**Jurnal Manajemen Informatika Jayakarta**
Volume 5, Nomor 2, April 2025: halaman 122-134

P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v5i2.1721

# ANALISIS KESESUAIAN KEBIJAKAN PERLINDUNGAN DATA KANTOR PUSAT PERUSAHAAN MULTINASIONAL DENGAN UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI INDONESIA

**[1]Fritz Gamaliel*, [2] P. Yudi Dwi Arliyanto**

[1]Program Studi Teknologi Rekayasa Perangkat Lunak, Politeknik META Industri Cikarang
[2]Program Studi Teknik Industri, Politeknik META Industri Cikarang
Jln. Inti 1 Blok C1 No 7 Lippo Cikarang

*e-mail: fritzgamaliel@gmail.com

## Abstrak

Dalam menjamin keamanan informasi, maka kantor pusat mengeluarkan program perlindungan data untuk diterapkan oleh kantor-kantor cabangnya. Untuk menerapkan suatu program maka kantor cabang memiliki kebijakan untuk terlebih dahulu melaksanakan penilaian berdasarkan peraturan yang berlaku di Indonesia. Oleh karena itu dalam penelitian ini, melaksanakan penilaian antara program perlindungan data dari kantor pusat tersebut dengan peraturan perlindungan data yang berlaku di Indonesia. Metode yang digunakan dalam penelitian ini adalah studi literatur-literatur yang terkait dengan penelitian. Pada hasil penelitian didapatkan bahwa terdapat beberapa hal yang masih belum sesuai antara program perlindungan data dari kantor pusat dengan peraturan perlindungan data yang berlaku di Indonesia.

**Kata kunci:** penilaian, perlindungan data, keamanan informasi

## *Abstract*

*To ensure information security, the head office has issued a data protection program to be implemented by its branch offices. Branch offices have a policy to assess the head office program based on the regulations applicable in Indonesia. Therefore, the objective of this study is to evaluate the correlation between the head office' data protection program and the data protection regulations applicable in Indonesia. This study adopts an approach focused on reviewing relevant literature to support the research objectives. The study findings indicate that there are several aspects of the data protection program from the head office that are not yet fully aligned with the data protection regulations applicable in Indonesia.*

***Keywords:*** *assessment, data protection, information security*

## 1 Pendahuluan

Tiap-tiap negara di dunia ini memiliki peraturannya masing-masing. Peraturan-peraturan tersebut salah satunya adalah peraturan tentang perlindungan data. Indonesia telah memiliki peraturan perlindungan data, salah satunya adalah Undang-Undang Nomor 27 Tahun 2022. Uni Eropa memiliki peraturan perlindungan data, GDPR (*General Data Protection Regulation*). Dalam penelitian ini, kantor pusat di Amerika mengeluarkan peraturan perlindungan data untuk dapat diterapkan oleh kantor-kantor cabangnya.

Sebagai kantor cabang yang berlokasi di Indonesia, maka melaksanakan penilaian terhadap peraturan perlindungan data yang dikeluarkan oleh kantor pusat tersebut untuk mengetahui apakah telah sesuai atau belum sesuai dengan peraturan perlindungan data yang berlaku di Indonesia. Oleh karena itu penelitian ini bertujuan untuk menilai peraturan perlindungan data dari kantor pusat

Jurnal Manajemen Informatika Jayakarta
Volume 5, Nomor 2, April 2025: halaman 122-134
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v5i2.1721

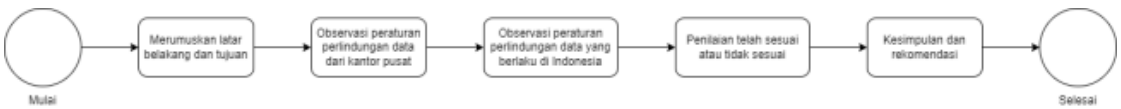
berdasarkan peraturan perlindungan data yang berlaku di Indonesia. Hasil penelitian ini dapat menjadi landasan dalam menerapkan program perlindungan data dari kantor pusat yang sesuai dengan peraturan perlindungan data yang berlaku di Indonesia.

