Conception of an Independent Surveillance Authority in the Efforts to Protect Population Data

**Daffa Ladro Kusworo**  
State Administrative Court, Lampung, Indonesia  
daffalkusworo@gmail.com

**Andre Arya Pratama**  
Tabihita Lampung, Indonesia  
andrearyapratama9@gmail.com

**Maghfira Nur Khaliza Fauzi**  
State Administrative Court, Lampung, Indonesia  
maghfira0601@gmail.com

**Maya Shafira**  
Universitas Lampung, Indonesia  
mayashafira2@gmail.com

Submitted: Feb 11, 2022; Reviewed: June 27, 2022; Accepted: June 28, 2022

<table>
<thead>
<tr>
<th>Article’s Info</th>
<th>Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Keywords:</strong> Authority; EU GDPR; Population Data; Protection</td>
<td>The progress of digital transformation requires efforts to protect personal data as a guarantee of individual rights to overcome the large number of cases of data leakage and misuse, one of which is population data. The concretization of the government's efforts based on Article 28 G of the 1945 Constitution is realized through providing access to population data to all institutions, both state and private institutions for data verification. In addition, there is an obligation for data user parties to implement a Zero Data Sharing Policy with provisions prohibiting the dissemination or sharing of population data with third parties. However, various basic factors are influenced by the limited aspects of legal protection related to the</td>
</tr>
</tbody>
</table>

**DOI**  
https://doi.org/10.25041/aelr.v3i1.2530
Conception of an... Daffa Ladro, Andre Arya Pratama, Maghfira Nur Khaliza Fauzi, Maya Shafira

class of personal data, and the authority between the data owner and the user, which makes it imperative to enact the current regulation on personal data protection. In addition, the establishment of an Independent Surveillance Authority is a must in ensuring the implementation of these regulations, because their duties and authorities are in line with the government’s efforts in protecting population data. This study uses a normative legal research method with an approach to legislation and literature study, and uses descriptive analysis in managing qualitative data by applying a deductive method. The results of the study indicate that the need for legal guarantees must be accompanied by an element of optimal supervision through the establishment of an Independent Surveillance Authority in accordance with the standardization of the European Union General Data Protection Regulation (EU GDPR). Its independent position will prevent intervention from various parties for certain interests. Functionally, it is considered appropriate in optimizing the implementation of the Zero Data Sharing Policy through the conception of investigative authority and collective rights as a guarantee of human rights.

A. Introduction

Various dynamics of the current covid-19 pandemic have an impact on accelerating digital transformation. This rapid development provides easy access to information for individual users as well as government and private agencies. This needs to be accompanied by efforts to protect personal data as a fulfillment of constitutional rights guarantees. Human rights are essentially an important part that is constitutionally based on the 1945 Constitution as a general rule, the scope of the protection of human rights for all citizens through the preparation of laws and regulations with provisions oriented to the provision of guarantees of human rights for the protection of human rights. rights that must be achieved by citizens. It is mandatory for individuals to have a private place and are entitled to protection through the certainty of legal protection for their personal data, so that there are no criminal acts related to the misuse of personal data. Such protection is a form of harmonization of law which in essence has been regulated in the national and international scope.

Fundamentally that privacy is something that is so fundamental to the rights of everyone in maintaining the integrity and dignity of the individual. Alan Westin provides a view regarding the rights of individuals, groups or communities that essentially have the right to regulate restrictions on access to personal information of individuals to others in an important component that underlies the increasing use of technology today, demands for disclosure of information and data control by various parties. The correlation between personal data and information with security guarantees and supervision in the

