Strategi Terintegrasi Dalam Perancangan *Assessment* Pelindungan Data Pribadi

1st Mutiara Oktaviena Lestari
Departemen Sistem Informasi
Telkom University
Bandung, Indonesia
moktaviena@student.telkomuniversity.ac.id

2nd Dhata Praditya
Departemen Sistem Informasi
Telkom University
Bandung, Indonesia
dhatap@telkomuniversity.ac.id

3rd Ari Fajar Santoso
Departemen Sistem Informasi
Telkom University
Bandung, Indonesia
arifajar@telkomuniversity.ac.id

***Abstrak* — Keamanan dan pelindungan data pribadi menjadi perhatian di era digital, terutama dengan meningkatnya ketergantungan pada teknologi dan penetrasi internet di Indonesia serta perlunya kepatuhan terhadap Undang-Undang Pelindungan Data Pribadi. Penelitian ini bertujuan untuk mengidentifikasi parameter yang mampu mengukur tingkat kesiapan organisasi dalam mematuhi Undang-Undang Pelindungan Data Pribadi. Pendekatan ini melibatkan proses agregasi berbagai standar dan framework seperti SKKNI, COBIT 2019, DAMA-DMBOKv2, ASEAN Data Management Framework (DMF), NIST Privacy Framework, dan CIPM Body of Knowledge dalam menciptakan kerangka kerja. Kerangka kerja yang dirancang berfokus pada lima aspek Data Privacy Governance, Legal basis and Consent Management, Data Security, Audit Trail dan Incident Management. Melalui validasi dengan metode Best-Worst, framework ini dirancang untuk dapat memberikan pandungan dalam meningkatkan kepatuhan terhadap Undang-Undang Perlindungan Data Pribadi. Hasil penelitian menunjukkan bahwa kerangka kerja yang dirancang dapat relevan membantu organisasi dalam meningkatkan kepatuhan. Framework ini menyajikan pendekatan strategis untuk mengatasi tantangan operasional terkait pelindungan data. Framework ini diharapkan dapat menjadi alat yang bermanfaat bagi organisasi di Indonesia dalam melindungi data pribadi, sekaligus mendukung implementasi dari Undang-Undang Pelindungan Data Pribadi.*

***Kata kunci*— Pelindungan Data Pribadi, Keamanan Data, Kerangka kerja, Metode Best-Worst**

I. PENDAHULUAN

Pelindungan data pribadi sangat penting di era digital, dimana segala informasi mengalir terus menerus, ketergantungan terhadap teknologi juga semakin tinggi [1]. Berdasarkan data dari Dokumen Lanskap Keamanan Siber 2023, Badan Siber dan Sandi Negara (BSSN) berhasil melakukan deteksi pada 103 dugaan insiden kebocoran data yang terjadi dari bulan januari hingga desember tahun 2023, dengan kasus terbanyak pada bulan maret sebanyak 20 kasus [2]. Berdasarkan regulasi pemerintah bahwa “Setiap orang berhak atas pelindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan pelindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi” Pasal 28G ayat (1) [3]. Penelitian sebelumnya memiliki pembahasan yang sama terkait penentuan kerangka kerja dalam melindungi data sesuai dengan Undang-Undang Pelindungan Data Pribadi menggunakan pendekatan *Analytical Hierarchy Process* (AHP) [4]. Oleh karena itu, belum adanya kerangka kerja untuk menilai kesiapan organisasi dalam memastikan pelindungan data pribadi yang selaras dengan peraturan perundang-undangan yang ada di Indonesia menggunakan metode *best-worst multi-criteria decision making.*

II. KAJIAN TEORI

A. *Data Privacy*

Privasi data memastikan penggunaan data sesuai izin dan mencegah akses ilegal [5], [6]. Praktik terbaik dalam mengakses, memanfaatkan dan memperoleh keuntungan dari data perlu menentukan syarat dan tanggung jawab dari setiap tahapan siklus hidup data untuk memastikan privasi data [6]. Dalam mengurangi risiko privasi data dalam kondisi sosial dan lingkungan yang buruk, konsistensi, proporsionalitas, dan transparansi adalah hal-hal yang harus diperhatikan karena dapat meningkatkan kemungkinan pelanggaran privasi data [7].