## 2 Tinjauan Literatur

Terdapat penelitian-penelitian sebelumnya yang juga meneliti hubungan dengan peraturan perlindungan data yang berlaku di Indonesia. Dalam penelitian yang dilaksanakan oleh Inggrit Rismauli Siahaan dan kawan-kawan menganalisis kesesuaian perlindungan data pribadi aplikasi satusehat dengan regulasi hukum di Indonesia [1]. Dalam penelitian yang dilaksanakan oleh Rico Ardi Wijaya dan Mochammad Tanzil Multazam menganalisis perlindungan data pribadi aplikasi shopee [2]. Dalam penelitian yang dilaksanakan oleh Sinta Dewi Rosadi menelaah bagaimana perlindungan data pribadi dalam program e-health[3]**.** Dalam penelitian yang dilaksanakan oleh Ira Yanti dan Muhammad Irwan Padli Nasution menganalisis perlindungan data pribadi aplikasi grab [4]. Dalam penelitian yang dilaksanakan oleh Juwairiazizah Rasta dan Muhammad Irwan Padli Nasution mengetahui bagaimana perlindungan hukum terhadap data pribadi konsumen pengguna aplikasi gojek [5]. Dalam penelitian yang dilaksanakan oleh Rikson Simarmata dan kawan-kawan mengetahui perlindungan data pribadi konsumen lazada dalam transaksi e-commerce terdiri dari perlindungan hukum preventif dan perlindungan hukum represi [6]. Dalam penelitian yang dilaksanakan oleh Deni Bagus Prasetyo Aji menganalisis perlindungan data pribadi aplikasi tokopedia dan mengetahui permasalahan perlindungan data pribadi bukan hanya dari regulasi tapi juga kurangnya pengawasan yang dilakukan oleh pemerintah [7]. Dalam penelitian yang dilaksanakan oleh Hari Widiyanto dan Lunaraisah menganalisis perlindungan data pribadi aplikasi traveloka, mengetahui perlindungan hukum internal mengandung klausula eksonerasi, perlindungan hukum eksternal berdasarkan Undang-Undang Nomor 27 Tahun 2022 [8]**.** Dalam penelitian yang dilaksanakan oleh Syavina Nadhira Lubis dan Muhammad Irwan Padli Nasution mengetahui perlindungan data pribadi aplikasi media sosial [9]**.** Dalam penelitian yang dilaksanakan oleh Nurul Adliyah dan kawan-kawan menganalisis perlindungan data pribadi aplikasi OVO [10]**.** Dalam penelitian yang dilaksanakan oleh Dinda Novika Rahmahdhani dan kawan-kawan mengetahui model keamanan dan peraturan perlindungan data pribadi aplikasi m-banking [11]**.** Dalam penelitian yang dilaksanakan oleh Gillang Achmad Riyadi dan Toto Tohir Suriaatmadja mengetahui bahwa PT PLN tetap wajib bertanggungjawab atas kebocoran data pribadi konsumen PT PLN baik yang dilakukan secara sengaja maupun tidak sengaja [12]. Dalam penelitian yang dilaksanakan oleh Anida Fadla Silvia dan kawan-kawan menganalisis perlindungan data pribadi BPJS [13]. Dalam penelitian yang dilaksanakan oleh Nurmala Dunggio dan Andi Muhammad Fuad mengetahui perlindungan data pribadi dan pengaturan keamanan aplikasi cloud computing GoogleDrive [14]. Adapun yang menjadi pembeda antara penelitian ini dengan penelitian-penelitian tersebut adalah dalam penelitian ini menilai peraturan perlindungan data dari kantor pusat berdasarkan peraturan perlindungan data yang berlaku di Indonesia.

## 3 Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah studi pustaka dengan mempelajari jurnal-jurnal dan undang-undang yang terkait




**Gambar 1 Metode Penelitian**

Jurnal Manajemen Informatika Jayakarta
Volume 5, Nomor 2, April 2025: halaman 122-134
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v5i2.1721

### 3.1 Merumuskan Latar Belakang dan Tujuan

Langkah ini membutuhkan pemikiran dari peneliti untuk menggali latar belakang dan tujuan, serta melibatkan studi literatur. Langkah ini menghasilkan latar belakang dan tujuan yang kuat untuk menjadi dasar dalam penelitian ini.

### 3.2 Observasi Peraturan Perlindungan Data dari Kantor Pusat

Langkah ini mencari informasi terkait peraturan perlindungan data dari kantor pusat. Adapun kantor pusat merupakan organisasi nonprofit dan berlokasi di benua Amerika. Dalam penelitian ini meneliti 10 file tentang peraturan perlindungan data dari kantor pusat yang menjadi acuan dalam menilai telah sesuai atau tidak sesuai dengan peraturan perlindungan data yang berlaku di Indonesia. Adapun 10 file tersebut adalah sebagai berikut

