

Petugas/Pejabat Pelindungan Data Pribadi dalam Ekosistem Perlindungan Data Pribadi: Indonesia, Uni Eropa dan Singapura

Siti Yuniarti

Business Law Program, Law Department, Faculty of Humanities,
Bina Nusantara University
Jakarta 11480, Indonesia
yuniarti@binus.ac.id

*Correspondence: yuniarti@binus.ac.id

ABSTRACT

Personal data protection regulations have been adopted by 137 countries until the beginning of 2022. In addition to creating a data protection agency, personal data protection regulations have also created new professionalism, namely personal data protection officers. The main role of the data protection officer is to ensure compliance with personal data protection regulations placing the function of a data protection officer as an important factor in the personal data protection ecosystem. It raises the question of how the role of data protection officers in the personal data protection ecosystem when it is analyzed from the attributes attached to the profession. Therefore, using the normative juridical research method, this paper attempts to describe the role of the data protection officer in the personal data protection ecosystem by analyzing the attributes attached to the profession through a comparison of the General Data Protection Regulation (GDPR) in the European Union, Personal Data Protection Act Singapore and the draft of personal data regulation in Indonesia. This paper concluded that the existence of a data protection officer is part of the data protection regulation, whether it appears as an obligation or in terms of certain conditions. Independency of the data protection officer and organizational support is essential to optimize the data protection officer's role which has been adopted on GDPR. It also noticed the presence of data protection officers as a service to fulfill the needs of data protection officers by organizations. Further research regarding the attribute of data protection officers as studied in this paper is needed since the Indonesia personal data protection bill will impact many sectors, both private and public sectors.

Keywords: *Personal Data Protection; GDPR; Singapore; Indonesian.*

ABSTRAK

Regulasi perlindungan data pribadi telah diadopsi oleh 137 negara sampai dengan awal tahun 2022. Selain memunculkan lembaga perlindungan data pribadi (data protection agency), regulasi perlindungan data pribadi juga memunculkan suatu profesionalitas baru yakni pejabat/petugas perlindungan data pribadi (data protection officer). Peran utama data protection officer adalah memastikan kepatuhan terhadap regulasi perlindungan data pribadi sehingga menempatkan fungsi data protection officer sebagai aktor penting dalam ekosistem perlindungan data pribadi. Mengingat peran utama data protection officer tersebut selanjutnya menimbulkan pertanyaan bagaimana peran data protection officer dalam ekosistem perlindungan data pribadi tersebut ditinjau dari atribut-atribut yang melekat pada profesi tersebut. Oleh karena itu dengan menggunakan metode penelitian yuridis normatif, makalah ini berupaya menggambarkan peran data protection officer dalam ekosistem perlindungan data pribadi melalui perbandingan pengaturan dalam General Data Protection Regulation di Uni Eropa, Personal Data Protection Act Singapura dan Rancangan Undang-undang Perlindungan Data Pribadi di Indonesia. Dari penelitian yang dilakukan eksistensi data protection officer menjadi bagian dari regulasi

perlindungan data pribadi, baik muncul sebagai suatu kewajiban bagi seluruh organisasi maupun dalam hal terpenuhinya suatu kondisi tertentu. Perlunya penekanan pada independensi dan dukungan organisasi agar data protection officer optimal dalam menjalankan fungsi dan tugasnya yang mana telah diatur secara komprehensif dalam GDPR serta kehadiran layanan data protection officer as a service sebagai upaya memenuhi kebutuhan akan data protection officer oleh organisasi. Penelitian lanjutan terkait atribut-atribut data protection officer yang diteliti dalam makalah ini diperlukan mengingat RUU PDP Indonesia apabila disahkan akan membawa banyak implikasi baik pada sektor privat maupun publik.

Kata Kunci: *Perlindungan Data Pribadi; GDPR; Singapura; Indonesia*

PENDAHULUAN

Perihal *data protection officer* bukanlah suatu hal yang baru (Cliza & Spataru Negara, 2018). Regulasi perlindungan data pribadi di Jerman telah lama mengenal konsep *data protection officer* (Korff & Georges, 2019). Setelah *General Data Protection Officer* (GDPR) berlaku efektif pada tahun 2018, perhatian terhadap *data protection officer* pun meningkat.

Sanksi denda dalam jumlah yang signifikan menjadi salah satu alasan organisasi memastikan keberadaan *data protection officer*. Walaupun pada dasarnya kewajiban penunjukan *data protection officer* hanya muncul bagi organisasi tertentu yakni apabila organisasi tersebut memenuhi kondisi sebagaimana dipersyaratkan dalam *Article 37* GDPR. Terlebih jangkauan GDPR berlaku ekstra teritorial yang memungkinkan untuk menjangkau organisasi yang bertindak selaku *data controller* dan *data processor* di luar teritori Uni Eropa. Tercatat denda terbesar yang dijatuhkan dibawah regulasi GDPR sampai dengan awal tahun 2022 dikenakan kepada Amazon Europe Core S.a.r.l yakni sebesar €746,000,000 pada bulan Juli 2021 (Affairs, 2022). Tentunya insiden kegagalan perlindungan data pribadi juga terkait dengan reputasi dan kepercayaan (*trust*) pengguna terhadap organisasi. Berdasarkan laporan Deloit, 44% konsumen percaya bahwa organisasi lebih memperhatikan mengenai privasi konsumen setelah GDPR berlaku (Deloit, 2016).

