

Perlindungan Data Pribadi MENGENALI HAK-HAK SUBJEK DATA, SERTA KEWAJIBAN PENGENDALI DAN PROSESOR DATA



Wahyudi Djafar
M. Jodi Santoso

Perlindungan Data Pribadi
MENGENALI HAK-HAK SUBJEK DATA, SERTA
KEWAJIBAN PENGENDALI DAN PROSESOR DATA



Lembaga Studi dan Advokasi Masyarakat (ELSAM)

PERLINDUNGAN DATA PRIBADI:

Mengenali Hak-Hak Subjek Data, serta Kewajiban Pengendali dan Prosesor Data

Penulis:

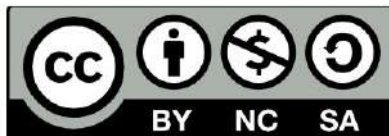
Wahyudi Djafar

M. Jodi Santoso

Pertama kali dipublikasikan dalam bahasa Indonesia oleh:

**Lembaga Studi dan Advokasi Masyarakat (ELSAM), dengan dukungan dari Australian Government-
Department of Foreign Affairs and Trade (DFAT), 2019.**

*Semua penerbitan ELSAM didedikasikan kepada para korban pelanggaran hak asasi manusia
selain sebagai bagian dari upaya pemajuan dan perlindungan hak asasi manusia di Indonesia.*



Except where otherwise noted, content on this paper is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0). Some rights reserved.

DAFTAR ISI

DAFTAR ISI	i
A. MEMAHAMI ALASAN PEMROSESAN DATA PRIBADI	1
B. MENGENALI HAK-HAK SUBJEK DATA PRIBADI	5
B.1. Hak Atas Informasi (<i>Right to Information</i>)	08
- Informasi mudah dimengerti	08
- Jenis informasi	08
- Waktu penyampaian informasi kepada subjek data	09
B.2. Hak Akses (<i>Right to Access</i>)	09
B.3. Hak Memperbaiki, Memblokir dan Menghapus (<i>Rights to Rectify, Restrict, and Erasure</i>)	11
- Hak untuk memperbaiki (<i>right to rectify</i>)	11
- Hak untuk memblokir (<i>right to restriction/block of processing</i>)	12
- Hak untuk menghapus (<i>rights to erasure—right to be forgotten</i>)	12
B.4. Hak untuk Menolak (<i>Right to Object</i>)	13
B.5. Hak Portabilitas Data (<i>Right to Data Portability</i>)	14
B.6. Hak Terkait Pengambilan Keputusan Otomatis dan Pembuatan Profil (<i>Rights Related to Automated Decision Making and to Profiling</i>)	15
B.7. Hak atas Pemulihan yang Efektif (<i>Right to an Effective Remedy</i>)	17
- Hak mengajukan pengaduan ke lembaga pengawas independen	17
- Hak mengajukan pengaduan ke pengadilan	17
B.8. Hak atas Kompensasi dan Pertanggungjawaban (<i>Right to compensation and Liability</i>)	18
C. PENGECUALIAN DAN BATASAN PENGECUALIAN	19
D. MEMASTIKAN KEWAJIBAN PENGENDALI DAN PROSESOR DATA	21
D.1. Tanggung Jawab dan Kepatuhan	21
- Tanggung Jawab Pengendali Data	22
- Tanggung Jawab dalam Pemrosesan Bersama	22
- Tanggung Jawab Prosesor Data	22
- Petugas Perlindungan Data (<i>Data Protection Officer</i>)	24
D.2. Memastikan Keamanan Pemrosesan	24
D.3. Merekam Kegiatan Pemrosesan	25
D.4. Kerahasiaan Data Pribadi	25
D.5. Pemberitahuan Pelanggaran	26
- Pelanggaran Perlindungan Data dan Jenis Pelanggaran	26
- Pemberitahuan Pelanggaran kepada Otoritas Pengawas	27
- Komunikasi dengan Pemilik Data Pribadi	27
D.6. Penilaian Dampak Perlindungan Data	28
E. TRANSFER DATA INTERNASIONAL	28
PROFIL ELSAM	30

A. MEMAHAMI ALASAN PEMROSESAN DATA PRIBADI

Perlindungan data pribadi merupakan bentuk penghormatan khusus hak privasi.¹ Tidak diperbolehkan untuk mengumpulkan, menggunakan atau mengungkapkan data pribadi seorang individu kecuali: ada persetujuan dari pemilik data atau disahkan/diharuskan oleh hukum dan peraturan.² Pengumpulan dan penyimpanan informasi pribadi di komputer, bank data dan perangkat lain, baik oleh otoritas publik atau individu atau badan privat, harus diatur oleh hukum. Negara harus memastikan bahwa informasi pribadi seseorang tidak sampai ke tangan orang yang tidak diizinkan oleh hukum untuk menerima, memproses dan menggunakannya, dan tidak pernah digunakan untuk tujuan yang tidak sesuai dengan hukum.³

Secara umum pemrosesan data pribadi hanya diperbolehkan dan sah jika didasarkan pada satu dasar hukum (*legal ground*) dari sejumlah alasan berikut ini:

- (1) ada persetujuan (*consent*) dari subjek data.
- (2) pelaksanaan kontrak (*performance of contract*) dimana subjek data menjadi pihak atau untuk mengambil langkah-langkah atas permintaan subjek data sebelum masuk ke dalam kontrak.
- (3) untuk kepatuhan dan kewajiban hukum (*legal obligation*).
- (4) untuk melindungi kepentingan vital (*vital interest*) subjek data atau orang lain.
- (5) untuk pelaksanaan tugas kepentingan umum (*public interest*) atau dalam pelaksanaan wewenang resmi pengendali data.
- (6) untuk tujuan kepentingan sah (*legitimate interest*) yang dilakukan oleh pengendali atau pihak ketiga, kecuali jika kepentingan tersebut dikesampingkan oleh kepentingan, hak atau kebebasan dari subjek data.

Salah satu dasar sahnya pemrosesan data pribadi adalah adanya persetujuan dari pemilik data pribadi atau disebut sebagai subjek data. Substansi penting dari adanya alasan persetujuan adalah penyelenggaraan data pribadi menempatkan subjek data sebagai pihak yang mengendalikan pemrosesan data pribadinya. Persetujuan dapat berupa pernyataan tertulis, atau bentuk lainnya, termasuk dengan cara elektronik. Pengendali data pribadi yang memproses data harus dapat menunjukkan bahwa mereka meminta dan mendapatkan persetujuan dari pemilik data pribadi, ketika menggunakan dasar hukum ini dalam pemrosesannya.⁴

Meski demikian, alasan persetujuan bukan satu-satunya dasar bagi keabsahan pemrosesan data pribadi, ada dasar hukum lainnya. Sebagai salah satu alasan dan prinsip keabsahan, persetujuan tidak boleh dilihat sebagai pengecualian dari prinsip-prinsip perlindungan data lainnya, tetapi sebagai upaya perlindungan. Persetujuan pemilik data merupakan dasar untuk keabsahan, dengan tidak mengabaikan penerapan prinsip-prinsip lain.⁵

¹ UN Doc. A/HRC/17/27, Report of The Special Rapporteur on the Promotion and Protection of The Right to Freedom of Opinion and Expression. para 58 (May 16, 2011).

² ASEAN Framework on Personal Data Protection: Principles of Personal Data Protection: Principles of Consent, Notification and Purpose.

³ UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, available at: <https://www.refworld.org/docid/453883f922.html>.

⁴ Privacy International, *The Keys to Data Protection* (2018), hlm. 63-64.

⁵ EU Article 29 Data Protection Working Party, "Opinion 15/2011 on the definition of consent", 01197/11/EN WP187, Adopted on 13 July 2011 (EU WP 01197/11/EN WP187).

Persetujuan subjek data harus merupakan indikasi yang diberikan secara bebas, berdasar informasi yang benar, spesifik, dan indikasi yang tidak ambigu tentang keinginan subjek data melalui pernyataan atau tindakan afirmatif, menandakan persetujuan untuk pemrosesan data pribadi yang berkaitan dengannya.⁶ Dengan demikian, persetujuan harus diberikan secara bebas, spesifik, mudah dimengerti dan tidak ambigu. Persetujuan yang sah semestinya mengandung elemen-elemen:

- *diberikan secara bebas*, “... *freely given* ...” berarti persetujuan hanya valid jika pemilik/ subjek data dapat menggunakan pilihan secara nyata, dan tidak ada risiko penipuan, intimidasi, paksaan atau konsekuensi negatif yang signifikan jika ia tidak menyetujui. Jika konsekuensi dari persetujuan merusak kebebasan pilihan individu, persetujuan tidak akan menjadi bebas.⁷ Persetujuan bebas berarti keputusan sukarela, oleh seorang individu yang memiliki semua datanya, diambil tanpa adanya paksaan dalam bentuk apa pun, baik itu sosial, finansial, psikologis atau lainnya.⁸ Persetujuan tidak dianggap diberikan secara bebas jika subjek data tidak memiliki pilihan asli atau pilihan bebas atau tidak dapat menolak atau menarik persetujuan tanpa merugikan.⁹
- *Spesifik*, agar valid, persetujuan harus spesifik. Persetujuan bersifat umum tanpa menentukan tujuan yang tepat dari pemrosesan tidak dapat diterima. Persetujuan harus dapat dipahami dan merujuk dengan jelas dan tepat pada ruang lingkup dan konsekuensi dari pemrosesan data. Ini tidak dapat diterapkan pada serangkaian kegiatan pemrosesan yang terbuka. Ini berarti persetujuan berlaku terbatas.¹⁰ Persetujuan khusus harus berhubungan dengan situasi konkret yang didefinisikan dengan baik dalam pemrosesan data.¹¹
- Mendapat informasi atau *informed consent* adalah persetujuan oleh subjek data berdasarkan pada pemahaman tentang fakta dan implikasi dari suatu tindakan. Subjek data harus diberikan, dengan cara yang jelas dan dapat dimengerti, informasi yang akurat dan lengkap dari semua masalah yang relevan, seperti sifat dari data yang diproses, tujuan pemrosesan, penerima transfer yang mungkin, dan hak-hak subjek data.¹²
- Tidak ambigu, indikasi yang jelas tentang keinginan subjek data yang dengannya dia, dengan pernyataan atau tindakan afirmatif yang jelas, menandakan persetujuan untuk pemrosesan data pribadi yang berkaitan dengannya.

Selain itu undang-undang juga harus memberikan perlindungan khusus berkaitan dengan sehubungan dengan data pribadi mereka, karena mereka mungkin kurang menyadari risiko, konsekuensi dan perlindungan dan hak-hak mereka sehubungan dengan pemrosesan data pribadi mereka. Undang-

⁶ EU General Data Protection Regulation, Article 4 (11): consent’ of the data subject.

⁷ EU WP 01197/11/EN WP187).

⁸ EU Article 29 Data Protection Working Party, “Opinion 15/2011 Working Document on the Processing of Personal Data Relating to Health in Electronic Health Records (EHR), 00323/07/EN WP 131 Adopted on 15 February 2007 (EU WP 00323/07/EN WP 131).

⁹ EU General Data Protection Regulation, Recital 42.

¹⁰ EU WP 01197/11/EN WP187.

¹¹ EU WP 00323/07/EN WP 131.