2 Majda El-Muhtaj, Hak Asasi Manusia Dalam Konstitusi Indonesia (Jakarta: Kencana Prenada Media Group, 2015).
realization of the concept of confidentiality is one aspect of privacy rights that is integrated with Human Rights. Dicey gave a statement that as one of the elements of the implementation of the rule of law the state is obliged to provide comprehensive guarantees of human rights. In line with Ali Zaidan’s perspective that human rights are basic human rights that have natural and universal nature to later become recognition before God Almighty at his creation as a creature. Fundamental rights are so important in the essential rule of law to become a discourse that guarantees fulfillment and protection, inclusion in international instruments needs to be further regulated in specific arrangements in Indonesia. In general, that it has been explained in Article 28 G paragraph (1) of the 1945 Constitution with a statement that there is a right granted related to the right to personal protection, furthermore the configuration related to protection that threatens and creates fear to do something becomes a substantial subject Human rights. In fulfilling this, Danriyanto gives the opinion that the rights granted to the private and private spheres will give rise to morality and human values, there is a link in improving the relationship between individuals and society, providing independence or autonomy in regulating freely and influences related to tolerance avoid discrimination and restrictions on power by the government. The description becomes a reference regarding personal and private data that needs to be regulated as a universal philosophy with written and unwritten rules such as laws. These rights will be related to spiritual needs in respecting feelings and the right to live their lives (the right to be let alone). The scope related to the realm of personal data is essentially the identity of a person who needs to get protection as described in Article 12 of the Universal Declaration of Human Rights. Sustainability is systemically compiled into information to determine the identity of a person who is either letters or numbers marked with individual characteristics with privacy characteristics called population data. The current acceleration of digital disruption makes population data utilized through government efforts to protect personal data. The current form of government priorities is interpreted through providing access to population data to all institutions, both government agencies and private institutions in the hope of avoiding potential data leakage practices. However, there are weaknesses in the aspect of legal protection, as well as the current technological system which is inadequate. The absence of regulations related to the categories of personal data that must be protected in the management of population data, as well as the absence of the rights and authority of the data owner in determining the limits of data users are obstacles for the government in guaranteeing the constitutional rights of citizens.

So there is a need for legal codification through the ratification of the Personal Data Protection Bill, one of which includes population data protection in providing comprehensive clarity and guarantees. In addition, there is an obligation to implement a Zero Data Sharing Policy which is expected to guarantee data protection through inter-institutional prohibitions to share population data with third parties sourced from government databases as data owners for data access provided to all data user institutions. However, there are limitations to the government's surveillance authority regarding the extent to which the data is managed, and to follow up if any violations of the policy are found. Moreover, currently there is a significant increase in the number of cases with various methods of theft of personal data by irresponsible persons in the last few years.}

The increase in the number of data leakage cases in 2015 – 2020 was caused by limited supervision, lack of adequate technology, and a security system that was very vulnerable in providing guarantees for the protection of personal data. The government's efforts in providing access to population data and implementing the Zero Data Sharing Policy have not been considered effective if they are not accompanied by legal protection aspects. In this case, it also needs to be based on the existence of supervision through an Independent Authority in ensuring the effectiveness of the implementation of PDP regulations in the future. These various obstacles, of course, do not only pay attention to the juridical element through the provisions of the established regulations, but also need to be accompanied by an element of supervision. The surveillance authority in its conception refers to the EU General Data Protection Regulation (GDPR) which is the guideline for various countries in the international scope in forming functions, powers, and positions that will later affect efforts to protect personal data.

The authority to carry out investigations and collective rights is considered to be in harmony with the Zero Data Sharing Policy through supervision of data users and third parties on access to population data management, as well as ensuring the effectiveness and efficiency of the implementation of the Personal Data Protection Act which is the background of this research. In this case, our topic of discussion is to reflect on the Dynamics of Legal Protection Aspects in the Context of Population Data Management and The Role of Independent Surveillance Authority In The Protection of Population Data.

This research refers to the normative legal research method through the approach of applicable laws and regulations, as well as the use of library research. The approach to legislation is sourced from primary data in the form of the 1945 Constitution of the Republic of Indonesia, the rules for protecting personal data are explicitly only contained in the 1945 Constitution regarding the existence of sectoral rights to privacy in the Administrative Law, the ITE Law and other statutory provisions regarding guarantee of population data. In the explanation regarding the conception of the Authority of an Independent Surveillance Body, it refers to the General Data Protection Regulation (GDPR) in the legal realm of the European Union (EU) which is the legal reference for the establishment of the authority of the agency, and other statutory regulations. Regarding the literature study, which will be sourced from secondary materials in the form of books, journals, and other legal materials. The author will use descriptive analysis in qualitative data management accompanied by a deductive method, through the acquisition of the data which will be processed descriptively in order to conclude general questions into

---

specific conclusions. It can be proven in this study that there is an urgency in the aspect of legal protection in overcoming various problems in providing access to population data and implementing the Zero data sharing policy as a government priority in fulfilling the guarantee of citizens' constitutional rights. In addition, there is an obligation to establish an Independent Surveillance Agency Authority which in its authority can ensure the effectiveness of the implementation of the Personal Data Protection Law in Indonesia.