B. Pelindungan Data Pribadi

Pelindungan data adalah salah satu masalah utama tata kelola data [8]. Data pribadi adalah sumber daya sistem yang mencakup keseluruhan "ekosistem" informasi yang saling terkait tentang individu yang dapat diidentifikasi [9]. Data pribadi meliputi nama, alamat, nomor telepon, dan informasi lainnya yang dikumpulkan oleh berbagai platform dan penyedia layanan menjadi sumber daya yang berharga bagi pihak-pihak tertentu. Berdasarkan Undang-Undang Republik Indonesia, menyatakan bahwa ”Pelindungan Data Pribadi adalah keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaian pemrosesan Data Pribadi guna menjamin hak konstitusional subjek Data Pribadi.” Pasal 1 ayat (2) [3].

C. Standar Kompetensi Kerja Nasional Indonesia (SKKNI) Keahlian Pelindungan Data Pribadi

Standar Kompetensi Kerja Nasional Indonesia (SKKNI) dibuat untuk mengukur kompetensi kerja PDP yang dapat diukur dalam pengetahuan (knowledge), keterampilan (skill), dan sikap tingkah laku (*attitude*). SKKNI pada bidang keahlian pelindungan data pribadi memiliki 19 kompetensi diantaranya meliputi Landasan Program Kerja Pelindungan Data Pribadi, Kebutuhan Struktur Tim Pelindungan Data Pribadi, Kerangka Kerja Pelindungan Data Pribadi, Peraturan Perundang-undangan Terkait Pelindungan Data Pribadi,

Strategi Pelindungan Data Pribadi, Kriteria Matriks Risiko Pelindungan Data Pribadi, dan kompetensi lainnya [10].

D. COBIT 2019

COBIT 2019 adalah pedoman untuk menerapkan tata kelola teknologi informasi yang dirancang untuk membantu auditor, manajemen, dan pengguna membuat kerangka kerja. Terdapat beberapa domain *Governance and Management Objectives* yang membahas terkait data, keamanan data,, insiden. Domain tersebut meliputi APO13, APO14, DSS02, DSS05, dan BAI09.

E. DAMA-DMBOKv2

Data Management dalam DAMA DMBOK memiliki prinsip-prinsip dasar yang harus ditaati untuk memastikan segala data dapat dikelola, meliputi data adalah asset dengan properti unik, manajemen data adalah manajemen siklus hidup, mengelola data adalah mengelola risiko yang terkait dengan data, dan prinsip lainnya [11]. Beberapa area yang membahas dalam pelindungan data terdiri dari *Data Governance, Data Security, dan Data Quality.*

F. ASEAN Data Management Framework

Kerangka ASEAN tentang Tata Kelola Data Digital menetapkan prioritas, prinsip dan inisiatif strategi dalam memandu *Asean Member States* dalam kebijakan dan peraturan mereka pendekatan terhadap tata kelola data digital dalam ekonomi digital. Terdapat 6 komponen dalam ASEAM DMF meliputi:

a. *Governance and oversight*
   Komponen ini terdapat 3 fungsi meliputi manajemen data, proses bisnis, dan manajemen risiko.
b. *Policies and procedural document*
   Komponen ini membahas kebijakan dan prosedur dalam manajemen data.
c. *Data Inventory*
   Komponen ini membahas inventaris data terhadap jenis data yang dikumpulkan.
d. *Impact/Risk Assessment*
   Komponen ini membahas penilaian dampak dan risiko terhadap data.
e. *Controls*
   Komponen ini membahas penerapan kontrol berbasis risiko dalam pelindungan data.
f. *Monitoring and continuous improvement*
   Komponen ini membahas proses pemanatauan dan perbaikan terhadap data yang dikumpulkan.

G. NIST Privacy Framework

Dalam membantu organisasi terkait privasi data dan memastikan pelindungan data pribadi, kerangka kerja NIST dapat memberikan pedoman yang mencakup standar, praktik, dan kebijakan dalam melindungi data [12]. NIST PF memiliki lima fungsi dasar dalam kerangka kerjanya [13]:

1. *Identify-P:* Pengidentifikasian dengan pengembangan pamahaman organisasi dalam mengelola risiko privasi.
2. *Govern-P:* Pengendalian dengan penerapan struktur tata kelola.
3. *Control-P:* Penerapan aktivitas dalam mengelola data.
4. *Communicate-P:* Pengkomunikasian dengan mengembangkan organisasi dalam pemahaman terkait cara data diproses.
5. *Protect-P:* Pelindungan dengan mengembangkan proses pengamanan data.