Di kawasan ASEAN, perlindungan data pribadi menjadi salah satu pembahasan pada *ASEAN Community Blueprint* di tahun 2015 dan terakhir menghasilkan *Framework on Personal Data Protection* tahun 2016 ((Telmin, 2016). Respon terhadap rezim perlindungan data pribadi juga diikuti dengan adopsi regulasi perlindungan data pribadi oleh beberapa negara di ASEAN, termasuk Singapura. Regulasi perlindungan data pribadi Singapura diatur dalam *Personal Data Protection Act 2012* (Singapore R. o., *Personal Data Protection Act 2012*, 2012) sebagaimana telah diubah dengan *Personal Data Protection (Amendment) Act 2020* (Singapore R. o., *Personal Data Protection (Amendment) Act 2020*, 2020) atau secara bersama-sama disebut sebagai UU PDP Singapura. Singapura merupakan negara pertama dan satu-satunya di dunia yang telah secara resmi memiliki kerangka kerja kompetensi dan peta jalan pelatihan *data protection officer* (Komunikasi, 2021).

Sampai dengan awal tahun 2022, Indonesia masih merupakan salah satu negara di kawasan ASEAN yang belum memiliki regulasi khusus pada level undang-undang terkait perlindungan data pribadi. Rancangan Undang-undang Perlindungan Data Pribadi Indonesia atau RUU PDP Indonesia yang telah dibahas oleh DPR dan Pemerintah sejak Desember 2015 sampai dengan saat ini masih belum rampung (DPR, 2022). RUU PDP versi Sekretariat Negara 2019 memuat pula ketentuan perihal *data protection officer*, selain perihal kelembagaan perlindungan data pribadi (*Data Protection Agency*) (Kominfo, n.d.). Pararel dengan proses pembahasan RUU PDP, Kementerian Komunikasi dan Informatika (Kominfo) menyusun *Grand Design* Pembentukan Ekosistem *Data Protection Officer* (DPO) Indonesia atau *Grand Design* DPO Indonesia sebagai salah satu upaya persiapan terhadap keberadaan fungsi dan posisi *data protection officer*. *Grand Design* DPO Indonesia memuat *road map* dan rencana strategis pembentukan ekosistem *data protection officer* periode 2022-2026.

Seiring dengan meningkatnya transaksi lintas batas negara, jumlah negara yang mengadopsi perlindungan data pribadi serta peningkatan infrastruktur internet, kebutuhan terhadap *data protection officer* semakin meningkat. Menurut *International Association of Privacy Professionals* (IAPP) pada tahun 2016 saja setidaknya 75,000 orang *data protection officer* dibutuhkan di Eropa dan negara-negara yang memiliki hubungan bisnis dengan Eropa (Heimess & Sam, 2016). Olehkarenanya, penelitian ini bermaksud menganalisa atribut yang melekat pada *data protection officer* untuk memberikan gambaran perihal peran *data protection officer* dalam ekosistem perlindungan data pribadi. Diharapkan hal tersebut dapat memberikan gambaran awal bagi organisasi yang melakukan pengumpulan dan pemrosesan data di Indonesia.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian hukum normatif yang menitikberatkan pada nilai, norma dan aturan tertulis. Sebagai penelitian hukum normatif, penelitian ini dilakukan melalui peraturan perundang-undangan dan studi pustaka yang tergolong data sekunder. Perundang-undangan yang digunakan adalah *Personal Data Protection Act 2012 Singapore* sebagaimana telah diubah dengan *Personal Data Protection (Amendment) Act 2020*, *General Data Protection Regulation* dan RUU PDP Indonesia. Kemudian, pendekatan penelitian yang digunakan adalah pendekatan undang-undang yang berfokus pada peraturan yang terkait dengan topik penelitian dan pendekatan perbandingan yang fokus pada pengaturan atribut yang menjadi pembahasan pada negara-negara yang dibandingkan yakni terminologi, persyaratan kewajiban penunjukan *data protection officer*, fungsi dan tugas, *DPO as a service* dan independensi *data protection officer*. Sesuai dengan metode pendekatan yang digunakan, penelitian ini terbatas pada analisa berdasarkan aspek regulasi.

HASIL DAN PEMBAHASAN

Rezim perlindungan data pribadi pada dasarnya berupaya memastikan bahwa proses pengumpulan, pengolahan, penyimpanan dan penghapusan/penghancuran data oleh pengendali data atau *data controller* dan pemroses data atau *data processor* dilakukan dengan menerapkan prinsip-prinsip perlindungan data pribadi serta meletakkan hak subyek data sebagai hal utama. Terkait dengan hal tersebut, rezim perlindungan data pribadi melahirkan suatu kelembagaan yakni lembaga perlindungan data (*data protection agency*) dan suatu profesionalitas baru yakni *data protection officer*. Kelembagaan menjalankan fungsi perumusan kebijakan, kerjasama dan pengawasan terhadap pelaksanaan regulasi perlindungan data. Adapun *data protection officer* menjalankan serangkaian fungsi guna memastikan kepatuhan *data controller* dan *data processor* terhadap regulasi perlindungan data pribadi.

Sikus pengumpulan dan pemrosesan data pribadi pada dasarnya melibatkan 3 (tiga) pihak yakni subyek data atau pemilik data, *data controller* dan *data processor*. Baik dalam GDPR maupun RUU PDP Indonesia, *data controller* pada dasarnya suatu istilah yang merujuk pada pihak yang menentukan tujuan dan kendali atas pemrosesan data pribadi. Istilah *data processor* merujuk pada pihak yang melakukan pemrosesan data pribadi untuk kepentingan *data controller*. Adapun UU PDP Singapura menggunakan terminologi *data intermediary* yang merujuk pada “*an organization which process personal data on behalf of another organization but does not include an employee of that other organization* (sebuah organisasi yang memproses data pribadi atas nama organisasi lain tetapi tidak termasuk karyawan dari organisasi lain tersebut)”. Terkait dengan tujuan penulisan guna menggambarkan peran *data protection officer* dalam ekosistem perlindungan data pribadi, berikut adalah analisa berdasarkan atribut-atribut yang melekat pada peran *data protection officer* yakni terminologi, persyaratan kewajiban penunjukan *data protection officer*, fungsi dan tugas, *data protection officer as a service* dan independensi jabatan *data protection officer*.