The author examines the relationship between personal data and personal information with security guarantees in the legal protection of personal data. The novelty of this research is expected to make a significant contribution in efforts to protect population data

B. Discussion

1. The Dynamics of Legal Protection Aspects in the Context of Population Data Management

The scope of human rights rules in the constitution of our country is one of the forms of efforts to crystallize the basic values contained in the basic norms (Grundnorms) in the content of Pancasila. The basic position of Pancasila regarding the level of rules for applying the constitution can be followed up into a juridical aspect which is impressively contained in the constitution through the applicable rules. Furthermore, in depth that the constitutional rights guaranteed by the state on Human Rights relate to the right to protect personal data which is contextually correlated with private rights.

There is a statement by Warren and Brandels in their thinking that related to privacy is a right that is used to deal with the dynamics of life that cannot be separated from demands for legal recognition through instruments and forms of supervision that are determined.

In this case, personal data becomes one of the important points in the fulfillment of personal rights, because in general it becomes something that is inherent in human identity. It is appropriate that personal data information has relevance to the conception of human rights that existentially can overcome the occurrence of arbitrary actions in accessing personal data protection by various parties.

The granting of recognition of constitutional rights through the fulfillment of individual rights to obtain data security and protection against errors in managed data (data habeas), especially in the protection of the current population data management.

In line with the statement that the basic guarantees related to the management of population data as personal data have been regulated in Law Number 23 of 2006 concerning Population Administration regarding amendments to Law Number 24 of 2013 with the material contents, namely:

“data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya”

---

21 Jimly Asshiddiqie, Konstitusi Dan Konstitusionalisme Indonesia, Ed. 3 (Jakarta: Sinar Grafika, 2004).
22 Taufiqurohman Syahuri, Tafsir Konstitusi Berbagai Aspek Hukum (Jakarta: Kencana Prenada Media Group, 2011).
28 Undang-Undang Republik Indonesia Nomor 24 Tahun 2013 Tentang Administrasi Kependudukan (Lembaran Negara Republik Indonesia Nomor 232 Tahun 2013, Tambahan Lembaran Negara Republik Indonesia Nomor 5475).
An embodiment of the government’s efforts contained in the policy through the provision of access and use of population information to integrate related to managing occupation data. The granting of such access becomes the validity of the digital data utilization program in all public service sectors to optimize the development of the digital era, later based on Permendagri No. 61 of 2015 there is an arrangement regarding the granting of permits between the Director General of Population and Civil Registration as the data owner and the user institution through an MoU agreement followed by a Cooperation Agreement. The grant of access to population data is essentially given by the Minister of Home Affairs to various organizing parties and agencies that are given access to population data in accordance with the permission given. Utilization of the existence of access to data verification through a functional technology system, one of which can minimize the misuse of personal data which has an impact on financial losses and individual dignity. As in the current modus operandi in cases of data theft used to break into accounts and other things that are fictitious without the consent of the data subject. The concretization of prevention through the provision of systemic access to population data will reduce the risk of data misuse.

Provisions regarding restrictions on access of these institutions through managed data can only be used for relevant purposes relating to verification related to whether or not the data provided by the community is related to the population database of the Department of Population and Civil Registration. Systemically, it will minimize the collection and use of user or institutional data outside the provisions of the applicable agreement in accordance with the Data Minimization principle by the General Data Protection Regulation (GDPR). In relation to the scope of the user institution to be able to gain access to and use of population data. There is a rule that both government and private institutions can have such access rights with such great opportunities. However, it needs to be accompanied by various considerations regarding the minimum aspect of guaranteeing optimal personal data protection. The vulnerability of cooperation agreements between the government and user institutions, especially to the private sector, creates the potential for misuse of data by certain individuals. Ardi Sutedja as Chair of the Indonesian Cyber Security Forum (ICSF) stated in a virtual discussion on August 10, 2020 with the theme "The Urgency of an Independent Supervisory Authority in the Protection of Personal Data, that the capability of personal data in Indonesia is still very minimal in cooperation agreements between the government and user institutions, especially to the private sector.

