Notaire
Vol. 01 No. 2, Oktober 2018
e-ISSN: 2655-9404
DOI: 10.20473/ntr.v1i2.9434
Article history: Submitted 3 October 2018; Accepted 10 October 2018; Available online 15 October 2018.

# Personal Data Protection Law Used in Mobile Phone Sim Card Registration in Indonesia

**Mahendri Putri Sholichah dan Dewi Rumaisa**
mahendriputris031311133023@gmail.com
Universitas Airlangga

## Abstract
The growths of technology make the privacy of personal information become an important issue in most countries, including Indonesia. Utilization of personal data is common things in most of our activity within the cyberspace and in this case, even the advancement of technology cannot neglect the privacy of personal information. The abusing of the data record, especially the data that belongs to the personal data category, the information that exists within this data could go to the public when it is leaked. One of the cases related to the personal data abuse is registration of thirty mobile phone SIM cards using one person's personal information without the consent of personal information owner. This paper explains about personal data cases related to the mobile phone SIM card registration, and from this case, some issues about the abusing of personal data will be taken as an example to give consideration for legislating personal data protection. Moreover, this paper also explores the purpose of personal data collection, sensitive data collection, limitation of data collection, storage of collected personal data, transfer of collected personal data, and deletion of collected personal data. This paper convinces the urgency drafting of personal data protection law for country likes Indonesia. Therefore it is hoped that this paper will become one of many considerations for the Indonesian government to include personal data protection law into their national legislation program and legislate the personal data protection law in recent times.
**Keywords:** Personal Data; Personal Information; Privacy; Human Rights.

## *Abstrak*
*Perkembangan teknologi membuat informasi privasi data pribadi menjadi isu penting di sebagian besar negara, termasuk Indonesia. Pemanfaatan data pribadi adalah hal yang umum dalam sebagian besar aktivitas kita di dunia maya dan dalam hal ini, kemajuan teknologi tidak dapat mengabaikan informasi privasi data pribadi. Penyalahgunaan catatan data, terutama data yang termasuk dalam kategori data pribadi, ketika bocor, maka informasi yang ada dalam data ini dapat masuk ke publik. Salah satu kasus yang terkait dengan penyalahgunaan data pribadi adalah pendaftaran tiga puluh kartu SIM ponsel menggunakan informasi pribadi satu orang tanpa persetujuan pemilik informasi pribadi. Selain itu, makalah ini juga mengeksplorasi masalah-masalah mendesak dalam perlindungan data pribadi, seperti tujuan pengumpulan data, pengumpulan data pribadi, pengumpulan data sensitif, pembatasan pengumpulan data, penyimpanan data pribadi yang dikumpulkan, transfer data pribadi yang dikumpulkan, dan penghapusan mengumpulkan data pribadi. Makalah ini berupaya untuk meyakinkan urgensi penyusunan undang-undang perlindungan data pribadi untuk negara seperti Indonesia. Oleh karena itu diharapkan bahwa makalah ini akan menjadi salah satu dari banyak pertimbangan bagi pemerintah Indonesia untuk memasukkan undang-undang perlindungan data pribadi ke dalam program legislasi nasional mereka dan membuat undang-undang perlindungan data pribadi dalam waktu dekat.*
***Kata Kunci:*** *Data Pribadi; Informasi Pribadi; Privasi; Hak Asasi Manusia.*

## Introduction

Information technology advances as one of the effects of globalization is something that can have a positive impact on a country. One of the most prominent due to the advancement of information technology is the change of how the way humans' live, including their interaction and even transactions those are no longer in the conventional way, that is the presence of new media, namely the internet. The term "new" brings understanding that on the other hand, there are old media. Croteau and Hoynes stated, "The differences between 'new' and 'old' forms of media are substantial in themselves.[1] This thing means that the difference between these two media lies in the medium used. Al this time, conventional media is identical to its massive character or one to many.[2] Information technology development activities have resulted in various sectors of life utilizing information technology systems, such as the implementation of electronic commerce (e-commerce) in the trade/business sector, electronic education (e-education) in the field of education, electronic health (e-health) in the health sector , electronic government (e-government) in the fields of government, search engines, social networks, smartphones and mobile internet and the development of cloud computing industries.[3] However, information technology can also be a double-edged sword, because in addition to contributing to the improvement of human welfare, progress, and civilization, as well as being an effective means of the act against the law.[4]

Based on data quoted from Wearesocial.com in January 2018, internet users in Indonesia reached around 132.7 million internet users out of a total population of 265.4 million inhabitants; it means that around 50% of Indonesia's total populations

---

[1] David Croteau and William Hoynes, *Media/Society: Industries, Images, and Audiences, Thousand Oaks* (Pine Forge Press 2003). [321].

