The Mandatory Designation of a Data Protection Officer in Indonesia's Upcoming Personal Data Protection Law*

Muhammad Iqsan Sirie**

DOI: https://doi.org/10.22304/pjih.v5n1.a2

Submitted: September 30, 2017 | Accepted: April 23, 2018

Abstract

It was only until recently that the Indonesian government deemed privacy and personal data as a pressing and urgent topic that requires an adequate legal and regulatory protection. In this respect, the government drafted a singular comprehensive personal data protection law (PDPL), which draft is currently pending passage in the parliament. Based on a 2016 version of the PDPL draft, organizations that process personal data are expected to comply with a myriad of obligations. However, the PDPL (per the 2016 version) does not appear to have anything to offer in terms of guaranteeing that organizations will actually implement the rules as laid down in the PDPL in practice. In the absence of any practical solution that could facilitate organizations' data protection compliance, the PDPL is bound to fail to achieve the prescribed objective, which is to better protect individuals' privacy rights, especially with regard to their personal data. Looking particularly at the practice that has already been developed within the European Union (EU) landscape, most of the member states adopt a self-monitoring mechanism to ensure compliance in the data protection sphere – and that self-monitoring mechanism takes form in a data protection officer (DPO). Under the General Data Protection Regulation (GDPR), EU's data protection law, organizations with certain characteristics are mandated to appoint a DPO (DPO Obligation). As the DPO Obligation is perceived as an effective practical data protection compliance tool amongst EU countries, this article discusses and ultimately suggests for the adoption of the same into the PDPL in order to boost compliance and accomplish its objectives.

Keywords: data protection officer, general data protection regulation, personal data protection law.

Menerapkan Kewajiban Penunjukkan Seorang Data Protection Officer di dalam Undang-Undang Perlindungan Data Pribadi

Abstrak

Pemerintah Indonesia belum lama ini baru menyadari bahwa persoalan terkait privasi dan perlindungan data pribadi merupakan permasalahan yang mendesak dan penting untuk segera ditanggulangi melalui payung hukum yang memadai. Berkenaan dengan ini, pemerintah telah menyusun sebuah undang-undang perlindungan data pribadi (UUPDP) yang bersifat komprehensif, yang saat ini berada dan sedang dibahas di Dewan Perwakilan

* This article is based on the author's LL.M thesis, which was submitted in fulfillment of the requirements of Universiteit Leiden's Master of Laws in Advanced Studies in Law and Digital Technologies. The author wishes to thank Prof. dr. mr. Gerrit-Jan Zwenne for supervising his LL.M thesis on which this article is based.

** Data protection trainee at Grünenthal B.V. (the Netherlands) and senior associate at Assegaf Hamzah & Partners, Capital Place, Level 36 and 37, Jalan Jenderal Gatot Subroto Kav. 18, Jakarta 12710, Indonesia, iqsanmsirie@gmail.com, S.H (Universitas Padjadjaran), LL.M (Universiteit Leiden).

Rakyat. Berdasarkan rancangan UUPDP versi tahun 2016, pihak-pihak yang memproses data pribadi dipastikan perlu untuk mematuhi berbagai macam kewajiban berdasarkan aturan-aturan yang terdapat di dalam UUPDP. Namun demikian, di dalam rancangan tersebut tidak ada mekanisme yang bersifat praktis yang ditawarkan kepada para pihak yang terkait agar mereka benar-benar menjalankan aturan yang ada di dalam UUPDP. Tanpa mekanisme tersebut, penerapan UUPDP bisa dipastikan gagal untuk mencapai tujuannya, yaitu untuk meningkatkan perlindungan terhadap hak privasi seseorang, tepatnya hak atas data pribadi mereka. Berkaca pada praktik yang sudah lama berkembang di negara-negara Uni Eropa (UE), mekanisme yang diterapkan oleh kebanyakan negara-negara di sana untuk menjamin terlaksananya aturan perlindungan data pribadi adalah dengan menghadirkan fungsi 'data protection officer' (DPO). Berdasarkan General Data Protection Regulation (GDPR), aturan mengenai perlindungan data pribadi di UE, pihak-pihak yang melakukan pemrosesan data pribadi tertentu wajib untuk memiliki dan menunjuk seorang DPO (Kewajiban Penunjukkan DPO). Hal ini dikarenakan kewajiban penunjukkan DPO dianggap sebagai mekanisme yang efektif, tulisan ini membahas dan diakhiri dengan sebuah saran agar UUPDP mengadopsi mekanisme tersebut ke dalam UUPDP agar tujuan dari undang-undang tersebut dapat tercapai.

Kata kunci: *data protection officer, general data protection regulation, hukum perlindungan data pribadi.*

A. Introduction

In the past seven years, the number of cases of unsolicited calls or messages, credit card fraud, identity theft, online harassment, cyber stalking and other cases relating to personal data has been significantly high in Indonesia. Many believe that the increase of such cases is caused by the lack of regulatory framework that protects personal data.

For a country with a large number of Internet users, which according to one research has reached 132.7 million people by the end of 2016[1] (that is six times the population in the Netherlands plus their bicycles), it is problematic that it has not yet have a robust data privacy regime in place.

At the moment, data privacy rules in Indonesia are scattered across at least 30 different laws and regulations.[2] Nevertheless, this will change once the Indonesian parliament passes the Personal Data Protection Law (PDPL). The PDPL is a comprehensive data protection legislation that will serve as *lex generalis* to all of the existing laws and regulations containing personal data protection.

The Indonesian government (led by the Ministry of Communications and Informatics (MOCIT) first drafted the PDPL in 2006; however, the drafting process of

---

1 Asosiasi Penyelenggara Jasa Internet Indonesia, "Infografis Penetrasi & Perilaku Pengguna Internet Indonesia: Survei 2016", https://pt.slideshare.net/OyhonxdCalista/infografis-penetrasi-dan-perilaku-pengguna-internet-indonesia-2016-apjii, accessed on March 2017.

2 Wahyudi Djafar (et.al.), "Perlindungan Data Pribadi: Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia", *Seri Internet dan HAM*, 2016, pp. 30-31.

the PDPL was put on hold.[3] It was as early as 2012 that MOCIT resumed its work on the draft.[4]

MOCIT, as the representative of the government, had delivered its final draft to the parliament. Following the parliamentary hearing, changes to the draft, rehearing and other political process on the Bill of Law on the Personal Data Protection (PDPL draft),[5] the parliament will then enact it into law. The PDPL draft is a part of the 2015-2019 National Legislation Program (*Prolegnas*), a list of legislations that the Indonesian parliament must pass between 2015 and 2019. The bill, however, is not amongst this year's prioritized *Prolegnas*, so it will not be enacted in 2017. It is also unlikely that it will be enacted in 2018 as all the process for a bill to be passed into law in the Indonesian parliament generally takes at least a year. Hence, the author expects 2019 as the year the PDPL draft will be enacted.

Once the PDPL has been enacted and come into force, it is expected that organizations that will be subject to the PDPL will be presented with various compliance challenges, especially since the law provides a bundle of new requirements (as is evident from a 2016 version of the PDPL draft).

While organizations will be required to align their existing practice to comply with the rules under the PDPL and monitor the same from time to time, the PDPL (per the 2016 draft) does not provide any effective mechanism or tool that could facilitate organizations to comply with the rules set out under the PDPL.

The European Union (EU) and its member states are well-known for their data privacy regimes. Under the GDPR, a newly-issued EU data protection legislation which will apply as of 25 May 2018, certain organizations are required to appoint a data protection officer (DPO) as a way to facilitate their compliance with rules in the General Data Protection Regulation (GDPR).

The concept of DPO, or as the Working Party calls it the 'compliance orchestrator',[6] is not new. Although the previous EU data privacy legislation (Directive 95/46/EC) did not have any provision on mandatory designation of DPOs, the practice of appointing a DPO has nevertheless developed in several EU member states over the years and is generally perceived as an effective, practical compliance solution.

