p–ISSN: 2723 - 6609 e-ISSN: 2745-5254
Vol. 5, No. 5 Mei 2024 http://jist.publikasiindonesia.id/

Application of Personal data protection on electronic signatures in Indonesia

Viola Meiryan Azza[1*], Hartana[2], G.nyoman Tio Rae[3]
Universitas Bung Karno, Indonesia
Email: Viola.crewdible@gmail.com[1*], hartana.palm99@gmail.com[2], nrae88good@gmail.com[3]
*Correspondence

Keywords: Protection of Personal Data; Electronic signature; Indonesian Legal Compliance.

ABSTRACT

The Industrial Revolution 4.0 and digital transformation have brought significant changes in various aspects of life, including the business and administrative world. This revolution, driven by digital technologies such as the Internet of Things (IoT), artificial intelligence (AI), big data, and cloud computing, enables automation in various industrial sectors and increases efficiency and productivity. This study aims to analyze the process of collecting, processing, and using personal data in using electronic signatures in Indonesia and knowing the compliance and legal consequences of personal data protection violations in using electronic signatures in Indonesia. This research approach is juridical normative. The research found that although the use of electronic signatures has increased rapidly during the COVID-19 pandemic, many challenges are still faced. Electronic signatures are often considered prestigious and challenging, although they have been widely used in signings by notaries. The author realizes that although much progress has been made, there is still room for improvement in adopting and understanding electronic signatures in Indonesia.

Introduction

The Industrial Revolution 4.0 and digital transformation have brought significant changes in human life, including business and administration. The Industrial Revolution 4.0 is a phenomenon of technological disruption that utilizes digital technologies such as the Internet of Things (IoT), artificial intelligence (AI), big data, cloud computing, and others (Arrasuli & Fahmi, 2023). This revolution has enabled automation in various industrial sectors and significantly increased efficiency and productivity. According to Saeful, in his book "The Fourth Industrial Revolution," Industrial Revolution 4.0 has changed how we work and how we live, relate to each other, and view the world (Satrio

& Widiatno, 2020). This revolution has integrated the physical, digital, and biological worlds unprecedentedly (Azzani, Purwantoro, & Almubaroq, 2023).

Digital transformation is also an essential part of the Industrial Revolution 4.0. Digital transformation refers to integrating digital technology into all aspects of a business, fundamentally changing how it operates and delivering new value to customers (Budiyatno, 2023). This process involves using digital technologies such as cloud computing, mobile computing, big data, Internet of Things (IoT), and artificial intelligence (AI) to create new opportunities and improve operational efficiency (Cahyadi, 2020).

The development of digital technology has brought about a massive transformation in the global entertainment and media industry. According to PwC's report, the industry's total revenue jumped 5.4% in 2022 to US$2.32 trillion, despite slowing down from 10.6% growth in 2021 as the economy and industry recovered from the COVID-19 pandemic. While revenue growth is projected to slow in the next five years to 2027 due to weaker consumer spending, the entertainment and media industry is expected to reach a value of US$2.8 trillion by 2027 (Rosadi, 2016). Digitalization is increasingly dominating, with an estimated share of digital revenue reaching nearly 71% of total industry revenue by 2027, up from 55.2% in 2018. In addition, global internet access will approach a US$1 trillion market as data consumption nearly triples from 2022 to 2027 (Damayanti, Setiawan, & Firman, 2024). The prospect of massive growth in regions such as Asia and opportunities in hot sectors such as advertising, gaming, and emerging technologies such as generative AI will be critical drivers amid adjusted expectations and weakening consumer purchasing power.

Sectors that have experienced a significant increase in the use of information technology include:

1. Financial and Banking Sector: According to a report from Deloitte, most financial institutions have adopted technologies such as mobile banking, digital payments, artificial intelligence, and blockchain to improve efficiency, security, and customer experience.
2. Healthcare Sector: Digital transformation in healthcare has become a significant necessity, with the adoption of technologies such as electronic medical records, telemedicine, and health data analytics to improve quality of care and operational efficiency.
3. Education Sector: The use of technology in education, such as online learning, video conferencing, and learning management platforms, has increased significantly during the COVID-19 pandemic.

Government Sector: Governments worldwide have adopted information technology to improve public services, transparency, and civic participation through initiatives such as e-government and open data.

