

# **BAB I**

## **PENDAHULUAN**

### **1.1 Latar Belakang Masalah**

Berdasarkan amanat konstitusional sebagaimana disebutkan dalam Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 alinea keempat, pemerintahan Indonesia memegang tanggung jawab untuk menyediakan perlindungan kepada seluruh bangsa dan wilayah Indonesia, mengupayakan kesejahteraan masyarakat, meningkatkan kualitas pendidikan bangsa, serta berperan aktif dalam menciptakan dunia yang damai dengan berlandaskan kemerdekaan, perdamaian berkelanjutan dan keadilan sosial. Pada lingkup peningkatan teknologi informasi serta komunikasi modern, mandat konstitusional tersebut direalisasikan melalui upaya pengamanan data personal bagi seluruh warga negara Indonesia.

Kesadaran akan pentingnya perlindungan data personal mengalami peningkatan seiring dengan pertumbuhan signifikan pengguna perangkat seluler dan internet. Berbagai insiden yang terungkap, khususnya yang berkaitan dengan kebocoran informasi pribadi yang mengarah pada tindak penipuan atau kejahatan pornografi, memperkuat urgensi pembentukan kerangka hukum untuk melindungi data personal. Pelindungan data personal yang bertujuan untuk menjaga integritas dan martabat seseorang memiliki korelasi erat dengan gagasan privasi. Selain itu, kapasitas seseorang untuk

menentukan akses terhadap penggunaan informasi dirinya juga termasuk ke dalam hak privasi.<sup>1</sup>

Prinsip perlindungan data menekankan bahwa setiap manusia memiliki otoritas terkait keputusan tentang membagikan informasi pribadinya atau tidak. Lebih lanjut, individu juga berhak menetapkan ketentuan- ketentuan dalam proses pengalihan data pribadi masing-masing. Dalam perkembangannya, perlindungan data berkaitan erat terhadap konsep hak privasi yang sudah berkembang sebagai dasar untuk membentuk hak perlindungan data personal.<sup>2</sup>

Rancangan ide Pelindungan data sendiri menyatakan bahwa keputusan terkait pembagian data pribadi merupakan kewenangan yang dimiliki sepenuhnya oleh suatu individu atau pemilik data tersebut. Selain hak tersebut, hak untuk menetapkan persyaratan terkait pemindahan data pribadi juga dimiliki oleh tiap-tiap manusia. Lebih jauh, konsep hak atas privasi juga dikenal dalam perlindungan data pribadi. Terdapat perubahan pada hak atas privasi sehingga perlindungan data pribadi dapat dijelaskan dengan hak ini.<sup>3</sup>

Pada saat ini, Indonesia sudah mulai berada di era Revolusi Industri 4.0, yang mana jaringan internet dan perangkat yang terkoneksi dapat membantu dalam berbagai aktivitas secara jarak jauh. Transformasi digital ini membawa dampak signifikan dalam kehidupan masyarakat sehari-

---

<sup>1</sup> Wahyudi Djafar dan Asep Komarudin, *Pelindungan Hak Atas Privasi di Internet- Beberapa Penjelasan Kunci*, Elsam, Jakarta, 2014, hlm. 2

<sup>2</sup> Lord Ester dan D, Pannick (ed.) dalam *ibid*, hlm. 6.

<sup>3</sup> Human Rights Committee General Comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17) seperti yang dikutip dalam *Privacy International Report*, 2013, hlm. 1-2.

hari, seperti peningkatan efisiensi kerja, pembangunan relasi sosial ekonomi, dan simplifikasi berbagai proses.<sup>4</sup>

Era ini berdampak besar ketika masyarakat dalam kehidupan sehari-harinya mulai menggunakan teknologi berbasis digital. Hal ini dapat digunakan dalam banyak bidang seperti meningkatkan produktivitas kerja, membangun relasi sosial ekonomi, dan mempermudah berbagai hal.<sup>5</sup> Terdapat pertumbuhan pesat terkait dengan teknologi informasi komunikasi berdasarkan komputer. Perkembangan teknologi ini memberikan kemudahan kepada masyarakat. Konsep ini menegaskan bahwa pilihan untuk melakukan pembagian data (*sharing data*) dan persyaratan untuk melakukan pembagian tersebut merupakan hak tiap orang atas nasibnya masing-masing. dalam sebuah komunitas.<sup>6</sup>