Having said the above, this article seeks to establish (and enquire as the main question of this article) whether there is a need for Indonesia, given its state of affairs, to take into consideration the same approach as that of in the GDPR and

---

[3] Rosarita Niken Widiastuti, "Perlindungan Data Pribadi: Menghadirkan Negara dalam Melindungi Segenap Bangsa dan Memberikan Rasa Aman pada Seluruh Warga Negara", https://www.slideshare.net/idigf/id-igf-2016-hukum1-perlindungan-data-pribadi-menghadirkan-negara, accessed on March 2017. There was no mention of the rationale behind MOCIT having to put the drafting process of the PDPL on the back burner, but typically it is due to other urgent matter that they need to shift their focus on.

[4] *Ibid*.

[5] Ministry of Communication and Informatics, Bill of Law on the Personal Data Protection, http://peraturan.go.id/rancangan-undang-undang-tentang-perlindungan-data-pribadi.html, accessed on March 2017 (PDPL draft).

[6] Article 29 Data Protection Working Party, Appendix on Core Topics in the View of Trilogue, 2015, p. 18.

adopt the DPO Obligation into the PDPL in order to fill the gap in the Indonesian data protection framework.

To set the scene for this article, Chapter C briefly dissects the anatomy of the DPO Obligation in the GDPR in order to understand how the DPO Obligation is regulated under the EU regulatory framework. To better understand the rules associated with DPO Obligation under the GDPR, special attention will also be given on the guidelines issued by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Working Party), an independent European advisory body on data protection and privacy.

Subsequently, Chapter D focuses on the Indonesian laws and regulations pertaining to personal data protection, particularly the content of the PDPL (based on the 2016 version). The author also discusses the shortcomings of such draft, especially in relation to the unavailability of any effective mechanism that could promote organizations' data protection compliance. Accordingly, Chapter E explains why the DPO Obligation may serve as an answer to the legal and regulatory problems that presently exist in Indonesia. Furthermore, this chapter outlines the benefits of having a DPO and why there is a need for the PDPL to install a provision of DPO Obligation. In order to have an objective view on this matter, this chapter also describes the drawbacks if the PDPL were to adopt the DPO Obligation. Finally, Chapter F concludes by answering the main question as described above.

B. Data Protection Officers vis-à-vis the General Data Protection Regulation

1. Anatomy of the Data Protection Officer Obligation in the General Data Protection Regulation

The GDPR introduces the concept of DPO Obligation, and it dedicates an exclusive section on the subject matter (i.e., Section 4 of the GDPR), which is comprised of three articles, all of which will be discussed and dissected below.

a. Who are the Data Protection Officers?

At the outset, it is important to clarify that a DPO refers to the function introduced in the EU context, particularly as stipulated in the GDPR, and does not include other privacy professionals, such chief information officers (CIOs), chief privacy officers (CPOs), chief data officers (CDOs) or other types of c-suite officer with similar function.

The above distinction is made because DPOs and c-suite officers naturally have different roles and responsibilities. Under the GDPR, a DPO must perform its duties independently and does not receive instructions when carrying out its role in an organization.[7] This is somewhat in conflict with the role of c-suite officers as they are likely to be under a 'competing commercial imperative'[8] from other organs in the organization, such as the board of directors or shareholders.

---

7 Article 38(3) of the European Union General Data Protection Regulation, adopted on April 27, 2016 (GDPR).

8 King and Wood Mallesons, "Chief Data Officer is not a Data Protection Officer", http://www.kwm.com/en/uk/knowledge/insights/a-chief-data-officer-is-not-a-data-protection-officer-20150218, accessed on April 2017.

In respect of the individuals who could be a DPO, Article 37(6) of the GDPR provides that an employee of the controller[9] or processor[10] can be designated as a DPO as long as he or she has the necessary qualifications (a topic that will be discussed in the subsequent sub-chapter). Alternatively, the controller or processor could appoint, on a contractual basis, an external person to be a DPO,[11] such as lawyers or privacy consultants. As with the case of internal DPOs, the same qualifications apply to external DPOs.[12]

b. Who is required to appoint a Data Protection Officer?

The first article in Section 4, Article 37(1), stipulates the mandatory appointment of DPOs and lays down the type of organizations that are subject to the said requirement. Organizations that meet one of the following criteria are subject to the DPO's obligation:

1) where the processing is carried out by a public authority or body (except for courts acting in their judicial capacity);
2) where the core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects[13] on a large scale; or
3) where the core activities consist of processing on a large scale of special categories of data[14] and personal data relating to criminal convictions and offences.

From the above, we can see that the DPO Obligation is not applicable across the board and only certain organizations that fall within one of the above criteria are bound by Article 37(1) and therefore must appoint a DPO.

There is, however, ambiguity as to some elements within Article 37(1). As such, we refer to the Working Party's most recent guidelines to better understand the key terms used in Article 37 (1),[15] as set forth below:

1) 'Public authority or body': The GDPR leaves this phrase undefined in order for the EU member states to interpret based on their national laws. Interestingly, the Working Party points out that the phrase should also extend to private organizations that undertake public tasks. The typical public tasks that are carried out by private organizations include, for example, public transport services, water and energy supply, and road infrastructure. In this regard, the

---

9 The term 'controllers' in the context of personal data law generally refers to individuals or organizations that carries out processing of personal data. 'Processing of personal data' means any operation or set of operations which is performed on personal data or on sets of personal data, including, but not limited to, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

10 'Processors' are individuals or organizations that process personal data on behalf of the controllers.

11 Article 37(6) of the GDPR.

12 Article 29 Data Protection Working Party, Guidelines on Data Protection Officers, 16/EN WP 243, adopted on December 13, 2016, p. 12.

13 'Data subject' in the context of personal data generally means a natural person who is the subject of a personal data.

14 'Special categories of data' (or 'sensitive data') refers to personal data revealing health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, etc.

15 Article 29 Data Protection Working Party, Guidelines on Data Protection Officers, *Op.cit.*, p. 4.

Working Party recommends that such private organizations designate a DPO.[16]

2) 'Core activities': The Working Party defines this phrase as 'the key operations necessary to achieve the controller's or processor's goals'[17] and reminded that such definition should not (i) *exclude* the processing of personal information that is inextricably linked to the main objective of the organizations[18] and (ii) *include* activities that are deemed as 'ancillary functions'.[19] Although the line between these two caveats remain unclear, the guidelines has provided some helpful guidance as to the possible extent of this phrase and the member states may greatly benefit from it when drafting their national laws on this issue.
3) 'Large scale': The Working Party did not attempt to define what this phrase entails since it is a very subjective and difficult endeavor. Nevertheless, it gave several factors that can be considered when deciding on whether certain processing of personal data is carried out on a large scale,[20] which are: (a) the number of individuals affected; (b) the volume of data and/or the types of different data being processed; (c) the period of time or permanence required for the data processing; and (d) the geographic scope of the data processing. To further explain what the phrase 'large scale' constitutes (and what not), the Working Party lists down several examples:[21]

Table 1

Examples	
Large-Scale Processing Activities	**Non-Large-Scale Processing Activities**
• Processing of patient data in the regular course of business by a hospital. • Processing of travel data of users of a public transportation (e.g. tracking through travel cards). • Processing of real-time geo-location data of customers of an international fast food chain for statistical purposes by a processor. • Processing of customer data in the regular course of business by an insurance company or a bank. • Processing of personal data for behavioral advertising by a search engine. • Processing of communications data by telephone companies or Internet service providers.	• Processing of patient data by an individual physician. • Processing of personal data relating to criminal offences by an individual lawyer.

16 Article 29 Data Protection Working Party, Guidelines on Data Protection Officers, *Op.cit.*, p. 6.

17 *Ibid*.

18 *For example* hospitals need to process health data in order for them to provide their main objective of providing health care services. Since the processing of the said data is significant to hospitals, it should be deemed as one of the hospitals' core activities, which means hospitals are subject to the rule on mandatory appointment of a DPO. *See* Article 29 Data Protection Working Party, Guidelines on Data Protection Officers, *Op.cit.*, pp. 6-7.

19 *For example* the processing of personal information for the purpose of organizations' payroll or internal IT-related services. *See* Article 29 Data Protection Working Party, Guidelines on Data Protection Officers, *Op.cit.*, p. 7.

20 *Ibid*.

