 60 Undang – Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *SINERGI : Jurnal Riset Ilmiah* 1, no. 4 (2024): 234-242: 239. https://doi.org/10.62335/8qf44b59.

Yolanda, Erlyns, and Rugun Romaida Hutabarat. "Urgensi Lembaga Pelindungan Data Pribadi Di Indonesia Berdasarkan Asas Hukum Responsif." *Jurnal Ilmiah Indonesia* 13, no. 1 (2023): 4166-4182: 4168.

***

Acknowledgment
None.

Funding Information
None

Conflicting Interest Statement
There is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement
All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.