#### 3.2.1 Kebijakan Keamanan Informasi

Dalam kebijakan keamanan informasi ini salah satunya tertulis berikut

1) *Implement and maintain the Information Security Program at company*
2) *Comply with all regulatory and legal requirements and mandatory standards*
3) *Continuously improve and reasonably align information security practices to global best practices and standards.*
4) *Information security policies shall be reviewed annually*
5) *Company employees shall acknowledge their adherence to these information security policies and practices annually.*
6) *Security awareness training shall be provided annually or as mandated by compliance requirements.*
7) *Internal assessments or reviews of company's Information Security Program shall be performed periodically, and any gaps or findings shall be remediated promptly.*
8) *A risk assessment process for company's information assets shall be defined and followed. Risk reduction shall be carried out through continuous improvement.*
9) *Company's information asset inventories shall be reviewed and updated when a new asset is added and/or an existing asset is upgraded.*
10) *Business continuity plans (BCPs) and backup plans shall be reviewed and tested at least annually.*
11) *Roles and responsibilities shall be clearly defined and communicated to relevant individuals.*
12) *Information should be classified and handled according to its criticality and sensitivity as mandated by relevant legislative, regulatory, and contractual requirements.*
13) *Appropriate contacts shall be maintained with relevant authorities, special interest groups or other specialist security forums.*
14) *Security incidents shall be reported according to company's Incident Response Plan.*
15) *Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for protecting information shall be identified, regularly reviewed, and documented.*
16) *Prevention, detection, and recovery controls to protect against malware shall be implemented by company, and these will be combined with appropriate user awareness training and supplemental communications.*
17) *An incident management process shall be established to correctly identify, contain, investigate, and remediate incidents that threaten the security or confidentiality of company's information assets.*
18) *Company shall develop and maintain a vendor management process for third-party vendor engagement and assessment.*
19) *Change and vulnerability management controls shall be established and implemented.*

**Jurnal Manajemen Informatika Jayakarta**
Volume 5, Nomor 2, April 2025: halaman 122-134
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v5i2.1721

### 3.2.2 Kebijakan Perlindungan Data

Dalam kebijakan perlindungan ini salah satunya tertulis berikut

1) *Company is committed to compliance with applicable Data Protection Laws in respect of personal data,*
2) *this policy applies to all of company's personal data processing functions,*
3) *the register of processing found in the Data Protection Impact Assessment (DPIA) tool will be reviewed annually*
4) *any breach of this policy will be dealt with under company's disciplinary policy and the appropriate authorities in accordance with applicable law.*
5) *no third party may access personal data held by company without having first entered into a confidential data non-disclosure agreement (NDA)*
6) *Consent cannot be inferred from non-response to a communication. In most instances, consent to process personal and sensitive data is obtained routinely by CBN using standard consent documents*
7) *Where company provides online services to children, parental or custodial authorization must be obtained. This requirement applies to children under the age of 18 (unless the country and/or the applicable law has made provision for a different age limit).*
8) *Care must be taken to ensure that PC screens and terminals are not visible except to authorized Employees/Staff, including offsite work.*
9) *Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed before disposal.*
10) *must ensure that personal data is not disclosed to unauthorized third parties which includes family members, friends, government bodies,*
11) *All exports of data to 'third countries' are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".*
12) *Data protection impact assessments (DPIAs) are carried out in relation to the processing of personal data. Medium and High risks to individual rights and freedoms are recorded in a Risk Register, with recommended actions to mitigate the identified risks.*

### 3.2.3 Kebijakan Prosedur Penilaian Dampak Perlindungan Data (DPIA / *Data Protection Impact Assessment*)

Dalam kebijakan prosedur penilaian dampak perlindungan data ini salah satunya tertulis berikut

1) *Company must carry out a DPIA where a planned or existing processing operation is "likely to result in a high risk"*
2) *In cases where it is not clear whether a DPIA is required or not, company is required to carry out a DPIA anyway as a tool to support compliance with data protection laws*
3) *Create a diagram to identify all of the systems that will be used to process personal data and how the data will be transferred between them. This diagram can be referenced within the DPIA Report.*
4) *Using the data flows above, consider how unauthorized parties could view the data, how data integrity would be compromised, or data could be rendered unavailable and include that information in the appropriate portions of the DPIA Report.*
5) *Management reviews and approves the final version of the DPIA Report. In cases where the identified risks cannot be sufficiently addressed, and the residual risks remain high, GDPR Article 36 requires company to consult the relevant supervisory authority.*

Jurnal Manajemen Informatika Jayakarta
Volume 5, Nomor 2, April 2025: halaman 122-134
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v5i2.1721

### 3.2.4 Kebijakan Pemberitahuan Privasi untuk Website

Dalam kebijakan pemberitahuan privasi untuk website ini salah satunya tertulis berikut

1) *Company must provide people from whom personal data is collected with a privacy notice in each website.*
2) *Company must include the following information in its privacy notice:*
   - 2.1 *the identity and the contact details of the controller and, where applicable, of the controller's representative;*
   - 2.2 *the contact details of the data protection officer, where applicable;*
   - 2.3 *the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing;*
   - 2.4 *where required, the legitimate interests pursued by the controller or by a third party;*
   - 2.5 *the recipients or categories of recipients of the personal data, if any;*
   - 2.6 *where applicable, the fact that the controller intends to transfer personal data outside the European Union or European Economic Area to a third country or international organization.*
   - 2.7 *the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;*
   - 2.8 *the existence of the right to request from the controller access to and rectification or erasure of personal data, or restriction of processing concerning the data subject, or to object to processing as well as the right to data portability;*
   - 2.9 *where required, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;*
   - 2.10 *the right to lodge a complaint with a supervisory authority;*
   - 2.11 *whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; and*
   - 2.12 *the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.*
   - 2.13 *The categories of personal data obtained*
   - 2.14 *a list of the rights of data subjects, and how to exercise those rights*
3) *The privacy notices must be available orally upon request to ensure comprehension and to aid the visually impaired.*
4) *The privacy notices will be reviewed and updated periodically,*