According to a McKinsey Global Institute analysis covering over 800 jobs and 2,000 work activities, digitization and process automation have great potential to increase productivity and efficiency in various industries (Dermawan, 2021). Globally, nearly half

of employee activities, which account for nearly $16 trillion in wages, have the potential to be automated using existing technologies (Nasiroh & Priyadi, 2018). Although less than 5 percent of jobs can be fully automated with current technology, at least 30 percent of employee activities in about 60 percent of job types can be automated. Among the industries studied, the potential for automation ranged from 27 to 73 percent, while in the healthcare industry, the potential reached 36 percent (Fitri, 2022). Large-scale automation can help address various issues facing health insurers, such as improving workflow efficiency, speeding up decision-making based on accurate data, and lowering operational costs.

The previous research that the author used as a reference in writing this research is: "Thesis by Andrew Giovanni Alexander Palealu Universitas Atma Jaya Yogyakarta 2018 titled: Legal Protection of Consumer Personal Data in E-Commerce Transactions".

The author finds that the discussion discussed by the previous author is based on data breaches when making transactions on e-commerce, resulting in material losses for users of these e-commerce services. Of course, transactions carried out online seem easy and save time. However, the problem of personal data breaches, considered a problem in this thesis, refers to Law No. 11 of 2008 and Law No. 19 of 2016 concerning Information and Electronic Transactions as the basis for solving the problem. The author sees that there are things that need to be improved in surgery and research on the thesis written by the previous author, namely the use of Law No. 27 of 2022 concerning Personal Data Protection as a basis for solving problems when there are personal data breach activities and leakage of personal data of e-commerce consumers.

"Thesis by Bagus Satryo Ramadha, S.H. Universitas Islam Indonesia 2021 titled: The Ability of Criminal Law Against Cybercrime Related to Personal Data Protection in Indonesia."

The author feels that the previous author of this thesis discussed personal data protection and cybercrime before Law No. 27 of 2022 concerning Personal Data Protection. So, the author gets a complete point of view when writing his research material, supported by these two previous studies. The author discusses in this thesis how the government carries out the personal data protection and how the use of personal data in internet/digital products should be carried out. The rapid era of information and technology makes humans more pampered; shopping does not need to go to the market, watching movies does not always have to go to the cinema, and additional business capital does not need to go to the Bank do it online and many other activities can be done "at home." This previous research also included proving cyber crimes when they arrived in court. Where in the problem formulation, the previous author asked, "How is the criminal ability of the Electronic Information and Transaction Law in tackling cyber crimes related to personal data protection?". The author feels the need to perfect the answer to the previous research problem formulation because Law Number 27 of 2022 concerning Personal Data Protection had not yet been published when the previous research was written. Therefore, because it is based on this, the author feels it is important to examine

additional research to improve the protection of personal data used in electronic transactions.

Based on the two previous studies, the author feels that the basis for discussing the research to be carried out can be refined with new findings and new regulatory laws that the author will examine and collect into new research material.

The objectives of this study are:

1. To analyze the process of collecting, processing, and using personal data in the use of electronic signatures in Indonesia
2. To determine the compliance and legal consequences of personal data protection violations in the use of electronic signatures in Indonesia

Research Methods

The problem approach used in this study is carried out with a normative juridical approach. A normative approach is an approach that is carried out based on the primary legal material, examining theoretical matters concerning legal principles, legal conceptions, views, legal doctrines, regulations, and legal systems. With a normative juridical problem approach, it is hoped that it can help solve problems related to using personal data embedded in electronic signatures where not all people understand that their data is attached and never lost as long as the soft copy document still exists and has not been destroyed.

Research Specifications

The research specifications used are descriptive-analytical, describing applicable laws and regulations associated with legal theories and positive law implementation practices related to problems. Analytical descriptive research is the research conducted by the author because, in this study, the author tries to describe existing realities or existing facts and describe a problem related to the application of personal data protection in the management of personal data from electronic signatures carried out by electronic certificate providers in Indonesia.

Legal Material Collection Techniques

The technique of collecting legal materials that the author uses in this study is library research. Collection of legal material from secondary legal material derived from articles on the internet and other sources. Document study is a tool for collecting legal materials carried out through written legal materials using (content analysis). This technique helps obtain a theoretical basis by reviewing and studying books, laws and regulations, documents, scientific journals, reports, archives, and other research results, both printed and electronic, related to protecting personal data embedded in electronic signatures.