Terminologi

Dalam regulasi perlindungan data pribadi, terminologi yang digunakan untuk merujuk pada fungsi dan tugas *data protection officer* beragam. Dalam regulasi perlindungan data pribadi di Cina digunakan terminologi *personal information protection officer*; terminologi *information officer* digunakan di Afrika Selatan, *privacy officer* di Australia dan *privacy official* di Amerika Serikat.

Tabel 1. Perbandingan Penggunaan Terminologi *Data Protection Officer*

| Komponen | GDPR | UU PDP Singapura | RUU PDP Indonesia |
|-----------------------|--------------------------------|--------------------------------|---|
| Terminologi Digunakan | <i>Data protection officer</i> | <i>Data Protection Officer</i> | Pejabat atau Petugas yang melaksanakan fungsi perlindungan data pribadi |

Terminologi *data protection officer* digunakan dalam GDPR namun tidak diberikan pengertian secara definitif. *Article 38 (1) GDPR* menyebutkan bahwa “*the controller and the processor shall ensure that the data*

protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data (pengontrol dan pemroses wajib memastikan bahwa petugas perlindungan data adalah terlibat, dengan benar dan tepat waktu, dalam semua hal yang berkaitan dengan perlindungan data pribadi)”. Apabila merujuk pada rumusan *Article 38 (1) GDPR* tersebut di atas dan rumusan tugas dan fungsi *data protection officer* pada *Article 39 GDPR*, terminologi *data protection officer* merujuk pada suatu fungsi dalam organisasi yang memastikan kegiatan pemrosesan data pribadi yang dilakukan oleh organisasi memenuhi regulasi perlindungan data pribadi yang ada.

Dalam UU PDP Singapura, tidak ditemui secara eksplisit terminologi yang digunakan untuk merujuk pada pengertian *data protection officer*. *Article 11 (3) UU PDP Singapura* sebagai basis eksistensi *data protection officer* hanya memuat ketentuan penunjukan “...one or more individuals to be responsible for ensuring that the organization complies with this Act (...menunjuk satu atau beberapa orang yang bertanggungjawab untuk memastikan organisasi memenuhi undang-undang ini). Namun selanjutnya kebijakan yang disusun oleh *Personal Data Protection Commission Singapore* merujuk pada penggunaan terminologi *Data Protection Officer* (Singapore P. D., 2022).

RUU PDP menggunakan terminologi Pejabat atau Petugas yang melaksanakan fungsi perlindungan data pribadi. Penjelasan Pasal 45 ayat (1) RUU PDP menjelaskan bahwa yang dimaksud dengan Pejabat atau petugas yang melaksanakan fungsi perlindungan data pribadi adalah pejabat atau petugas yang bertanggungjawab untuk memastikan pemenuhan kepatuhan atas prinsip perlindungan data pribadi dan mitigasi risiko perlindungan data pribadi. Dalam *Grand Design DPO Indonesia* dikemukakan bahwa terminologi *data protection officer* berbeda dengan lingkup dari Pejabat atau Petugas yang melaksanakan fungsi perlindungan data pribadi sebagaimana dimaksud dalam Pasal 45 (1) RUU PDP Indonesia. Perbedaan tersebut merujuk pada perbedaan fungsi utama yakni tugas *data protection officer* diartikan sebagai konsultan internal yang memastikan fungsi perlindungan data pribadi dilaksanakan dalam organisasinya dengan tugas pelaksanaannya yang diemban oleh okupasi atas jabatan yang berbeda. Sementara, Pejabat atau Petugas yang melaksanakan fungsi perlindungan data pribadi yang meliputi fungsi legal dan kepatuhan, tata kelola, manajemen dan teknis (Komunikasi, 2021). Guna penyeragaman terminologi, makalah ini menggunakan terminologi *data protection officer*.

Pesyaratan Kewajiban Penunjukan *Data Protection Officer*

Penunjukan *data protection officer* oleh organisasi diatur secara berbeda dalam ketiga regulasi yang dijadikan perbandingan. Terpenuhinya kondisi yang menjadi persyaratan menimbulkan kewajiban penunjukan *data protection officer* oleh organisasi berdasarkan GDPR dan RUU PDP Indonesia. Adapun penunjukan *data protection officer* dibawah regulasi UU PDP Singapura merupakan suatu keharusan bagi setiap organisasi yang melakukan pengumpulan dan pengolahan data pribadi.

Tabel 2. Perbandingan Kewajiban Penunjukan *Data Protection Officer*

| Komponen | GDPR | UU PDP Singapura | RUU PDP Indonesia |
|---|------------------------------------|-------------------------------|------------------------------------|
| Penunjukan <i>Data Protection Officer</i> | Apabila terpenuhi kondisi tertentu | Wajib bagi seluruh organisasi | Apabila terpenuhi kondisi tertentu |

Merujuk pada GDPR, kewajiban penunjukan *data protection officer* berlaku sepanjang organisasi tersebut memenuhi salah satu kondisi yang dipersyaratkan dalam *Article 37 GDPR* yakni: (a) organisasi merupakan organisasi publik (*public authority*); (b) pemrosesan data pribadi merupakan kegiatan inti yang dilakukan secara teratur dan sistematis serta dalam skala besar; dan/atau (c) kegiatan inti dari *data controller* atau pengolah terdiri dari pemrosesan data kategori khusus dalam skala besar (*Article 9 GDPR*) atau data pribadi terkait pemidanaan dan pelanggaran (*Article 10 GDPR*).