### 3.2.5 Kebijakan Prosedur Pemberitahuan Privasi

Dalam kebijakan prosedur pemberitahuan privasi ini salah satunya tertulis berikut

1) *The privacy notice link will be provided at the bottom of every webpage*
2) *a link will be included as well wherever explicit consent is requested when collecting data on an online form.*
3) *Each update to the corporate privacy notice will be translated into the other languages and republished to the related site within a 60 day period.*

Jurnal Manajemen Informatika Jayakarta
Volume 5, Nomor 2, April 2025: halaman 122-134
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v5i2.1721

### 3.2.6 Kebijakan Prosedur Hak Akses Subjek Data

Dalam kebijakan prosedur hak akses subjek data ini salah satunya tertulis berikut

1) *Data Subjects have the right to request access to their personal data processed by company. When a Data Subject makes such requests, company will take the required steps as described in the "Process Workflow" section below. Company will review the personal data requested to see if they contain the personal data of other Data Subjects. If they do, company may redact the personal data of those other Data Subjects prior to providing the Data Subject with their personal data, unless those other Data Subjects have consented to the disclosure of their personal data.*
2) *Data Subjects have the right to have their inaccurate personal data rectified. Where such a request is made, company will, unless there is an exemption (see "Exemptions" section below), rectify the personal data without undue delay.*
3) *Data Subjects have the right, in certain circumstances, to request that company erase their personal data. When a Data Subject makes a request for erasure in the circumstances set out above, company will, unless there is an exemption (see "Exemptions" section below), take the required steps as described in the "Process Workflow" section below.*
4) *Data Subjects have the right, in certain circumstances, to receive their personal data that they have provided to company in a structured, commonly used, and machine-readable format that they can then transmit to another company. Where such a request is made, company will, unless there is an exemption (see "Exemptions" section below), provide the personal data without undue delay if: the legal basis for the processing of the personal data is consent or pursuant to a contract; and company processing of those data is automated.*
5) *Data Subjects have the right to object to the processing of their personal data. Where such an objection is made by Data Subjects, company will, unless there is an exemption (see "Exemptions" section below), no longer process a Data Subject's personal data.*
6) *Data Subjects may be extended additional rights related to personal data if local, country or regional laws require that those rights be recognized and honored by company. In that case local procedures will be developed and implemented to addres those rights in the appropriate office or region.*
7) *Before responding to any request, company will check whether there are any exemptions that apply to the personal data that are the subject of the request*
8) *Data Subject requests must be processed and replied to, within one month of receipt of such requests or of validating and clarifying the request. If the request is complex, or there are a number of requests, company may extend the period for responding by a further two months.*
9) *The third parties are required to be notified whenever a request is received from a Data Subject.*

### 3.2.7 Kebijakan Prosedur Transfer Internasional Data Pribadi

Dalam kebijakan prosedur transfer internasional data pribadi ini salah satunya tertulis berikut

1) *Any transfer of personal data to a third country or an international organization must be performed by company based on adequacy decisions.*
2) *If the country or one or more of the countries to which personal data is to be transferred is not subject to an adequacy decision from the European Commission, then appropriate safeguards must be put in place by company to provide for data subjects' rights and enforceable legal remedies.*
   *2.1 a legally binding and enforceable instrument between public authorities or bodies;*

Jurnal Manajemen Informatika Jayakarta
Volume 5, Nomor 2, April 2025: halaman 122-134
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v5i2.1721

*2.2 binding corporate rules;*
*2.3 standard data protection clauses adopted by the Commission or the relevant supervisory authority;*
*2.4 a code of conduct; or*
*2.5 a certification mechanism.*

3) *In the absence of an adequacy decision or appropriate safeguards, including BCRs, international data transfers may still occur where company determines that derogation conditions are met.*

### 3.2.8 Kebijakan Penyimpanan dan Pembuangan Data

Dalam kebijakan penyimpanan dan pembuangan data ini salah satunya tertulis berikut

1) *In general, company's data assets should be retained per the applicable record retention requirements of each department*
2) *All PII and PHI data shall be retained for as long as there is a business purpose or a legal requirement to do so*
3) *All active customer personal data shall be retained for as long as the customer continues to be an active customer of company or unless the active customer has requested the deletion of data and the data is not required for legal or business purposes*
4) *CHD (Card Holder Data) shall only be stored in approved locations and disposed of when no longer required. Credit or debit card numbers will not be stored in company systems.*
5) *Upon request of the customer, personal data no longer falling within legal or regulatory retention requirements shall be deleted or anonymized.*
6) *Company shall securely delete or dispose of CHD to prevent the data from being recreated or re-rendered*
7) *Shred paper documents using approved destruction methods and certified shredding services (minimally cross-cut shredding) prior to disposal*
8) *Suspension of Disposal in the Event of Litigation or Claims. Any further disposal of documents shall be suspended until legal counsel determines otherwise.*