¹² EU WP 00323/07/EN WP 131, EU WP 01197/11/EN WP187.

undang harus mengatur, khususnya untuk penggunaan data pribadi anak-anak untuk tujuan pemasaran, membuat profil pribadi, atau pengumpulan dan penggunaan data pribadi anak ketika menggunakan layanan yang ditawarkan langsung kepada anak. Persetujuan dari pemegang tanggung jawab orang tua seharusnya tidak diperlukan dalam konteks layanan pencegahan atau konseling yang ditawarkan langsung kepada seorang anak.¹³ Di Eropa, sehubungan dengan penyediaan layanan informasi masyarakat secara langsung kepada seorang anak, pemrosesan data pribadi seorang anak dianggap sah menurut hukum jika anak tersebut setidaknya berusia 16 tahun. Jika anak di bawah usia 16 tahun, pemrosesan semacam itu hanya akan sah jika dan sejauh persetujuan itu diberikan atau disahkan oleh pemegang tanggung jawab orang tua atas anak tersebut. Negara dapat menetapkan usia yang lebih rendah asalkan usia tidak lebih rendah di bawah 13 tahun.¹⁴

Lebih jauh subjek data pribadi juga memiliki hak untuk menarik persetujuan (*withdrawing consent*) kapan saja, dengan mudah, gratis, dan tidak ada konsekuensi negatif. Hak untuk menarik persetujuan harus diberitahukan kepada subjek data sebelum subjek data memberikan persetujuan. Ini berarti bahwa sebelum mengumpulkan data, pengendali data wajib memberitahukan kepada subjek data tentang hak untuk menarik persetujuan. Jika subjek data menarik persetujuan, maka pengendali data harus mengonfirmasi subjek data bahwa permintaan mereka telah diproses, persetujuan mereka ditarik, dan data mereka dihapus. Tidak ada persyaratan untuk memberikan alasan penarikan dan tidak ada risiko konsekuensi negatif selain penghentian manfaat yang mungkin berasal dari penggunaan data yang disepakati sebelumnya. Penarikan persetujuan harus semudah memberikan persetujuan. Secara khusus EU General Data Protection Regulation pada Pasal 7 tentang persetujuan menyebutkan:

1. Jika pemrosesan didasarkan pada persetujuan, Penyelenggara/pengontrol harus dapat menunjukkan bahwa subjek data telah menyetujui untuk memproses data pribadinya.
2. Jika persetujuan subjek data diberikan dalam pernyataan tertulis yang juga memuat masalah lain:
 - permintaan persetujuan harus disajikan secara jelas dapat dibedakan dari masalah lain,
 - dalam bentuk yang mudah dipahami dan mudah diakses,
 - menggunakan formulir yang jelas dan mudah diakses,
 - menggunakan bahasa sederhana.
 - Bagian mana pun dari pernyataan tersebut yang merupakan pelanggaran terhadap Peraturan ini tidak akan mengikat.
3. Subjek data memiliki hak untuk menarik persetujuannya kapan saja.
 - Penarikan persetujuan tidak akan memengaruhi keabsahan pemrosesan berdasarkan persetujuan sebelum penarikannya.
 - Sebelum memberikan persetujuan, pemilik data harus diberitahu bahwa pemilik data akan mudah untuk menarik pemberian persetujuan.
4. Ketika menilai apakah persetujuan diberikan secara bebas, harus dipertimbangkan, antara lain apakah kinerja kontrak, termasuk penyediaan layanan, tergantung pada persetujuan terhadap pemrosesan data pribadi yang tidak diperlukan untuk kinerja kontrak itu.¹⁵

¹³ EU General Data Protection Regulation, Recital 38.

¹⁴ EU General Data Protection Regulation, Art. 8 (1).

¹⁵ EU General Data Protection Regulation, Article 7: Conditions for consent.

Berikutnya, pemrosesan data pribadi sah menurut hukum jika didasarkan pada alasan melaksanakan isi kontrak (*performance of contract*) dimana subjek data sebagai pihak alasan ini mencakup hubungan pra-kontrak. Jika satu pihak perlu memproses data untuk tujuan pelaksanaan kontrak, maka pemrosesan tersebut sah selama diperlukan untuk mengambil langkah-langkah atas permintaan subjek data sebelum masuk ke dalam kontrak.¹⁶

Sementara itu, alasan pemrosesan karena kepatuhan atau kewajiban hukum berlaku untuk pengendali data baik sektor publik maupun swasta. Pada sektor swasta, Perusahaan atau pengusaha yang menjalankan kewajiban memproses data karyawan untuk alasan perpajakan dan jaminan sosial. Agar tidak terjadi penyalahgunaan data pribadi, undang-undang harus mengatur secara tegas tentang tujuan pemrosesan, menetapkan spesifikasi pengendali, jenis data pribadi yang akan diproses, subjek data yang terkait, entitas yang menjadi tujuan data dapat diungkapkan, batasan tujuan, periode penyimpanan dan tindakan lain untuk memastikan pemrosesan yang sah dan adil.¹⁷

Berkaitan dengan kepentingan umum (*public interest*), tidak semua undang-undang mendefinisikan dengan jelas. Ketidaktepatan definisi tentang pengertian 'kepentingan publik' dan interpretasinya yang luas, menimbulkan banyak celah penyalahgunaan data pribadi. Untuk menghindari penyalahgunaan data pribadi dengan alasan kepentingan publik, otoritas pengawas independen dalam perlindungan data pribadi perlu melakukan pengujian secara berkala tentang 'kepentingan publik', khususnya terkait dengan jenis data pribadi sensitif yang diproses.¹⁸

Seperti halnya alasan kepentingan umum, pemrosesan data dengan alasan untuk kepentingan yang sah (*legitimate interest*) juga perlu diatur secara jelas. Dalam pemrosesan data, pengendali data harus memberikan informasi secara jelas kepada pemilik data tentang kepentingan sah secara spesifik yang menjadi dasar pemrosesan data. Ketika menggunakan alasan hukum ini, subjek data memiliki hak untuk menolak setiap saat terhadap pemrosesan, dengan alasan yang berkaitan dengan situasi khususnya. Pengendali data harus menghentikan pemrosesan, kecuali jika menunjukkan alasan sah untuk melanjutkannya.¹⁹

Selain itu, dalam konteks pemrosesan data pribadi untuk tujuan pembuatan profil, pengumpulan dan pemrosesan data pribadi hanya dapat dilakukan jika diizinkan oleh hukum dan diperlukan untuk keperluan kepentingan yang sah dari pengendali atau pihak ketiga atau pihak-pihak yang profil atau datanya diungkapkan, kecuali jika kepentingan tersebut ditimpa oleh hak-hak dasar dan kebebasan subjek data.²⁰

Terakhir terkait pemrosesan data pribadi untuk tujuan ilmiah, historis, atau statistik cakupannya memang sangat luas. Oleh karena itu, untuk menghindari penyalahgunaan dan interpretasi yang luas alasan tersebut, perlu ada sebuah kerangka penyelenggaraan/pemrosesan, seperti:

- Ada kebutuhan untuk kejelasan tentang apa tujuan statistik dan ilmiah. Rincian lebih lanjut harus dimasukkan dalam perturan perundang-undangan dan/atau pedoman yang dikembangkan

¹⁶ EU General Data Protection Regulation, Article. 6 (1) (b)., Modernised Convention 108, para. 46.

¹⁷ EU General Data Protection Regulation, Recital 45.

¹⁸ Privacy International, *The Keys to Data Protection... Op.Cit.*

¹⁹ EU General Data Protection Regulation, Article 21 (1).

²⁰ Council of Europe, Recommendation CM/Rec (2010)13 and Explanatory Memorandum on The Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling, adopted by the Committee of Ministers of the Council of Europe. on 23 November 2010.

- untuk mendefinisikan lebih lanjut.
- Dasar tersebut tidak boleh mengecualikan pengontrol data atau prosesor dari semua kewajiban mereka, dan mereka harus menyediakan perlindungan yang sesuai untuk pemrosesan data pribadi untuk tujuan ini.
- Perlindungan mencakup dan memastikan bahwa data tidak akan digunakan untuk mengambil keputusan berkaitan dengan pemilik data bahwa pemrosesan dilarang jika akan menyebabkan kerugian.
- Subjek data harus tetap memiliki hak atas data mereka termasuk hak untuk mendapat informasi dan hak untuk menolak data mereka diproses untuk tujuan ini.

B. MENGENALI HAK-HAK SUBJEK DATA PRIBADI

Subtansi penting dari hukum perlindungan data pribadi adalah adanya pengaturan tentang perlindungan hak individu atau disebut sebagai subjek data.²¹ Bahkan *ASEAN Framework on Personal Data Protection* dalam uraian tentang *Prinsples of Consent, Notification and Purpose* dengan tegas menyatakan bahwa “... tidak boleh mengumpulkan, menggunakan atau mengungkapkan data pribadi seorang individu kecuali: (i) individu tersebut telah diberitahu dan menyetujui tujuan pengumpulan, penggunaan atau pengungkapan dirinya. data pribadi; atau (ii) pengumpulan, penggunaan atau pengungkapan tanpa pemberitahuan atau persetujuan disahkan atau diharuskan oleh hukum dan peraturan nasional...”²²

Lebih jauh *ASEAN Framework on Personal Data Protection*, sebagai kerangka kerja yang memuat kesepakatan dan keinginan dasar negara anggota ASEAN, tidak memuat secara rinci hak-hak subjek data. Uraian tentang hak subjek data menjadi bagian dari prinsip-prinsip perlindungan data pribadi. Prinsip-prinsip Perlindungan data pribadi yang memuat hak pemilik data dalam *ASEAN Framework On Personal Data Protection* adalah: *Consent, Notification and Purpose, Accuracy of Personal Data, Security Safeguards, Access and Correction, Transfers to Another Country or Territory, Retention, Accountability*.²³ Sebagai gambaran di Kawasan, UU perlindungan Data Pribadi Philipina 2012 (Republic Act 10173 – Data Privacy Act of 2012), mengatur enam hak subjek data pribadi, yaitu: (i) hak atas informasi, (ii) hak akses; (iii) hak perbaikan; (iv) hak untuk menanggapi, menarik, pemblokiran, menghapus atau menghancurkan; (v) ganti rugi; dan (vi) hak atas portabilitas data.²⁴

Pelindungan hak subjek data berkaitan erat dengan prinsip transparansi pemrosesan data pribadi dan kewajiban pengendali serta prosesor data pribadi. OECD dalam *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* menegaskan bahwa seharusnya ada kebijakan umum tentang keterbukaan, perkembangan, praktik, dan kebijakan berkenaan dengan data pribadi. Sarana harus tersedia untuk menetapkan keberadaan dan sifat data pribadi, dan tujuan utama penggunaannya, serta identitas dan tempat tinggal pengontrol data. Prinsip keterbukaan (*transparency/openness*) dapat dipandang sebagai prasyarat keberlakuan prinsip partisipasi individu, yaitu prinsip

²¹ Pembahasan mengenai siapa dan apa subjek data lihat dalam Wahyudi Djafar dan M. Jodi Santoso, *Perlindungan Data Pribadi: Konsep, Instrumen, dan Prinsipnya*, (Jakarta: ELSAM, 2019).

²² *ASEAN Framework on Personal Data Protection: Prinsples of Consent, Notification and Purpose*.

²³ *ASEAN Framework on Personal Data Protection: Principles of Personal Data Protection*.

²⁴ Philipina Republic Act 10173 – Data Privacy Act of 2012, Sec. 16. Sec. 18.

perlindungan data yang memberikan hak kepada subjek data.²⁵

Dalam *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980 (amandemen 2013)* dan *APEC Privacy Framework 2004 (amandemen 2015)* tidak mengatur secara khusus hak-hak pemilik data tetapi masuk dalam/bagian dari uraian prinsip-prinsip keterbukaan dan prinsip partisipasi individu. Tentang *Individual Participation Principle* diuraikan bahwa seorang individu harus memiliki hak:

- a. untuk memperoleh informasi dari pengendali data berkaitan dengan apakah pengendali data memiliki data yang berkaitan dengan itu.
- b. untuk berkomunikasi dengannya, tentang data yang berkaitan dengannya dalam waktu yang wajar, jika ada biaya yang diperlukan, dengan cara yang masuk akal, dan dalam bentuk yang mudah dipahami subjek data.
- c. untuk diberikan alasan jika permintaan yang dibuat berdasarkan sub-ayat (a) dan (b) ditolak, dan untuk dapat menantang penolakan tersebut.
- d. untuk menggugat berkaitan dengan data pribadi dirinya dan jika berhasil, data dihapus, diperbaiki, diselesaikan atau diubah.