Techniques for analyzing legal materials

After the legal material is processed, it is then continued with legal material analysis techniques using qualitative analysis, namely discussing the legal material obtained by referring to the existing theoretical foundation. The data that has been obtained from the results of this study is compiled and analyzed qualitatively. The data is described

descriptively to obtain a picture that can be understood clearly and directed to answer the problems studied. On the other hand, this analysis reviews cases related to the issues faced, including the application of personal data protection in Indonesia's use of electronic signatures.

Research Location

Carried out online and offline, considering that the author also lives his daily life as a practitioner in the world of the digital financial support sector, where the use of electronic signatures embedded with customer personal data is encountered daily, researchers have a good relationship with the subject of research, so the research was carried out at the office of the electronic certificate provider company in Jakarta, namely at PT DJELAS TANDATANGAN BERSAMA.

Results and Discussion

Electronic Certification and Electronic Signature Organizer

An Electronic Certification Provider (PSrE) is a legal entity that functions as a party worthy of the trust that provides and audits Electronic Certificates. PSrE is here to increase public trust in transacting digitally by protecting online transactions from fraud and data forgery.

Electronic Transaction Implementation is a series of electronic transactions performed by the sender and recipient using an electronic system.

An electronic certificate is an electronic certificate containing an Electronic Signature and identity indicating the status of the legal subject of the parties to an Electronic Transaction issued by an Electronic Certification Operator.

Personal Data Protection Concept

Personal data protection covers various aspects, including collecting, processing, using, storing, and disclosing personal data. Its measures prevent unauthorized access, misuse, or infringement of individuals' personal information. This becomes particularly relevant in the context of using personal data in electronic signatures.

The Personal Data Protection Law has regulated how the concept of protecting personal data is ideal and appropriate, how the personal data Controller, the Processor of personal data, and the Subject of personal data obtain their rights and must comply with their obligations.

Legal Basis for the Use of Electronic Signatures

What regulates the security of personal information and data in Indonesia is Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). Article 11 of the ITE Law states that electronic signatures have the same legal force and consequences as wet signatures. This reflects the government's recognition of the importance of electronic signatures in electronic transactions and provides a clear legal basis for their use. This legal foundation also aligns with information and communication technology development that increasingly allows using electronic signatures in various aspects of life.

Indonesian Electronic Certification Provider, Certificate Policy (CP), and Certificate Practices Statement (CPS)

Electronic Certificate Provider Company (PSrE) runs its business referring to the rules and regulations supervised by the Regulator, in this case, the Financial Services Authority (OJK), registered as a particular cluster to support financial sector inclusion with a quarterly reporting process and in order to secure user's personal data, encryption technology, privacy policies, and security standards must be used, by the Kominfo Regulation as the Indonesian Electronic Certificate Operator (PSrE Induk). The author chooses one of the Electronic Certificate Providers (PSrE) that the author knows from creation, incubation, and operation until business closure. So, in this study, it will be able to be seen comprehensively how the application of the personal data protection system embedded in Electronic Signatures can be maintained even though the Electronic Certificate Operator (PSrE) chooses not to continue its business.

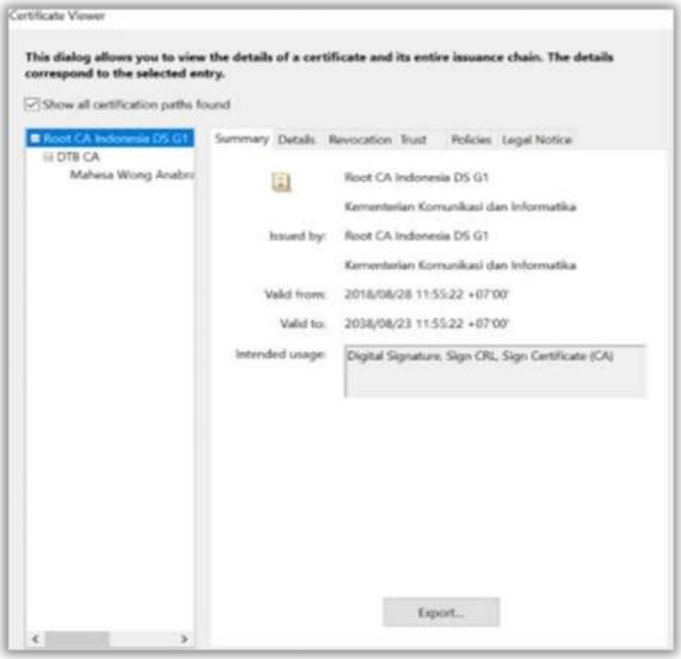

Figure 1. PSrE Certificate Example

The following can be seen from the image from the top correct list and the signer data in the top left, in order:

1. Root (root/origin) issued a certificate from Indonesia (PSrE Induk) by Kominfo (Kominfo Certificate)
2. PSrE Certificate (TekenAja Certificate)
3. At the top left with the name Mahesa Awong (Certificate of Signatory)
4. Electronic Certificate validity period

Figure 2 Example of an uncertified Electronic signature

The above document is digitally signed but does not use a certified electronic signature. Therefore, it cannot be signed data, does not encounter a PSrE Certificate, and is not valid in the eyes of the law. In accordance with the regulations of Law Number 1 of 2024, Electronic Information and/or Electronic Documents are declared valid if they use Electronic Systems in accordance with the provisions stipulated in this Law.

Analysis based on Law No. 27 of 2022 concerning Personal Data Protection

Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) provides a solid legal foundation for regulating the mechanism for collecting personal data, including using electronic signatures. Article 23, paragraph (1) of the PDP Law states that the collection of personal data must be limited, specific, legally valid, fair, and transparent for explicit purposes, as well as with the knowledge and consent of the owner of the personal data. This provision emphasizes the importance of individuals' consent in collecting their data.

The PDP Law also regulates the principle of accountability in collecting personal data. Article 25 paragraph (1) states that the personal data controller must be responsible for compliance with the PDP Law in carrying out the processing of personal data, including data collection. This means that the electronic signature operator, as the controller of personal data, has an obligation to ensure that the collection of personal data is carried out in accordance with the provisions of the PDP Law.

With the provisions in the PDP Law, the mechanism for collecting personal data using electronic signatures must be carried out legally, transparently, and with the consent of the personal data owner. Electronic signature operators, as controllers of personal data,

must also be responsible for ensuring compliance with the PDP Law in the data collection process. The rights of personal data owners regarding data collection must also be respected and fulfilled by the provisions of the PDP Law. Thus, the PDP Law provides comprehensive protection for individuals' data in the data collection mechanism using electronic signatures.

Application of personal data protection principles in data collection

Applying personal data protection principles in data collection is essential to ensuring the preservation of individual rights and compliance with applicable regulations. One of the main principles is the restriction of data collection, which emphasizes that the collection of personal data should be carried out on a limited basis and only for legitimate and specific purposes. In the context of the use of electronic signatures, the collection of personal data should be limited to information that is relevant and necessary for identity verification and electronic signing of documents.

The principle of transparency is also fundamental in the collection of personal data. Electronic signature operators must provide clear and accessible information to users regarding the data's purpose, the types of data collected, and how the data will be used and protected. This transparency allows users to provide informed consent and understand the implications of collecting their data. In addition, the operator must also provide a mechanism for users to withdraw their consent if they no longer want their data to be processed, as stated in Article 6 paragraph (1) of the Regulation of the Minister of Communication and Information Number 20 of 2016.

The principle of data accuracy also needs to be applied in the personal data collection mechanism. Based on Article 24, paragraph (1) of the PDP Law, the data collected must be accurate, complete, and updated regularly. This is important to ensure reliability and integrity when using electronic signatures. The Operator shall provide a mechanism for users to access, correct, or update their data if necessary. In addition, the organizer must also have procedures to delete or anonymize personal data that is no longer needed for the original purpose of collection, as stated in Article 15 paragraph (2) of the Regulation of the Minister of Communication and Information Number 20 of 2016.

In addition, the principle of accountability must also be applied when collecting personal data. Based on Article 28, paragraph (1) of the PDP Law, electronic signature operators must be able to demonstrate their compliance with the principles of personal data protection and be responsible for the data processing they carry out. They must appoint a data protection officer responsible for overseeing compliance, handling requests or complaints from data owners, and cooperating with relevant supervisory authorities as stated in Article 34 paragraph (1) of the Minister of Communication and Information Regulation Number 20 of 2016. By comprehensively applying the principles of personal data protection in the data collection mechanism, electronic signature operators can build user trust and comply with the applicable legal framework.