Dari kondisi yang menyebabkan organisasi menunjuk *data protection officer* tersebut, lingkup “kegiatan inti (*core activity*)” dan “skala besar” merupakan kata kunci yang menjadi tolak ukur selain atribut seperti teratur dan sistematis, data kategori khusus dan data terkait pemidanaan. Makna dari “kegiatan inti (*core activity*)” dari *data controller* dijelaskan dalam *Recital 97 GDPR* sebagai “*primary activities and do not relate to the processing of personal data as ancillary activities* (kegiatan utama dan tidak berhubungan dengan pemrosesan data pribadi sebagai kegiatan tambahan)”. Adapun makna “skala besar” tidak dijabarkan lebih lanjut dalam GDPR.

Pada dasarnya GDPR merupakan pengaturan berbasis prinsip (*principled based regulation*) yang memberikan kebebasan untuk melakukan penafsiran pada norma yang terkandung didalamnya. *Guidelines on Data Protection Officers* (DPOs) 2017 selanjutnya mencoba menjabarkan lebih lanjut terkait lingkup “kegiatan inti (*core activity*)” dan “skala besar”. Menurut *Guidelines on Data Protection Officers* (DPOs) 2017, “kegiatan inti (*core activity*)” pada dasarnya merupakan operasional kunci yang diperlukan untuk mencapai tujuan *data controller* atau *data processor*. Namun demikian, kegiatan inti (*core activity*) tidak boleh diartikan sebagai mengecualikan kegiatan dimana pemrosesan data merupakan bagian yang tidak terpisahkan dari aktivitas *data controller* dan/atau *data processor*. Misal, kegiatan inti rumah sakit adalah memberikan layanan kesehatan. Namun, layanan kesehatan tersebut tidak dapat diberikan secara aman dan efektif tanpa memproses data kesehatan. Olehkarenanya, memproses data harus dianggap sebagai kegiatan inti rumah sakit (Party, 2017).

Lebih lanjut, terminologi “skala besar” direkomendasikan dalam *Guidelines on Data Protection Officers* (DPOs) 2017 merujuk pada komponen-komponen berupa (a) jumlah subyek data terkait, dapat berupa spesifik jumlah atau proporsional dari populasi terkait; (b) volume data dan/atau cakupan data berbeda yang diproses; (c) durasi atau permanen aktivitas pemrosesan data; dan (d) jangkauan geografis aktivitas pemrosesan data. Komponen yang dijabarkan dalam *Guidelines on Data Protection Officers* (DPOs) 2017 masih belum menetapkan secara tegas perihal lingkup dari terminologi “skala besar”, sehingga selanjutnya komponen-komponen tersebut pada umumnya akan merujuk pada kebijakan dari *Data Protection Agency* masing-masing negara. Sebagai contoh *Data Protection Agency* Jerman telah menetapkan pemrosesan data skala besar mencakup lebih dari 5 (lima) juta orang atau setidaknya 40 persen dari jumlah penduduk yang relevan dengan memperhitungkan jenis data yang diproses serta subyek data yang terlibat dalam pemrosesan (Breitbarth, 2018).

Dibawah aturan UU PDP Singapura, penunjukan *data protection officer* berlaku bagi seluruh organisasi yang melakukan pengumpulan dan pengolahan data yang menjadi lingkup UU PDP Singapura, tanpa kecuali. Perlu digarisbawahi bahwa UU PDP Singapura mengecualikan lingkup keberlakuannya terhadap beberapa aktivitas pengumpulan dan pemrosesan data, salah satunya adalah tidak berlaku bagi badan publik (*public agency*) sebagaimana diatur dalam *Article 4* UU PDP Singapura. Perihal penunjukan *data protection officer* disebutkan secara eksplisit pada *Article 11(3)* UU PDP Singapura bahwa “*an organization must designate one or more individuals to be responsible for ensuring that the organization complies with this Act* (sebuah organisasi harus menunjuk satu atau lebih individu untuk bertanggungjawab memastikan organisasi mematuhi Undang-undang ini)”.

Penunjukan *data protection officer* yang diatur dalam RUU PDP Indonesia secara garis besar serupa dengan GDPR, yakni menjadi suatu kewajiban apabila terpenuhinya kondisi tertentu. Kondisi tertentu yang menimbulkan kewajiban bagi organisasi untuk menunjuk *data protection officer* diatur dalam Pasal 45 (2) RUU PDP Indonesia, yakni apabila: (a) pemrosesan data pribadi untuk kepentingan pelayanan publik; (b) pemrosesan merupakan kegiatan inti *data controller* memiliki sifat, ruang lingkup dan/atau tujuan yang memerlukan pemantauan secara teratur dan sistematis atas data pribadi dengan skala besar; dan (c) kegiatan inti *data controller* dalam skala besar untuk data pribadi yang bersifat spesifik dan/atau data pribadi yang berkaitan dengan tindak pidana. Dalam RUU PDP, termasuk dalam data pribadi yang bersifat spesifik yakni data dan informasi kesehatan, data biometric, data genetika, kehidupan/orientasi seksual, pandangan politik, catatan kejahatan, data anak, data keuangan pribadi; dan/atau data lainnya sesuai dengan ketentuan peraturan perundang-undangan. Ketentuan lebih lanjut perihal *data protection officer* nantinya diatur lebih lanjut dalam suatu Peraturan Pemerintah.

Fungsi dan Tugas *Data Protection Officer*

Fungsi dan tugas *data protection officer* pada regulasi yang dianalisa pada dasarnya merujuk pada 3 (tiga) fungsi utama yakni kepatuhan, risiko dan respon. Kepatuhan merujuk pada tidak saja fungsi pengawasan pada aktivitas, namun juga membangun kesadaran internal organisasi. Risiko merujuk pada fungsi manajemen risiko. Serta respon merujuk pada fungsi sebagai narahubung bagi subyek data, organisasi dan *data protection agency*. Olehkarenanya, posisi *data protection officer* merupakan titik temu dan kordinasi antara antara subyek data, *data protection agency* dan organisasi.