### 3.2.9 Kebijakan Manajemen Insiden Keamanan Informasi

Dalam kebijakan manajemen insiden keamanan informasi ini salah satunya tertulis berikut

1) *Intrusion attempts, security breaches, theft or loss of hardware, suspicion of an incident, or other security related incidents perpetrated against the organization must be reported to the Information Security Incident Response Team (ISIRT) or designated personnel*
2) *The team responding to the incident shall perform incident handling activities consistent with the Information Security Incident Response Process to ensure the evidence gathered, both digital and physical, during the security or privacy incident can be used successfully during prosecution, if appropriate.*
3) *Lessons learned from incidents shall be incorporated into company's risk assessment process for continual improvements.*
4) *For all high-severity incidents, the ISIRT must provide a post-incident report within three business days to the Director of Global Information Security.*

### 3.2.10 Kebijakan Prosedur Pemberitahuan Kegagalan Perlindungan Data

Dalam kebijakan prosedur pemberitahuan kegagalan perlindungan data ini salah satunya tertulis berikut

1) *Suspected data breaches should be reported promptly to the Director of Information Security*

**Jurnal Manajemen Informatika Jayakarta**
Volume 5, Nomor 2, April 2025: halaman 122-134
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v5i2.1721

2) *A data breach will be notifiable when it is deemed by company as likely to pose a risk to the rights and freedoms of individuals*
3) *Where a notifiable breach has occurred, company must notify the appropriate international Supervisory Authority with undue delay but no later than 72 hours if the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach*
4) *Where a notifiable breach has occurred, company must notify the affected data subjects if the personal data breach is likely to result in a high risk to the rights and freedoms of the data subjects affected by the breach.*
5) *(applicable to Data Processor only) When the personal data breach or suspected data breach affects personal data that is being processed on behalf of a third party (i.e. controller), the Data Protection Officer/Privacy Officer of company must report any personal data breach to the respective data controller/controllers without undue delay*
   *Once the personal data breach has been contained, company should conduct a review of existing measures in place and explore the possible ways in which these measures can be strengthened to prevent a similar breach from reoccurring*

### 3.3 Observasi Peraturan Perlindungan Data yang Berlaku di Indonesia

Langkah ini mencari informasi terkait peraturan perlindungan data yang berlaku di Indonesia. Di bawah ini adalah peraturan perlindungan data yang berlaku di Indonesia, yang digunakan sebagai pedoman untuk mengevaluasi peraturan perlindungan data dari kantor pusat.

1) RPP Undang-Undang Nomor 27 Tahun 2022
2) Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
3) Undang Undang No. 27 tahun 2022 tentang Perlindungan Data Pribadi
4) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
5) Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik
6) Peraturan Pemerintah Nomor 87 Tahun 1999 tentang Tata Cara Penyerahan dan Pemusnahan Dokumen Perusahaan
7) Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik
8) Undang-Undang Nomor 24 Tahun 2013 tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan

### 3.4 Penilaian telah sesuai atau tidak sesuai

Pada langkah ini dilaksanakan penilaian apakah peraturan perlindungan data dari kantor pusat telah sesuai atau tidak sesuai dengan peraturan perlindungan data yang berlaku di Indonesia. Hasil penilaian disajikan dalam bentuk tabel penilaian.

### 3.5 Kesimpulan dan Rekomendasi

Pada akhirnya, kesimpulan dan rekomendasi dibuat berdasarkan hasil penilaian dengan tujuan untuk menjadikan landasan dalam menerapkan program perlindungan data dari kantor pusat yang sesuai dengan peraturan perlindungan data yang berlaku di Indonesia.

Jurnal Manajemen Informatika Jayakarta
Volume 5, Nomor 2, April 2025: halaman 122-134
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v5i2.1721

### 3.6 Metode Perangkat Lunak

Penelitian ini tidak memberikan solusi dalam bentuk perangkat lunak karena ruang lingkup penelitian ini adalah menilai kesesuaian kebijakan perlindungan data dari kantor pusat dengan Undang-Undang perlindungan data pribadi yang berlaku di Indonesia. Walaupun demikian hasil penelitian ini dapat digunakan sebagai salah satu masukan supaya tahap design *Software Development Life Cycle* juga memikirkan aspek *Confidentiality*, *Integrity*, dan *Availability* yang merupakan tujuan utama program keamanan informasi.

## 4 Hasil dan Pembahasan

Dalam subab ini, peneliti menyajikan hasil penilaian terkait peraturan perlindungan data dari kantor pusat berdasarkan peraturan perlindungan data yang berlaku di Indonesia. Hasil dari penelitian ini mengungkapkan daftar peraturan yang masih belum sesuai dengan peraturan perlindungan data yang berlaku di Indonesia sehingga perlu disesuaikan lebih lanjut sebelum dapat diterapkan dalam operasional kantor cabang.