Mekanisme yang dirumuskan oleh OECD di atas banyak diterapkan di Amerika Serikat, yang menggunakan prinsip-prinsip yang diatur dalam *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* sebagai acuan.²⁶

Sementara dalam EU GDPR, pengaturan tentang transparansi diletakkan pada BAB III tentang Hak Subjek Data.²⁷ Sedangkan EU Modernised Convention 108 meletakkan ketentuan transparansi sebelum pengaturan tentang hak data subjek. Kaitannya dengan hak subjek data, disebutkan dalam EU *Modernised Convention 108* pada ketentuan Pasal 9:

1. Setiap individu memiliki hak:
 - a. tidak tunduk pada keputusan yang secara signifikan mempengaruhi dirinya hanya berdasarkan pemrosesan data otomatis tanpa pertimbangannya dipertimbangkan.
 - b. untuk mendapatkan, berdasarkan permintaan, pada interval yang wajar dan tanpa penundaan atau pengeluaran yang berlebihan, konfirmasi pemrosesan data pribadi yang berkaitan dengannya, komunikasi dalam bentuk data yang dapat dimengerti yang diproses, semua informasi yang tersedia tentang asal mereka, tentang pelestarian periode serta informasi lain yang harus disediakan oleh pengontrol untuk memastikan transparansi pemrosesan sesuai dengan Pasal 8 paragraf 1.
 - c. untuk mendapatkan, berdasarkan permintaan, pengetahuan tentang alasan pemrosesan data yang mendasarinya di mana hasil pemrosesan tersebut diterapkan kepadanya.
 - d. keberatan kapan saja, dengan alasan yang berkaitan dengan situasinya, dengan pemrosesan data pribadi tentang dia kecuali pengontrol menunjukkan alasan yang

²⁵ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980-amandemen 2013), Detail Comment Openness Principle dan Par 57 dan 58.

²⁶ NITS, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology. NITa Special Publication 800-122.

²⁷ Ibid., BAB III mengatur tentang Hak Subjek Data yang terdiri dari Bagian 1 (Transparansi dan modalitas).

- sah untuk pemrosesan yang mengesampingkan kepentingan atau haknya dan kebebasan mendasar.
- e. untuk mendapatkan, berdasarkan permintaan, secara gratis dan tanpa penundaan, perbaikan atau penghapusan yang berlebihan, tergantung dari masalahnya, dari data tersebut jika ini sedang, atau telah, diproses bertentangan dengan ketentuan Konvensi ini.
 - f. untuk mendapatkan pemulihan berdasarkan Pasal 12 di mana hak-haknya berdasarkan Konvensi ini dilanggar.
 - g. untuk mendapatkan manfaat, apa pun kebangsaan atau tempat tinggalnya, dari bantuan otoritas pengawas dalam arti Pasal 15, dalam melaksanakan hak-haknya berdasarkan Konvensi ini.
2. Paragraf 1.a tidak akan berlaku jika keputusan disahkan oleh undang-undang di mana pengontrol tunduk dan yang juga menetapkan langkah-langkah yang sesuai untuk melindungi hak, kebebasan, dan kepentingan subjek data.

Sedikit berbeda dengan pengaturan dalam *EU General Data Protection Regulation* yang mengatur perihal hak-hak subjek data secara lebih rinci dan detail.

B.1. Hak Atas Informasi (*Right to Information*)

Subjek data pribadi memiliki hak untuk mendapatkan informasi dari pengendali data secara transparan, lengkap, dan mudah diakses, dengan menggunakan bahasa yang jelas dan mudah dimengerti berkaitan dengan pemrosesan data pribadi, pada saat data pribadi diperoleh, jika data pribadi diperoleh tidak langsung dari subjek data, atau dalam jangka waktu yang wajar setelah memperoleh data pribadi, tetapi paling lambat dalam waktu satu bulan jika data pribadi diperoleh dari sumber lain.

Informasi yang harus diberikan pengendali data kepada subjek data mencakup dan tidak terbatas pada: *identitas penyelenggara, tujuan pemrosesan serta dasar hukum pemrosesan, penerima atau kategori penerima data pribadi, untuk mentransfer data pribadi ke negara ketiga atau organisasi internasional dan tingkat perlindungannya, periode penyimpanan data pribadi, serta tersedianya hak subjek data berkaitan dengan hak akses, hak perbaikan, menghapus data, pembatasan memproses, atau hak portabilitas, hak untuk menarik persetujuan setiap saat, hak untuk mengajukan pengaduan, pemulihan, dan kompensasi, keberadaan pengambilan keputusan otomatis dan pembuatan profil, serta konsekuensi dari kegagalan menyediakan data* (Rekomendasi Materi Muatan tentang Hak Atas Informasi).

Tujuan hak mendapatkan dan/atau diberi informasi adalah bahwa subjek data dapat mengambil keputusan yang tepat untuk menggunakan sistem atau layanan serta memberikan data pribadi mereka secara sadar. Untuk itu subjek data harus diberi tahu siapa pengendali data, informasi apa yang dikumpulkan dari subjek data, apa hak subjek data, mengapa dilakukan pengumpulan dan pemrosesan data, bagaimana data diproses, bagaimana akses terhadap data.²⁸

Hak atas informasi tidak bergantung atas permintaan subjek data tetapi keharusan dan menjadi

²⁸ Baca Privacy International, *The Keys to Data Protection...* hlm 51

kewajiban pengendali data pribadi untuk memberikan informasi kepada subjek data. Individu (subjek data) memiliki hak untuk mendapatkan informasi dan harus diberi informasi berkaitan penggunaan dan pemrosesan data pribadi mereka, baik data pribadi yang mereka berikan secara langsung ke *controller* atau data pribadi mereka yang didapat *controller* dari sumber lain.

- **Informasi mudah dimengerti**

Informasi yang disampaikan pengendali data kepada subjek data harus disampaikan secara transparan, singkat dan lengkap, dapat diakses dengan mudah, menggunakan bahasa yang jelas dan mudah dimengerti. Informasi disediakan dalam bentuk tertulis. Informasi disampaikan tanpa penundaan yang berlebihan dan tanpa biaya.²⁹ Kecuali ada permintaan dari subjek data yang tidak berdasar atau berlebihan, atau sifatnya mengulang, maka pengendali data dapat membebaskan biaya yang wajar atau menolak permintaan.³⁰

- **Jenis informasi**

Jika pengendali data memperoleh data pribadi langsung dari pemilik data, maka pengendali data wajib memberikan informasi kepada subjek data, berupa:³¹

- a. identitas dan detail kontak pengendali dan perwakilan pengendali (jika ada).
- b. perincian kontak petugas perlindungan data (jika ada).
- c. tujuan pemrosesan serta dasar hukum pemrosesan data.
- d. pemrosesan yang didasarkan kepentingan sah dan pengecualiannya.
- e. penerima atau kategori penerima data pribadi.
- f. keinginan untuk mentransfer data pribadi ke negara ketiga atau organisasi internasional dan tingkat perlindungannya.
- g. untuk memastikan pemrosesan yang adil dan transparan, informasi tambahan yang harus disediakan adalah:³²
 - (1) periode penyimpanan data pribadi.
 - (2) tersedianya hak subjek data berkaitan dengan hak akses, hak perbaikan, menghapus data, pembatasan pemrosesan, atau hak portabilitas.
 - (3) adanya hak untuk menarik persetujuan setiap saat, tanpa mempengaruhi keabsahan pemrosesan berdasarkan persetujuan sebelumnya (berkaitan dengan persetujuan subjek data atas pemrosesan data pribadinya untuk satu atau lebih tujuan spesifik).
 - (4) hak untuk mengajukan pengaduan ke otoritas pengawas.
 - (5) informasi tentang menyediakan data pribadi sebagai kewajiban atau sukarela.
 - (6) keberadaan pengambilan keputusan otomatis dan pembuatan profil.
 - (7) konsekuensi dari kegagalan menyediakan data.

Terhadap data pribadi yang diperoleh dari sumber selain subjek data, maka informasi yang harus diberikan pengendali kepada subjek data adalah selain informasi di atas, ditambah informasi kategori

²⁹ Modernised Convention 108, Art. 8 (1) (b). General Data Protection Regulation, Article 13 (5).

³⁰ EU General Data Protection Regulation, Article 12 (5).

³¹ EU General Data Protection Regulation, Article 13 (1), Modernised Convention 108, Article 9 (1) (b).

³² EU General Data Protection Regulation, Article 13 ayat (1).

data pribadi yang bersangkutan dan asal sumber data pribadi berasal, serta apakah berasal dari sumber yang dapat diakses publik.³³

- ***Waktu penyampaian informasi kepada subjek data***

Terhadap data pribadi diperoleh langsung dari subjek data, pengendali data harus memberikan semua informasi kepada subjek data pada saat data pribadi diperoleh.³⁴ Sedangkan terhadap data yang tidak diperoleh langsung dari subjek data, pengendali data wajib memberikan informasi tentang pemrosesan data kepada subjek data dalam jangka waktu yang wajar setelah memperoleh data pribadi, tetapi paling lambat dalam waktu satu bulan, dengan memperhatikan keadaan khusus di mana data pribadi diproses. Selain itu, jika data pribadi digunakan untuk komunikasi dengan subjek data, paling lambat pada saat komunikasi pertama dengan subjek data tersebut harus diinformasikan, dan apabila disampaikan kepada penerima lain, selambat-lambatnya ketika data pribadi pertama kali diungkapkan.³⁵

B.2. Hak Akses (*Right to Access*)

Subjek data pribadi dapat mengajukan permintaan akses yang memadai berkaitan dengan pengendali dan pemrosesan data pribadi, perlindungan dan pemenuhan hak subjek data, serta salinan atas data pribadi miliknya kepada pengendali data pribadi yang mengelola data pribadi miliknya (Rekomendasi Materi Muatan tentang Hak Hak Akses).

Hak akses adalah hak esensial bagi individu/subjek data untuk memahami apa dan bagaimana data mereka diproses. Dengan cara mengakses data, pemilik data memungkinkan dirinya dapat memeriksa apakah proses data sesuai dengan hukum dan harapan mereka. Subjek data dapat mengambil tindakan lebih lanjut, seperti menggunakan hak mereka untuk menolak. Hak akses adalah alat penting bagi individu untuk menginvestigasi, mereview, dan mengekspos bagaimana data pribadi sedang diproses. Adanya pengaturan yang jelas adalah titik awal untuk mewujudkan hak-hak akses dalam praktik.³⁶

Modernised Convention 108 mengatur hak akses pada Pasal 9 (1) (b) yang didalamnya juga memuat hak atas informasi. Sementara EU General Data Protection Regulation mengatur *right of access* pada Pasal 15 (1), yang intinya adalah sebagai berikut:

1. Subjek data mempunyai hak untuk mendapatkan konfirmasi dari pengendali data untuk akses data pribadi mereka tentang:
 - a. tujuan pemrosesan.
 - b. kategori data pribadi yang diproses.
 - c. penerima atau kategori penerima yang mendapatkan atau akan mendapatkan data pribadinya, termasuk negara ketiga atau organisasi internasional.
 - d. jika mungkin, rentang waktu periode dan tempat penyimpanan data pribadi atau jika tidak mungkin kriteria menggunakan batas periode.

³³ EU General Data Protection Regulation, Article 14.

³⁴ EU General Data Protection Regulation, Article 13 ayat (1).

³⁵ EU General Data Protection Regulation, Article 14 (3); *Modernised Convention* 108, Art. 9 (1) (b).

³⁶ Privacy International, *The Keys to Data Protection... Op.Cit.*, hlm. 53.