21 Article 29 Data Protection Working Party, Guidelines on Data Protection Officers, *Op.cit.*, p. 8

4) 'Regular and systematic monitoring': 'Regular and systematic' means one or more of the following:[22]

Table 2

'Regular'	'Systematic'
• Occurring at particular intervals for a particular period. • Repeated at fixed times. • Periodically takes place.	• Occurring based on a particular system. • Organized or methodical. • Occurring as part of a general plan for data collection. • Carried out as part of a strategy.

The Working Party provides a few examples to illustrate the phrase, which include: (i) profiling and scoring for purposes of risk assessment such as credit scoring or fraud prevention; (ii) location tracking through mobile apps; and (iii) behavioral advertising.[23]

5) 'Special categories of data and data relating to criminal convictions or offences': The Working Party provides a clarification with regard to this phrase, stating that the phrase should use the word 'or' instead of 'and' since 'there is no policy reason for the two criteria (i.e., special data and criminal data) having to be applied simultaneously.'[24] The Working Party did not clarify the meaning of the phrase 'special categories of data' as it is already explained under Article 9 of the GDPR.

c. Qualifications of the Data Protection Officers

Under Article 37 (5) of the GDPR, the qualifications of a DPO are vaguely set out in that he or she must possess 'professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil [his/her] tasks.' The Working Party, in its guidelines, explains that such 'qualities' entail sufficient understanding of data protection laws in the relevant country and in the EU, especially the GDPR.[25] In addition, the DPOs should have '[k]nowledge of the business sector and of the organization of the controller.'[26]

In relation to DPOs who work for a public authority or body, they should also understand about the rules and procedures that exist within such public authority or body.[27]

d. Position of the Data Protection Officers

The discussion in the second article of Section 4 of the GDPR, Article 38, revolves around the position of the DPOs within an organization. Position in this respect does not mean the DPO's place within the corporate structure of an organization, but relates to the DPO's involvement in an organization's data processing activities,

---

22 *Ibid*.
23 Article 29 Data Protection Working Party, Guidelines on Data Protection Officers, *Op.cit.*, p. 9
24 *Ibid*.
25 Article 29 Data Protection Working Party, Guidelines on Data Protection Officers, *Op.cit.*, p. 11.
26 *Ibid*.
27 *Ibid*.

whereby such involvement must be at 'the earliest stage possible.'[28] Position also refers to several other matters, as follow:

1) Organizations are required to provide the necessary resources in order for the DPO to be able to undertake his or her duties. The provision of necessary resources includes (i) sufficient time, (ii) adequate financial, facilities and personnel and (iii) access to relevant files or departments (IT, legal, finance, etc.);[29]
2) DPOs must be granted assurance that they will be able to perform their tasks independently and without having to be bound by any instructions from anyone else in the organization;[30]
3) In the course of performing its tasks, DPOs must act independently. For that reason, it cannot be subjected to any arbitrary dismissal and penalties. Penalties vary and may include 'absence or delay of promotion; prevention from career advancement; denial from benefits that other employees receive';[31] and
4) A person appointed as a DPO within an organization remains free to handle other tasks and duties not related to the protection of personal data. Nevertheless, the GDPR requires that this must not conflict with his or her role as the organization's DPO. To name a few, the tasks and duties of a senior management (chief executive officer, chief financial officer, chief operating officer, etc.), human resource manager and marketing manager are typically the positions that have a potential of conflict of interest with the role of a DPO.[32]

e. Tasks of the Data Protection Officers

The last provision of Section 4, Article 39, regulates about the tasks that DPOs are entrusted with, and those tasks should *at least* be, as follow:[33]

1) to inform and advise the organizations where the DPOs work in respect of those organizations' obligations under the GDPR;
2) to monitor compliance (not just with laws and regulations, but also on internal policies on protection of personal data). The GDPR explicitly states that compliance monitoring includes monitoring the delegation of responsibilities within the organization insofar related to data processing-related activities, awareness-raising and providing training to staffs and performing audits;
3) to advise and monitor anytime the organization where the DPO work intends to carry out a data protection impact assessments (DPIA).[34] The Working Party gave some examples as to what types of DPIA-related issues that an organization should consult with its DPO: (i) on the methodology of the DPIA, (ii) on whether

[28] Article 29 Data Protection Working Party, Guidelines on Data Protection Officers, *Op.cit.*, p. 13.
[29] Article 29 Data Protection Working Party, Guidelines on Data Protection Officers, *Op.cit.*, p. 14.
[30] *Ibid*.
[31] Article 29 Data Protection Working Party, Guidelines on Data Protection Officers, *Op.cit.*, p. 15.
[32] Article 29 Data Protection Working Party, Guidelines on Data Protection Officers, *Op.cit.*, p. 15 and p. 16.
[33] Article 39(1) of the GDPR.
[34] A data protection impact assessments (DPIA) is somewhat an audit on any new or existing data processing operation carried out by a controller or processor in order to assess whether such operation is likely to result in a high risk to the protection of personal data of an individual.

to do the DPIA internally or through a third party consultant and (iii) on the relevant safeguards;[35] and

4) to become the intermediary between the national data protection authority and the organization, particularly as a point of contact of the organization for matters related to the national data protection authority.

2. Effectiveness of the Data Protection Officer Obligation to Boost Compliance

The function of a DPO has an essential status within organizations, especially because it plays a crucial role in enabling organizations to ensure and demonstrate data privacy compliance. The Working Party, to name a few, has always maintained such a view, even before the GDPR was adopted.[36] With high praise, the Working Party in 2015 asserted that:

> [t]he DPO is a cornerstone of accountability and a real tool of competitiveness for companies. Tasked with the implementation of accountability tools (e.g.: documentation, PIA, etc…), they should be considered as the "compliance orchestrator" and the intermediary between all relevant stakeholders (e.g. supervisory authorities, data subjects, business partners).[37]

Under the GDPR framework, the appointment of a DPO is made mandatory to organizations that meet the requirements set out in Article 37(1). After the GDPR enters into force, the requirement may likely increase the number of organizations that will designate a DPO. Eventually, it will improve both the level of data privacy compliance of such organizations and privacy protection of individuals. In order to achieve this goal, the GDPR provides sanctions in the form of administrative fines for those failing to comply with such a requirement. These fines are significant as it may reach up to € 10 million or two percent of the organization's total worldwide annual turnover.[38]

Nevertheless, the GDPR itself will only become effective on May 25, 2018. Hence, whether or not the mandatory appointment of DPO will boost data privacy compliance remains to be seen. One could, however, refer to Germany as it has already implemented the mandatory designation of DPO since 1977.[39] From the experience of Germany, we can perhaps deduce a conclusion as to whether the mandatory appointment of DPOs works effectively in increasing organizations' compliance with data protection rules.

Under the *Bundesdatenschutzgesetz* (German Data Protection Act), the

---

35 Article 29 Data Protection Working Party, Guidelines on Data Protection Officers, *Op.cit.*, p. 17.

36 Article 29 Data Protection Working Party, Guidelines on Data Protection Officers, *Op.cit.*, p. 4. *See* also Article 29 Data Protection Working Party, Appendix on Core Topics in the View of Trilogue.

37 Article 29 Data Protection Working Party, Appendix on Core Topics in the View of Trilogue.

38 Article 83(4)(a) of the GDPR.

39 *See* Global DataHub, "The Compliance Burden under the GDPR – Data Protection Officers", https://www.taylorwessing.com/globaldatahub/article-compliance-burden-under-gdpr-data-protection-officers, accessed on May 2017.

appointment of a DPO (or in Germany, *Datenschutzbeauftragter*) is compulsory for every organization that has more than nine people handling the data processing activities within the organization.[40] The function of a DPO is considered as the 'crown jewel'[41] and 'inherit pillar'[42] of the German data protection landscape. The mandatory appointment of DPO is one of Germany's data protection policies that is heavily relied on, and that the overall German data protection system (including the mandatory appointment of DPO) has proven so successful that it is widely regarded as amongst the best in Europe.[43] The system has proven very effective in Germany partially due to the fact that the German Data Protection Act provides an administrative fine up to € 50,000 (or in certain cases, higher than € 50,000) for organizations that fail to adhere to the DPO Obligation.[44] Furthermore, the DPO Obligation rules (including the sanctions) are strictly enforced in Germany as is evident from the 1990s reports published by the Hessen government on how regular it brought cases against non-compliant organizations.[45]

F. The Upcoming Indonesian Personal Data Protection Law

In Indonesia, personal data of individuals is protected by law. As of now, the way in which the Indonesian regulatory system regulates issues relating to personal data is through different sector-specific laws and regulations. However, despite having specifically addressing personal data issues in different sectors, these different, sector-based laws and regulations are generally problematic (mainly owing to their lack of comprehensiveness).