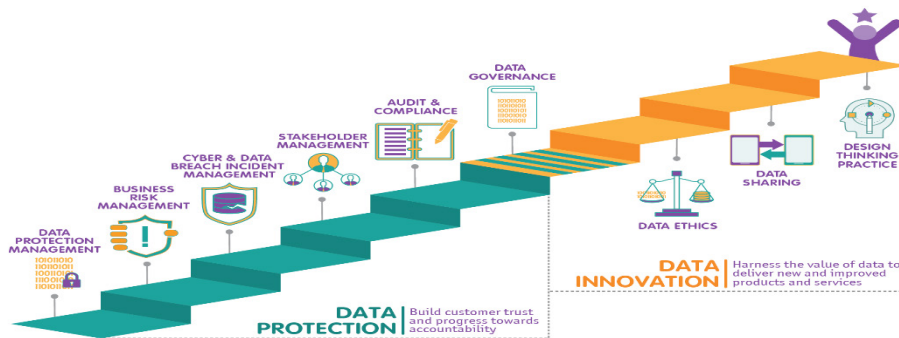
Tabel 3. Fungsi dan Tugas *Data Protection Officer* Menurut GDPR, UU PDP Singapura dan RUU PDP Indonesia

| | |
|--------------------------|---|
| GDPR | <i>Article 38 dan 39 GDPR</i> Narahubung bagi subyek data; Memberikan informasi dan saran kepada organisasi tentang kewajiban berdasarkan GDPR dan ketentuan perlindungan data pribadi anggota Uni Eropa lainnya; Memantau kepatuhan organisasi terhadap GDPR dan ketentuan perlindungan data pribadi anggota Uni Eropa lainnya, memberikan pelatihan kepada karyawan dan melakukan audit; Melakukan <i>data protection impact assessment (Article 35 GDPR)</i> ; Bekerja sama dengan otoritas perlindungan data; Narahubung bagi otoritas perlindungan data termasuk konsultasi pendahuluan (<i>Article 36</i>) dan hal lain yang dianggap perlu. |
| UU PDP Singapura | Personal Data Protection Commission Singapore: Bertanggungjawab termasuk namun tidak terbatas pada: Memastikan kepatuhan terhadap PDP ketika membangun dan menerapkan kebijakan dan proses penanganan data pribadi; Mendorong budaya perlindungan data pribadi diantara karyawan dan mengkomunikasikan kebijakan perlindungan data pribadi kepada pemangku kepentingan; Mengelola pertanyaan dan keluhan terkait perlindungan data pribadi; Menginformasikan kepada manajemen tentang risiko apapun yang mungkin timbul terkait data pribadi; dan Berhubungan dengan otoritas perlindungan data pribadi tentang masalah perlindungan data pribadi, jika diperlukan. |
| RUU PDP Indonesia | Pasal 46 (1) Pejabat atau petugas yang melaksanakan fungsi perlindungan data pribadi memiliki tugas paling sedikit: Menginformasikan dan memberikan saran untuk Pengendali Data Pribadi atau Prosesor Data Pribadi agar mematuhi ketentuan dalam Undang-undang ini; Memantau dan memastikan kepatuhan terhadap Undang-undang ini dan kebijakan Pengendali Data Pribadi atau Prosesor Data Pribadi, termasuk penugasan, tanggung jawab, peningkatan kesadaran dan pelatihan pihak yang terlibat dalam pemrosesan Data Pribadi, dan audit terkait; Memberikan saran mengenai penilaian dampak perlindungan Data Pribadi dan memantau kinerja Pengendali Data Pribadi dan Prosesor Data Pribadi; dan Berkoordinasi dan bertindak sebagai narahubung untuk isu yang berkaitan dengan pemrosesan Data Pribadi, termasuk melakukan konsultasi mengenai mitigasi risiko dan/atau hal lainnya. |

Optimalisasi fungsi *data protection officer* didorong dalam GDPR dengan memastikan organisasi melibatkan *data protection officer* dalam segala hal terkait perlindungan data dan menyediakan sumber-sumber (*resources*) yang diperlukan oleh *data protection officer* untuk menjalankan tugasnya sebagaimana diatur dalam *Article 38 (1) dan (2) GDPR*. Dukungan organisasi terhadap optimalisasi fungsi *data protection officer* berupa: (a) dukungan terhadap fungsi *data protection officer* oleh manajemen; (b) waktu yang cukup bagi *data protection officer* untuk memenuhi tugasnya; (c) dukungan yang memadai dalam hal sumber daya keuangan, infrastruktur (tempat, fasilitas, peralatan) dan staff, apabila diperlukan; (d) informasi penunjukan *data protection officer* kepada seluruh karyawan; (e) akses ke layanan lain dalam organisasi sehingga *data protection officer* dapat menerima bantuan/dukungan, masukan atau informasi penting dari layanan/unit lainnya; dan (f) pelatihan berkelanjutan (Party, 2017).

Walaupun salah satu fungsi dan tugas *data protection officer* adalah memastikan kepatuhan terhadap regulasi, namun pemahaman terhadap regulasi bukanlah satu-satunya kompetensi yang dibutuhkan dari seorang *data protection officer*. Kompetensi *data protection officer* merujuk pada *Article 37 (5) GDPR* diatur secara umum yakni ditunjuk berdasarkan kualitas profesional, memiliki pengetahuan tentang hukum dan praktik perlindungan data pribadi serta mampu memenuhi fungsi dan tugas yang ditentukan dalam *Article 39 GDPR*. Tingkatan pengetahuan yang diperlukan tergantung pada kompleksitas pemrosesan data dan ukuran organisasi. Dalam *Guidelines on Data Protection Officers (DPOs) 2017*, keterampilan dan keahlian yang relevan dengan fungsi dan tugas *data protection officer* adalah ahli dalam hukum dan praktik perlindungan data pribadi di level nasional dan Uni Eropa, memahami operasional pemrosesan, memahami teknologi informasi dan keamanan data (*data security*), pengetahuan tentang sektor bisnis dan organisasi serta kemampuan untuk mempromosikan budaya perlindungan data dalam organisasi (Party, 2017)