These efforts do not guarantee protection against misuse of personal data because current digital advances in Deep Data Mining technology will continuously become more sophisticated. To find loopholes in the personal data hacking system. Moreover, the number of institutions that use data verification access rights, totaling 3,856 ministries and institutions across sectors, is currently accompanied by many cases of data theft that require priority efforts to handle the current government.

---

30 Peraturan Kementerian Dalam Negeri Nomor 61 Tahun 2015 Tentang Persyaratan, Ruang Lingkup Dan Tata Cara Pemberian Hak Akses Serta Pemanfaatan Nomor Induk Kependudukan, Data Kependudukan Dan Kartu Tanda Penduduk Elektronik.
Table 1. Personal Data Leak Case

<table>
<thead>
<tr>
<th>Type of Institution</th>
<th>Institution</th>
<th>Number of Data Leaks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Government</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e-HAC Kementerian Kesehatan</td>
<td>1,3 Million</td>
</tr>
<tr>
<td></td>
<td>BPJS Kesehatan</td>
<td>279 Million</td>
</tr>
<tr>
<td></td>
<td>BRI Life</td>
<td>2 Million</td>
</tr>
<tr>
<td></td>
<td>Komisi Pemilihan Umum</td>
<td>2,3 Million</td>
</tr>
<tr>
<td>2</td>
<td>Private</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tokopedia</td>
<td>91 Million</td>
</tr>
<tr>
<td></td>
<td>Bhinneka.com</td>
<td>1,2 Million</td>
</tr>
<tr>
<td></td>
<td>Kreditplus</td>
<td>890 Thousand</td>
</tr>
<tr>
<td></td>
<td>RedDoorz</td>
<td>5,8 Million</td>
</tr>
<tr>
<td></td>
<td>Cermati[</td>
<td>2,9 Million</td>
</tr>
</tbody>
</table>

Source: Classification of Personal Data Leakage Cases 2020-2021

Based on the data above, the prevalence of data leakage cases in the past 2 years, both in state and private institutions, is a form of government's failure to anticipate. Regarding the type of user data stolen, it is very sensitive, such as names, home addresses, and work data, to Family Cards which are still in the personal data category. The potential for misuse of the data is evidenced by the discovery that later the hacked results will be sold on hacker forums as a means of exchange and database transactions such as RaidForums. The government's obligation to deal with data leakage is the urgency of establishing special rules regarding protection and the existence of a sketch that guarantees the right to privacy of a person regarding personal data in specifically regulating the scope and granting authority to owners and users of personal data. The need to map the risk of granting access rights based on the reference to the Population Administration Law with the necessity to continue to pay attention to aspects of personal data protection.

In the essential explanation regarding the definition and scope of personal data, there is a requirement for personal data to be treated, stored, and protected the truth of the data and to keep the confidentiality of certain individual data or in large numbers based on the Population Administration Law and Government Regulation Number 40/2019. However, there are limitations regarding the scope of the data which concretely only includes biometric data such as fingerprints, irises and furthermore on a person's physical and/or mental disabilities, signatures and other data elements that are considered a person's disgrace. Whereas personal data should also include Name, KK, NIK, Date of Birth, to the

address of an individual who needs to get protection for his confidentiality. So that later it will cause new problems, considering that the data is still used as a criterion for accessing population data by other institutions. Explicit rules are only contained in the 1945 Constitution regarding the existence of sectoral rights to privacy in the Administrative Law, ITE Law and other statutory provisions regarding population data security.

In addition, regarding granting access to ministries or institutions as a public service sector, there are no rules that explain significantly the various regulations. The existence of such ambiguity cannot provide certainty of protection for parties who gain access not to take actions outside the provisions of the cooperation agreement such as processing and collecting population data. So it can be concluded that comprehensively there is a need for regulations governing the provision of information on failures and data processing actions outside the provisions, unilateral data deletion in guaranteeing the constitutional rights of individuals as data subjects in the formation of personal data management according to valid principles and criteria, as well as specific arrangements regarding the rights and obligations of controllers and data owners in their fulfillment in the form of accurate data verification.