Dengan fokus pada langkah-langkah preventif dan pelibatan pemangku kepentingan non-pemerintah dalam mekanisme implementasinya, implementasi standar profesional dan teknis yang spesifik berdasarkan sektor dapat dilengkapi oleh pendekatan regulasi bersama dalam perlindungan data pribadi. Dalam sektor jasa keuangan di Indonesia, asosiasi industri menjalankan pengawasan terhadap entitas dalam lingkup regulasi sebagai perannya selaku "organisasi regulator mandiri". Sementara itu, pemerintah tetap menjalankan fungsi pengawasan untuk memastikan adanya implementasi yang adil dan selaras pada inisiatif industri namun tetap sesuai

---

<sup>4</sup> Klaus Schwab, *Revolusi Industri Keempat*, (Jakarta : PT. Gramedia Pustaka Utama, 2019), hal. 211 – 223.

<sup>5</sup> Syarifudin A., “Pelindungan Hukum terhadap Para Pihak di dalam Layanan Financial Technology Berbasis Peer to Peer (P2P) Lending (Studi Kasus di PT. Pasar Dana Pinjaman Jakarta)”, *Dinamika*, Vol. 26, No. 4 2020, hal. 408-421.

<sup>6</sup> Fanny Priscyllia, “Pelindungan Privasi Data Pribadi Perspektif Perbandingan Hukum”, *Jatiswara*, Vol. 34, No. 3 2019, hal. 239-249.

dengan prinsip kompetisi pasar. Alternatif implementasi regulasi bersama dapat dilakukan melalui pemberdayaan profesi Petugas Pelindungan Data yang diharapkan terciptanya praktik terbaik pada pelindungan data pribadi dengan adanya standar komunitas profesional.

Berdasarkan regulasi pelindungan data pribadi, terdapat perbedaan bahasa dari berbagai negara yang digunakan untuk mendefinisikan fungsi dan tugas *data protection officer*. Regulasi Tiongkok menggunakan istilah *personal information protection officer*, Afrika Selatan menggunakan *information officer*, Australia menggunakan *privacy officer*, dan Amerika Serikat menggunakan *privacy official*. Istilah *data protection officer* merujuk kepada fungsi pada suatu organisasi yang bertanggung jawab untuk menjamin bahwa pemrosesan data pribadi sesuai dengan regulasi yang berlaku. Undang-Undang PDP Singapura tidak secara eksplisit mencantumkan terminologi untuk *data protection officer*, sementara UU PDP Indonesia menggunakan istilah Petugas atau pejabat selaku pihak yang menjalankan tugas pelindungan data pribadi.<sup>7</sup>

Terdapat keharusan bagi organisasi yang telah memenuhi salah satu persyaratan pada hukum pelindungan data pribadi Eropa untuk menunjuk *data protection officer*. persyaratan tersebut adalah:<sup>8</sup>

- a. Organisasi merupakan organisasi publik (*public authority*);
- b. Kegiatan inti dilakukan secara teratur dan sistematis serta dalam skala besar terhadap pemrosesan data pribadi; dan/atau

---

<sup>7</sup> 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>

<sup>8</sup> *ibid*

- c. Pemrosesan data dengan kategori khusus dalam skala besar termasuk dalam kegiatan inti untuk data controller dan atau pengolah data

Organisasi harus menunjuk *data protection officer* apabila memenuhi kondisi di atas. Kata kunci serta tolak ukur selain atribut seperti teratur dan sistematis, data kategori khusus dan data terkait pemidanaan adalah "kegiatan inti (core activity)" dan "skala besar".