- e. adanya hak meminta untuk mengubah atau menghapus data pribadi atau batasan pemrosesan data pribadi atau menolak untuk memproses.
 - f. hak mengajukan keberatan ke lembaga pengawas yang berwenang.
 - g. jika data pribadi tidak memperoleh langsung dari subjek data, maka subjek data berhak mendapatkan informasi sumbernya.
 - h. keberadaan membuat putusan otomatis, mencakup pembuatan profil, mendapat informasi signifikansi dan konsekuensi pemrosesan bagi subjek data.
2. Jika data pribadi ditransfer ke negara ketiga atau organisasi internasional, subjek data mempunyai hak diberi informasi jaminan keamanan.
 3. Pengendali data harus menyediakan salinan data pribadi yang sedang diproses (termasuk cara elektronik). Untuk beberapa permintaan salinan data, pengendali data dapat membenarkan biaya rasional sebagai biaya administrasi.
 4. Hal mendapatkan salinan tersebut di atas tidak mengganggu hak dan kebebasan orang lain.

Sementara *ASEAN Framework on Personal Data Protection*, menguraikan bahwa *atas permintaan individu, suatu organisasi harus: memberikan individu akses ke data pribadinya yang dimiliki atau di bawah kendali organisasi dalam periode waktu yang wajar*.³⁷ Sedangkan OECD dalam *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, memuat materi hak akses dalam uraian *individual participation principle* yang menguraikan bahwa seorang individu/subjek data harus memiliki hak:

- a. untuk memperoleh dari pengendali data berkaitan dengan apakah pengendali data memiliki data pribadinya.
- b. untuk berkomunikasi dengannya, tentang data yang berkaitan dengannya dalam waktu yang wajar; dengan biaya, jika ada, itu tidak berlebihan; dengan cara yang masuk akal; dan dalam bentuk yang mudah dipahami baginya.
- c. untuk diberikan alasan jika permintaan yang dibuat berdasarkan sub-ayat (a) dan (b) ditolak, dan untuk dapat menantang penolakan tersebut.
- d. untuk menggugat berkaitan dengan data pribadi dirinya dan, jika berhasil, data dihapus, diperbaiki, diselesaikan atau diubah.³⁸

Lebih jauh Privacy International berpendapat bahwa undang-undang harus menyediakan persyaratan minimum, termasuk untuk proses memperoleh data yang berkaitan dengan persyaratan tersebut, yaitu:

- (a) Jangka waktu: ini harus dalam waktu yang wajar dan dinyatakan.
- (b) Biaya: individu tidak boleh dikenakan biaya untuk memperoleh informasi tentang pemrosesan dan salinan data pribadi mereka.
- (c) Format: informasi yang diberikan kepada subjek data harus dalam bentuk yang mudah dipahami oleh mereka dan tidak mengharuskan mereka untuk memiliki keahlian atau pengetahuan tertentu untuk memahami informasi yang diberikan kepada mereka.
- (d) Penjelasan dan banding: jika permintaan ditolak, subjek data memiliki hak untuk diberi alasan mengapa, dan untuk dapat mengajukan penolakan tersebut. Lebih jauh, jika tantangan mereka berhasil, mereka harus memiliki hak untuk menghapus, memperbaiki,

³⁷ ASEAN Framework on Personal Data Protection: Principles of Access and Correction.

³⁸ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980 (sebagaimana diamandemen tahun 2013): Individual Participation Principle, Paragraph 12.

menyelesaikan, atau mengubah data.

- (e) Kejelasan: jika ada pengecualian untuk hak ini, hal ini harus ditetapkan dengan jelas dalam undang-undang dan aplikasinya dijelaskan kepada subjek data.³⁹

B.3. Hak Memperbaiki, Memblokir dan Menghapus (*Rights to Rectify, Restrict, and Erasure*)

Subjek data harus memiliki hak untuk mengajukan perbaikan data pribadinya yang diproses oleh pengendali data pribadi dan *right to be forgotten* jika penyimpanan data tersebut melanggar undang-undang. Secara khusus, subjek data harus memiliki hak untuk menghapus data pribadinya dan tidak lagi diproses jika: data pribadi tidak lagi diperlukan sesuai tujuan pengumpulan atau pemrosesan data tersebut, atau subjek data telah menarik persetujuannya, atau diajukannya keberatan atas pemrosesan data pribadinya, atau jika pemrosesan data pribadinya tidak sesuai dengan hukum.⁴⁰

Modernised Convention 108 Article 9 (1) (e), menyebutkan bahwa berdasarkan permintaan, subjek data mempunyai hak untuk mendapatkan, secara gratis dan tanpa penundaan, perbaikan atau penghapusan yang berlebihan, tergantung dari masalahnya, dari data tersebut jika data pribadinya sedang atau telah, diproses bertentangan dengan ketentuan Konvensi. Sedangkan EU General Data Protection Regulation mengatur secara terpisah hak untuk memperbaiki (diatur pada Pasal 16) dan hak untuk menghapus (diatur pada Pasal 17).

- Hak untuk memperbaiki (*right to rectify*)

Undang-undang harus mengatur hak individu untuk meminta penyelenggara data memperbaiki, memperbarui, atau memodifikasi data jika tidak akurat, salah, menyesatkan, atau tidak lengkap. Individu juga memiliki hak untuk membatasi atau memblokir pemrosesan data pribadi dalam keadaan tertentu. Data pribadi dapat disimpan tetapi tidak diproses lebih lanjut sampai masalah terselesaikan.⁴¹ EU *General Data Protection Regulation* dalam Pasal 16 (*Right to rectification*) menyebutkan bahwa subjek data memiliki hak untuk memperoleh dari pengendali tanpa menunda, pembetulan data pribadi yang tidak akurat mengenai dirinya. Dengan mempertimbangkan tujuan pemrosesan, subjek data harus memiliki hak untuk melengkapi data pribadi yang tidak lengkap, termasuk dengan cara memberikan pernyataan tambahan.⁴² Secara lengkap dikatakan:

- (1) *Subjek data memiliki hak mengajukan permintaan kepada pengendali untuk memperbaiki data pribadi miliknya yang salah dan/atau tidak akurat tanpa penundaan.*
- (2) *Subjek data memiliki hak untuk melengkapi data pribadi yang dikelola pengendali data pribadi, termasuk dengan cara memberikan pernyataan tambahan.*

Sedangkan ASEAN Framework on Personal Data Protection menguraikan bahwa, "... atas permintaan individu, suatu organisasi harus: ... (ii) memperbaiki kesalahan atau kelalaian dalam data pribadinya, kecuali jika undang-undang dan peraturan domestik mewajibkan atau mengizinkan organisasi untuk

³⁹ Privacy International, *The Keys to Data Protection...* Op.Cit., hlm. 52-53.

⁴⁰ EU General Data Protection Regulation, Recital 65.

⁴¹ Privacy International, *The Keys to Data Protection...* Op.Cit., hlm. 54.

⁴² EU General Data Protection Regulation, Article 16 (Right to rectification).

tidak menyediakan akses atau memperbaiki data pribadi dalam keadaan tertentu”.⁴³

- Hak untuk memblokir (*right to restriction/block of processing*)

Pembatasan pemrosesan data pribadi dapat dilakukan dengan cara, antara lain: memindahkan sementara data yang dipilih ke sistem pemrosesan lain atau menghapus sementara data yang dipublikasikan dari situs web. Dalam sistem pengarsipan otomatis, pembatasan pemrosesan harus dipastikan dengan cara sedemikian rupa sehingga data pribadi tidak dapat dilakukan pemrosesan lebih lanjut.⁴⁴

Subjek data memiliki hak membatasi pemrosesan jika salah satu dari yang berikut ini berlaku:

- a. keakuratan data pribadi dipermasalahkan oleh subjek data, untuk suatu periode yang memungkinkan pengendali data untuk memverifikasi keakuratan data pribadi.
- b. pemrosesan dilakukan secara melawan hukum dan subjek data menolak penghapusan data pribadi dan meminta pembatasan penggunaannya sebagai gantinya;
- c. pengendali data tidak lagi membutuhkan data pribadi untuk keperluan pemrosesan, tetapi mereka diharuskan oleh pengendali data untuk keperluan pembelaan gugatan hukum;
- d. subjek data keberatan untuk diproses sambil menunggu verifikasi apakah alasan yang sah dari pengendali mengesampingkan subjek data.

Jika pemrosesan dibatasi maka semua data pribadi (kecuali penyimpanan) hanya akan diproses dengan persetujuan subjek data atau untuk pembelaan gugatan hukum atau untuk perlindungan hak-hak orang lain/badan hukum atau karena alasan kepentingan publik. Subjek data yang telah mendapatkan pembatasan pemrosesan harus diberitahu oleh pengendali sebelum pembatasan pemrosesan dihapus.⁴⁵

- Hak untuk menghapus (*rights to erasure—right to be forgotten*)

Setiap subjek data pribadi memiliki hak untuk meminta penghapusan/pemusnahan data pribadi miliknya kepada pengendali data pribadi melalui permohonan secara tertulis. Penghapusan/pemusnahan data pribadi tersebut dilakukan terhadap data pribadi yang datanya: tidak memiliki nilai guna lagi; pemilik data menarik persetujuan pemrosesan; pemilik data menolak pemrosesan; telah habis retensinya; data diproses tidak sesuai dengan tujuan pemrosesan dan atau secara tidak sah; data pribadi harus dihapus karena kewajiban hukum; tidak berkaitan dengan penyelesaian proses suatu perkara.

Hak subjek data untuk menghapus atau memusnahkan atau *rights to erasure*, di Eropa dikenal juga dengan '*right to be forgotten*', yang bermula dari kasus Google Spain SL, Google Inc v. Agencia Española de Protección de Datos, Mario Costeja González (2014). Kemudian untuk pertama kalinya, '*right to be forgotten*' dikodifikasi dan dimasukkan dalam Peraturan Perlindungan Data Umum (GDPR) di samping hak untuk menghapus. Hak ini dibuat untuk memastikan bahwa saat memproses permintaan, pengendali data akan mempertimbangkan kepentingan publik dan kepentingan subjek

⁴³ ASEAN Framework on Personal Data Protection: Principles of Access and Correction.

⁴⁴ EU General Data Protection Regulation, Recital 67.

⁴⁵ EU General Data Protection Regulation, Article 18.

data. Hak untuk menghapus memberikan perlindungan hak individu serta mengurangi potensi penyalahgunaan. Detailnya, ketentuan Pasal 17 EU General Data Protection Regulation menyebutkan:

1. Subjek data mempunyai hak meminta pengendali data untuk menghapus data pribadi tanpa penundaan yang tidak semestinya dan pengendali data wajib menghapus data tanpa penundaan yang tidak semestinya untuk menghapus data pribadi dalam salah satu dari hal-hal sebagai berikut:
 - a. data pribadi tidak lagi diperlukan sehubungan dengan tujuan pengumpulan atau pemrosesan data tersebut.
 - b. subjek data menarik persetujuan pemrosesan;
 - c. subjek data keberatan terhadap pemrosesan dan tidak ada alasan sah yang mengesampingkan untuk pemrosesan;
 - d. data pribadi telah diproses secara tidak sah;
 - e. data pribadi harus dihapus untuk kepatuhan dengan kewajiban hukum
 - f. data pribadi telah dikumpulkan sehubungan dengan tawaran layanan informasi masyarakat
2. Apabila pengendali telah mempublikasikan data pribadi dan berkewajiban untuk menghapus data pribadi dengan mempertimbangkan teknologi yang tersedia, biaya implementasi, dan harus mengambil langkah-langkah yang wajar termasuk langkah-langkah teknis untuk menghapus data pribadi termasuk tautan apa pun atau salinan atau replikasi data pribadi tersebut.
3. Hak menghapus tidak berlaku sepanjang pengolahan diperlukan:
 - a. untuk melaksanakan hak kebebasan berekspresi dan informasi;
 - b. untuk kepatuhan dengan kewajiban hukum yang berdasarkan undang-undang atau untuk pelaksanaan tugas untuk kepentingan umum atau dalam pelaksanaan wewenang resmi pengendali;
 - c. untuk alasan kepentingan publik di bidang kesehatan;
 - d. untuk tujuan pengarsipan untuk kepentingan umum, tujuan penelitian ilmiah atau historis atau keperluan statistik jika hak tersebut menghambat pencapaian tujuan yang pengolahan; atau
 - e. untuk pembelaan gugatan hukum.