Currently there is a Zero Data Sharing Policy implementation by the Ministry of Home Affairs through the obligation for users to comply with the policy through a prohibition on data sharing and its use by third parties sourced from Dukcapil population data. There are restrictions on access rights to population data by the data users, namely they are only allowed to access the data for the purpose of verifying the suitability of the data. In this case, it was motivated by the leakage of population data by the General Elections Commission which allegedly came from a third party. Whereas population data is static and it is feared that changes will occur in the database. The government's efforts are not accompanied by optimal legal instruments for the rights or authorities of data owners (rights of data subject). So there is ambiguity regarding the position and legitimate interest of the Ministry of Home Affairs in determining who can use access. Moreover, until now there is no rule regarding the rights of the data owner to be able to refuse (Right to object) the granting of third party access rights to the personal data data.

The urgency regarding the formulation until the ratification of the Personal Data Protection Bill is essentially a fulfillment of Human Rights in an effort to legal instruments to prevent and overcome cases of personal data theft. The government should first apply the Personal Data Protection Law rather than the rules regarding cooperation in managing population data which are only contained in the Cooperation Agreement which causes the inability to find violations of the restrictions on the cooperation pattern. So that there are clear and comprehensive guidelines to protect and minimize the potential for misuse of Indonesian population data. In addition, the ratification of the Personal Data Protection Bill is necessary to provide certainty of protection for third parties who are only allowed to access the data for the purpose of verifying the suitability of the data. In this case, it was motivated by the leakage of population data by the General Elections Commission which allegedly came from a third party. Whereas population data is static and it is feared that changes will occur in the database. The government's efforts are not accompanied by optimal legal instruments for the rights or authorities of data owners (rights of data subject). So there is ambiguity regarding the position and legitimate interest of the Ministry of Home Affairs in determining who can use access. Moreover, until now there is no rule regarding the rights of the data owner to be able to refuse (Right to object) the granting of third party access rights to the personal data data.

The urgency regarding the formulation until the ratification of the Personal Data Protection Bill is essentially a fulfillment of Human Rights in an effort to legal instruments to prevent and overcome cases of personal data theft. The government should first apply the Personal Data Protection Law rather than the rules regarding cooperation in managing population data which are only contained in the Cooperation Agreement which causes the inability to find violations of the restrictions on the cooperation pattern. So that there are clear and comprehensive guidelines to protect and minimize the potential for misuse of Indonesian population data. In addition, the ratification of the Personal Data Protection Bill is necessary to provide certainty of protection for third parties who are only allowed to access the data for the purpose of verifying the suitability of the data. In this case, it was motivated by the leakage of population data by the General Elections Commission which allegedly came from a third party. Whereas population data is static and it is feared that changes will occur in the database. The government's efforts are not accompanied by optimal legal instruments for the rights or authorities of data owners (rights of data subject). So there is ambiguity regarding the position and legitimate interest of the Ministry of Home Affairs in determining who can use access. Moreover, until now there is no rule regarding the rights of the data owner to be able to refuse (Right to object) the granting of third party access rights to the personal data data.

The urgency regarding the formulation until the ratification of the Personal Data Protection Bill is essentially a fulfillment of Human Rights in an effort to legal instruments to prevent and overcome cases of personal data theft. The government should first apply the Personal Data Protection Law rather than the rules regarding cooperation in managing population data which are only contained in the Cooperation Agreement which causes the inability to find violations of the restrictions on the cooperation pattern. So that there are clear and comprehensive guidelines to protect and minimize the potential for misuse of Indonesian population data. In addition, the ratification of the Personal Data Protection Bill is necessary to provide certainty of protection for third parties who are only allowed to access the data for the purpose of verifying the suitability of the data. In this case, it was motivated by the leakage of population data by the General Elections Commission which allegedly came from a third party. Whereas population data is static and it is feared that changes will occur in the database. The government's efforts are not accompanied by optimal legal instruments for the rights or authorities of data owners (rights of data subject). So there is ambiguity regarding the position and legitimate interest of the Ministry of Home Affairs in determining who can use access. Moreover, until now there is no rule regarding the rights of the data owner to be able to refuse (Right to object) the granting of third party access rights to the personal data data.