Pemberian sumber-sumber (resources) yang dibutuhkan oleh *data protection officer* dalam menjalankan tugasnya serta melibatkan *data protection officer* dalam seluruh Pelindungan data dilakukan untuk mengoptimalkan fungsi data protection. Dukungan yang dapat diberikan oleh organisasi untuk optimalisasi fungsi *data protection officer* berupa:<sup>9</sup>

- a. Dukungan manajemen untuk fungsi data protection officer;
- b. Alokasi waktu yang memadai untuk pelaksanaan tugas;
- c. Dukungan sumber daya finansial, infrastruktur, dan personel yang mencukupi;
- d. Sosialisasi penunjukan data protection officer kepada seluruh karyawan;
- e. Akses terhadap berbagai unit pada organisasi untuk memperoleh dukungan dan informasi; dan
- f. Program pengembangan kompetensi berkelanjutan.

Peningkatan permintaan terkait data protection officer membuka peluang pelaksanaan profesi tersebut melalui mekanisme data protection officer as a service (DPOaaS). DPOaaS adalah jasa yang disediakan untuk membantu organisasi menjalankan kewajiban pemenuhan persyaratan

---

<sup>9</sup> Party, D. P. (2017). Guidelines on Data Protection Officers ('DPOs'). Brussel: Data Protection Working Party.

terhadap ketentuan PDP. Hal ini bisa dilakukan apabila ketentuan perlindungan data pribadi dalam kekuasaan tersebut mengizinkan dilakukannya fungsi data protection officer dari pihak luar maupun pihak dalam organisasi.

Kehadiran *data protection officer* bisa didapatkan secara eksternal maupun internal organisasi. Dasar layanan yang diperlukan dan disediakan oleh penyelenggara DPOaaS kepada organisasi adalah kontrak layanan (service contract). Berdasarkan peraturan GDPR, tidak ada perbedaan bagi *data protection officer* baik secara fungsi maupun perlindungan. Jika tugas sebagai data protection officer dilaksanakan oleh penyedia layanan eksternal, tim yang ditugaskan untuk mendukung organisasi dapat menjalankan perannya secara efektif sebagai *data protection officer* secara kolektif, dengan tanggung jawab berada pada kontak utama yang ditunjuk dan penanggung jawab klien. Terdapat kriteria berlaku yang harus dipenuhi oleh *data protection officer* untuk menjalankan tugasnya bagi seluruh anggota organisasi eksternal.<sup>10</sup>

Sebuah grup organisasi dapat bersama-sama melakukan pemilihan *data protection officer* dengan syarat adanya kemudahan akses bagi masing-masing perusahaan terhadap *data protection officer* tersebut. Otoritas atau badan publik juga dapat melakukan pemilihan bersama setelah mengadakan pertimbangan terkait struktur dan ukuran organisasi. Selanjutnya, apabila beberapa organisasi memilih satu *data protection officer* sebagaimana disebutkan sebelumnya, perlu dipastikan bahwa terdapat sarana komunikasi

---

<sup>10</sup> Party, D. P. (2017). Guidelines on Data Protection Officers ('DPOs'). Brussel: Data Protection Working Party.hlm37

seperti petugas, hotline, atau sarana komunikasi lainnya yang aman guna memenuhi fungsi narahubung antara subyek data dan Data Protection Agency.<sup>11</sup> Terdapat alternatif untuk mengalihdayakan fungsi Pelindungan data pribadi bagi organisasi melalui DPOaaS. Layanan DPOaaS yang terdaftar pada Infocomm Media Development Authority (IMDA) dapat digunakan oleh organisasi. IMDA yang telah disebutkan di atas adalah badan yang bertugas dan berwenang untuk mengembangkan dan mengatur sektor informasi komunikasi dan media, termasuk Pelindungan data. Badan ini dinaungi oleh Singapore Ministry of Communications and Information (MCI).