**Tabel 1 Tabel Penilaian**

| No | Nama Kebijakan | Penilaian |
|---|---|---|
| 1. | Kebijakan Keamanan Informasi | Tidak ada tulisan yang tidak sesuai dengan peraturan perlindungan data yang berlaku di Indonesia |
| 2. | Kebijakan Perlindungan Data | Terdapat tulisan yang tidak sesuai dengan peraturan perlindungan data yang berlaku di Indonesia yaitu pada tulisan berikut: *Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'.* Adapun jika menurut Peraturan Pemerintah Nomor 87 Tahun 1999 pasal 16 maka naskah asli dokumen perusahaan masih tetap perlu disimpan karena mengandung nilai tertentu demi kepentingan perusahaan atau kepentingan nasional. Metode Perangkat Lunak: fitur agar dokumen demikian tetap hanya dapat diakses oleh pihak yang sah (*Confidentiality*) dan tetap utuh ketika diakses oleh pihak yang sah (*Integrity* dan *Availability*). |
| 3. | Kebijakan Prosedur Penilaian Dampak Perlindungan Data (DPIA / *Data Protection Impact Assessment)* | Tidak ada tulisan yang tidak sesuai dengan peraturan perlindungan data yang berlaku di Indonesia |
| 4. | Kebijakan Pemberitahuan Privasi Untuk Website | Menurut peneliti terdapat kalimat yang masih kurang sesuai yaitu pada kalimat berikut *The privacy notices will be reviewed and updated periodically* yang seharusnya misalnya dirobah ke kalimat berikut *The privacy notices will be reviewed and updated periodically, so company must provide function to reconfirm the updated privacy notices*. Hal tersebut agar dapat lebih sesuai dengan Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 pasal 30 yang mana penyelenggara sistem elektronik wajib menyediakan fitur paling sedikit yang salah satunya untuk memberikan konfirmasi atau rekonfirmasi. Metode Perangkat Lunak: fitur rekonfirmasi terhadap |

**Jurnal Manajemen Informatika Jayakarta**
Volume 5, Nomor 2, April 2025: halaman 122-134
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v5i2.1721

| | | |
|---|---|---|
| | | update kebijakan privasi. |
| 5. | Kebijakan Prosedur Pemberitahuan Privasi | Tidak ada tulisan yang tidak sesuai dengan peraturan perlindungan data yang berlaku di Indonesia |
| 6. | Kebijakan Prosedur Hak Akses Subjek Data | Terdapat tulisan yang tidak sesuai dengan peraturan perlindungan data yang berlaku di Indonesia yaitu pada tulisan berikut: *Data Subject requests must be processed and replied to, within one month of receipt of such requests or of validating and clarifying the request. If the request is complex, or there are a number of requests, company may extend the period for responding by a further two months.* Adapun jika menurut Undang-Undang Nomor 27 Tahun 2022 pasal 32, pasal 40, pasal 41 maka paling lambat adalah 3 x 24 (tiga kali dua puluh empat) jam. Metode Perangkat Lunak: fitur pemberitahuan deadline penyelesaian permintaan subjek data. |
| 7. | Kebijakan Prosedur Transfer Internasional Data Pribadi | Terdapat tulisan yang tidak sesuai dengan peraturan perlindungan data yang berlaku di Indonesia yaitu pada tulisan berikut: *If the country or one or more of the countries to which personal data is to be transferred is not subject to an adequacy decision from the European Commission, then appropriate safeguards must be put in place by company to provide for data subjects' rights and enforceable legal remedies. * a legally binding and enforceable instrument between public authorities or bodies; * binding corporate rules; * standard data protection clauses adopted by the Commission or the relevant supervisory authority; * a code of conduct; * or a certification mechanism.* Adapun jika menurut RPP Nomor 27 Tahun 2022 pasal 181 sampai dengan pasal 196 maka tidak ada tertulis tentang apakah kode etik (*a code of conduct*) dan apakah mekanisme sertifikasi (*a certification mechanism*) termasuk baik dalam tingkat perlindungan data yang setara atau lebih tinggi maupun dalam tingkat perlindungan data yang memadai dan mengikat. Metode Perangkat Lunak: menggunakan praktis terbaik global dalam segala proses perangkat lunak. |
| 8. | Kebijakan Penyimpanan dan Pembuangan Data | Terdapat tulisan yang tidak sesuai dengan peraturan perlindungan data yang berlaku di Indonesia yaitu pada tulisan berikut: *CHD (Card Holder Data) shall only be stored in approved locations and disposed of when no longer required. Credit or debit card numbers will not be stored in company systems.* Adapun jika menurut Peraturan Pemerintah Nomor 87 Tahun 1999 pasal 16 maka naskah asli dokumen perusahaan masih tetap perlu disimpan karena mengandung nilai tertentu demi kepentingan perusahaan atau kepentingan nasional. Metode Perangkat Lunak: fitur *intelligence* sebagai salah satu masukkan dalam proses pembuatan keputusan tentang dokumen apa saja yang boleh |