H. CIPM Body Of Knowlede

Certified Information Privacy Manager (CIPM) Body of Knowledge merupakan sebuah kerangka yang menunjukan konsep dan topik untuk memperoleh sertifikasi. Kerangka ini mendokumentasikan pengetahuan yang mencakup domain yang harus diketahui oleh profesional privasi. CIPM *Body of Knowledge* memiliki 6 domain terkait Program Privasi [14]:

1. *Domain I Privacy Program: Developing a Framework*: Pembentukan model tata kelola program privasi dalam menciptakan landasan, tujuan, dan tanggung jawab.
2. *Domain II Privacy Program: Establishing Program Governance*: Persyaratan pribasi dengan menetapkan peran, pelatihan, dan kebijakan.
3. *Domain III Privacy Program Operational Life Cycle: Assessing Data*: Cara mengidentifikasi dna mengurangi ancaman privasi serta menilai dampak.
4. *Domain IV Privacy Program Operational Life Cycle: Protecting Personal Data*: Cara melindungi aset data selama penggunaan melalui penerapan kontrol privasi dan teknologi.
5. *Domain V Privacy Program Operational Life Cycle: Sustaining Program Performance*: Proses menanggapi permintaan dan insiden.
6. *Domain VI Privacy Program Operational Life Cycle: Responding to Requests and Incidents*

III. METODE

A. Pendekatan *Design Science Research* (DSR)

Design Science Research (DSR) merupakan sebuah pendekatan penelitian yang berfokus pada menciptakan pengetahuan praktis untuk merancang solusi atas berbagai masalah di kehidupan nyata [15]. . Hasil dari DSR dalam sistem informasi adalah sebuah artefak TI yang dibuat dalam menangani masalah organisasi [16]. Henver mendefinisikan Design Science Research (DSR) dalam sistem informasi ke dalam sebuah kerangka konseptual yang akan menjelaskan hubungan antara lingkungan dan basis pengetahuan. Kerangka konseptual terdiri dari tiga lingkup.

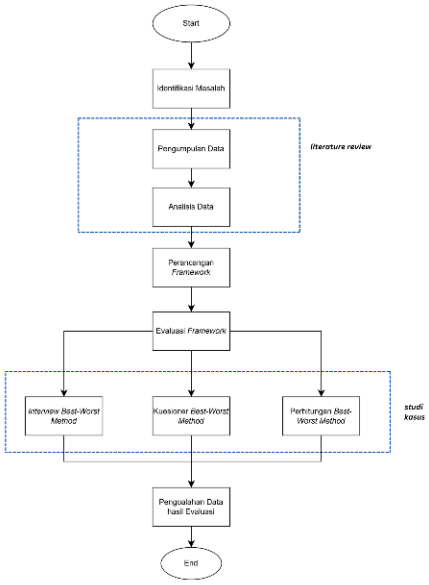
1. Lingkungan atau *environment*
   Mencakup semua komponen yang merujuk pada ruang dalam sebuah fenomena di dalamnya. Dua komponen didalamnya yaitu *organization* yang meliputi segala industri yang menjadi entitas bisnis serta infrastruktur, aplikasi, dan data menjadi bagian dari teknologi.
2. Penelitian Sistem informasi atau *IS Research*
   a. *Build*: Mengintegrasikan standar dan kerangka kerja keamanan dan pelindungan terkait data, seperti SKKNI bidang Pelindungan Data Pribadi, COBIT 2019, DAMA-DMBOKv2, ASEAN *Data Management Framework*, NIST PF, CIPM *Body of Knowledge*, untuk dapat menghasil kerangka kerja yang selaras dengan UU PDP.

b. *Evaluate*I: Kerangka kerja diuji melalui proses desk research, wawancara dan *questionnaire* untuk memastikan efektivitas dan kesesuaiannya dengan kebutuhan organisasi.

3. Dasar Pengetahuan *atau Knowledge base*
   Landasaran teori yang memberikan pemahaman teoritis untuk mengembangkan dan mengevaluasi kerangka kerja. Landasan tersebut meliputi tata kelola data, manajemen data, keamanan data, standar dan kerangka kerja pelindungan data pribadi, serta metodologi seperti *literature review* dan *best-worst method,* yang digunakan untuk memastikan bahwa kerangka kerja memenuhi standar ilmiah (rigor) dan relevansi (*relevance*)

Proses tersebut dapat menghasilkan kerangka kerja yang relevan, praktik, dan teoritis dalam pelindungan data pribadi

B. Sistematika Penelitian



Gambar 1 Sistematika Penelitian

Dalam Penelitian ini proses dilakukan secara sistematis dengan proses tahapan sebagai berikut:

1. Identifikasi Masalah
   Proses identifikasi masalah yang terjadi dalam pelindungan data pribadi, yaitu kurangnya integrasi kerangka kerja yang patuh terhadap Undang-Undang Pelindungan Data Pribadi.
2. Pengumpulan Data
   Tahapan pengumpulan yang melibatkan proses *literature review*, yang mencakup standar dan kerangka kerja seperti SKKNI bidang Pelindungan Data Pribadi, COBIT 2019, DAMA-DMBOKv2, ASEAN *Data Management Framework*, NIST PF, CIPM *Body of Knowledge*. Data pendukung dari hasil wawancata dan kuesioner.
3. Analisis data
   Tahapan yang dilakukan setelah pengumpulan data, untuk menganalisis parameter dari standar dan kerangka kerja yang dikumpulkan untuk memahami relevansi kerangka kerja.
4. Perancangan *Framework*
   Kerangka kerja *assessment* pelindungan data pribadi diagregasikan dan dirancang berdasarkan hasil analisis data dengan menggabungkan aspek terbaik.

IV. HASIL DAN PEMBAHASAN

A. Hasil Penelitian

Penelitian ini menghasilkan sebuah kerangka kerja pelindungan data pribadi dengan proses pemetaan parameter dari SKKNI bidang Pelindungan Data Pribadi, COBIT 2019, DAMA-DMBOKv2, ASEAN *Data Management Framework*, NIST PF, CIPM *Body of Knowledge.* Kerangka kerja ini bertujuan untuk meningkatkan kesiapan organisasi terhadap kepatuhan Undang-Undang Pelindungan Data Pribadi. Dengan aspek utama yang mencakup *Data Privacy Governance*, *Legal Basis and Consent Management*, *Data Security*, *Audit Trail*, dan *Incident Management.* Proses pemetaan ini menunjukan sejauh mana kontribusi setiap standar dan kerangka kerja terhadap parameter pelindungan data pribadi. Berikut merupakan hasil pemetaan :

Tabel 1 Pemetaan Parameter SKKNI

Parameter	**ID**	**SKKNI**
Scope and Purpose of personal data protection program.	P01	UK1
Structure, roles, and responsibilities of the Data Protection Officer team	P02	UK2
Training and awareness program for Data Privacy Practice	P03	UK5
Data Classification	P04	UK11
Data processing lifecycle and mechanism	P05	UK10&UK13
Transfer of Personal Data Policy	P06	UK9
Personal data protection principles.	P07	UK10&UK11
Privacy Control Procedure	P08	UK3
Legal basis for personal data processing.	P09	UK3&UK11
Data subject rights	P10	UK10&UK11
Data access request procedure	P11	UK11
Mechanism for withdrawal of consent	P12	UK16
Statement of consent electronically or non-electronically.	P13	UK16
Risk Assessment for data processing.	P14	UK7
DPIA (Data Protection Impact Assessment).	P15	UK7
Measure the performance of the privacy program	P16	UK12
Personal data protection Policy	P17	UK10
Encryption of sensitive data for storage and transmission.	P18	UK2
Data loss prevention Mechanism	P19	UK10
Data Protection Technology	P20	UK10
Data Access and User Activity Logs	P21	UK10
Data Breach Records	P22	UK10
Granular transaction tracking	P23	UK7
Data Subject Requests	P24	UK10
Audit Logs and Monitoring	P25	UK9&UK10
Tools for complaint handling.	P26	UK17
Priority for urgent complaints.	P27	UK17
Incident response management.	P28	UK18
Classification of data protection failures.	P29	UK19
Procedures for handling failures.	P30	UK19
Documentation of incident reports.	P31	UK19

UK dalam tabel 1 mendefinisikan Uji Kompetensi dalam Standar Kompetensi Kerja Nasional Indonesia (SKKNI) Keahlian Pelindungan Data Pribadi.

Tabel 2 Hasil Pemetaan Pelindungan Data Pribadi *Data Privacy Governance*

ID	COBIT 2019	DAMA	ASEAN DMF	NIST PF	CIPM
P01	✓	✓	✓	✓	✓
P02	✓	✓	✕	✓	✓
P03	✓	✓	✕	✓	✓
P04	✓	✓	✓	✓	✓
P05	✓	✓	✓	✓	✓
P06	✕	✓	✕	✓	✕
P07	✓	✓	✓	✓	✓

Tabel 3 Hasil Pemetaan Pelindungan Data Pribadi *Legal Basis and Consent Management*