[2] Hermin Indah Wahyuni, *Kebijakan Media Baru Di Indonesia: (Harapan Dinamika Dan Capaian Kebijakan Media Baru di Indonesia)* (UGM PRESS 2013).[97].

[3] Academic Text on Personal Data Protection Law, National Law Development Agency (BPHN).[1].

[4] Ahmad M. Ramli, *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia* (Rafika Aditama 2004).[1].

are active internet users.[5] As internet users increase the issue of the importance of protecting personal data is also getting stronger. Especially after the emergence of various cases that have a connection with the leakage of one's personal data and lead to cybercrime action so that the discourse of the discourse of the importance of making legal rules to protect personal data is getting stronger.

The policy regarding the protection of personal data is based on concerns that there is a violation of the privacy of personal information caused by present information technology which is very fast. Protection of personal data is closely related to the concept of privacy.[6] The concept of privacy is an idea to maintain personal integrity and dignity.[7] Privacy is clearly stated as human rights law, but personal data is about individual data. Personal is human rights law and the protection of personal data is one way to respect these human rights.[8] Therefore the collection and dissemination of personal data is a violation of individual privacy rights. According to the United Nations Commission on Human Rights, the reason for privacy is classified as a basic human right that is protected because humans as individuals need to develop their personality by providing space for themselves. Meanwhile, personal data is an asset or commodity of high economic value,[9] therefore personal data must be protected so that the privacy rights of individuals are guaranteed. Privacy rights include the right to determine whether providing or not providing the personal data, as well as allowing their use by others as long as they are in accordance with the specified conditions.[10]

Universal Declaration of Human Rights 1948 (UDHR) is one of the important international instruments because it has been agreed upon by almost all countries.

---

[5] Simon Kemp, *Digital In 2018: World's Internet Users Pass The 4 Billion Mark* https://wearesocial.com/blog/2018/01/global-digital-report-2018, accesed on 23-07-2018.

[6] Article 28 (f) and Article 28 (g) Constitution of the Republic of Indonesia 1945 and Electronic Privacy Invormation Center (EPIC) and Privacy International (PI): "Privacy & Human Rights 2006", Overview of Privacy, https://www.privacyinternational.org/

[7] Wahyudi Djafar and Asep Komarudin, *Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci* (Elsam 2014).[2].

[8] Rizka Nurdinisari, *Perlindungan Hukum terhadap Privasi dan Data Pribadi Pengguna Telekomunikasi dalam Penyelenggaraan Telekomunikasi Khususnya dalam Menerima Informasi Promosi yang Merugikan (Spamming)* (Fakultas Hukum, Program Pasca Sarjana, Universitas Indonesia 2013).[53].

[9] Edmon Makarim, *Kompilasi Hukum Telematika* (PT. Raja Grafindo Perkasa 2003).[ 3].

[10] Human Rights Committee General Comment No. 16/1988.

The substance in the UDHR regulates comprehensively about basic human rights or also called the common standard of achievement for all peoples and all nations, privacy is one of the basic rights protected in the UDHR. Based on Article 12 of the 1948 Universal Declaration of Human Rights/UDHR, it is affirmed, "No one shall be subject to arbitrary interference with his privacy family, home or correspondence, nor attacks upon his honor and reputation. Everyone has the right to the protection of the law such as interference or attacks. " This means that all people must be protected by law because they have the right that their privacy, family, place of residence and correspondence or even their honor and reputation not to be disturbed. Substantially the privacy regulation in article 12 UDHR is very broad because it consists of:

1. Physical Privacy, that is the privacy protection related to his place of residence, for example, someone is not allowed to enter someone else's house without the owner's permission, the State may not search someone's home without a warrant of detention, the state may not conduct wiretapping of someone's residence.
2. Decisive Privacy, that is the protection of privacy against the right to determine his own life including the life of his family, for example, he has the right to determine his own household life and how to educate his children.
3. Dignity, which means protecting one's self-esteem including one's honor and reputation.
4. Informational Privacy that is the privacy of information. Means the right to determine the way a person conducts and stores his personal information.