Furthermore, according to the academic transcript (*naskah akademik*)[46] for the PDPL draft, modern technology and the Internet, such as social networking platforms, cloud computing and search engines, pose a serious threat of protection towards of personal data.[47] Given all these reasons, there is an urgent demand for a general – yet comprehensive – personal data protection law.

---

40 Gerald Spindler, "Consumer Data Protection in Germany" in Rainer Metz (et.al), *Consumer Data Protection in Brazil, China & Germany: A Comparative Study*, Göttingen: Göttingen University Press, 2016, p. 129.

41 Jeroen Terstegge, "Data Protection and the New Face of Privacy Compliance", https://www.pmpartners.nl/wp-content/uploads/2014/07/Businesscompliance-Data-Protection-and-the-new-face-of-privacy-compliance.pdf, accessed on May 2017.

42 Tobias Rothkegel, "New Data Protection Rules: What is a Data Protection Officer and Do I Need One?", http://marketinglaw.osborneclarke.com/data-and-privacy/new-data-protection-rules-what-is-a-data-protection-officer-and-do-i-need-one/, accessed on May 2017.

43 Francesca Bignami, "Cooperative Legalism & the Non-Americanization of European Regulatory Styles: The Case of Data Privacy", *American Journal of Comparative Law*, Volume 59, Issue 2, 2011, p. 428.

44 DLA Piper Data Protection, "Data Protection Laws of the World: Germany (2017)", http://www.dlapiperdataprotection.com, accessed on May 2017.

45 Francesca Bignami, *Op.cit.*, p. 427.

46 An academic transcript (*naskah akademik*) is a legal research or analysis on a particular subject matter and is typically carried out by academics and/or researchers. This document is part of the law-making process in Indonesia and is authoritative document that is referred to as the basis for law-makers to draft a bill on the same subject matter.

47 Naskah Akademik RUU tentang Perlindungan Data Pribadi, http://www.bphn.go.id/data/documents/na_perlindungan_data_pribadi.pdf, accessed on June 2017.

As mentioned in the beginning of this article (see Chapter A), MOCIT has been preparing the PDPL draft since 2006 in response to the increasingly high personal data-related problems in Indonesia. MOCIT had completed and submitted the PDPL draft to the parliament for discussion, while simultaneously waiting for other inputs from other ministries.[48] The PDPL draft, if enacted, will significantly transform the Indonesian data protection regulatory framework. This chapter discusses the key features of the PDPL draft (based on the 2016 version)[49] that are relevant to the scope of this article.

1. Personal Data

The PDPL draft provides a new definition of personal data, i.e., every data about an individual that is identifiable, whether directly or indirectly, with reference to such data alone or in combination with other information by means of an electronic or non-electronic system.[50] These data may include each or a combination of any of the following: an individual's name, place and data of birth, or identification document (e.g. ID card and driving license), biometric data (e.g. fingerprint and digital picture).[51] In comparison to the one available per the existing laws/regulations (e.g. the one provided in Ministry of Communication and Informatics Regulation Number 20 of 2016 on Personal Data Protection in Electronic Systems),[52] the definition of personal data provided pursuant to the draft PDPL is broader and clearer.

In addition to personal data, the PDPL draft introduces a new category of data, i.e., sensitive data. These data are defined as personal data that requires special protection[53] and may include religion/believes, health information, physical/mental condition, personal habit, information about sex life, political views, criminal record, financial data and family data.[54]

2. The Actors

Akin to the GDPR approach, the main actors that are involved in a data processing

---

[48] Kompas, "Lindungi Data Pribadi Warga", https://www.pressreader.com/indonesia/kompas/20170530/281771334145041, accessed on June 2017.

[49] The 2016 version of the PDPL draft can be found in the annex to the academic transcript of the PDPL. *See* Naskah Akademik RUU tentang Perlindungan Data Pribadi 2016, *Op.cit.*, pp. 164-199.

[50] Article 1(1) of the PDPL draft.

[51] Article 6(2) of the PDPL draft.

[52] Ministry of Communication and Informatics Regulation Number 20 of 2016 on Personal Data Protection in Electronic Systems (PDPES Regulation) refers to Law Number 23 of 2006 on Citizen Administration (as amended) (Citizen Admin Law) when defining personal data, which is 'certain personal data of which the accuracy is kept, treated, and maintained, and of which the confidentiality is protected.' Although both instrument refers to the same definition, the PDPES Regulation goes further by explaining the meaning of the phrase 'certain personal data' as 'every accurate and actual information that are associated and identifiable, whether directly or indirectly, to an individual, which the use of such information must be in accordance with laws and regulations.' On the other hand, the Citizen Admin Law does not provide any explanation about the phrase, though it stipulates that personal data that should be protected are (i) information on physical and/or mental disability; (ii) signatures; (iii) fingerprints; and (iv) iris of an eye.

[53] Article 1(3) of the PDPL draft.

[54] Article 6(3) of the PDPL draft.

activity as recognized under the draft PDPL consist of three parties: (i) the data subjects (*pemilik data pribadi*); (ii) data controllers (*penyelenggara data pribadi*); and (iii) data processors (*pemroses data pribadi*), all of which will be described respectively in the table below.

Table 3

Data Subjects	Data Controllers	Data Processors
Data subject means an individual who is the subject of a personal data and is identifiable based on the said personal data.[1] Based on the author's reading of the explanation of Article 1 (1) of the draft PDPL, it seems that the definition of data subjects excludes a deceased person.	Controllers mean natural persons, legal persons (both private and public bodies) and public organizations, whether alone or jointly with others, that carry out the processing of personal data.[2] Processing of personal data includes collection, analysis, storing, displaying, modification, disclosure, transfer, publication and erasure.[3]	Processors are natural persons, legal persons (both private and public bodies) and public organizations, whether alone or jointly with others, that carry out the processing of personal data on behalf of the controllers.[4]
	It is noteworthy that based on the definition set forth in the draft PDPL, a public organization means the executive, legislative, judicative and other organizations (i) whose main functions and duties are related to the state affairs and (ii) are partially or entirely funded by the state/ regional government's budget. Based on this definition, private organizations undertaking activities that fulfill the criteria above will be deemed a public organization.	

In addition to the main actors above, there is also the so-called 'third party' in a data processing activity. Under the PDPL draft, a third party is a natural person or legal entity that is neither the data subjects nor the party that processes personal data which has been allowed by the data subjects to do so.[55] Based on the given definition, the latter category will certainly include data processors as they do not typically obtain direct authorization from the data subjects when processing data on behalf of the controllers. As such, it is unclear whether or not it was the drafters' intention to incorporate data processors under the term 'third parties.'

3. Personal Data Processing

The term 'processing of personal data' under the PDPL draft refers not only to automated processing but also manual processing.[56] The PDPL draft provides a limited concept of processing and lists down an exhaustive list of the types of operations falling under the term 'processing of personal data.' These operations arecollection, analysis, storing, displaying, modification, disclosure, transfer, publication and erasure.[57]

[55] Article 1(12) of the PDPL draft.
[56] Article 1(8) of the PDPL draft.
[57] Article 9 of the PDPL draft.

4. Obligations of Data Controllers

The PDPL draft sets forth a list of obligations for controllers throughout Articles 16 to 29. The table below will show some of those key obligations.