51 Rodes Ober Adi Guna Pardosasi and Yuliana Primawardani, “Perlindungan Hak Pengguna Layanan Pinjaman Online Dalam Perspektif Hak Asasi Manusia (Protection of the Rights of Online Loan Customers from a Human Rights Perspective),” n.d.
Protection Law needs to be accompanied by a Personal Data Protection supervisory agency through an independent authority as a fulfillment of guarantees in implementing the Personal Data Protection Law.\textsuperscript{53} The increase in cases of data leakage and misuse does not only require a juridical element in the formulation of laws and regulations as legal certainty, but also needs to prioritize aspects of supervision of personal data.\textsuperscript{54} Specific surveillance authority that can provide effectiveness and efficiency in implementing the Zero Data Sharing Policy through comprehensive monitoring of the operation of population data access management.\textsuperscript{55}

2. The Role of Independent Surveillance Authority In The Protection of Population Data

The establishment of the PDP Independent Monitoring authority refers to international juridical rules such as the UN Guidelines for the Regulation of Computerized Personal Data Files 1990 which are based on the general guarantee principle, through the interpretation of the establishment of an independent surveillance body.\textsuperscript{56} The statement contained in the rules of the European convention regarding the processing of personal data explains that there is responsibility in the establishment of a supervisory agency in law enforcement. Efforts to ensure the protection of personal data are a must contained in the rules of the European Union General Data Protection Regulation (EU GDPR).\textsuperscript{57} Intrinsically that personal data has a relationship between a person's personal life with human rights. The establishment of a surveillance authority will provide innovative anticipatory procedures by the government as a fulfillment of constitutional rights guarantees.\textsuperscript{58}

The international standardization reference substantially influences the formulation of the PDP Bill which is a factor in the formation of an independent surveillance authority in the provision of functions, duties, and positions related to the data protection authority that has authority over the government.\textsuperscript{59} Although some time ago there were obstacles regarding an order to the Jokowi government that stated a prohibition on the creation of new institutions with efficiency factors, but in the context of the affordability of the PDP Law, it must include supervision of state and private public bodies. The existence of the establishment of an independent surveillance authority is crucial in increasing cases of data leakage and misuse, which is accompanied by a large number of personal data whose access is

\begin{itemize}
  \item U N OHCHR, “Guidelines for the Regulation of Computerized Personal Data Files,” Adapted by General Assembly Resolution 45 (1990): 95.
  \item I T Governance Privacy Team, Eu General Data Protection Regulation (GDPR)–An Implementation And Compliance Guide (IT Governance Ltd, 2020).
  \item Antonio Cassese, Hak Asasi Manusia Di Dunia Yang Berubah (Yayasan Obor Indonesia, 1994).
\end{itemize}
granted to various institutions/agencies. In addition, the need for adequacy or equality between personal data protection laws and other countries is the government’s task in implementing the principle of extraterritorial jurisdiction in statutory provisions. The independence of the surveillance authority is assessed in accordance with the principle that a single authority will obtain certainty of data control, or on individual rights they can claim rights with the involvement of the current independent commission to stakeholders within the government, namely the Ministry of Communication and Information and outside government elements, namely private institutions in the business and business sectors and other.

The continuity of the development of the position model can essentially be placed in non-ministerial institutions, both in the form of special agencies in the realm of executive power (Executive branch agencies), as well as in independent regulatory agencies. The decision-making model of authority through an independent position is very important in its compatibility with the protection of personal data. The harmonization of the functions of independent data protection authorities in the public sphere will ensure protection through the compliance of processors and controllers of personal data, both for individuals, public bodies, and institutions in the private sector based on the provisions of laws and regulations later. Not only implementing a privacy policy, but as an effort to provide awareness, provide consultation, and develop technology governance. It is expected that later entities in ministries/state and private institutions will be monitored in a complex manner, such as in financial and business companies and other government institutions with regard to personal data protection.