Other arrangements regarding privacy are found in the International Covenant on Civil and Political Rights 1966 (ICCPR). Specifically in Article 17 because the Article has a comprehensive set of various types of privacy violations so that according to Byegrave, this arrangement is the strongest legal basis in international law and the State must protect the privacy of personal information through law. Article 17 of the ICCPR affirms, "No one shall be subject to arbitrary interference with his privacy, family, home or correspondence, not to an unlawful attack upon his honor and reputation." In subsection (2), "Everyone has the right to the protection of the law against such interference or attacks."

Other international instruments governing the protection of privacy for personal information are OECD Guidelines Governing the Protection of Privacy and

Trans boundary Flows of Personal Data 1980. These instruments contain guidelines provided as recommendations for countries to make arrangements for accessing, managing, and disseminating personal data. There are 8 principles as contained in the second chapter of the Guidelines which constitute minimum standards, meaning that the state is given the freedom to add other arrangements if it is still lacking. These principles are as follows:

1. Personal data must be obtained honestly, legally, and must consent of the owner of the data (The collection limitation principle)
2. Personal data obtained must be in accordance with the main purpose and the data must be accurate and up-to-date (The data quality principle)\
3. Personal data must be processed in accordance with the purpose and the data collection process and must be notified to the owner at the time the data is obtained (The purpose specification principle)
4. The data should not be given to third parties without the consent of the owner of the data unless specified by law (The use limitation principle)
5. The security safeguard principle measures appropriate safeguards should be taken to deal with the processes of acquisition of data that can lead to lost, damaged, and the unauthorized use of personal data.
6. The openness principle, data owners must know the purpose of using their personal data.
7. The individual participation principle, the data owner has the right to correct the incorrect data.
8. The accountability principle, the parties must carry out the principles above.

Indonesia's Constitution does not explicitly mention privacy. However, Article 28 (g) protects the right to dignity and "to feel secure", the concepts that are often related to the right to privacy in national constitutions, "(1) Every person shall have the right to protection of him/herself, family, honor, dignity, and property, and shall have the right to feel secure against and receive protection from the threat of fear to do or not do something that is a human right." And article 28 (f) guarantees the right to communication, though it does not mention privacy, "Every person shall have the right to communicate and to obtain information for the purpose of the development of his/her self and social environment, and shall have the right to seek, obtain, possess, store, process and convey information by employing all available types of channels." Even Indonesia has ratified a number of international human rights treaties with privacy implications. These include the UDHR, the ICCPR 1996, the

International Convention on the Elimination of All Forms of Racial Discrimination and the ASEAN Human Rights Declaration. However, the protection of personal data is not currently regulated in separate legislation but they are scattered in various laws and regulations. Furthermore, according to Institute for Policy Research and Advocacy (ELSAM), there are at least 30 Laws that are associated with personal data protection, even though these Laws overlap one another.[11]

Personal data according to the Personal Data Protection Law is any data about a person's life whether identified and/or can be identified separately or combined with other information either directly or indirectly through electronic and/or non-electronic systems. According to Article 1 number 22 of the Population Administration Law, "Personal Data are certain personal data that is stored, maintained, and kept truthfully and protected by confidentiality." Personal data of the population that must be protected according to Article 84 of the Population Administration Law Number 24 of 2013: a. KK number (Family Card); b. NIK (National Identity Number); c. date/month/year of birth; d. information about physical and/or mental disability; e. NIK biological mother; f. NIK father; and g. some contents of Important Event notes.

Resident Personal Data must be protected by the state and become information that is exempted in Article 17 (h) of Law Number 14 of 2008 concerning Public Information Openness (KIP). Based on that Article, the identity contained in the KTP and KK becomes exempt information to be opened to anyone.

According to the ECHR a data is personal data if it relates to someone or the data can define someone as the subject of the data.[12] Whereas according to Black's Law Dictionary personal or private means: "Relating or belonging to an individual, as opposed to the public or the government" and "confidential"; secret".[13] In

[11] Sanjaya, D, *Kebutuhan Akan UU Perlindungan Data Pribadi Kian Mendesak* (*ELSAM* 2017). http://elsam.or.id/2017/05/kebutuhan-akan-uu-perlindungan-data-pribadi-kian-mendesak/ , accessed on 24-07-2018.

[12] European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law* (Publication Office of the European Union 2014).[36].