**Jurnal Manajemen Informatika Jayakarta**
Volume 5, Nomor 2, April 2025: halaman 122-134
P-ISSN: 2746-5985
e-ISSN: 2797-0930
DOI: https://doi.org/10.52362/jmijayakarta.v5i2.1721

| | | | |
|---|---|---|---|
| | | | disimpan dan dokumen apa saja yang tidak boleh disimpan. |
| 9. | Kebijakan Insiden Informasi | Manajemen Keamanan | Menurut peneliti terdapat kalimat yang masih kurang sesuai yaitu pada kalimat berikut *For all high-severity incidents, the ISIRT must provide a post-incident report within three business days to the Director of Global Information Security* yang seharusnya misalnya dirobah ke kalimat berikut *For all high-severity incidents, the ISIRT must provide a post-incident report within three business days to the Director of Global Information Security and Lembaga PDP*. Hal tersebut agar dapat lebih sesuai dengan Undang-Undang Nomor 27 Tahun 2022 pasal 46 dan RPP Undang-Undang Nomor 27 Tahun 2022 pasal 125 yang mana dokumentasi insiden kegagalan perlindungan data pribadi yang disusun oleh Pengendali Data Pribadi wajib disampaikan kepada Lembaga PDP. Metode Perangkat Lunak: fitur pelaporan insiden keamanan informasi ke Direktur Keamanan Informasi Global dan ke Lembaga PDP. |
| 10. | Kebijakan Pemberitahuan Pelanggaran | Prosedur | Menurut peneliti terdapat kalimat yang masih kurang sesuai yaitu pada kalimat berikut *Where a notifiable breach has occurred, company must notify the appropriate international Supervisory Authority with undue delay but no later than 72 hours if the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach* yang seharusnya misalnya dirobah ke kalimat berikut *Where a notifiable breach has occurred, company must notify the appropriate international Supervisory Authority and Lembaga PDP with undue delay but no later than 72 hours if the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach.* Hal tersebut agar dapat lebih sesuai dengan Undang-Undang Nomor 27 Tahun 2022 pasal 46 dan RPP Undang-Undang Nomor 27 Tahun 2022 pasal 125 yang mana dokumentasi insiden kegagalan perlindungan data pribadi yang disusun oleh Pengendali Data Pribadi wajib disampaikan kepada Lembaga PDP. Metode Perangkat Lunak: fitur pelaporan insiden keamanan informasi ke *Internasional Supervisory Authority* dan ke Lembaga PDP. |

## 5 Kesimpulan

Dari penelitian yang telah dilakukan oleh peneliti terhadap peraturan perlindungan data dari kantor pusat berdasarkan peraturan-peraturan perlindungan data yang berlaku di Indonesia maka peneliti membuat kesimpulan sebagai berikut:

1) Di dalam peraturan perlindungan data dari kantor pusat juga terdapat tulisan-tulisan yang saling bertentangan. Misalnya saja di dalam Kebijakan Prosedur Hak Akses Subjek Data terdapat tulisan

P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v5i2.1721

berikut *Data Subjects have the right to have their inaccurate personal data rectified. Where such a request is made, company will, unless there is an exemption (see "Exemptions" section below), rectify the personal data without undue delay* bahwa memproses permintaan subjek data tanpa delay. Sedangkan masih di dalam Kebijakan Prosedur Hak Akses Subjek Data yang sama terdapat tulisan berikut *Data Subject requests must be processed and replied to, within one month of receipt of such requests or of validating and clarifying the request. If the request is complex, or there are a number of requests, company may extend the period for responding by a further two months* bahwa memproses permintaan subjek data dalam waktu 1 bulan.

2) Dari Hasil dan Pembahasan didapatkan bahwa terdapat tulisan dalam peraturan perlindungan data dari kantor pusat yang tidak sesuai dengan peraturan perlindungan data yang berlaku di Indonesia walau di dalam peraturan perlindungan data dari kantor pusat terdapat tulisan berikut *Comply with all regulatory and legal requirements and mandatory standards*. Selain itu, menurut peneliti, peraturan perlindungan data dari kantor pusat tersebut juga terdapat tulisan yang masih kurang lengkap. Misalnya saja di dalam Kebijakan Perlindungan Data terdapat tulisan berikut *must ensure that personal data is not disclosed to unauthorized third parties which includes family members, friends, government bodies,* bahwa belum tertuliskan bagaimana caranya agar pihak perusahaan dapat memastikan bahwa data pribadi yang dikelolanya tidak diungkapkan oleh karyawannya kepada anggota keluarga, teman, badan pemerintah.