Kompetensi *data protection officer* Singapura merujuk pada klasifikasi fungsi pekerjaan (*job function*) dari *data protection officer* tersebut, yakni *data protection executive*, *data protection officer* dan *regional data protection officer* (PDPC, 2022). Ada 6 (enam) kompetensi krusial yang wajib dimiliki oleh *data protection officer*, yakni: (1) manajemen perlindungan data; (2) manajemen risiko bisnis; (3) siber dan manajemen insiden kegagalan perlindungan data (*data breach incident*); (4) manajemen pemangku kepentingan; (5) audit dan kepatuhan; dan (6) tata kelola data (*data governance*). Minimal kompetensi bagi *data protection officer* adalah manajemen perlindungan data (*data protection management*). Selain itu diperlukan pula kompetensi terkait *data innovation* yang meliputi etika data (*data ethic*), berbagi data (*data sharing*) dan *design thinking practice*. Kompetensi terkait *data innovation* dianggap perlu karena organisasi semakin memanfaatkan data sebagai aset strategis untuk produk dan layanan baru dan lebih baik. Oleh karenanya, *data protection officer* diharapkan dapat membantu organisasi dalam menggunakan data secara bertanggungjawab untuk mendukung inovasi dan memperoleh keunggulan kompetitif untuk memaksimalkan kemitraan berbagi data (*data sharing*) dengan tetap memastikan kepercayaan dan akuntabilitas (PDPC, 2022).



Gambar 1. Kompetensi Data Protection Officer Singapura (PDPC, 2022)

Dalam RUU PDP Indonesia, kompetensi *data protection officer* serupa dengan hal yang diatur dalam GDPR yakni memiliki kualitas profesional, pengetahuan mengenai hukum dan praktik perlindungan data pribadi dan kemampuan memenuhi tugas-tugas dalam Pasal 45(3) RUU PDP. Dalam *Grand Design* DPO Indonesia, kompetensi *data protection officer* dipetakan berdasarkan tujuan utama yang diturunkan dari Pasal 46 RUU PDP dan 3 (tiga) fungsi yakni fungsi kunci, fungsi utama dan fungsi dasar. Fungsi kunci merupakan fungsi-fungsi skema kompetensi yang secara spesifik diidentifikasi dengan pendekatan berbasis ketrampilan yaitu *asses*, *protect*, *sustain* dan *respond* terhadap RUU PDP. Fungsi utama merupakan tugas dan tanggungjawab *data protection officer* berdasarkan pendekatan berbasis keterampilan manajemen perlindungan data pribadi dan privasi terhadap RUU PDP. Adapun, fungsi dasar akan diuji kelayakan dan kepatutan dari pemangku kepentingan untuk memastikan fungsi dasar disepakati (Komunikasi, 2021). Selanjutnya, berdasarkan hal tersebut disusun kompetensi pelatihan bagi *data protection officer* yang diklasifikasikan menjadi tingkat dasar yang fokus pada pemahaman mengenai regulasi perlindungan data pribadi, tingkat lanjutan yang fokus pada bagaimana memenuhi ketentuan regulasi tersebut dan tingkat khusus yang sifatnya opsional disesuaikan pada masing-masing sektor (Komunikasi, 2021).

Data Protection Officer as a Services

Meningkatnya kebutuhan terhadap *data protection officer* memungkinkan dilakukannya fungsi tersebut oleh pihak lain melalui mekanisme *data protection officer as a service* atau DPOaS. DPOaS merupakan layanan yang diberikan kepada organisasi untuk memenuhi kebutuhan organisasi atas kepatuhan terhadap regulasi PDP. Hal tersebut dimungkinkan apabila regulasi perlindungan data pribadi pada yurisdiksi tersebut membuka memungkinkan pelaksanaan fungsi *data protection officer* dari eksternal dan internal organisasi.

Tabel 4. Perbandingan Eksistensi *Data Protection Officer as a Services*

| Komponen | GDPR | UU PDP Singapura | RUU PDP Indonesia |
|---|---|------------------|--|
| Eksistensi <i>Data Protection Officer as a Services</i> | Dimungkinkan. DPO dapat berasal dari eksternal atau internal organisasi. | Dimungkinkan | Dimungkinkan. DPO dapat berasal dari eksternal atau internal organisasi |

Di bawah regulasi GDPR, eksistensi *data protection officer* dimungkinkan berasal dari eksternal atau internal organisasi. Kontrak layanan (*service contract*) menjadi dasar layanan yang diberikan oleh penyelenggara DPOaS kepada organisasi. Tidak ada perbedaan fungsi dan perlindungan bagi *data protection officer* di bawah regulasi GDPR. Ketika fungsi *data protection officer* dijalankan oleh penyedia layanan eksternal, tim individu yang bekerja untuk organisasi tersebut dapat secara efektif melaksanakan tugas *data protection officer* sebagai sebuah tim, dibawah tanggung jawab kontak utama yang ditunjuk dan penanggungjawab klien. Setiap anggota organisasi eksternal yang menjalankan fungsi *data protection officer* harus memenuhi semua persyaratan yang berlaku (Party, 2017).