Table 4

Data Subjects Consent	Prior to processing personal data, controllers must first seek and obtain the consent of data subjects. The PDPL draft requires the following information to be disclosed by data controllers when seeking after data subjects' consent: the purpose of the data processing activity; the types of personal data that will be collected; the retention period; the processing period and when personal data will be erased or destroyed.[5] Furthermore, in the event there are changes made to any of the above information, data controllers must notify the same to data subjects.[6]
Privacy Policy and Internal Data Processing Guidelines	Data controllers are required to disclose their privacy policies.[7] This requirement implicitly means that data controllers must create a privacy policy with regard to the processing of personal data. In addition to a privacy policy, data controllers must also prepare their own internal guidelines containing the necessary steps to protect personal data they hold from being damaged or unlawfully modified, disclosed or processed.[8]
Access to Data, Rectification of Data and Erasure of Data	Data controllers must provide access to the personal data that they hold upon request from data subjects.[9] The access must be provided as soon as reasonably possible.[10] Provided that a data subject deems that someone's personal data is inaccurate or incorrect, he/she has the right to request to the relevant data controller to rectify such data.[11] The said data controller must comply with such a request immediately.[12] Data controllers must also destroy personal data that they hold, without any delay, upon: (i) the end of the retention period; (ii) completion of the purpose of the data processing activity; or (iii) request from data subjects.[13] The PDPL draft also requires that the erasure or destruction of personal data be permanent and the data cannot be restored at any time in the future.[14]
Notification	In case of a data breach, data controllers must, without any delay, notify the relevant data subjects about the details of such a breach, including: (i) when and how the personal data was breached; and (ii) the actions that have been taken by data controllers to remedy the breach.[15]

5. Sanctions

The PDPL draft provides criminal sanctions specifically for cases of theft and forgery related to personal data. For such cases, individual criminals are subjected to a

maximum imprisonment of 1 year and/or penalty of IDR 300 million (equivalent to ± € 21,000),[58] or if the violator is a legal entity, the penalty would be higher, reaching up to IDR 1 billion (equivalent to ± € 67,000).[59]

In addition to criminal sanctions, administrative sanctions may also be imposed upon violations of the any provision of PDPL. These sanctions are imposed by the Information Commission (*Komisi Informasi*), an independent body that was established originally for matters pertaining to public information[60] but under the draft PDPL, it is empowered with additional authorities for personal data-related matters.[61] The administrative sanctions are, however, limited to written reprimands.[62]

6. Promoting Compliance

Based on the author's reading of the PDPL draft, there are only two instruments offered to promote the compliance efforts of personal data users (be it a controller or processor). First, personal data users are required to prepare an internal guideline for data security purposes, containing steps that the organization must take to protect the personal data that they hold from any damage or unlawful disclosure and modifications.[63] Second, a code of conduct on the processing of personal data *may* also be drawn up by an industry's association.[64] For example, the Indonesian Association of Internet Service Providers (*Asosiasi Penyelenggara Jasa Internet Indonesia*/APJII) and Indonesian e-Commerce Association (iDEA) may prepare their respective codes of conduct with respect to the processing of personal data and such rule be applied to their members on a voluntary or mandatory basis.

In practice, however, implementing the mechanisms above will be a considerable challenge. With respect to the internal data security guidelines, the Information Commission will be the national supervisory authority that oversees whether or not controllers (i) have such guidelines and they cover the appropriate topics, and (ii) carry out their personal data processing activities in accordance with the said guidelines. As generally perceived, relying too much in the national supervisory authority to provide effective oversight over a myriad of controllers would not be a practical solution; they are not in a position to do so given the widespread scarcity of resources, such as staffing and budgetary.[65]

Hence, in the context of the enforcement of the PDPL, the Information Commission will bear a heavy burden if they are tasked as the sole responsible party

---

58 Article 43 of the PDPL draft.

59 Article 44 of the PDPL draft.

60 Article 1(11) of the PDPL draft.

61 Article 31 of the PDPL draft.

62 Article 32(3)(a) of the PDPL draft.

63 Article 20(a) of the PDPL draft.

64 Article 39(1) of the PDPL draft.

65 *See* Sebastian J. Golla, "Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR", *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law*, Volume 8, Issue 1, 2017, p. 72. *See* also Bert-Jaap Koops, "The Trouble with European Data Protection Law*", International Data Privacy Law*, 2014, p. 8.

to oversee organizations' compliance with the PDPL. In effect, the guidelines will not be a practical solution for ensuring data protection compliance. As for a code of conduct, it is not a legal requirement and if an association issues one, it will neither be strictly binding to members of the association nor directly enforceable to them. Even if such a code of conduct is binding, the legal provisions will not apply to non-members.

G. Introducing the Data Protecton Officer Obligation in the Upcoming Indonesian Personal Data Protection Law

As pointed out in the previous chapter, the PDPL draft provides a raft of obligations for users of personal data. While some mechanisms to promote compliance have been offered under the draft PDPL, the author believes, as already argued above, those mechanisms will not be effective enough to ensure optimal implementation of the data protection rules under the PDPL. Inspired by the GDPR model, this chapter explores whether by introducing the DPO Obligation in the PDPL, there will be a better protection of personal data and more chances for the rules to be implemented in practice.

1. Benefits of Having a Data Protection Officer

Adopting the DPO Obligation mechanism under the PDPL would mean that users of personal data will then be required to employ a DPO within their organizations. How beneficial having a DPO can be, can be displayed through the vantage points of the different stakeholders. First, from the view point of users of personal data (e.g. controllers and processors), having a DPO within their organization would mean that there will be a privacy and data protection specialist who monitors and assists such organization's compliance with the provisions of the existing data protection law, association code of conduct and internal guidelines. By having such a DPO, it may also improve the way organizations protect and control personal data when they perform their respective data processing activities.[66] Furthermore, a DPO will help and manage organizations' relationship with the other stakeholders since it can act as an intermediary between the organization that it works for and data subjects or the government authorities. At the same time, having such a function would have a reputational benefit for the organization as having a DPO portrays 'a positive image factor which helps creating trust'[67] and shows that the organization has a competitive advantage.[68]

From data subjects perspective, the positive attribute is that there would be more assurance for data subjects as there is someone inside the data controllers/

[66] Christoph Klug, "Improving Self-Regulation Through (Law-Based) Corporate Data Protection Officials", Privacy Laws & Business International Newsletter, Issue No. 63, 2002, p.8.

[67] Confederation of European Data Protection Officers, "Improve for the Protection of (our/your) Data: 6 Incentives for Appointment of DPO", http://www.cedpo.eu/wp-content/uploads/2015/01/CEDPO_Position_Paper_Incentives_DPO_20130924.pdf, accessed on June 2017.

[68] Christoph Klug, *Loc.cit*.

processors' organization that can ensure that any data processing activity carried out by such controllers/processors is consistent with the applicable rules. Moreover, in terms of correspondence between data subjects and data controllers/processors, a DPO can be the point of contact. So, if a data subject has a request fo r certain matters pertaining to personal data (e.g. request to access, rectify or erase personal data that such a data controller/processor holds about the data subject), the data subject could contact and submit his or her request to the controller/processor through the DPO.

Another positive feature of the role of a DPO is in the manner in which it is able to create an effective self-monitoring environment in terms of data protection compliance within each and every data controller/processer. DPOs will be in charge of many different legal, technical and organizational problems linked to processing personal data. Thus, with DPOs' presence inside the users of personal data, the role of which can be seen as an extension of the supervisory/governmental authority, the supervisory/governmental authority's supervision and intervention can be considerably reduced.[69] Further, with the data protection compliance task being taken care of, to a certain extent, by DPOs, the supervisory/governmental authority will be able to focus on other tasks (e.g. providing guidance, enforcement actions, adjudications, etc.)[70] and save the state budget. Empirical evidence in Germany (a country that has adopted the concept of mandatory DPO since 1977) suggests that this approach has proven to be successful 'in guaranteeing both effective data protection and reasonable economic freedom.'[71]

The inclusion of the DPO Obligation under the PDPL will also give rise to a new industry in Indonesia. This new industry will then create job opportunities. As an illustration, the GDPR, which also provides provisions on mandatory designation of DPO, will force organizations to look for and appoint qualified individuals to be their DPO. The International Association of Privacy Professionals (IAPP) estimated that there will be a demand of at least 75,000 DPOs worldwide subsequent to the GDPR taking into force in 2018.[72] Additionally, there will be a niche market for educating and training people wishing to be a DPO.