B.4. Hak untuk Menolak (*Right to Object*)

Data pribadi dapat diproses secara sah karena pemrosesan diperlukan untuk pelaksanaan tugas yang dilakukan untuk kepentingan umum atau dalam pelaksanaan wewenang resmi yang diberikan kepada pengendali, atau dengan alasan kepentingan sah pengontrol atau pihak ketiga. Akan tetapi, subjek data harus diberi hak untuk menolak pemrosesan data pribadi apa pun yang berkaitan dengan situasi khususnya. Oleh karena itu, pengendali harus menunjukkan tindakannya berdasar pada kepentingannya yang sah dan meyakinkan untuk mengesampingkan kepentingan atau hak-hak dasar dan kebebasan subjek data.⁴⁶

Hak menolak pemrosesan dapat dilaksanakan jika subjek data mengajukan keberatan dengan alasan yang valid. Pengendali data harus berhenti memproses data kecuali jika pengontrol data dapat membuktikan dan memberikan alasan sah. Hal ini berbeda dengan jika data pribadi diproses untuk

⁴⁶ Baca EU General Data Protection Regulation, Recital 69.

tujuan pemasaran langsung. Subjek data memiliki hak untuk menolak kapan saja dan gratis berkaitan dengan pemrosesan untuk tujuan pemasaran langsung, termasuk membuat profil, baik yang berkaitan dengan pemrosesan awal atau selanjutnya. Hak menolak dari subjek data harus menjadi perhatian dalam proses legislasi dan diatur secara jelas dan terpisah dari informasi lainnya.⁴⁷ Dalam praktiknya, berkaitan dengan pemasaran langsung, di negara-negara Asia seperti Hong Kong dan Korea Selatan telah memberlakukan persyaratan yang lebih keras, dengan hukuman keuangan yang berat terhadap pelanggaran terkait pemasaran langsung.

Sementara ketentuan Pasal 21 EU General Data Protection Regulation menyebutkan terkait dengan *right to object* yang pada intinya adalah sebagai berikut:

- a. Subjek data memiliki hak untuk menolak, dengan alasan yang berkaitan dengan situasi khususnya, setiap saat untuk memproses data pribadi mengenai dirinya, termasuk pembuatan profil. Pengendali tidak akan lagi memproses data pribadi kecuali dapat menunjukkan alasan yang sah untuk pemrosesan yang mengesampingkan kepentingan, hak dan kebebasan subjek data, atau untuk pelaksanaan atau pembelaan dalam gugatan hukum.
- b. Jika data pribadi diproses untuk tujuan pemasaran langsung, subjek data memiliki hak untuk menolak setiap saat untuk memproses data pribadi yang terkait dengannya untuk pemasaran tersebut, yang mencakup pembuatan profil sejauh hal itu terkait dengan pemasaran langsung tersebut.
- c. Jika subjek data melakukan pemrosesan untuk tujuan pemasaran langsung, data pribadi tidak akan lagi diproses untuk tujuan tersebut.
- d. Paling lambat pada saat komunikasi pertama dengan subjek data, hak menolak harus secara eksplisit diberikan kepada subjek data dan harus disajikan secara jelas dan terpisah dari informasi lainnya.
- e. Dalam konteks penggunaan layanan informasi masyarakat, subjek data dapat menggunakan haknya untuk menolak dengan cara otomatis.
- f. Apabila data pribadi diproses untuk tujuan penelitian ilmiah atau historis atau keperluan statistik, subjek data, dengan alasan yang berkaitan dengan situasi khususnya, memiliki hak untuk menolak pemrosesan data pribadi mengenai dirinya atau dia, kecuali pemrosesan diperlukan untuk pelaksanaan tugas yang dilakukan karena alasan kepentingan umum.⁴⁸

B.5. Hak Portabilitas Data (*Right to Data Portability*)

Setiap individu sebagai subjek data memiliki hak untuk menerima data pribadinya yang diproses oleh pengendali data, yang tersedia dalam format yang dapat dibaca mesin secara universal, dan untuk mengirimkan ke layanan lain, dengan persetujuan khusus dari individu tersebut. Hak ini adalah langkah untuk memastikan bahwa subjek data ditempatkan di posisi sentral dan memiliki kekuasaan penuh atas data pribadinya.

Hak portabilitas data memungkinkan subjek data untuk menerima data pribadi yang telah mereka berikan kepada pengontrol, secara terstruktur, biasa digunakan dan format yang dapat dibaca mesin, serta untuk mengirimkan data tersebut ke pengontrol data lainnya. Hak ini memberdayakan subjek data dan memberinya lebih banyak kontrol atas data pribadinya. Tujuan utama portabilitas

⁴⁷ Baca EU General Data Protection Regulation, Recital 70.

⁴⁸ EU General Data Protection Regulation, Art. 21.

data adalah meningkatkan kontrol individu atas data pribadi mereka dan memastikannya mereka memainkan peran aktif dalam ekosistem data.⁴⁹

Secara khusus ketentuan Pasal 20 EU GDPR menyatakan bahwa subjek data memiliki hak untuk menerima data pribadi mengenai dirinya, yang telah diberikannya kepada pengontrol, dalam format yang terstruktur yang umum digunakan dan dapat dibaca mesin dan memiliki hak untuk mengirimkan data tersebut ke pengontrol lain tanpa halangan dari pengontrol yang menyediakan data pribadi, di mana pemrosesan didasarkan pada persetujuan dan pemrosesan dilakukan dengan cara otomatis.

Dalam melaksanakan haknya atas portabilitas data, subjek data memiliki hak untuk memiliki data pribadi yang dikirimkan secara langsung dari satu pengendali ke pengendali lainnya, jika memungkinkan secara teknis. Selain itu pelaksanaan hak ini juga tidak mengurangi atau tidak menghilangkan hak subjek data untuk menggunakan hak akses. Namun demikian hak ini tidak berlaku untuk pemrosesan yang diperlukan untuk pelaksanaan tugas yang dilakukan untuk kepentingan umum atau dalam pelaksanaan kewenangan resmi yang diberikan kepada pengendali. Harus dipastikan pula bahwa pelaksanaan hak ini tidak akan berdampak buruk terhadap hak dan kebebasan orang lain. Lebih jauh elemen hak atas portabilitas data meliputi:

- Hak untuk menerima data pribadi: portabilitas data adalah hak subjek data untuk menerima data pribadi yang diproses oleh pengendali dan menyimpan data tersebut lebih lanjut untuk digunakan pribadi. Penyimpanan dapat di perangkat pribadi atau di *cloud* pribadi, tanpa memerlukan mentransmisi data ke pengendali lainnya. Dalam konteks ini, hak portabilitas data melengkapi hak akses.
- Hak untuk mengirimkan data pribadi dari satu pengendali data ke pengendali data lainnya. Dalam hal ini subjek data mempunyai hak untuk mengirim data pribadi dari satu pengendali data ke pengendali data lainnya “tanpa halangan” dari pengendali data pribadi. Data juga bisa ditransmisikan secara langsung dari satu pengendali data ke yang lain atas permintaan subjek data (apabila memungkinkan secara teknis).
- Kontrol: portabilitas data menjamin hak subjek data untuk menerima data pribadi dan memprosesnya, sesuai keinginan subjek data. Konsekuensinya adalah pengendali data tidak bertanggung jawab atas pemrosesan yang ditangani oleh subjek data atau oleh pengendali/perusahaan lain yang menerima data pribadi. Pengendali data I bertindak atas nama subjek data, termasuk ketika pribadi data secara langsung dikirim ke pengendali data lainnya (Pengendali data II/Penerima).⁵⁰

B.6. Hak Terkait Pengambilan Keputusan Otomatis dan Pembuatan Profil (*Rights Related to Automated Decision Making and to Profiling*)

Setiap subjek data memiliki hak untuk tidak tunduk pada keputusan yang didasarkan pada pemrosesan otomatis, termasuk pembuatan profil, yang memiliki dampak hukum terhadap dirinya atau yang secara signifikan mempengaruhi dirinya. Namun demikian, hal tersebut dikecualikan jika pemrosesan merupakan bagian dari kontrak antara subjek data dengan pengendali data atau sesuai

⁴⁹ EU Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability, 16 / EN, WP 242 rev.01, Adopted on 13 December 2016 As last Revised and adopted on 5 April 2017 (EU WP, 16 / EN, WP 242 rev.01).

⁵⁰ EU WP, 16 / EN, WP 242 rev.01.

ketentuan perundang-undangan, atau didasarkan pada persetujuan tertulis dari subjek data.⁵¹

Pemrosesan otomatis termasuk ‘pembuatan profil’ mencakup segala bentuk pemrosesan otomatis data pribadi yang ditujukan untuk mengevaluasi aspek-aspek pribadi khususnya untuk menganalisis atau memprediksi aspek-aspek yang berkaitan dengan kinerja subjek data di tempat kerja, situasi ekonomi, kesehatan, preferensi pribadi atau minat, keandalan atau perilaku, lokasi atau pergerakan, di mana ia menghasilkan efek hukum mengenai dirinya atau yang secara signifikan memengaruhi dirinya.

Oleh karena itu, untuk memastikan pemrosesan yang adil dan transparan, pengendali harus menggunakan prosedur yang sesuai untuk pembuatan profil, menerapkan langkah-langkah teknis dan organisasi yang sesuai untuk memastikan tidak terjadi ketidakakuratan data pribadi dan menekan risiko kesalahan. Juga harus mengamankan data pribadi dengan cara yang memperhitungkan potensi risiko yang terlibat untuk kepentingan dan hak-hak subjek data, dan mencegah, antara lain, efek diskriminatif pada orang perseorangan atas dasar ras atau asal etnis, opini politik, agama atau kepercayaan, keanggotaan serikat pekerja, status genetik atau kesehatan dan lainnya. Pengambilan keputusan dan pembuatan profil otomatis berdasarkan kategori khusus data pribadi harus diizinkan hanya dalam kondisi tertentu.⁵²

Pembuatan profil dan pengambilan keputusan otomatis dapat menimbulkan risiko signifikan bagi hak dan kebebasan individu yang membutuhkan perlindungan yang tepat. Individu subjek data mungkin tidak tahu atau tidak mengerti bahwa mereka sedang diprofilkan. Oleh karenanya harus ada aturan yang tegas mengenai pemrofilan dan pengambilan keputusan otomatis individu (apakah ini termasuk profil atau tidak) agar tidak digunakan dengan cara yang berdampak pada ketidakadilan terhadap hak-hak individu.⁵³ Namun demikian, pengambilan keputusan otomatis dengan efek hukum atau yang secara signifikan mempengaruhi individu mungkin dapat diterima jika diperlukan untuk menjalankan kontrak atau kinerja kontrak antara pengendali data dan subjek data, atau jika subjek data memberikan persetujuan eksplisit. Selain itu, pengambilan keputusan otomatis dapat diterima jika disahkan oleh hukum dan jika hak, kebebasan, dan kepentingan subjek data data dilindungi secara tepat.⁵⁴

Subjek data harus diberitahu tentang preferensi dan karakteristiknya karena kesalahan identifikasi, kesalahan klasifikasi, dan kesalahan penilaian, merupakan risiko yang tidak terhindarkan terkait dengan pembuatan profil. Pengendali data juga harus memberi tahu subjek data tentang risiko-risiko ini dan hak-hak mereka, termasuk untuk mengakses, memperbaiki dan menghapus. Hak-hak individu perlu diterapkan pada data yang diperoleh, disimpulkan, dan diprediksi, sepanjang memenuhi syarat sebagai data pribadi.