[13] Bryan A. Garner, *Black's Law Dictionary* (West Publishing Co., 2009). [1343].

national law, the legislation does not explicitly specify the definition of personal data in the existing articles, but the understanding of personal data can be found in Government Regulation No. 82 of 2012. Article 1 The Government Regulation defines personal data as certain personal data that is stored, maintained and kept by the truth and protected by confidentiality.

**The Benefits of Personal Data Protection Law**

With the existence of comprehensive rules regarding personal data protection law, it is expected to prevent and provide protection from the negative impacts of current technological developments that are closely related to personal data. Personal data is a commodity of high economic value so it must be protected in order to avoid misuse that can occur such as abuse of data and leaked to public without any consent from the personal data owner. If viewed from other countries' examples that are more comprehensive in regulating the protection of their personal data as one of them is the Hong Kong with the Personal Data of the Hong Kong Privacy Ordinance of 1995 (PDPO 1995). The norms contained in the PDPO Ordinance clearly show that the PDPO Ordinance is guided by the European Commission Directive and the OECD Guidelines. No wonder, because the PDPO ordinance is basically a means for Hong Kong to adjust to international practices.[14] Major changes were made to the PDPO in 2012, namely the Hong Kong Government imposed an amendment to PDPO 1995. After 18 years of implementation by authorities in Hong Kong dealing with privacy issues, namely the PCPD (Privacy Commissioner for Personal Data) the principles of privacy protection contained in the PDPO cannot be fully held.[15]

The amendment process was felt by the society to be accelerated so that the PDPO applied in 2013. It was not separated from the consequences of scandals involving the Hong Kong government as well as proving that the PDPO was not effective in preventing the scandal. The scandal originated from the Octopus Group

[14] Graham Greenleaf, *Asian Data Privacy Laws – Trade Human Rights Prespectives* (Oxford University Press 2014).[86-87].

[15] *Ibid.*,[80].

of Companies, which is the operator of the Hong Kong Transit card operator taking economic benefits by utilizing the details of its customers, even though the Hong Kong Government at that time was the majority shareholder in the Octopus Group of Companies. This scandal while providing lessons on human rights for the Hong Kong community triggered political tensions and encouraged the government to accelerate the ratification of the PDPO amendment.[16] The type of data regulated in the PDPO includes personal data, data, and documents. Personal data or privacy data based on the understanding described by PDPO must relate to individuals who are still alive, directly or indirectly.[17] Privacy data of legal entities and individuals who have died are not regulated by PDPO. Data is defined in Section 2 of the Hong Kong PDPO, that is: "Any representation of information, including expression of opinion, in any document"

Thus, the data is every representation of information, including the disclosure of one's opinion in each document. Privacy data can be used to identify someone either directly or indirectly. Privacy data must also be in a form that allows for further access and processing. Information can be referred to as data if the information has been stored in a document, not just in the form of a memory in one's head.

Privacy data protection in other countries, besides Hong Kong, that is South Korea which has a Personal Information Protection Act (PIPA) 2011. The law has comprehensive coverage, has the principles of innovative privacy protection, and allows enforcement methods strong privacy protection.[18] PIPA regulates privacy data protection in the public sector and the private sector. PIPA uses the definition of personal information, as stated in Article 2 PIPA states that: "Personal information shall mean the information pertaining to any living person that makes it possible to identify such individual by his/her name and resident registration number, image, etc…"

PIPA is influenced by the Data Protection Directive EU so as to provide the understanding of "processing" as referred to in Article 2 of the PIPA namely all types

[16] *Ibid.*,[86-87].
[17] *Ibid.*,[89].
[18] *Ibid.*, [124].

of actions that can be carried out relating to private data. The "personal information processor" is any person or organization that processes or processes privacy data directly or indirectly to use private data files for official or business use.[19] Various categories of privacy data are excluded from the principles of privacy data protection (contained in Chapters 3-7 of the PIPA), namely: privacy data collected under the Statistics Act, for national security analysis, to be processed temporarily when there is an urgent need in terms of community safety and welfare, public health, used for reporting press news, missionary activities of religious organizations or used for nominating candidates from political parties (Article 58 (1) PIPA). If these exceptions are applied, the privacy data processor must process privacy data as little as possible to achieve the purpose of processing privacy data.