Di Indonesia sendiri, berdasarkan UU PDP, *data protection officer* wajib dipilih oleh organisasi apabila telah memenuhi persyaratan yang ditetapkan pada Pasal 46 (1). Sesuai dengan pasal 45 (3) UU PDP, ketentuan terkait *data protection officer* dapat dipilih baik dari internal maupun eksternal organisasi. Oleh karenanya, jasa DPOaaS dapat dilakukan di Indonesia. Seseorang diperbolehkan menjalankan fungsinya selaku *data protection officer* terhadap beberapa organisasi secara bersamaan dengan syarat menjaga kerahasiaan dan tidak adanya benturan kepentingan.<sup>12</sup> Lebih jauh lagi, selain berbentuk perusahaan, suatu asosiasi dapat melakukan penyelenggaraan DPOaaS kepada anggota asosiasi tersebut. Pada dasarnya, *data protection officer* bertugas untuk memastikan organisasi tersebut telah patuh dengan peraturan terkait Pelindungan data pribadi yang diberikan kepada subyek data dan juga menekankan bahwa seluruh proses pengumpulan dan pengolahan

---

<sup>11</sup> *Ibid*, Hal 40

<sup>12</sup> 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 Data Protection Officer (DPO) Indonesia. Jakarta: Kominfo.

data di organisasi sudah mengikuti prinsip terkait Pelindungan data. Maka dari itu, independensi dari *data protection officer* sangat diperlukan. Dalam prosesnya, *data protection officer* harus memiliki pendirian terhadap saran dan pengawasan kepada organisasi sehingga perlu menjadi badan independen. Independensi *data protection officer* diberikan oleh GDPR yang juga mewajibkan *data protection officer* untuk menjaga kerahasiaan data.

Berdasarkan GDPR, ada tiga peraturan yang digunakan untuk memastikan *data protection officer* tetap independen, yakni:

- a. Bebas terhadap instruksi/perintah pengendali dan/atau pengolah data;
- b. Pelindungan dari pemberhentian atau sanksi oleh pengendali dan/atau pengolah data; dan
- c. Bebas dari konflik kepentingan<sup>13</sup>

Ketentuan “benturan kepentingan (*conflict of interest*)” diberikan untuk memastikan *data protection officer* dalam menjalankan tugasnya dapat melaksanakan tugas utama atau lainnya secara bersamaan. Oleh karena itu, Ketika *data protection officer* menjalankan tugas lainnya tersebut, data controller dan/atau processor harus memastikan bahwa tidak terdapat benturan kepentingan antara dua tugas tersebut.

Benturan kepentingan dapat terjadi bila *data protection officer* juga bertugas pada posisi apapun yang menetapkan tujuan dan saran pengolahan data pribadi serta posisi manajemen senior seperti *chief executive*, *chief operation*, *chief financial*, *chief medical officer*, *head of marketing*

---

<sup>13</sup> 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.

*department, head of human resources atau head of IT departments*). Benturan kepentingan juga dapat dilakukan pada *data protection officer* eksternal yang hadir pada suatu perkara pengadilan untuk mewakili data controller dan/atau processor tentang Pelindungan data pribadi.<sup>14</sup>

Berdasarkan peraturan GDPR, sanksi berupa denda akan dikenakan kepada suatu badan apabila menunjuk *data protection officer* dari Head of compliance and risk, audit and risk management. *data protection officer* memungkinkan untuk terlibat dalam proses pengambilan keputusan terkait aktivitas pemrosesan jika ia memegang peran operasional atau menetapkan keputusan strategis. Hal ini bertentangan dengan tugas *data protection officer* selaku pemberi saran, sedangkan keputusan adalah kewenangan dan tanggung jawab organisasi. Segala ketidakpatuhan terhadap peraturan Pelindungan data pribadi bukan menjadi tanggung jawab *data protection officer*. Hal itu merupakan tanggung jawab organisasi.<sup>15</sup>

Sifat independen dari *data protection officer* tidak diatur secara eksplisit dalam UU PDP. Berdasarkan dari *Grand Design* terkait DPO di Indonesia, pembekalan kompetensi dan pendelegasian kewenangan dari organisasi kepada *data protection officer* bertujuan untuk memastikan independensi dan penghindaran atas benturan kepentingan. *Grand Design* DPO Indonesia juga menyatakan bahwa pejabat dan direksi pada suatu organisasi dapat menjadi *data protection officer* sesuai dengan penugasan

---

<sup>14</sup> 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.