Application of legal certainty theory in compliance with electronic signature organizers

The theory of legal certainty is one of the main principles in the rule of law that aims to ensure stability and predictability in the legal system. According to Gustav Radbruch, a German legal philosopher, legal certainty is one of the fundamental legal

values that must be upheld, along with justice and expediency. In compliance with electronic signature providers or Electronic Certification Providers (PSrE), applying legal certainty theory is very important to protect users' data and maintain public trust in electronic signature services.

Minister of Communication and Information Regulation No. 11 of 2022 concerning Governance for the Implementation of Electronic Certification is a tangible manifestation of the application of legal certainty theory in regulating PSrE compliance in Indonesia. These regulations set out clear and detailed requirements, obligations, and responsibilities for PSrE in carrying out its services. Article 21, paragraph (1) of the regulation outlines explicitly various obligations that must be fulfilled by PSrE Indonesia, such as checking the correctness of the identity of prospective owners and Electronic Certificate Owners, managing and securing systems that store the identity of Electronic Certificate Owners, and guaranteeing losses due to failure of Electronic Certification services. These clear and detailed provisions provide legal certainty for PSrE in carrying out its obligations and for users to understand their rights.

Conclusion

After researching and following technological developments and legal updates, the author realizes many things that have been optimally encountered in the field. However, the author finds that using electronic signatures is still considered a prestigious product, and its use is problematic. The author has researched Electronic Signatures from 2020, right when the Covid 19 pandemic hit the World and rapidly impacted digitalization, especially in signing carried out underhand by the Parties; even face-to-face signing at Notaries also used electronic signatures in some of their agreements.

Indeed, the COVID-19 pandemic has inevitably urged us to limit space for movement, face-to-face, and other outdoor activities. Therefore, the author finds that online signing can be an alternative that brings many conveniences and more benefits if Regulators and the Public are ready to accept electronic signatures as an option when signing something.

Bibliography

Arrasuli, Beni Kharisma, & Fahmi, Khairul. (2023). Perlindungan Hukum Positif Indonesia Terhadap Kejahatan Penyalahgunaan Data Pribadi. *UNES Journal of Swara Justisia*, *7*(2), 369–392.

Azzani, Ihsania Karin, Purwantoro, Susilo Adi, & Almubaroq, Hikmat Zakky. (2023). Urgensi Peningkatan Kesadaran Masyarakat Tentang Kasus Penipuan Online Berkedok Kerja Paruh Waktu Sebagai Ancaman Negara. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, *10*(7), 3556–3568.

Budiyatno, Kevin Chrisanta. (2023). Transformasi Digital Sebagai Bagian Dari Strategi Pemasaran Di Rumah Sakit Siloam Palangka Raya Tahun 2020. *Jurnal Administrasi Rumah Sakit Indonesia*, *8*(2), 66–73.

Cahyadi, Thalis Noor. (2020). Aspek Hukum Pemanfaatan Digital Signature Dalam Meningkatkan Efisiensi, Akses Dan Kualitas Fintech Syariah. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *9*(2), 219.

Damayanti, Putri Aisya, Setiawan, Ramadhani, & Firman, Firman. (2024). Analisis Pengembangan Smart City Di Kota Tanjungpinang. *WISSEN: Jurnal Ilmu Sosial Dan Humaniora*, *2*(1), 79–103.

Dermawan, Rizki. (2021). Pemanfaatan Tanda Tangan Digital Tersertifikasi di Era Pandemi. *Jurnal Hukum Lex Generalis*, *2*(8), 762–781.

Fitri, Okta Rina. (2022). Hak atas Pelindungan Data Pribadi pada Proses Penegakan Hukum Pidana. *Jurnal Hak Asasi Manusia*, *15*(1), 91–108.

Nasiroh, Yiyin, & Priyadi, Maswar Patuh. (2018). Pengaruh penerapan good corporate governance terhadap financial distress. *Jurnal Ilmu Dan Riset Akuntansi (JIRA)*, *7*(9).

Rosadi, Sinta Dewi. (2016). Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia. *Yustisia*, *5*(1), 35–53.

Satrio, Muhamad Bayu, & Widiatno, Men Wih. (2020). Perlindungan Hukum Terhadap Data Pribadi Dalam Media Elektronik (Analisis Kasus Kebocoran Data Pengguna Facebook Di Indonesia). *JCA of Law*, *1*(1).