South Korea's legislation contains provisions to minimize the collection of privacy and collection data is limited by the rules regarding the use of notifications, in terms of sensitive information and identification card numbers and in limiting visual surveillance/wiretapping. Requirements regarding the specific purpose of processing privacy data, approval and notification are regulated in Article 3 and 4 of the PIPA. Personal information processor or privacy data processor must explain explicitly and specifically what the purpose is for the processing of privacy data (Article 3). Data subjects have the right to be notified of the purpose and the choice to approve the processing of privacy data (Article 4). Article 15 PIPA requires the approval of data subjects before making such privacy or processing data must be carried out on the basis of exceptions, for example, the implementation of obligations under the law, contractual agreements, data subject interests and so on.

The PIPA permit only minimal privacy data collection is limited to the achievement of the purpose of collection of data privacy (Article 16 (1) PIPA). PIPA regulates unusual things in the regulation of privacy data protection in various countries, namely restrictions on visual supervision. There are strict limits on the use of visual data processing equipment, such as Closed-circuit television (CCTV)

[19] *Ibid.*, [138].

both in open and closed places. Visual data processing equipment is limited to devices that are installed continuously in certain places to retrieve and store or send pictures of objects or people (Article 2 PIPA). Thus human photographers and road speed measuring devices are not subject to this arrangement.

Approval to disclose privacy data from data processors to third parties is loaded with the implementation of privacy data activities. Data subjects are entitled to get detailed information about third parties who receive privacy data.[20] Sensitive data processing and population identification numbers also require approval, just like other privacy data processing. This type of sensitive privacy data in South Korea as stipulated in Article 63 of the PIPA is privacy data regarding ideology, trust, entering or leaving membership of trade unions or political parties, political mindset, health and sexual life.

**Mandatory SIM Card Registration**

SIM cards registration has been mandated in 147 countries in 2018 where proof-of-identity is required to register a prepaid mobile SIM card in one's own name.[21] But half of the countries mandating prepaid SIM registration have no or inadequate privacy/data protection frameworks in place with consumers potentially having limited, if any, rights to seek legal redress against possible violations of their privacy or personal data.[22] Indonesia has obliged the reregistration of SIM Cards in 2016, with the existence of Minister of Communication and Information Technology Regulation No. 12 of 2016 juncto Minister of Communication and Information Technology Regulation No. 14 of 2017 regarding Telecommunication Services Customer Registration, issued a mandatory SIM Card registration for all Indonesian. The regulation essentially requires mobile phone users to register new numbers or re-register for the old users of their numbers by entering their

[20] *Ibid.*, [142].

[21] https://www.gsma.com/mobilefordevelopment/tag/mandatory-sim-registration/ , accessed on 24-07-2018.

[22] https://www.gsma.com/mobilefordevelopment/tag/mandatory-sim-registration/ , accessed on 24-07-2018

resident card number and family card number. Taufik Hasan as practitioners of IT regulation in Indonesia as well as the committee members of the Indonesian Telecommunication Regulatory Authority said, SIM Card's re-registration policy is only a small part of Indonesia's efforts towards digital civilization.[23]

The obligation to register NIK and KK can be assumed to violate someone's privacy if he does not want to. Therefore, the collection of personal data must apply several principles, including the principle of the collection that is reasonable and in accordance with the law. In national law, this principle is stated in Article 26 (1) and Article 27-37 of Law No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE). Naturally here means that the data is collected by authorized parties to collect data and personal data collected in accordance with the purpose of collecting personal data.[24]

In the process of implementing the registration obligation several problems arise. The earliest problem arising during the registration process is the request of some operators to name the biological mother.[25] The request can be justified under Article 6 (2) of the Minister of Communication and Information Regulation No. 12 of 2016 which allows the use of biological mother's name as an alternative to NIK. This can be a problem because personal data such as birth date and biological mother's name are truly sensitive data and are even related to banking data security, and can serve as a way to get someone's banking account.[26] *Kominfo* is quick to respond and immediately removes these points by deleting the 2016 Minister of Communication and Informatics Regulation with the Minister of Communication and Information Technology Regulation No. 14 of 2017 regarding Telecommunication Services Customer Registration.

---

[23] [*Press Release*] *Responding to the Sim Card Re-Registration Policy, Kominfo Holds a Public Discussion* (Fisipol Ugm 2017) http://cfds.fisipol.ugm.ac.id/article/185/press-release-responding-to-the-sim-card-re-registration-policy-kominfo-holds-a-public-discussion-at-fisipol-ugm , accessed on 20-07-2018.