Lebih jauh, karena meningkatnya risiko terhadap hak asasi manusia dan kebebasan dan masalah-masalah seperti keadilan, transparansi dan akuntabilitas, kerangka kerja perlindungan data dapat memberlakukan pembatasan dan perlindungan pada cara-cara di mana data dapat digunakan untuk membuat keputusan.

⁵¹ Baca EU General Data Protection Regulation Recital 71.

⁵² Baca EU General Data Protection Regulation Recital 71.

⁵³ EU Article 29 Data Protection Working Party, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679”, 17/EN-WP251rev.01, Adopted on 3 October 2017. As last Revised and Adopted on 6 February 2018 (EU WP 17/EN-WP251rev.01).

⁵⁴ EU General Data Protection Regulation, Art. 22 (2).

Perlindungan ini harus merupakan hak untuk tidak tunduk pada keputusan otomatis tertentu karena ini penting di mana keputusan ini penting bagi individu, dan khususnya di mana mereka mempengaruhi hak-hak mereka.

Pada sisi lain, pemrosesan otomatis termasuk 'pembuatan profil' melekat hak intervensi manusia. Ketika ada pengecualian untuk pengambilan keputusan otomatis, seorang individu harus memiliki hak untuk mendapatkan intervensi manusia. Pengambilan keputusan otomatis tanpa campur tangan manusia harus tunduk pada batasan yang sangat ketat. Ini sangat penting dalam sektor penegakan hukum, karena potensi ketidakadilan dapat melukai seseorang dan memengaruhi kesejahteraan mereka seumur hidup.

B.7. Hak atas Pemulihan yang Efektif (*Right to an Effective Remedy*)

Dalam *Modernised Convention* 108 disebutkan bahwa hukum perlindungan data salah satunya harus menetapkan solusi dan sanksi yang tepat terhadap pelanggaran hak perlindungan data.⁵⁵ Subjek data memiliki hak pemulihan yang disebabkan terjadinya pelanggaran hak-hak mereka. Hak pemulihan ini dapat dilakukan melalui mekanisme penyelesaian di luar pengadilan maupun melalui pengadilan. Penyelesaian di luar pengadilan dapat dilakukan melalui negosiasi, mediasi, konsiliasi, arbitrase, atau pilihan lain sesuai dengan kesepakatan subjek data pribadi dan pengendali data pribadi. Apabila tidak ada kesepakatan maka, subjek data dapat mengajukan melalui mekanis pengadilan.

- Hak mengajukan pengaduan ke lembaga pengawas independen

Apabila subjek data menganggap pemrosesan data pribadi yang dilakukan oleh pengendali data tidak sesuai dengan undang-undang dan peraturan perundang-undangan pelaksanaannya, maka subjek data yang bersangkutan memiliki hak untuk mengajukan pengaduan keluhan kepada otoritas pengawas independen. Lembaga pengawas independen ini dapat melakukan penyelesaian pengaduan dan sengketa yang timbul. Mekanisme penyelesaian sengketa dapat dilakukan dengan mediasi atau bentuk lain upaya penyelesaian sengketa di luar pengadilan. Jika tidak tercapai lembaga independen dapat melakukan penyelesaian melalui mekanisme adjudikasi.

- Hak mengajukan pengaduan ke pengadilan

Tanpa mengurangi mekanisme pemulihan secara administratif atau upaya penyelesaian di luar pengadilan, setiap subjek data memiliki hak atas pemulihan hukum yang efektif dengan mengajukan keberatan terhadap keputusan yang mengikat dari otoritas pengawas. Selain itu, mekanisme penting dan efektif untuk meminta pertanggungjawaban mereka yang gagal mematuhi hukum perlindungan data adalah ganti rugi kolektif.

Mekanisme pengaduan atau gugatan atau bentuk langkah hukum apapun ke pengadilan bergantung pada kebijakan politik hukum peradilan yang akan digunakan dalam menyelesaikan sengketa penyelenggaraan data pribadi. Secara umum setidaknya terdapat tiga pilihan:

- a. Penyelesaian melalui komisi/badan independen sebagai mekanisme penyelesaian yang putusannya bersifat final dan mengikat. Dalam hal ini maka tidak ada upaya hukum apapun

⁵⁵ Menurut Konvensi Modern 108.

- baik gugatan/banding/peninjauan kembali atas keberatan putusan komisi/badan.
- b. Putusan komisi atau badan bersifat final tetapi terdapat upaya peninjauan kembali ke Mahkamah Agung.
- c. Putusan komisi/badan sebagai putusan yang dapat diajukan upaya banding ke Pengadilan TUN/PT TUN.

Dalam praktiknya, seringkali individu tidak memiliki sumber daya untuk menginvestigasi dan mengungkap ketidakpatuhan, menyusun komplain, dan mengambil tindakan hukum lebih lanjut. Oleh karena itu, mekanisme ganti rugi kolektif harus memungkinkan LSM dengan pengetahuan tentang perlindungan data untuk mengejar pelanggaran perlindungan data atas inisiatif mereka sendiri.⁵⁶

B.8. Hak atas Kompensasi dan Pertanggungjawaban (*Right to compensation and Liability*)

Setiap orang yang telah menderita kerusakan material atau non-material sebagai akibat dari pelanggaran terhadap undang-undang perlindungan data berhak untuk menerima kompensasi dari pengendali data pribadi atas kerusakan yang diderita. Setiap pengendali yang terlibat dalam pemrosesan harus bertanggung jawab atas kerugian yang disebabkan oleh pemrosesan yang melanggar undang-undang.

Pengendali data (*data controller*) bertanggung jawab dan dapat dikenakan kompensasi jika mereka tidak memenuhi kewajiban mereka berdasarkan peraturan tersebut. Sementara prosesor data pribadi (*data processor*) bertanggung jawab atas kerusakan yang disebabkan oleh pemrosesan hanya jika tidak mematuhi kewajiban peraturan yang secara khusus ditujukan kepada prosesor, atau jika telah bertindak di luar, atau bertentangan dengan, instruksi yang sah dari pengendali data. Dalam hal ini, EU GDPR pada *Recital 146* menegaskan bahwa:⁵⁷

- a. Pengendali atau prosesor data harus mengganti kerusakan yang diderita seseorang akibat pemrosesan yang melanggar peraturan (EU GDPR).
- b. Pengendali atau prosesor data harus dibebaskan dari tanggung jawab jika terbukti tidak bertanggung jawab atas kerusakan.
- c. Konsep kerusakan harus ditafsirkan secara luas dalam terang kasus-hukum di Pengadilan dengan cara yang sepenuhnya mencerminkan tujuan dari hukum (EU GDPR).

Dalam melaksanakan hak subjek data atas pemulihan yang efektif, individu dapat diwakili oleh organisasi nirlaba yang aktif di bidang perlindungan data. Organisasi nirlaba ini harus memiliki tujuan dan perhatian terhadap kepentingan publik dan aktif di bidang perlindungan data. Urgensi lembaga nirlaba ini adalah membantu memperkuat posisi subjek data dihadapan pengendali/prosesor data pribadi. Oleh karena ada ketidakseimbangan kekuatan dan asimetri informasi antara individu subjek data dengan mereka yang mengendalikan data pribadi.

C. PENGECUALIAN DAN BATASAN PENGECUALIAN

Hak atas privasi bukanlah merupakan hak absolut (*non-derogable rights*) yang tidak dapat dibatasi

⁵⁶ Privacy International, *The Keys to Data Protection... Op.Cit.*, hlm. 68.

⁵⁷ EU General Data Protection Regulation, Recital 146.

(*limitation*) dan dikurangi (*restriction*). Meski demikian pembatasan terhadap hak atas privasi termasuk data pribadi harus dilakukan berdasarkan undang-undang dan dilakukan seketat mungkin. Ketentuan Pasal 17 ayat (2) ICCPR secara eksplisit menyatakan bahwa setiap orang memiliki hak atas perlindungan hukum terhadap campur tangan yang tidak sah atau sewenang-wenang dengan privasi mereka. Ini berarti setiap kegiatan yang mengintervensi privasi seseorang, termasuk yang terkait data pribadi seseorang, harus dilakukan atas dasar hukum yang dapat diakses publik, yang pada pelaksanaannya juga harus sesuai dengan hukum (*the rule of law*). Dalam konteks aksesibilitas negara terhadap privasi warganya, rezim konstitusional dan hak asasi manusia internasional tidak hanya menuntut diterbitkannya hukum sebagai dasar akses tersebut (*prescribed by law*), tetapi juga musti secara ketat mengatur prosedur pelaksanaannya, serta konsekuensi yang mungkin terjadi, sehingga memerlukan adanya pemulihan bagi setiap orang yang privasinya dilanggar secara semena-mena.

Kendati demikian, meskipun secara konseptual pentingnya perlindungan hak ini telah diperdebatkan semenjak lama, akan tetapi mekanisme perlindungan hak asasi manusia internasional belum secara spesifik dan mendetail memberikan rumusan mengenai pengaturan hak ini. Akibat kurangnya penjelasan tegas dari isi hak ini telah berimplikasi pada terjadinya kesulitan dalam penerapan dan penegakannya. Sebagai hak, privasi memang memenuhi syarat, namun dalam penerapannya telah menimbulkan tantangan interpretasi yang besar, terutama menyangkut pemilahan mengenai ruang privat dan ruang publik. Belum lagi kian pesatnya perkembangan teknologi informasi dan komunikasi yang kian berpengaruh pada ketidakjelasan batas-batas antara ruang privat dan publik. Salah satu masalah yang kerap mengemuka dalam penerapan dan penegakan hak atas privasi adalah terkait dengan mekanisme pembatasannya. Ketentuan Pasal 17 ICCPR memang memungkinkan dilakukannya pembatasan yang diperlukan, dilakukan secara sah dan proporsional. Namun demikian, berbeda dengan ketentuan Pasal 19 (3) ICCPR, yang secara jelas menguraikan unsur-unsur dari tes/prasayarat untuk melakukan suatu pembatasan yang dibolehkan, rumusan Pasal 17 tidak secara tegas menjelaskan mengenai klausul/prinsip pembatasan yang dapat dilakukan.

Di Eropa sendiri hak-hak yang terkait dengan perlindungan data pribadi dapat dibatasi karena tujuan kepentingan umum atau untuk melindungi hak dan kebebasan orang lain. Namun demikian pembatasan tersebut hanya dapat dilakukan, jika:

- a. dilakukan berdasarkan hukum/*in accordance with the law*.
- b. melaksanakan tujuan yang sah/*pursues a legitimate aim* (keamanan nasional, keselamatan publik, ketertiban umum, moral publik, kesehatan publik, hak dan kebebasan orang lain).
- c. menghormati esensi hak-hak dasar dan kebebasan/*respects the essence of the fundamental rights and freedoms*.
- d. diperlukan dan proporsional dalam masyarakat demokratis untuk mencapai tujuan yang sah/*necessary and proportionate in a democratic society to achieve a legitimate purpose*.
- e. menghormati esensi hak/*respects the essence of the right*.
- f. tunduk pada prinsip proporsionalitas/*subject to the principle of proportionality, is necessary*.
- g. melaksanakan tujuan kepentingan umum yang diakui oleh Uni Eropa, atau kebutuhan untuk melindungi hak orang lain/*pursues an objective of general interest recognised by the European Union, or the need to protect the rights of others*.⁵⁸

⁵⁸ EU dalam Handbook on European data protection law (2018), hlm. 35-36.