Penunjukan *data protection officer* dapat juga dilakukan bersama-sama oleh grup organisasi sebagaimana diatur dalam *Article 37 (2) dan (3) GDPR* sepanjang *data protection officer* tersebut dapat mudah diakses oleh setiap perusahaan. Hal tersebut juga dapat dilakukan oleh otoritas atau badan publik dengan mempertimbangkan struktur dan ukuran organisasi. Lebih lanjut, dalam hal ditunjuk satu *data protection officer* untuk beberapa organisasi, terkait dengan fungsi sebagai narahubung dengan subyek data dan *Data Protection Agency*, perlu dipastikan bahwa adanya sarana komunikasi yang memungkinkan ketersediaan akses baik berupa kehadiran petugas, hotline atau bentuk sarana komunikasi lainnya yang aman (Party, 2017).

Di Singapura, keberadaan *data protection officer* merupakan suatu kewajiban bagi setiap organisasi, termasuk usaha kecil dan menengah. Organisasi dengan keterbatasan sumber daya dapat mengalihdayakan fungsi operasional *data protection officer* kepada penyedia layanan, namun demikian tanggung jawab tetap ada pada organisasi tersebut (Singapore P. D., 2022) DPOaS adalah alternatif bagi organisasi untuk mengalihdayakan fungsi perlindungan data pribadi organisasi. Organisasi dapat menggunakan layanan DPOaS yang terdaftar pada *Infocomm Media Development Authority (IMDA)*. *IMDA* merupakan institusi di bawah *Singapore Ministry of Communications and Information (MCI)* yang memiliki tugas dan kewenangan untuk mengembangkan dan mengatur sektor informasi komunikasi dan media, termasuk perlindungan data.

Dalam RUU PDP Indonesia, setiap organisasi yang memenuhi kondisi sebagaimana disebutkan dalam Pasal 46 (1) RUU PDP wajib menunjuk seorang *data protection officer*. *Data protection officer* tersebut dapat berasal dari dalam dan/atau luar organisasi sebagaimana diatur dalam Pasal 45 (3) RUU PDP. Oleh karena itu, layanan DPOaS dapat dilakukan di Indonesia. Seseorang dapat menjadi *data protection officer* dengan fungsi tertentu untuk beberapa organisasi sekaligus selama dapat menjaga kerahasiaan dan bebas benturan kepentingan (Komunikasi, 2021) Lebih lanjut, penyelenggara DPOaS selain berbentuk perusahaan, juga dapat dilakukan oleh asosiasi kepada anggotanya (Komunikasi, 2021).

Independensi Data Protection Officer

Fungsi utama *data protection officer* pada dasarnya adalah memastikan kepatuhan organisasi terhadap regulasi perlindungan data pribadi. Merujuk pada tujuan dari perlindungan hukum data pribadi, fungsi tersebut memastikan bahwa perlindungan hukum diberikan kepada subyek data di satu sisi dan di sisi lain memastikan pengumpulan dan pengolahan data oleh organisasi dilakukan sesuai dengan prinsip-prinsip perlindungan data. Untuk mencapai hal tersebut diperlukan independensi dari *data protection officer*. Independensi tersebut diperlukan agar *data protection officer* memiliki kemandirian dalam memberikan saran dan pengawasan terhadap organisasi. GDPR secara spesifik mengakomodir perihal independensi tersebut, selain juga memunculkan kewajiban untuk menjaga kerahasiaan bagi *data protection officer*.

Dalam GDPR, setidaknya ada 3 (tiga) hal yang diatur untuk memastikan independensi *data protection officer*, yakni: (a) independensi dari instruksi/perintah oleh *data controller* dan/atau *data processor*; (b) larangan pemberhentian atau hukuman oleh *data controller* dan/atau *data processor*; serta (c) tidak adanya benturan kepentingan (*conflict of interest*). Dua komponen awal diakomodir dalam *Article 38 (3) GDPR* sebagai berikut: “*the controller and processor shall ensure that the data protection officer does not receive any instruction regarding the exercise of those tasks. He or she shall not be dismissed or penalized by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor* (Pengontrol dan pemroses harus memastikan bahwa petugas perlindungan data tidak menerima instruksi apapun mengenai pelaksanaan tugas-tugas tersebut. Ia tidak boleh diberhentikan atau dihukum oleh Pengawas atau Pengolah karena melakukan tugasnya. Petugas perlindungan data harus langsung melapor ke tingkat manajemen tertinggi dari pengontrol atau pemroses)”.

Perihal “benturan kepentingan (*conflict of interest*)” muncul karena *data protection officer* diperbolehkan untuk menjalankan fungsi atau tugas lainnya sebagaimana diatur dalam *Article 38 (6) GDPR*. Oleh karenanya, dalam hal *data protection officer* melaksanakan fungsi lain tersebut, *data controller* dan/atau *data processor* wajib memastikan bahwa fungsi atau tugas lain tersebut tidak menimbulkan benturan kepentingan dengan fungsi utama *data protection officer*. Benturan kepentingan mungkin muncul apabila *data protection officer* menempati posisi senior pada manajemen seperti *chief executive, chief operation, chief financial, chief medical officer, head of marketing department, head of human resources* atau *head of IT departments*) atau pada posisi lain yang lebih rendah dalam struktur organisasi jika posisi tersebut menentukan tujuan dan sarana pengolahan data pribadi. Termasuk pula pada benturan kepentingan apabila eksternal *data protection officer* diminta untuk mewakili *data controller* dan/atau *data processor* di pengadilan dalam kasus yang melibatkan masalah perlindungan data pribadi (Party, 2017). Di bawah regulasi GDPR, sebuah entitas dikenakan sanksi denda pada bulan April 2020 karena menunjuk *Head of compliance and risk, audit and risk management* sebagai *data protection officer* (Turku & Helga, 2020).

Jika *data protection officer* membuat keputusan strategis untuk organisasi atau jika *data protection officer* memegang peran operasional, ia mungkin terlibat dalam pengambilan keputusan tentang aktivitas pemrosesan. Padahal tugas dari *data protection officer* adalah memberikan saran, keputusan menjadi kewenangan dan tanggung jawab dari organisasi. *Data protection officer* tidak bertanggung secara pribadi atas ketidakpatuhan regulasi perlindungan data pribadi. Kepatuhan perlindungan data merupakan tanggungjawab organisasi (Party, 2017).