[24] Abu Bakar Munir, Siti Hajar Mohd. Yasin, *Privacy & Data Protection (*Sweet & Maxwell Asia 2002). [189-191].

[25] https://www.cnnindonesia.com/teknologi/20171019081018-213-249391/kominfo-tak-perlu-nama-ibu-untuk-registrasi-kartu-prabayar accessed on 20-07-2018.

[26] Eko Arryawan, *SmitDev Community Password is Nothing*, (PT Elex Media Komputindo 2010). [213]

Another example is the registration process that fails because of the incompatibility of NIK and KK. Even a number of sites were born that provided free ID cards and family cards on the internet. Some websites that are reported to provide NIK and KK for free include ktp.bonanza.co.id, ktp.usa.to, ktp.oneindonesia.co.id, ktp.bnpt.go.id, ktp.geologi.id, and ktp.kopi.co.id. But at this time these sites were inaccessible, even some of those who had tried to state that the NIK and KK provided by these sites made them successful in registering.[27] The existence of these sites is suspected to be the main cause of the failure of registration of the actual data owner.

Data collection without any comprehensive regulation can be certain parties to abuse the data record. Abuse of data records, especially data that belongs to the personal data category, when it is leaked, the data could go to the public. Examples of complaints are submitted by Aninda Indrastiwi. On March 5, 2018, she stated in her social media account, Twitter @anindrastiwi, *"How come my NIK can be used by more than 50 numbers when I check registration on the Indosat @kemkominfo web, please help me with the solution. Fear of being used by bad people."*[28] This rumor was clarified by Plt. The Head of the Public Relations Bureau, Noor Iza, assures that there was no data leakage, but only abuse or unauthorized use of NIK and FC Numbers by some irresponsible individuals.[29] As of now, the reports concerning the misuse of NIK and KK are currently being investigated by the Ministry and the police. The Ministry of Communication and Informatics stated that it had anticipated from the start by giving the "NIK Check Feature" so that the public would know what numbers were registered for their NIK.[30] In order to the NIK and KK community is used without the right to contact the operator's outlet.

---

[27] Eka Santhika, *Kominfo Sebut Situs Berikan NIK dan KK Gratis "Pelanggaran"*, https://www.cnnindonesia.com/teknologi/20180301173056-213-279773/kominfo-sebut-situs-berikan-nik-dan-kk-gratis-pelanggaran, accessed on 20-07-2018.

[28] https://www.liputan6.com/tekno/read/3347093/beredar-situs-web-diduga-penyedia-kk-dan-nik-gratis, accessed on 20-07-2018.

[29] https://www.kominfo.go.id/content/detail/12713/siaran-pers-no-66hmkominfo032018-tentang-kemungkinan-yang-terjadi-saat-ini-penyalahgunaan-nik-dan-kk-yang-digunakan-registrasi-secara-tanpa-hak-dan-bukan-kebocoran-data/0/siaran_pers, accessed on 19-07-2018.

[30] https://www.kominfo.go.id/content/detail/12713/siaran-pers-no-66hmkominfo032018-tentang-kemungkinan-yang-terjadi-saat-ini-penyalahgunaan-nik-dan-kk-yang-digunakan-registrasi-secara-tanpa-hak-dan-bukan-kebocoran-data/0/siaran_pers, accessed on 19-07-2018.

Although the Ministry of Communication and Information Technology has issued *Permenkominfo* No.20 of 2016 concerning Personal Data Protection in Electronic Systems, it does not guarantee the leakage of one's data to the public. Article 6 of the *Permenkominfo* 20 of 2016 stated that, "Electronic System Operators who carry out the process referred to in Article 3 are obliged to provide an approval form in Indonesian to request approval from the Owner of the Personal Data in question". But in practice, these obligations are generally not implemented.

## Conclusion

Arrangements regarding the protection of personal data are very important in a country, especially Indonesia which still does not comprehensively regulate the protection of personal data. This is due to Personal Data being part of the Privacy that is mentioned as rights protected under international human rights rules. Thus, it is expected that with the discussion that we have described above, a conclusion can be drawn that it is one of many considerations for the Indonesian government to include personal data protection law into their national legislation programs and validate the personal data protection law in this close proximity.

## Bibliography

### Books

Abu Bakar Munir and Siti Hajar Mohd. Yasin, *Privacy & Data Protection* (Sweet & Maxwell Asia 2002).