Lebih jauh berdasarkan Pasal 2 ayat (2) EU DGPR,⁵⁹ pengecualian terhadap perlindungan data pribadi hanya dapat dilakukan dalam hal:

- (a) tindakan yang berada di luar wilayah hukum.
- (b) oleh negara-negara anggota (EU) ketika melakukan kegiatan yang berada dalam lingkup *Section 2 Title V (Specific provisions on the common foreign and security policy)* yang diatur dalam Treaty on European Union (TEU).⁶⁰
- (c) aktifitas individu yang murni bersifat pribadi atau rumah tangga.
- (d) oleh otoritas yang kompeten untuk tujuan pencegahan, penyelidikan, deteksi atau penuntutan atas tindak pidana atau pelaksanaan hukuman pidana, termasuk perlindungan terhadap dan pencegahan ancaman terhadap keamanan publik.
- (e)

Sementara *UN Guidelines for the Regulation of Computerized Personal Data Files* menentukan salah satu prinsip penting dalam perlindungan data adalah *principle of power to make exceptions*. Implementasi prinsip perlindungan data ini dapat dikecualikan hanya jika diperlukan untuk: melindungi keamanan nasional, ketertiban umum, kesehatan masyarakat atau moralitas, serta, antara lain, hak dan kebebasan orang lain, terutama orang-orang yang teraniaya. Pengecualian tersebut harus secara tegas ditentukan dalam undang-undang atau peraturan yang setara dengan undang-undang, yang diundangkan sesuai dengan sistem hukum negara dan secara tegas menyatakan batasnya.⁶¹

Meski dimungkinkan adanya pengecualian tetapi terdapat beberapa batasan terhadap pengecualian tersebut. OECD memberikan penekanan bahwa pengecualian perlindungan data pribadi atas nama kedaulatan nasional, keamanan nasional dan ketertiban umum harus: (a) dilakukan sesedikit mungkin, dan (b) diumumkan kepada publik.⁶²

Sementara itu, Privacy International berpendapat pengecualian dalam perlindungan data pribadi dapat dilakukan dengan alasan-alasan karena:⁶³

- (a) keamanan nasional
- (b) pertahanan
- (c) keamanan publik
- (d) pencegahan, investigasi, deteksi atau penuntutan pelanggaran pidana
- (e) kepentingan publik
- (f) imigrasi
- (g) kepentingan ekonomi atau keuangan, termasuk masalah anggaran dan perpajakan
- (h) kesehatan dan keamanan masyarakat
- (i) perlindungan independensi peradilan dan persidangan
- (j) fungsi pemantauan, inspeksi atau pengaturan yang terkait dengan pelaksanaan otoritas resmi terkait keamanan, pertahanan, kepentingan publik penting lainnya atau pencegahan kejahatan

⁵⁹ Regulation (EU) 2016/679.

⁶⁰ Treaty on European Union (TEU), Consolidated version. As amended by the Amsterdam Treaty signed 1997-10-02, in force 1999-05-01; Title V - General provisions on the Union's external action and specific provisions on the common foreign and security policy, Chapter 2 - Specific provisions on the common foreign and security policy.

⁶¹ UN, "Guidelines for the Regulation of Computerized Personal Data Files", Adopted by General Assembly Resolution 45/95 of 14 December 1990 A.6. Power to make exceptions.

⁶² OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.

⁶³ Privacy International, *The Keys to Data Protection... Op.Cit.*, hlm. 28.

- (a) perlindungan individu, atau hak dan kebebasan orang lain
- (b) penegakan masalah hukum perdata.

Namun demikian pengecualian hanya dapat dibenarkan dan berlaku dalam keadaan terbatas dan penting, untuk memastikan hal itu, pengecualian apa pun harus:⁶⁴

- a. didefinisikan dengan jelas dan ditentukan oleh hukum,
- b. menghormati hak dan kebebasan dasar individu,
- c. diperlukan dan proporsional dalam masyarakat demokratis, dan
- d. hanya berlaku ketika kegagalan dalam melakukan tindakan itu—pengecualian tidak akan bertentangan dengan tujuan yang sah (*legitimate aim*).

Selain itu, berkaitan dengan pengecualian karena alasan keamanan dan aktifitas intelijen, maka penting untuk memastikan bahwa setiap pemrosesan data pribadi (mis. database yang dikelola pemerintah), oleh badan keamanan, badan intelijen dan penegak hukum tunduk pada undang-undang perlindungan data. Tegasnya pengecualian apa pun harus dibatasi, dijabarkan secara jelas, tepat dan tidak ambigu, dipublikasikan, dan ditafsirkan secara sempit sesuai dengan prinsip-prinsip kebutuhan dan proporsionalitas. Pendekatan pengecualian ini akan memastikan bahwa perlindungan yang diatur dalam undang-undang perlindungan data tidak dianggap berlebihan dalam kaitannya dengan fungsi lembaga keamanan dan intelijen.

D. MEMASTIKAN KEWAJIBAN PENGENDALI DAN PROSESOR DATA

D.1. Tanggung Jawab dan Kepatuhan

Pengendali data (*data controller*) adalah orang perseorangan atau badan hukum, otoritas publik, agensi atau badan lain yang, secara sendiri atau bersama-sama dengan orang lain, menentukan tujuan dan cara pemrosesan data pribadi.⁶⁵ Tanggungjawab merupakan salah satu aspek kunci dalam keberhasilan perlindungan data pribadi. Oleh karena itu, undang-undang harus secara jelas mengidentifikasi pihak-pihak yang bertanggung jawab untuk mematuhi hukum, serta kewajiban dan tugas mereka untuk memastikan kepatuhan dan perlindungan tentang hak-hak individu, dan tindakan apa yang harus mereka ambil jika mereka gagal melakukannya.

Selain itu pengendali data bertanggungjawab dan harus menunjukkan kepatuhan terhadap undang-undang dalam pemrosesan data pribadi (akuntabilitas).⁶⁶ Tanggung jawab dan kewajiban dalam setiap pemrosesan data pribadi yang dilakukan pengendali data atau atas nama pengendali data harus ditetapkan undang-undang, dan pengendali berkewajiban patuh pada ketentuan undang-undang tersebut. Namun demikian pengaturan tersebut juga harus mempertimbangkan sifat, ruang lingkup, konteks dan tujuan pemrosesan dan risiko terhadap hak dan kebebasan orang perseorangan.⁶⁷

⁶⁴ *Ibid.*

⁶⁵ EU General Data Protection Regulation, Art. 4 (7).

⁶⁶ EU General Data Protection Regulation, Art. 5 (2).

⁶⁷ EU General Data Protection Regulation, Recital 74.

- Tanggung Jawab Pengendali Data

Sebagai pihak yang bertanggungjawab terhadap akuntabilitas pemrosesan data pribadi, maka undang-undang harus mengatur tanggungjawab pengendali, yang meliputi:

- a. menerapkan langkah-langkah teknis dan organisasi yang mencakup implementasi kebijakan perlindungan data untuk memastikan pemrosesan dilakukan sesuai dengan peraturan perundang-undangan, dan langkah-langkah tersebut harus ditinjau dan diperbarui secara berkala.
- b. patuh pada kode perilaku dan/atau mekanisme sertifikasi yang dapat digunakan sebagai elemen menunjukkan kepatuhan terhadap kewajiban pengendali data.⁶⁸
- c. menerapkan perlindungan data dalam desain dan secara default (*privacy by design, privacy by default*).⁶⁹
- d. pengendali data pada saat penentuan cara memproses dan pada saat pemrosesan, harus menerapkan langkah-langkah teknis dan organisasi yang sesuai, seperti nama samaran, yang dirancang untuk menerapkan prinsip-prinsip perlindungan data, seperti minimalisasi data, cara efektif dan untuk mengintegrasikan perlindungan yang diperlukan ke dalam pemrosesan untuk memenuhi persyaratan perundang-undangan dan melindungi hak-hak subjek data.
- e. pengendali data harus menerapkan langkah-langkah teknis dan organisasi yang sesuai untuk memastikan bahwa, secara *default*, hanya data pribadi yang diperlukan untuk setiap tujuan spesifik dari pemrosesan yang diproses.

- Tanggung Jawab dalam Pemrosesan Bersama

Apabila pemrosesan data pribadi dilakukan oleh dua atau lebih pengendali data secara Bersama-sama, maka berlaku ketentuan:⁷⁰

- a. harus secara bersama-sama menentukan tujuan dan cara pemrosesan.
- b. harus menjadi pengendali bersama.
- c. harus secara transparan menentukan tanggung jawab masing-masing untuk kepatuhan dengan kewajiban berdasarkan UU, khususnya terkait dengan pelaksanaan hak-hak subjek data dan tugas masing-masing untuk memberikan informasi kepada subjek data.
- d. dilakukan dengan cara pengaturan di antara mereka kecuali ditentukan oleh undang-undang.
- e. pengaturan mekanisme bersama harus mencerminkan peran dan hubungan masing-masing pengendali data ketika bersama-sama berhadapan dengan subjek data.
- f. subjek data dapat menggunakan haknya terhadap masing-masing pengendali data.

- Tanggung Jawab Prosesor Data

Prosesor data adalah orang (natural person) atau badan hukum (natural legal person), otoritas publik, agensi atau badan lain yang memproses data pribadi atas nama pengendali.⁷¹ Pengendali data hanya dapat menunjuk prosesor data yang memberikan jaminan yang cukup untuk menerapkan langkah-langkah teknis dan organisasi untuk memastikan pemrosesan memenuhi ketentuan peraturan

⁶⁸ EU General Data Protection Regulation, Article 24.

⁶⁹ EU General Data Protection Regulation, Article 25.

⁷⁰ EU General Data Protection Regulation, Article 26.

⁷¹ EU General Data Protection Regulation, Art. 4 (8).

perundang-undangan.⁷² Prosesor dan setiap orang yang bertindak di bawah otoritas pengendali atau prosesor, yang memiliki akses ke data pribadi, tidak boleh memproses data tersebut kecuali atas perintah pengendali data. Hal ini dikecualikan jika diperintahkan undang-undang.⁷³ Detailnya tanggung jawab prosesor berkaitan dengan:⁷⁴

- a. Tindakan pemrosesan oleh prosesor harus diatur dalam kontrak atau perbuatan hukum lain sesuai undang-undang:
 - (1) kontrak atau tindakan hukum lainnya harus tertulis, termasuk dalam bentuk elektronik.
 - (2) kontrak memuat setidaknya tentang subjek dan durasi pemrosesan, sifat dan tujuan dari pemrosesan, jenis data pribadi dan kategori subjek data, serta kewajiban dan hak-hak pengendali.
- b. Bertindak berdasarkan perintah tertulis dari pengendali data, kecuali atas perintah undang-undang.
- c. Atas nama pengendali data menerapkan langkah-langkah teknis dan organisasi yang tepat dan memastikan perlindungan terhadap hak-hak subjek data.
- d. Mematuhi aturan tentang penunjukan sub-prosesor. Prosesor data tidak boleh menggunakan prosesor lain tanpa izin dari pengendali. Jika menggunakan prosesor lain atas izin pengendali, maka kewajiban prosesor lain/baru sama seperti kewajiban prosesor lama/utama yang ditetapkan dalam kontrak antara pengendali dan prosesor utama. Jika prosesor baru gagal memenuhi kewajiban perlindungan datanya, prosesor awal/utama tetap bertanggung jawab kepada pengendali atas kinerja kewajiban prosesor baru.
- e. Memastikan bahwa orang yang berwenang untuk memproses data pribadi menjaga kerahasiaan data pribadi.
- f. Membantu pengendali data melakukan langkah-langkah teknis dan organisasi untuk memenuhi kewajiban pengendali untuk menanggapi permintaan pelaksanaan hak-hak dari subjek data.
- g. Membantu pengendali data dalam memastikan kepatuhan dengan kewajiban untuk keamanan pemrosesan dan konsultasi dampak pemrosesan.
- h. Membantu pengendali dalam memastikan kepatuhan dengan kewajiban menjamin keamanan pemrosesan, pemberitahuan tentang pelanggaran data pribadi kepada otoritas pengawas, mengkomunikasikan pelanggaran data pribadi kepada subjek data, penilaian dampak perlindungan data, konsultasi sebelumnya, dengan mempertimbangkan sifat pemrosesan dan informasi yang tersedia untuk prosesor.
- i. Atas perintah dari pengendali data, menghapus atau mengembalikan semua data pribadi ke pengendali setelah layanan pemrosesan berakhir, dan menghapus salinan yang ada kecuali undang-undang mengharuskan penyimpanan data pribadi.
- j. Menyediakan semua informasi yang diperlukan untuk audit, termasuk inspeksi, yang dilakukan oleh pengendali atau auditor lain yang diamanatkan oleh pengendali data.
- k. Jika ada suatu instruksi yang melanggar hukum perlindungan data, prosesor data harus segera memberi tahu pengendali data.
- l. prosesor data juga tunduk dan patuh pada kode perilaku atau mekanisme sertifikasi yang dapat digunakan sebagai elemen untuk menunjukkan jaminan perlindungan.