Lastly, from a macro perspective, the PDPL (based on the provisions of the 2016 draft) is expected to have the greatest impact on Indonesia's economy as it will create a more conducive and trusted investment destination for investors wanting to set up businesses involving the processing of personal data.[73] By adding the DPO

---

69 Christoph Klug, *Op.cit.*, p. 2; *see* also Annete Demmel and Monika Kuschewsky, "GDPR – The Data Protection Officer: Requirement, Role and Implementation" , http://www.squirepattonboggs.com/~/media/files/insights/events/2017/01/need-to-know-gdpr-the-data-protection-officer-requirement-role-and-implementation/gdpr_data_protection_officer_role_requirement_and_implementation_jan17.pdf, accessed on June 2017.

70 Jeroen Terstegge, *Op.cit.*, p. 42.

71 Christoph Klug, *Loc.cit.*

72 The International Association of Privacy Professionals, "The GDPR Demands 75k DPOs", https://iapp.org/media/pdf/DPA-Whitepaper.pdf, accessed on April 2017.

73 Naskah Akademik RUU tentang Perlindungan Data Pribadi 2016, *Op.cit.*, pp. 84-85.

Obligation in the PDPL, the author believes that it will boost the country's economic growth even more. In the end, the country's competitiveness will be enhanced and it may put Indonesia on par with others countries that had already enacted data privacy legislation.

2. Urgency of Applying the Data Protection Officer Obligation

In order to fully reap the benefits as explained above, the appointment of DPO should be made compulsory. Without a DPO Obligation, controllers and processors will likely be more inclined not to appointment a DPO since it is (i) financially, a burden, (ii) operationally, a disruption and (iii) legally, a non-violation (see more explanation in sub-chapter E.3. below). In the end, it may undermine the Indonesian government in achieving the main goal of enacting the PDPL in the first place, which is to better protect the privacy rights of individuals, especially with regard to their personal data.[74]

Furthermore, the DPO Obligation will create a level playing field. Today, many Indonesian-subsidiary of American and European companies have generally already adhered to strict data protection standards (typically the same standards applied to their parent companies), whereas their local competitors generally have little regard (or no regard at all) to privacy and the protection of personal data.[75] The previous companies may also have appointed a DPO (or a person whose role and function is in common with a DPO), whilst the latter companies may likely not. As a result, the latter companies may have some competitive advantageous over the previous type of companies when carrying out their business operation. With the introduction of the DPO Obligation, the latter companies will then be required to appoint a DPO and thus creating a level playing field between both companies.

3. Challenges of Applying the Data Protection Officer Obligation

Requiring controllers and processors to designate a DPO within their organization is nevertheless without any challenge. It would seem that the one major impediment for adopting the mechanism into the PDPL relates to the financial burden that it will bring to businesses.

Although drafters of the academic transcript did not raise the potential negative impact towards businesses following the PDPL taking into force,[76] the author is of the view that even based on the current version of the draft PDPL (before including the appointment of DPO requirement), it is expected that the requirements therein will

[74] Chapter I of the explanation of the PDPL draft.

[75] This is so due to the fact that Indonesian people and businesses in general are known for not placing serious attention to privacy. Most likely that phenomenon exists because Indonesian people traditionally live in a communal society and is very open to one and another. *See* Naskah Akademik RUU tentang Perlindungan Data Pribadi 2016, *Op.cit.*, p. 91.

[76] Drafters of the academic transcript provided a financial impact analysis, but only in respect of the state's budget; it did not provide any impact assessments towards businesses. With regard to the impact on businesses, the academic transcript only focuses on the benefits that businesses will gain from the implementation of the PDPL. *See* Naskah Akademik RUU tentang Perlindungan Data Pribadi 2016, *Op.cit.*, pp. 86-89.

put a great financial burden on businesses.[77] An example is the obligation imposed on controllers and processors to provide comprehensive information to data subjects prior to seeking their consents.[78] Such a requirement would force controllers and processors to overhaul their internal personal data processing policy/strategy. The process for doing that may result in substantial unwanted costs for the controllers/processors, for example, payments for (legal) advice.

Another example is in relation to the requirement for controllers or processors to provide access to personal data upon a data subject's request.[79] The provision, however, is silent on whether controllers or processors are allowed to require that data subject to pay prior to viewing into his or her personal data. If such a condition is not permitted, then that will put additional financial burden on businesses (especially micro, small and medium enterprises (MSMEs) as it will open the door for many (or even excessive) access requests.

The designation of DPO requirement in the PDPL will, on one hand, bring many benefits, but on the other hand, it will clearly place a greater burden on businesses. Controllers and processors will need to allocate an additional budget to hire or employ someone with the required qualifications, be it as an in-house or external DPO. Certain businesses, such as MSMEs, will be even more devastated by such a requirement.

Though unrelated to the issue of financial burden, adding the DPO function within controllers/processors' organizational structure may disrupt their existing business operations. For example, controllers/processors will have to restructure the current reporting lines and integrate the DPO with the other business functions.

Finally, there is also the fear that the role of a DPO will just be a formality and he or she will only be carrying out tick-box exercise. This, as a result, will be counterproductive to achieve the aim of the law. This particular concern was also shared in the EU in respect of the GDPR.[80] However, the probability of this phenomenon taking place in Indonesia is higher due to the lack of awareness of the

---

77 There is currently no available financial impact assessment of the PDPL (moreover the PDPL with the DPO Obligation in it). As such, the author refers to the study that had been made in other jurisdiction whose data protection law is as comprehensive (or more comprehensive than) the PDPL in order to support his argument that typically the enactment of a data protection legislation will result a great financial burden for businesses. According to a study carried out by the United Kingdom's Ministry of Justice (UK MOJ) on the expected impact of the implementation of GDPR to "affected sectors of society in the UK", it is predicted that it may "lead to a net cost to business of between £ 80 million and £ 320 million per year." Furthermore, the study reveals that there may be a negative net present value of the GDPR to the UK in the next fourteen years, which may result in £ 2.1 billion overall losses. *See* London Economics, "Implications of the European Commission's Proposal for a General Data Protection Regulation for Business", Final Report to the Information Commissioner's Office, 2013, p. 19.

78 Article 16(2) of the PDPL draft.

79 Article 21 of the PDPL draft.

80 Chris Payne, "GDPR and the DPO: Five Things to Know about Your Next Job Vacancy", https://www.tripwire.com/state-of-security/security-data-protection/gdpr-and-the-dpo-five-things-to-know-about-your-next-job-vacancy/, accessed on July 2017. *See* also David Meyer, "What Will Mandatory DPOs Look Like under the GDPR? Germany Could Tell You", https://iapp.org/news/a/what-will-mandatory-dpos-look-like-under-the-gdpr-germany-could-tell-you/, accessed on July 2017.

Indonesian society (including businesses) in terms of the protection of personal data and privacy.

4. Recommendations

From the above assessments, it can be observed that the inclusion of DPO Obligation into the PDPL has both advantageous and weaknesses. However, looking at this from a utilitarian perspective, it would appear that Indonesia as a whole will gain more benefit if the DPO Obligation is adopted into the PDPL. The author, therefore, proposes to adopt such a mechanism into the PDPL, but bearing in mind that it should cover the features as described below.

a. Risk-Based Approach

Although mandatory in nature, the appointment of DPO requirement should not be made as a general requirement that applies to all types of organization. Only organizations fulfilling certain thresholds should be required to appoint a DPO.

It is important that the thresholds adopted in the PDPL are not based on non-objective criteria, such as the size of the controllers/processors. The GDPR version that was proposed by the EU Commission in 2012 had initially contained a non-objective criterion, whereby requiring controllers/processors having 250 or more employees to appoint a DPO.[81] The proposal was highly criticized as being arbitrary and such proposal ended up being scrapped in the final text of the GDPR.[82] The danger in adopting such an approach is as what Jeroen Terstegge astutely points out:

> [T]he degree of risk to the privacy of the individual posed by an organization is almost never related to its size. Very small organizations, especially those which operate online, may pose significant threats to the individual's privacy, where some large industrial organizations may have almost no privacy issues.[83]

So, rather than using non-objective criteria, it would be better if the PDPL adopts a risk-based approach. This risk-oriented approach is 'a core element of the accountability principle' under the GDPR[84] and is employed to scale whether the risk (e.g. the potential negative impact on data subjects' rights, freedom and interests) posed by a data processing operation necessitates a certain preventive measure. Article 37(1) of the GDPR applies this approach when determining whether or not an organization should appoint a DPO.