## Referensi (Reference)

[1] I. R. Siahaan *et al.*, "Analisis Praktik Perlindungan Data Pribadi pada Aplikasi 'Satusehat terhadap Regulasi Hukum di Indonesia," *J. Teknoinfo*, vol. 18, no. 1, pp. 141–150, 2024, [Online]. Available: https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index.

[2] R. A. Wijaya and M. T. Multazam, "Analysis of the Implementation of Personal Data Protection in the Shopee Online Shopping Application [Analisis Implementasi Perlindungan Data Pribadi pada Aplikasi Belanja Online Shopee]," pp. 1–8, 2023, [Online]. Available: https://archive.umsida.ac.id/index.php/archive/preprint/view/3457/version/3449.

[3] S. D. Rosadi, "Implikasi Penerapan Program E-Health Dihubungkan Dengan Perlindungan Data Pribadi," *Arena Huk.*, vol. 9, no. 3, pp. 403–420, 2016, doi: 10.21776/ub.arenahukum.2016.00903.6.

[4] I. Yanti and M. I. P. Nasution, "Perlindungan Hukum Privasi Dan Data Pribadi Konsumen Pengguna Jasa Aplikasi Grab," *J. Akunt. Keuang. dan Bisnis*, vol. 01, no. 02, pp. 50–53, 2023, [Online]. Available: https://jurnal.ittc.web.id/index.php/jakbs/article/view/33%0Ahttps://jurnal.ittc.web.id/index.php/jakbs/article/download/33/29.

[5] J. Rasta and M. I. P. Nasution, "Perlindungan Data Privasi Konsumen Layanan Gojek Berdasarkan Hukum," *J. Akunt. Keuang. dan Bisnis*, vol. 1, no. 2, pp. 65–67, 2023, [Online]. Available: https://jurnal.ittc.web.id/index.php/jakbs/index.

[6] R. Simarmata, R. J. Akyuwen, and T. L. Pesulima, "Perlindungan Data Pribadi Konsumen Lazada Dalam Transaksi E-Commerce," *Pattimura Law Study Reviiew*, vol. 2, no. 1, pp. 145–161, 2024.

[7] D. B. P. Aji, "Perlindungan Data Pribadi dalam Transaksi Online Studi Putusan Nomor 235/Pdt.G/2020/Pn.Jkt.Pst," *Postulat*, vol. 1, no. 1, pp. 36–44, 2023, doi: 10.37010/postulat.v1i1.1149.

P-ISSN: 2746-5985
e-ISSN: 2797-0930

DOI: https://doi.org/10.52362/jmijayakarta.v5i2.1721

[8] H. Widiyanto and Lunaraisah, "Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen Traveloka Paylater Oleh Perusahaan," *J-CEKI J. Cendekia Ilm.*, vol. 3, no. 6, pp. 7351–7364, 2024.

[9] S. N. Lubis and M. I. P. Nasution, "Analisis Penyalahgunaan Data Pribadi Dalam Menggunakan Media Sosial," *JoSES J. Sharia Econ. Sch.*, vol. 2, no. 2, pp. 75–78, 2023.

[10] N. Adliyah, F. Jamaluddin, M. A. Kahfi, and Susisanti, "Perlindungan DataPribadi Pengguna Dompet Digital OVO," *Al-Amwal J. Islam. Econ. Law*, vol. 6, no. 1, pp. 76–90, 2021, doi: 10.25123/vej.3778.

[11] D. N. Rahmahdhani, M. I. P. Nasution, and S. S. A. Sundari, "Perlindungan Data Privasi Yang Dilakukan Perbankan Terhadap Penggunaan Layanan Mobile Banking," *JUEB J. Ekon. dan Bisnis*, vol. 2, no. 2, pp. 88–96, 2023, doi: 10.57218/jueb.v2i2.693.

[12] G. A. Riyadi and T. T. Suriaatmadja, "Perlindungan Hukum Atas Kebocoran Data Pribadi Konsumen PT PLN Dihubungkan Dengan Hak Atas Keamanan Pribadi Ditinjau Dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Bandung Conf. Ser. Law Stud.*, vol. 3, no. 1, 2023, doi: 10.29313/bcsls.v3i1.4945.

[13] A. F. Silvia, W. Saputra, H. Sunaryo, and F. Sinlae, "Analisis Keamanan Data Pribadi pada Pengguna BPJS Kesehatan : Ancaman , Risiko , Strategi," *Nusant. J. Multidiscip. Sci.*, vol. 2, no. 1, pp. 201–207, 2024.

[14] N. Dunggio and A. M. Fuad, "PERLINDUNGAN DATA PRIBADI CLOUD COMPUTING SYSTEM (GOOGLE DRIVE) DITINJAU DARI PERSPEKTIF UNDANG UNDANG NOMOR 19 TAHUN 2016 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK," *Sultan Amai Staatsr. J.*, vol. 1, no. 1, pp. 21–38, 2023.