Dalam RUU PDP Indonesia, perihal independensi *data protection officer* tidak diatur secara eksplisit. Merujuk pada *Grand Design DPO Indonesia*, independensi dan menghindari benturan kepentingan menjadi bagian dari tujuan pemberian kewenangan dan pembekalan kompetensi yang cukup oleh organisasi kepada *data protection officer*. Terkait penugasan pada fungsi lain, *Grand Design DPO Indonesia* menyebutkan bahwa posisi pejabat pada struktur organisasi dan direksi diperbolehkan untuk menjadi *data protection officer* sepanjang dapat dijaga independensi dan bebas benturan kepentingan. Adapun, Kepala Divisi IT tidak dapat menjabat sebagai *data protection officer* karena Kepala Divisi IT merupakan bagian dari pelaksana operasional IT yang penerapan keamanan data pribadi akan menjadi sasaran evaluasi dan pemantauan *data protection officer* (Komunikasi, 2021). Tentunya kepastian mengenai hal tersebut tetap perlu menunggu pada versi final dari RUU PDP dan aturan pelaksanaannya.

KESIMPULAN

Dalam ekosistem perlindungan data pribadi, *data protection officer* memiliki peran yang esensial. Tidak hanya memastikan kepatuhan organisasi terhadap regulasi perlindungan data, juga menjadi titik temu antara organisasi, *data protection agency* dan subyek data. Kebutuhan akan *data protection officer* dapat muncul karena hal tersebut merupakan kewajiban bagi setiap organisasi atau dalam hal dipenuhinya kondisi persyaratan tertentu sesuai dengan ketentuan masing-masing regulasi. Kebutuhan *data protection officer* dalam jumlah yang cukup besar melahirkan peluang baru berupa *data protection officer as a service* sebagai pihak eksternal yang menyediakan layanan *data protection officer* kepada organisasi. Dari analisa terhadap regulasi, secara garis besar, fungsi *data protection officer* dapat diklasifikasikan menjadi fungsi kepatuhan, risiko dan respon. Dalam menjalankan fungsi dan tugas, *data protection officer* memerlukan independensi dan dukungan organisasi agar optimal dalam pelaksanaannya. Hal tersebut telah diatur secara komprehensif dalam GDPR. Hal tersebut perlu menjadi perhatian pula di Indonesia, baik dalam regulasi level undang-undang maupun peraturan pelaksanaannya. Kebutuhan dan peran yang besar dari *data protection officer* serta masih sangat muda usia regulasi perlindungan data pribadi, khususnya di Indonesia, membutuhkan penelitian-penelitian lanjutan terkait atribut-atribut yang telah dibahas dalam makalah ini. Termasuk pula penelitian lanjutan terkait korelasi atribut tersebut dengan bidang hukum lainnya.

DAFTAR PUSTAKA

- (Telmin), A. T. (2016). *Framework on Personal Data Protection*. Brunei Darusalam: ASEAN.
- Affairs, P. (2022, Maret 16). <https://www.privacyaffairs.com>. Retrieved from <https://www.privacyaffairs.com/gdpr-fines/>
- Breitbarth, P. (2018, Agustus 28). <https://iapp.org/news/a/on-large-scale-data-processing-and-gdpr-compliance/>. Retrieved from <https://iapp.org/news/a/on-large-scale-data-processing-and-gdpr-compliance/>
- Cliza, M.-C., & Spataru Negura, L.-C. (2018). The General Data Protection Regulation: what does the public authorities and bodies need to know and to do? *Juridical Tribune*, 490-501.
- Deloit. (2016). *A New Era For Privacy-GDPR Six Months on*. United Kingdom: Deloit LLP.
- DPR. (2022, Maret 16). <https://www.dpr.go.id/uu/detail/id/47>. Retrieved from <https://www.dpr.go.id/uu/detail/id/47>
- Heimess, R., & Sam, P. (2016). <https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/>. Retrieved from <https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/>
- Kominfo. (n.d.). <https://www.dpr.go.id/uu/detail/id/47>. Retrieved from <https://www.dpr.go.id/uu/detail/id/47>
- Komunikasi, K. I. (2021). *Grand Design Pembentukan Ekosistem Data Protection Officer (DPO) Indonesia*. Jakarta: Kominfo.
- Korff, D., & Georges, M. (2019). *The DPO Handbook-Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation*. Europe: T4Data.
- Party, D. P. (2017). *Guidelines on Data Protection Officers ('DPOs')*. Brussel: Data Protection Working Party.
- PDPC. (2022, Maret 20). <https://www.pdpc.gov.sg/Help-and-Resources/2020/03/DPO-Competency-Framework-and-Training-Roadmap#competencies>. Retrieved from <https://www.pdpc.gov.sg/Help-and-Resources/2020/03/DPO-Competency-Framework-and-Training-Roadmap#competencies>
- Singapore, P. D. (2022, Maret 3). <https://www.pdpc.gov.sg/Overview-of-PDPA/Data-Protection/Business-Owner/Data-Protection-Officers>. Retrieved from <https://www.pdpc.gov.sg/Overview-of-PDPA/Data-Protection/Business-Owner/Data-Protection-Officers>
- Singapore, R. o. (2012). *Personal Data Protection Act 2012*. Singapore: The Law Revision Commission.
- Singapore, R. o. (2020). *Personal Data Protection (Amendment) Act 2020*. Singapore: Republic of Singapore.
- Turku, & Helga. (2020, Juni 23). <https://iapp.org/news/a/how-to-ensure-you-appoint-an-independent-dpo/>. Retrieved from <https://iapp.org/news/a/how-to-ensure-you-appoint-an-independent-dpo/>