---

[81] *See* Article 35(1)(b) of the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, or the General Data Protection Regulation, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012PC0011#document1, accessed on June 2017.

[82] Jeroen Terstegge, *Op.cit.*, at 42; *see* also Baker & Mc Kenzie LLP, "EU Data Protection Officer – Must Have, Nice to Have or Safe to Ignore?", https://www.lexology.com/library/detail.aspx?g=80683a4c-66f1-4f61-bf67-9d092378c231, accessed on June 2017.

[83] Jeroen Terstegge, *Op.cit.*, p. 43.

[84] Article 29 of Data Protection Working Party, Statement on the Role of a Risk-Based Approach in the Data Protection Legal Frameworks, 14/EN WP 218, adopted on 30 May 2014, p. 2.

In addition to having risk-based criteria, the PDPL should also add other factors into the criteria, such as the nature of personal data (sensitive or not), the number of personal data processed and/or the category of data subject (minor or not).

b. In-house and External Data Protection Officers

Article 37 (6) of the GDPR explicitly allows for a DPO to be either an employee or external person, the latter is subject to the terms of a service contract as agreed and signed by and between that person and the organization that engages him/her as their DPO. With such an option, this will provide organizations with some degree of flexibility in complying with the DPO Obligation. For example, MSMEs are more likely attracted to procure the services of external company offering DPO services instead of employing an in-house DPO, since the previous option is much more cost-effective for them.[85] For this reason, the PDPL should adopt the same approach as set out in Article 37(6) of the GDPR.

c. Proportionately Competent Data Protection Officers

Along with the above features, the PDPL should also set out the competencies of a DPO. This requirement will ensure that the person that will be appointed to monitor privacy and security of the processing of personal data within an organization is the right one for the job. If it is otherwise, in that the PDPL does not impose any qualification for DPOs, organizations will likely appoint incompetent individuals just for the sake of meeting the obligation, and thus, potentially undermining the objective of the PDPL.

It would be counterproductive for the PDPL to include a provision that demands a DPO to have high-standard qualities. With reference to the GDPR, Article 37(5) stipulates that DPOs 'shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil [his/her] tasks'. The provision is further explained in recital 97, which provides that the necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed. So, following the approach of the GDPR, the PDPL could have a similar provision which essentially only require DPOs to have the expertise and skills that are proportionate to the complexity of the personal data operations of the organizations that they will work for.

d. 'In-Country' Requirement

The GDPR is silent about the physical presence of a DPO.[86] In the same vein, the Working Party did not provide any explanation about the subject matter in the guidance that it published in 2016, though it states that a DPO should be readily contactable and make him/her available if needed.[87] The Working Party, however,

---

85 Jeroen Terstegge, *Op.cit.*, p. 37.

86 Article 37(2) of the GDPR only requires a DPO to be 'easily accessible.' The Working Party explains that easily accessible refers to the role of a DPO as a contact point of a controller or processor in relation to any enquiries or requests from data subjects or supervisory authorities. *See* Article 29 of Data Protection Working Party, Guidelines on Data Protection Officers, *Op.cit*, p. 10.

87 Article 29 of Data Protection Working Party, Guidelines on Data Protection Officers, *Loc.cit.*

clarified this in the revised version of the guidelines, which was issued on April 5, 2017, recommending that DPOs be located within the EU territory, regardless of the users of the personal data having establishments in the EU, for the sake of ease of accessibility by other stakeholders.[88]

In the PDPL, the author suggests a different approach to be taken and that is to explicitly require DPOs (whether an employee or external person) that are appointed by Indonesian-based organizations to reside within Indonesia. Besides this being a common requirement in Indonesian laws and regulations,[89] the 'in-country' requirement is important since the tasks of a DPO typically relates to the day-to-day operations of an organization. As such, it is essential that the DPO closely monitors the data processing operations of the organization on a daily basis. Additionally, the DPO must make him/herself available to speak and/or meet with colleagues, data subjects or the local supervisory/governmental authority, especially during business hours in Indonesia. All of these can only be achieved if the DPO resides in Indonesia.

e. Independent Status

Another important feature is that a DPO must have and should be included in the PDPL pertains to the status of the DPO within the organization that he or she works for. In order to perform his or her duties and tasks as mandated by law, a DPO must be independent, such that he or she is able to exercise such duties and tasks autonomously, without being intervened or threatened by others. Referring to the GDPR, the approach taken to protect a DPO's independency is by way of prohibiting dismissal and penalties (see sub-chapter C.1.d above for further explanation). The PDPL should incorporate a similar approach as well as to put in an additional prohibition on arbitrary termination of contract (the latter is specifically meant to protect the independency of an external DPO). A generic caveat should also be added into the provision, particularly a reference to the prevailing laws and regulations in Indonesia, in order to ensure that the said prohibitions will be interpreted in accordance with relevant and existing laws, such as the labor law which contains rules on dismissal and the Indonesian Civil Code which contains contract-related rules.

In addition to requiring DPOs to carry out their duties and tasks in an independent manner, the PDPL must also provide that the function cannot have a dual role within the organization so as to avoid a conflict of interest.

f. Specific Sanctions

To ensure the PDPL objectives are met, the appointment of DPO requirement should be equipped with sanctions. The main reason is because a legal obligation without a sanction is bound to fail. As Peter Clawson avers, 'if you're going to put

---

88 Article 29 of Data Protection Working Party, Guidelines on Data Protection Officers, 16/EN WP 243 rev.01, adopted on 5 April 2017, p. 11.

89 *For example* individuals (whether an Indonesian citizen or expat) that are appointed as a corporate secretary in an Indonesian listed company or a director in a limited liability company must reside in Indonesia due to their day-to-day functions in the company.

something in place, if there aren't teeth it won't happen.'[90]

The GDPR adopts such an approach and provides a heavy administrative fines of up to € 10 million or, in case of a company, 2% of the annual turnover of the organization, in order to force organizations to comply with the appointment of DPO requirement in Section 4 of the GDPR.[91] However, these administrative fines are criticized because they are unlikely to be imposed and are excessive in nature (especially for a mere case of failure to appoint a DPO).[92] Furthermore, the provision seems to suggest that such steep fines can be imposed immediately.

In synergy with the GDPR, the PDPL should also have a specific provision on sanctions for failure to comply with the DPO Obligation-related rules. However, unlike the sanctions in the GDPR, the author proposes that the sanctions introduced in the PDPL be applied in layers, in that the supervisory/governmental authority should impose a lighter sanction (e.g. written reprimands) to any infringing organization. If such an organization remains non-compliant with the rule, then a heavier sanction can be imposed.

g. Adjustment Period

The current draft PDPL allows existing controllers and processors for a period of one year to make adjustment to the requirements set out by the PDPL.[93] The author estimates that organizations will need more time to accomplish this, especially if the DPO Obligation-related rules will be added to the PDPL. Implementing the said rules is not an easy exercise for organizations. These organizations may need to seek for (legal) advices on whether they are subject to the requirement, look for the right individual to be appointed as their DPO, restructure the existing reporting lines, integrate the DPO with the other business functions and perhaps many more. Combined with the time required to make adjustment with the other PDPL requirements, it is, therefore, advisable that the adjustment period is extended to at least two years – the same period of time granted for organizations pursuant to the GDPR,[94] such that the affected organizations will have sufficient time to prepare themselves before the PDPL kicks in.

H. Conclusions

Indonesia currently witnesses a lack of data protection law and to that effect, the Indonesian government has planned to enact a general and comprehensive law regarding personal data protection. The draft of the law is now in the pipeline, waiting for it to be finalized and passed into law by the parliament, which is expected to be in 2019. Based on the 2016 version of the PDPL draft, the author found that the PDPL draft is still lacking, especially in terms of the compliance solutions and measures that it offers to organizations in facilitating their data protection

---

90 *See* Olavsrud, Thor, "Data Protection Officer Role Will Be Key If You Operate in the E.U." http://www.cio.com/article/2395511/legislation/data-protection-officer-role-will-be-key-if-you-operate-in-the-e-u-.html, accessed on June 2017.