ID	COBIT 2019	DAMA	ASEAN DMF	NIST PF	CIPM
P08	✕	✕	✓	✕	✓
P09	✓	✓	✓	✓	✓
P10	✓	✓	✕	✓	✓
P11	✕	✓	✕	✓	✓
P12	✕	✕	✕	✓	✓
P13	✕	✓	✕	✓	✕

Tabel 4 Hasil Pemetaan Pelindungan Data Pribadi *Data Security*

ID	COBIT 2019	DAMA	ASEAN DMF	NIST PF	CIPM
P14	✓	✓	✓	✕	✓
P15	✕	✕	✕	✕	✓
P16	✕	✕	✕	✕	✓
P17	✓	✓	✕	✓	✓
P18	✓	✓	✓	✕	✓
P19	✕	✓	✓	✓	✓
P20	✕	✓	✕	✓	✓

Tabel 5 Hasil Pemetaan Pelindungan Data Pribadi *Audit Trail*

ID	COBIT 2019	DAMA	ASEAN DMF	NIST PF	CIPM
P21	✓	✓	✕	✓	✕
P22	✓	✓	✓	✓	✕
P23	✕	✓	✓	✕	✕
P24	✕	✓	✕	✓	✓
P25	✓	✓	✓	✓	✓

Tabel 6 Hasl Pemetaan Pelindungan Data Pribadi *Incident Management*

ID	COBIT 2019	DAMA	ASEAN DMF	NIST PF	CIPM
P26	✕	✕	✓	✓	✕
P27	✓	✕	✕	✓	✕
P28	✓	✓	✓	✓	✓
P29	✓	✕	✓	✓	✕
P30	✕	✓	✕	✓	✓
P31	✓	✓	✓	✓	✓

B. Analisis

Hasil analisis menunjukan bahwa seluruh parameter terdapat pada SKKNI bidang Pelindungan Data Pribadi yang patuh pada UU PDP, dalam segi kompetensi serta kriteria. Dalam penelitian ini telah diidentifikasi sebanyak 31 parameter dengan memetakan 15 kompetensi SKKNI bidang Pelindungan Data Pribadi untuk setiap parameternya. Selain itu, seluruh parameter yang dipetakan pada setiap 5 (lima) kerangka kerja standar Internasional memiliki perbedaan, fokus dan kekuatan yang saling terintegrasi. Pada COBIT 2019, berfokus pada tata kelola, prinsip, dan pengelolaan data dan/atau risiko terhadap data. Pada DAMA-DMBOKv2, berfokus pada tata kelola dan pengelolaan data, mekanisme, penanganan keamanan data, dan pencatatan audit dalam proses pelindungan data. Pada ASEAN DMF, berfokus pada kontrol dari area siklus hidup data, penilaian risiko serta inventaris data. Pada *NIST Privacy Framework*, kerangka kerja berfokus pada tata kelola, proses, kebijakan, prosedur, dan penanganan dalam pelindungan data. Sedangkan, pada CIPM berfokus pada tata kelola program privasi, pengelolaan keamanan data dan dasar hukum pelindungan data.

Berdasarkan hasil analisis pemetaan, proses penggabungan kelima kerangka kerja dilakukan untuk memastikan bahwa kerangka kerja tersebut telah mematuhi prinsip-prinsip pelindungan data pribadi sesuai dengan regulasi. Dengan menggunakan kombinasi kerangka kerja, proses perancangan *assessment* pelindungan data dapat memberikan panduan dalam memastikan keamanan, privasi dan pengelolaan yang optimal serta memenuhi persyaratan perundang-undangan, selain itu proses penggabungan ini dapat membantu dalam perancangan kerangka kerja *assessment* pelindungan data pribadi yang relevan untuk berbagai variasi industri.

V. KESIMPULAN

Penelitian ini berhasil mengidentifikasi parameter yang selaras terhadap Undang-Undang Pelindungan Data Pribadi dengan mengacu kepada variabel SKKNI bidang Pelindungan Data Pribad. Selain itu, untuk dapat memberikan kerangka kerjauntuk dapat memberikan kerangka kerja *assessment* PDP *readiness* yang komprehensif dan sesuai dengan kebutuhan implementasi Undang-Undang Pelindungan Data Pribadi dalam proses pemrosesan dan pengelolaan data pribadi. Penelitian ini memetakan lima kerangka kerja standar Internasional yang memiliki keterkaitan terhadap data meliputi pelindungan data, pengelolaan data serta keamanan data, yang terdiri dari COBIT 2019, DAMA-DMBOKv2, ASEAN *Data Management Framework*, NIST PF, CIPM *Body of Knowledge.*