<sup>15</sup> 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/>

pada fungsi lain selama individu tersebut dapat menjaga independensinya dan bebas dari benturan kepentingan. Namun, mengingat bahwa kepala IT merupakan bagian pelaksana operasional IT, Kepala Divisi tersebut tidak dapat menjadi *data protection officer* karena pelaksanaan divisi IT adalah subjek evaluasi.<sup>16</sup>

## 1.2 Rumusan Masalah

Permasalahan pentingnya *Data Protection Officer* dalam melakukan fungsi perlindungan data pribadi masih menjadi sebuah tantangan untuk menanggulangi masalah kebocoran data yang hingga saat ini masih sangat mungkin terjadi. Maka dari itu tulisan ini dibuat untuk mengkaji sejauh mana peran *Data Protection officer* dalam melaksanakan fungsi Pelindungan Data Pribadi dengan fokus masalah sebagai berikut :

- 1.2.1 Bagaimana Pengaturan Hukum atas Penugasan *Data Protection Officer* Pada Sektor Jasa Keuangan Non Bank Ditinjau Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi?
- 1.2.2 Bagaimana Implementasi dan Penerapan UU PDP pada Lembaga Jasa Keuangan Non Bank yang berkewajiban untuk menugaskan *Data Protection Officer* ?

## 1.3 Tujuan Penelitian

Yang menjadi tujuan dari penelitian ini antara lain sebagai berikut :

- 1.2.1 Memberikan solusi atas permasalahan hukum terkait Pelindungan Data Pribadi khususnya di Industri Keuangan Non Bank yang

---

<sup>16</sup> DPR. (2022, Maret 16). <https://www.dpr.go.id/uu/detail/id/47>. Retrieved from <https://www.dpr.go.id/uu/detail/id/47>

diharapkan bermanfaat bagi pemangku kepentingan dalam Pelindungan Data Pribadi dan pengembangan Ilmu Hukum.

1.2.2 Mengembangkan ide/teori hukum atau mekanisme penyelesaian sengketa hukum atas permasalahan dalam implementasi pelindungan data Pribadi.

1.2.3 Menganalisis regulasi terkait Pembentukan Data Protection Officer khususnya di Industri Keuangan Non Bank sebagaimana diatur dalam Undang-undang Pelindungan Data Pribadi untuk pengembangan ilmu hukum.

#### **1.4 Manfaat Penelitian**

Penelitian ini diharapkan memberikan manfaat teoretis dan praktis sebagai berikut:

1.4.1 Menjadi referensi implementasi Data Protection Officer dalam pelaksanaan fungsi pemanfaatan dan pelindungan data pribadi yang sesuai bagi industri keuangan non-bank berdasarkan Undang-undang Pelindungan Data Pribadi.

1.4.2 Hasil penelitian ini diharapkan dapat memberikan kontribusi dan sumbangan pemikiran bagi *Lembaga Jasa Keuangan Non Bank* dalam menstandarisasi penerapan *Data Protection Officer* dalam melakukan pemanfaatan data an pelindungan data pribadi agar terhindar dari sanksi baik perdata maupun pidana serta sanksi administratif dari regulator.

## **1.5 Sistematika Penulisan**

Penelitian ini disusun dalam lima bab dengan sistematika sebagai berikut:

### **BAB I PENDAHULUAN**

Menguraikan Latar Belakang Masalah, Rumusan Masalah, Tujuan Penelitian, Manfaat Penelitian, dan Sistematika Penulisan.

### **BAB II TINJAUAN PUSTAKA**

Membahas Tinjauan Teori dan Tinjauan Konseptual untuk memberikan pemahaman terkait permasalahan yang dibahas.

### **BAB III METODE PENELITIAN**

Menjelaskan Jenis Penelitian, Jenis Data, Metode Perolehan Data, Pendekatan Penelitian, dan Analisis Data.

### **BAB IV HASIL PENELITIAN DAN ANALISIS**

Memaparkan Hasil Penelitian tentang Pelindungan Data Pribadi dan Analisis berdasarkan bahan penelitian yang dikaitkan dengan Rumusan Masalah.

### **BAB V KESIMPULAN DAN SARAN**

Berisi Kesimpulan dan Saran yang dirumuskan berdasarkan pembahasan dari Bab Pertama hingga Bab Terakhir.