The conception of the current government’s efforts through the Zero Data Sharing Policy substantially regulates all institutions or agencies that have access to population data related to interests, including data verification not to disseminate or share with third parties. Government supervision through the Ministry of Home Affairs tends to have limitations on its authority which legally has not been regulated in various laws and regulations. Systemic supervision only looks at the suitability of access to population data and overcomes technical obstacles, without knowing the extent to which the data is accessed directly. The implementation of monitoring is only carried out through the submission of reports by various data user institutions which tend to appear reactive.

Efforts to limit access rights to the users of population data conceptually require an important component, namely an independent surveillance Agency Authority in achieving the optimization of the Zero Data Sharing Policy. The draft of the establishment relating to its powers and duties can be adjusted to the standardization of international agreements, one of which is stated in the EU GDPR. The regulation can be used as a reference for the government as a manifestation of the harmonization of supervision on its authority as a whole in accordance with Article 58 of the EU GDPR, such as its authority to investigate various dispute problems and their resolution, then the collective authority to carry out supervision and actions between actions against discretion taken between users. and the owner of the data, and as an advisory power in recommending advice on efforts to improve in managing population data.

Furthermore, the explanation of the conception of the author’s perspective in adjusting the EU GDPR can carry out investigations with third parties through their right to review certifications held by

---

user institutions as criteria for granting population data access rights, requesting any information needed from users and data owners regarding the implementation of supervision, and absolute access to the entire system in accordance with the provisions of the applicable legislation later.  

Then, in their collective authority, they can give warnings or warnings regarding the tendency to violate the provisions of the Zero Data Sharing Policy, give orders regarding the fulfillment of data subject rights as a guarantee of individual constitutional rights and carry out data management in accordance with the provisions of the legislation. Furthermore, it can provide sanctions for violations regarding data misuse through operational prohibitions and fines to the relevant institutions and withdraw the certification of population data access requirements if the applicable regulatory provisions are no longer met.  

Regarding its obligations in adjusting standard contract clauses, the context of cooperation through a memorandum of understanding (MoU) which is followed up by a Cooperation Agreement needs to be adjusted to the authority of the Independent Surveillance Agency Authority related to requirements, technology governance, and periodic monitoring in providing assurance of personal data protection.

C. Conclusion

The impact of digital transformation currently requires the protection of personal data, considering that currently there are an increasing number of cases of data leakage, both in state public institutions and in the private sector. The current weakness of the government’s technology system has become the potential for various data misuse practices for the interests of certain parties. The current concretization of the government’s efforts focuses on providing access to population data with the aim of minimizing irregularities that result in losses to one’s dignity and financially. In addition, there is an obligation to implement the Zero Data Sharing Policy, which is expected to ensure optimal data protection through inter-institutional prohibitions to share population data with third parties. However, there are limitations to the protection of personal data due to government authority and inadequate technology to determine the scope of population data used by data users.

The tendency that leads to ambiguity in the boundaries of data protection, so that the authorities and duties of the government require the codification of laws regarding the protection of personal data in providing clarity and effectiveness of protection. In addition, the urgency of the ratification of the Personal Data Protection Bill needs to be accompanied by considerations of establishing an Independent Monitoring Authority in accordance with European Union General Data Protection Regulation (EU GDPR) standards. Its independent position will prevent intervention from various parties that affect the implementation of supervision. Functionally it is considered appropriate to the implementation of the Zero Data Sharing Policy through the conception of investigative authority and collective rights as a guarantee of citizens’ constitutional rights in fulfilling human rights.

Acknowledgements

The authors would like to thank all those who have helped in the process of completing this article. Hopefully it can provide benefits for readers in terms of the urgency of the Personal Data Protection Bill and its form of supervision, as well as for other authors to be used as research references on the conception of the role of Independent Surveillance Authority in the Efforts to Protect Population Data in Indonesia.


Bibliography


Pardosi, Rodes Ober Adi Guna, and Yuliana Primawardani. “Perlindungan Hak Pengguna Layanan Pinjaman Online Dalam Perspektif Hak Asasi Manusia (Protection of the Rights of Online Loan Customers from a Human Rights Perspective),” n.d.