91 Article 83(4)(a) of the GDPR.

92 Jeroen Terstegge, *Op.cit.*, p. 42.

93 Article 53 of the PDPL draft.

94 Article 99 of the GDPR.

compliance efforts. In this regard, the author proposes that the PDPL includes a requirement for controllers and processors to appoint a DPO. Inspired from the GDPR, this mechanism has the goals of, amongst others, promoting and ensuring organization's compliance with the data protection rules as well as enhancing the awareness of privacy and personal data protection requirements in the organization.

The scope of this article has required consideration of whether the mechanism above should be included in the PDPL, and if so, how that mechanism should be formulated in the PDPL. To answer these questions, Section 4 of the GDPR (on DPOs) and the current legal provisions regarding personal data protection in Indonesia (specifically the PDPL draft) were analyzed. In the process of doing so, the potential advantageous and challenges of implanting the mechanism in the PDPL were considered.

In view of these findings, adopting the DPO Obligation in the PDPL may be the best option to improving the data protection regime in Indonesia as it will address the substantive issues of privacy and data protection in Indonesia as well as fill the gap in the PDPL. Taking into consideration the dynamics of the Indonesian regulatory system and practices, the mechanism is best transplanted into the PDPL conjointly with these recommended features:

1. The criteria that must be met in order for the DPO Obligation to be triggered by an organization should be risk-oriented;
2. A DPO can either be an employee or external person;
3. The level of competencies of a DPO should be measured proportionately in accordance to the type and complexity of the data processing carried out by the organization;
4. DPOs appointed by an Indonesia-based organization must reside in Indonesia;
5. DPOs must be able to perform their tasks and duties in an independent manner;
6. Specific sanctions should be made available for any organization failing to comply with the DPO Obligation-related rules; and
7. To accommodate organizations that will be affected by the PDPL (including the DPO Obligation), the PDPL should afford a minimum of two-year adjustment period to those organizations.

References

Books

Spindler, Gerald "Consumer Data Protection in Germany" in Rainer Metz (et.al.), *Consumer Data Protection in Brazil, China & Germany: A Comparative Study*, Göttingen University Press, Göttingen, 2016.

Other Documents

Asosiasi Penyelenggara Jasa Internet Indonesia, "Infografis Penetrasi & Perilaku Pengguna Internet Indonesia: Survei 2016", https://pt.slideshare.net/OyhonxdCalista/infografis-penetrasi-dan-perilaku-pengguna-internet-indonesia-2016-apjii, accessed on March 2017.

Baker & Mc Kenzie LLP, "EU Data Protection Officer – Must Have, Nice to Have or Safe to Ignore?", https://www.lexology.com/library/detail.aspx?g=80683a4c-66f1-4f61-bf67-9d092378c231, accessed on June 2017.

Bignami, Francesca "Cooperative Legalism & the Non-Americanization of European Regulatory Styles: The Case of Data Privacy", *American Journal of Comparative Law*, Volume 59, Issue 2, 2011.

Confederation of European Data Protection Officers, "Improve for the Protection of (our/your) Data: 6 Incentives for Appointment of DPO", http://www.cedpo.eu/wp-content/uploads/2015/01/CEDPO_Position_Paper_Incentives_DPO_20130924.pdf, accessed on June 2017.

Demmel, Annete and Monika Kuschewsky, "GDPR – The Data Protection Officer: Requirement, Role and Implementation", http://www.squirepattonboggs.com/~/media/files/insights/events/2017/01/need-to-know-gdpr-the-data-protection-officer-requirement-role-and-implementation/gdpr_data_protection_officer_role_requirement_and_implementation_jan17.pdf, accessed on June 2017.

DLA Piper Data Protection, "Data Protection Laws of the World: Germany (2017)", http://www.dlapiperdataprotection.com, accessed on May 2017.

Global DataHub, "The Compliance Burden Under the GDPR – Data Protection Officers", https://www.taylorwessing.com/globaldatahub/article-compliance-burden-under-gdpr-data-protection-officers, accessed on May 2017.

Golla, Sebastian J., "Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR", *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law*, Volume 8, Issue 1, 2017.

King and Wood Mallesons, "Chief Data Officer is not a Data Protection Officer", http://www.kwm.com/en/uk/knowledge/insights/a-chief-data-officer-is-not-a-data-protection-officer-20150218, accessed on April 2017.

Klug, Christoph "Improving Self-Regulation Through (Law-Based) Corporate Data Protection Officials", *Privacy Laws & Business International Newsletter*, Issue No. 63, 2002.

Kompas, "Lindungi Data Pribadi Warga", https://www.pressreader.com/indonesia/kompas/20170530/281771334145041, accessed on June 2017.

Koops, Bert-Jaap, "The Trouble with European Data Protection Law", *International Data Privacy Law*, 2014.

Meyer, David, "What Will Mandatory DPOs Look Like under the GDPR? Germany Could Tell You", https://iapp.org/news/a/what-will-mandatory-dpos-look-like-

under-the-gdpr-germany-could-tell-you/, accessed on July 2017.

Olavsrud, Thor, "Data Protection Officer Role Will Be Key If You Operate in the E.U." http://www.cio.com/article/2395511/legislation/data-protection-officer-role-will-be-key-if-you-operate-in-the-e-u-.html, accessed on June 2017.

Payne, Chris, "GDPR and the DPO: Five Things to Know about Your Next Job Vacancy", https://www.tripwire.com/state-of-security/security-data-protection/gdpr-and-the-dpo-five-things-to-know-about-your-next-job-vacancy/, accessed on July 2017.

Rosarita Niken Widiastuti, "Perlindungan Data Pribadi: Menghadirkan Negara Dalam Melindungi Segenap Bangsa dan Memberikan Rasa Aman Pada Seluruh Warga Negara", https://www.slideshare.net/idigf/id-igf-2016-hukum1-perlindungan-data-pribadi-menghadirkan-negara, accessed on March 2017.

Rothkegel, Tobias, "New Data Protection Rules: What is a Data Protection Officer and Do I Need One?", http://marketinglaw.osborneclarke.com/data-and-privacy/new-data-protection-rules-what-is-a-data-protection-officer-and-do-i-need-one/, accessed on May 2017.

Terstegge, Jeroen, "Data Protection and the New Face of Privacy Compliance", https://www.pmpartners.nl/wp-content/uploads/2014/07/Businesscompliance-Data-Protection-and-the-new-face-of-privacy-compliance.pdf, accessed on May 2017.

The International Association of Privacy Professionals, "The GDPR Demands 75k DPOs", https://iapp.org/media/pdf/DPA-Whitepaper.pdf, accessed on April 2017.

Wahyudi Djafar (et.al.), "Perlindungan Data Pribadi: Usulan Pelembagaan Kebijakan dari Perspektif Hak Asasi Manusia", *Seri Internet dan HAM*, 2016.

Legal Documents

Law Number 23 of 2006 on Citizen Administration.

Ministry of Communication and Informatics Regulation Number 20 of 2016 on Personal Data Protection in Electronic Systems.

Data Protection Working Party, Statement on the Role of a Risk-Based Approach in the Data Protection Legal Frameworks, 14/EN WP 218, adopted on May 30, 2014.

Data Protection Working Party, Appendix on Core Topics in the View of Trilogue, adopted on June 17, 2015.

European Union General Data Protection Regulation, adopted on April 27, 2016.

Data Protection Working Party, Guidelines on Data Protection Officers, 16/EN WP 243, adopted on December 13, 2016.

Ministry of Communication and Informatics, Bill of Law on the Personal Data Protection, http://peraturan.go.id/rancangan-undang-undang-tentang-perlindungan-data-pribadi.html, accessed on March 2017.

Naskah Akademik RUU tentang Perlindungan Data Pribadi, http://www.bphn.go.id/data/documents/na_perlindungan_data_pribadi.pdf, accessed on June 2017.

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, or the General Data Protection Regulation, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012PC0011#document1, accessed on June 2017.