COBIT 2019 memiliki keunggulan dalam aspek kebijakan tata kelola, manajemen risiko dan manajemen data, namun dalam hal pelindungan data COBIT 2019 masih

belum menjelaskan secara mendalam. DAMA-DMBOKv2 unggul dalam mekanisme pengelolaan dan keamanan terhadap data. ASEAN *Data Management Framework* berfokus pada siklus hidup pengelolaan data dari tahapan pengumpulan, penggunaan, pengiriman, penyimpanan serta penghapusan data, selain itu penilaian risiko dan penyimpanan data berdasarkan jenisnya juga menjadi fokus dalam kerangka kerja ini. NIST *Privacy Framework* menojol dalam aspek kebijakan pemrosesan data, privasi dan pelindungan data, serta penanganan risiko dan insiden keamanan data. Sementara, CIPM *Body of Knowledge* memiliki fokus dalam program privasi yang melibatkan kebijakan dan kebutuhan tata kelola, persetujuan dasar hukum dan keamanan terhadap data. Penggabungan kelima kerangka kerja tersebut menghasilkan kerangka kerja pelindungan data yang diharapkan dapat selaras dengan Undang-Undang Pelindungan Data Pribadi dalam aktivitas pemrosesan, pengelolaan serta pelindungan terhadap keamanan dan privasi data.

REFERENSI

[1] O. G. Fakeyede *et al.*, "Navigating Data Privacy Through IT Audits: GDPR, CCPA, and Beyond," *International Journal of Research in Engineering and Science (IJRES) ISSN*, vol. 11, pp. 184–192, 2023, [Online]. Available: www.ijres.org

[2] Badan Siber dan Sandi Negara (BSSN), "Lanskap Keamanan Siber Indonesia," 2023. Accessed: Jan. 02, 2025. [Online]. Available: https://csirt.kemenkeu.go.id/api/Medias/4b7a023f-7e86-43fa-b877-51697ab24594

[3] Republik Indonesia, *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*. 2022.

[4] A. A. Reksoprodjo, M. Dachyar, and N. R. Pratama, "A Decision-Making Model for Selecting Personal Data Protection Frameworks for Companies in Indonesia," *Journal of System and Management Sciences*, vol. 14, no. 2, pp. 156–171, 2024, doi: 10.33168/JSMS.2024.0210.

[5] D. H. Shin, "The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption," *Interact Comput*, vol. 22, no. 5, pp. 428–438, 2010, doi: 10.1016/j.intcom.2010.05.001.

[6] M. Amiri-Zarandi, R. A. Dara, E. Duncan, and E. D. G. Fraser, "Big Data Privacy in Smart Farming: A Review," *Sustainability (Switzerland)*, vol. 14, no. 15, Aug. 2022, doi: 10.3390/su14159120.

[7] V. Wylde *et al.*, "Cybersecurity, Data Privacy and Blockchain: A Review," *SN Comput Sci*, vol. 3, no. 2, Mar. 2022, doi: 10.1007/s42979-022-01020-4.

[8] E. Eryurek, U. Gilad, V. Lakshmanan, A. Kibunguchy-Grant, and J. Ashdown, *Data Governance The Definitive Guide People, Processes, and Tools to Operationalize Data Trustworthiness*, First. O'Reilly Media, 2021.

[9] N. Purtova, "The illusion of personal data as no one's property," *Law Innov Technol*, vol. 7, no. 1, pp. 83–111, 2015, doi: 10.1080/17579961.2015.1052646.

[10] "Keputusan Menteri Ketatanegaraan Republik Indonesia," 2023.

[11] Susan. Earley, Deborah. Henderson, and Data Management Association., *DAMA-DMBOK : data management body of knowledge*, 2nd ed. 2017.

[12] S. R. Ghorashi, T. Zia, M. Bewong, and Y. Jiang, "An Analytical Review of Industrial Privacy Frameworks and Regulations for Organisational Data Sharing," Dec. 01, 2023, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/app132312727.

[13] "NIST Privacy Framework," Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2020. doi: 10.6028/NIST.CSWP.01162020.

[14] "Certified Information Privacy Manager (CIPM) Body of Knowledge," 2024.

[15] R. Winter and J. Vom Brocke, "Teaching Design Science Research," in *Forty-Second International Conference on Information Systems*, 2021. [Online]. Available: https://www.researchgate.net/publication/355826960

[16] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," 2004. [Online]. Available: https://www.jstor.org/stable/25148625