Ahmad M. Ramli, *Cyber Law dan HAKI Dalam Sistem Hukum Indonesia* (Rafika Aditama 2004).

Bryan A. Garner, *Black's Law Dictionary* (West Publishing Co 2009).

David Croteau and William Hoynes, *Media/Society: Industries, Images, and Audiences* (Pine Forge Press 2003).

Edmon Makarim, *Kompilasi Hukum Telematika* (PT. Raja Grafindo Perkasa 2003).

Eko Arryawan, *SmitDev Community Password is Nothing* (PT Elex Media Komputindo 2010).

European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law* (Publication Office of the European Union 2014).

Graham Greenleaf, *Asian Data Privacy Laws – Trade Human Rights Prespectives* (Oxford University Press 2014).

Hermin Indah Wahyuni, *Kebijakan Media Baru Di Indonesia: (Harapan Dinamika Dan Capaian Kebijakan Media Baru di Indonesia)* (UGM PRESS 2013).

Rizka Nurdinisari, *Perlindungan Hukum terhadap Privasi dan Data Pribadi Pengguna Telekomunikasi dalam Penyelenggaraan Telekomunikasi Khususnya dalam Menerima Informasi Promosi yang Merugikan (Spamming)* (Fakultas Hukum, Program Pasca Sarjana, Universitas Indonesia 2013).

Wahyudi Djafar and Asep Komarudin, *Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci* (Elsam 2014).

**Journals**

Sanjaya, D. *Kebutuhan Akan UU Perlindungan Data Pribadi Kian Mendesak* (ELSAM 2017) http://elsam.or.id/2017/05/kebutuhan-akan-uu-perlindungan-data-pribadi-kian-mendesak/

**Websites**

*[Press Release] Responding to the Sim Card Re-Registration Policy, Kominfo Holds a Public Discussion* (Fisipol Ugm 2017) http://cfds.fisipol.ugm.ac.id/article/185/press-release-responding-to-the-sim-card-re-registration-policy-kominfo-holds-a-public-discussion-at-fisipol-ugm , accessed on 20-07-2018.

Eka Santhika, *Kominfo Sebut Situs Berikan NIK dan KK Gratis "Pelanggaran"*, https://www.cnnindonesia.com/teknologi/20180301173056-213-279773/kominfo-sebut-situs-berikan-nik-dan-kk-gratis-pelanggaran, accessed on 20-07-2018.

https://www.cnnindonesia.com/teknologi/20171019081018-213-249391/kominfo-tak-perlu-nama-ibu-untuk-registrasi-kartu-prabayar accessed on 20-07-2018.

https://www.kominfo.go.id/content/detail/12713/siaran-pers-no-66hmkominfo032018-tentang-kemungkinan-yang-terjadi-saat-ini-penyalahgunaan-nik-dan-kk-yang-digunakan-registrasi-secara-tanpa-hak-dan-bukan-kebocoran-data/0/siaran_pers, accessed on 19-07-2018.

https://www.kominfo.go.id/content/detail/12713/siaran-pers-no-66hmkominfo032018-tentang-kemungkinan-yang-terjadi-saat-ini-

penyalahgunaan-nik-dan-kk-yang-digunakan-registrasi-secara-tanpa-hak-dan-bukan-kebocoran-data/0/siaran_pers, accessed on 19-07-2018.

https://www.liputan6.com/tekno/read/3347093/beredar-situs-web-diduga-penyedia-kk-dan-nik-gratis, accessed on 20-07-2018.

Simon Kemp, *Digital In 2018: World's Internet Users Pass The 4 Billion Mark*, https://wearesocial.com/blog/2018/01/global-digital-report-2018, accessed on 23-07-2918.

**Regulations**

Academic Text on Personal Data Protection Law, National Law Development Agency (BPHN).

Human Rights Committee General Comment No. 16 (1988).

Article 28 (f) and Article 28 (g) Constitution of the Republic of Indonesia 1945 and Electronic Privacy Invormation Center (EPIC) and Privacy International (PI): "Privacy & Human Rights 2006".

**HOW TO CITE**: Mahendri Putri Sholichah dan Dewi Rumaisa, 'Personal Data Protection Law Used In Mobile Phone Sim Card Registration In Indonesia' (2018) Vol. 1 No. 2 Notaire.

**--Halaman ini sengaja dibiarkan kosong--**