⁷² EU General Data Protection Regulation, Art. 8 (1).

⁷³ EU General Data Protection Regulation, Article 29.

⁷⁴ EU General Data Protection Regulation, Article 28, art. 32-37.

- m. Jika prosesor data melanggar peraturan perundang-undangan, prosesor data dianggap sebagai pengendali data.
- n. Penunjukan petugas perlindungan data pribadi (*the data protection officer*)
- o. Bekerjasama dan berkonsultasi dengan otoritas pengawas data pribadi.

- Petugas Perlindungan Data (*Data Protection Officer*)

Salah satu kunci akutabilitas pemrosesan data pribadi adalah pengawasan yang efektif. Oleh karena itu pengendali dan prosesor data pribadi harus menunjuk Petugas Perlindungan Data Pribadi (*Data Protection Officer*) untuk memastikan pemrosesan data pribadi dilaksanakan secara akuntabel dan mematuhi peraturan perundang-undangan.

Lingkup pemrosesan data pribadi yang harus diawasi oleh petugas perlindungan data pribadi, meliputi: (a) pemrosesan dilakukan oleh otoritas atau badan publik, kecuali untuk penyidikan, penuntutan, dan perintah pengadilan yang bertindak dalam kapasitas yudisial mereka; (b) pemrosesan yang sifat, cakupan, dan/atau tujuannya, memerlukan pemantauan teratur dan sistematis terhadap subjek data dalam skala besar; atau (c) pemrosesan data pribadi kategori data spesifik (*sensitive*) dalam skala besar atau data pribadi yang berkaitan dengan hukuman dan pelanggaran pidana.

D.2. Memastikan Keamanan Pemrosesan

Setiap pengendali dan prosesor data harus menerapkan langkah-langkah teknis dan organisasi yang sesuai untuk memastikan tingkat keamanan yang tinggi dalam pemrosesan data pribadi. Kendati begitu dalam pelaksanaannya tetap mempertimbangkan keadaan kemampuan, biaya implementasi, sifat, ruang lingkup, konteks dan tujuan pemrosesan, serta risiko berbagai kemungkinan dan tingkat ancaman pelanggaran hak dan kebebasan individu. Langkah-langkah tersebut termasuk: anomisasi; pseudonimisasi; enkripsi data pribadi; memastikan sistem dan layanan pemrosesan menjaga kerahasiaan, integritas, ketersediaan dan ketahanan; memulihkan ketersediaan dan akses ke data pribadi jika terjadi kehilangan data secara tepat waktu; dan adanya suatu proses untuk menguji, menilai dan mengevaluasi efektivitas tindakan untuk menjamin keamanan pemrosesan data pribadi.⁷⁵

Selain itu pengendali dan prosesor data juga harus mengambil langkah-langkah untuk memastikan bahwa setiap orang yang bertindak di bawah otoritas pengendali atau prosesor yang memiliki akses ke data pribadi tidak memprosesnya kecuali atas perintah dari pengendali, kecuali undang-undang mengharuskan untuk melakukannya.⁷⁶ Keamanan data tidak hanya dicapai dengan memiliki peralatan yang tepat, tetapi juga membutuhkan aturan internal organisasi (*privacy policy*) yang sesuai dan mencakup masalah-masalah berikut:

- a. penyediaan informasi secara berkala kepada seluruh karyawan tentang aturan keamanan data dan kewajiban mereka di bawah hukum perlindungan data, terutama terkait dengan kewajiban kerahasiaan.
- b. distribusi tanggung jawab yang jelas dan garis koordinasi yang jelas dalam hal pemrosesan data, terutama mengenai keputusan untuk memproses data pribadi dan untuk mengirimkan data ke pihak ketiga atau ke subjek data.

⁷⁵ EU General Data Protection Regulation, Article 32 (1).

⁷⁶ EU General Data Protection Regulation, Article 32 (3) (4).

- c. penggunaan data pribadi hanya sesuai dengan instruksi orang yang kompeten atau menurut aturan yang ditetapkan secara umum.
- d. perlindungan akses ke lokasi dan ke perangkat keras dan lunak dari pengendali atau prosesor data, termasuk pemeriksaan otorisasi untuk akses.
- e. memastikan bahwa otorisasi untuk mengakses data pribadi telah ditetapkan oleh orang yang kompeten dan memerlukan dokumentasi yang tepat.
- f. protokol otomatis pada akses elektronik ke data pribadi dan pemeriksaan rutin protokol tersebut oleh meja pengawas internal (karena itu mengharuskan semua kegiatan pemrosesan data dicatat).
- g. dokumentasi yang cermat untuk bentuk pengungkapan lain selain akses otomatis ke data sehingga dapat menunjukkan bahwa tidak ada transmisi data ilegal yang terjadi.⁷⁷

D.3. Merekam Kegiatan Pemrosesan

Pengendali data pribadi diwajibkan untuk menyimpan catatan kegiatan pemrosesan yang menjadi tanggungjawabnya. Menyimpan catatan kegiatan pemrosesan memungkinkan pengendali dan prosesor data untuk menunjukkan kepatuhan terhadap peraturan. Menyimpan catatan juga memungkinkan otoritas pengawas melakukan pemantauan keabsahan pemrosesan. Catatan atau rekaman informasi yang harus dibuat adalah:

- a. nama dan rincian kontak pengendali/pengendali bersama, perwakilan pengendali, dan petugas perlindungan data pribadi.
- b. tujuan pemrosesan data pribadi.
- c. deskripsi kategori subjek data dan kategori data pribadi.
- d. kategori penerima kepada siapa data pribadi telah atau akan diungkapkan.
- e. pihak ketiga kepada siapa data pribadi telah atau akan ditransfer, termasuk rincian perlindungan yang diadopsi.
- f. batas waktu yang diperkirakan untuk penghapusan berbagai kategori data.
- g. deskripsi langkah-langkah keamanan teknis dan organisasi yang diambil untuk memastikan integritas dan kerahasiaan data.⁷⁸

D.4. Kerahasiaan Data Pribadi

Kerahasiaan data pribadi merupakan prinsip penting dalam penyelenggaraan data pribadi. Data pribadi harus diproses dengan cara yang menjamin keamanan yang tepat, termasuk perlindungan terhadap pemrosesan yang tidak sah atau melanggar hukum dan terhadap kehilangan, kerusakan atau kerusakan yang tidak disengaja, menggunakan tindakan teknis atau organisasi yang sesuai.⁷⁹

Oleh karenanya pengendali dan prosesor data harus menerapkan langkah-langkah dan organisasi untuk memastikan tingkat keamanan yang tinggi, termasuk, antara lain: nama samaran dan enkripsi data pribadi, kemampuan memastikan kerahasiaan, integritas, ketersediaan dan ketahanan pemrosesan, evaluasi dan pengujian efektivitas tindakan, dan kemampuan untuk mengembalikan pemrosesan.⁸⁰

⁷⁷ Handbook on European data protection law, 167-168.

⁷⁸ EU General Data Protection Regulation, Article 30.

⁷⁹ EU General Data Protection Regulation: 'integrity and confidentiality' Principles.

⁸⁰ EU General Data Protection Regulation, Article 32 (1).

Tegasnya pengendali dan prosesor data memiliki tugas dan tanggung jawab untuk menjaga keamanan data. Undang-undang harus memberikan perlindungan keamanan tidak hanya untuk melindungi data itu sendiri, tetapi kewajiban perlindungan harus diperluas untuk mencakup perangkat dan infrastruktur itu sendiri yang digunakan pada setiap tahap pemrosesan termasuk pembangkitan, pengumpulan, penyimpanan, dan berbagi—*sharing* (yaitu data saat istirahat (berhenti) dan saat data dalam perjalanan pengiriman).⁸¹

Dalam konteks kontrak antara pengendali dan prosesor data, kewajiban kerahasiaan harus dimuat dalam setiap kontrak antara pengendali dan prosesor. Selain itu, pengendali dan prosesor harus mengambil langkah-langkah khusus untuk membangun kewajiban hukum kerahasiaan bagi karyawan mereka, biasanya dicapai dengan memasukkan klausul kerahasiaan dalam mempekerjakan karyawan kontrak.

D.5. Pemberitahuan Pelanggaran

- Pelanggaran Perlindungan Data dan Jenis Pelanggaran

Pelanggaran dalam perlindungan data pribadi akan merugikan hak atas privasi, seperti pencurian atau penipuan identitas, kerugian finansial atau kerusakan materi, hilangnya kerahasiaan data pribadi yang dilindungi oleh kerahasiaan profesional, dan bahkan kerusakan reputasi subjek data. Secara umum pelanggaran memiliki tiga jenis dampak pada data pribadi: pengungkapan, kehilangan, dan/atau perubahan/pergantian (*alteration*) data.⁸²

Pelanggaran data pribadi sendiri adalah pelanggaran keamanan yang mengarah pada penghancuran, kerusakan, kehilangan, perubahan, pengungkapan, atau akses yang tidak sah terhadap, atau akses ke data pribadi yang dikirim, disimpan atau diproses.⁸³ Dari definisi tersebut terdapat beberapa istilah yang perlu dipahami maksudnya. *Destruction of personal data* (penghancuran data pribadi) yaitu data tidak lagi ada, atau tidak lagi ada dalam bentuk yang dapat digunakan oleh pengendali. *Damage* (kerusakan) adalah tempat data pribadi telah diubah, rusak, atau tidak lagi lengkap. *Loss* (kehilangan) data pribadi ditafsirkan data tersebut mungkin masih ada, tetapi pengendali data telah kehilangan kendali atau aksesnya, atau tidak lagi memilikinya. *Unauthorised or unlawful processing* (pemrosesan yang tidak sah atau melanggar hukum) mencakup pengungkapan data pribadi kepada atau diakses oleh penerima yang tidak berwenang untuk menerima (atau mengakses) data, atau segala bentuk pemrosesan lain yang melanggar peraturan.⁸⁴

Lebih detailnya, pelanggaran data pribadi dapat dikategorikan ke dalam tiga prinsip keamanan informasi berikut ini:

(a) *Confidentiality breach* (pelanggaran kerahasiaan), di mana ada pengungkapan yang tidak

⁸¹ Privacy International, *The Keys to Data Protection...* Op.Cit., hlm. 74.

⁸² EU Article 29 Data Protection Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP 18/EN WP250rev.01 Adopted on 3 October 2017 (As last Revised and Adopted on 6 February 2018) (EU WP 18/EN WP250rev.01).

⁸³ Article 4 (12).

⁸⁴ (EU WP 18/EN WP250rev.01).

- sah atau tidak disengaja, atau akses ke data pribadi.
- (b) *Integrity breach* (pelanggaran integritas), di mana ada perubahan data pribadi yang tidak sah atau tidak disengaja.
- (c) *Availability breach* (pelanggaran ketersediaan), di mana ada kehilangan akses yang tidak disengaja atau tidak sah, atau merusak data pribadi.⁸⁵

Sayangnya otoritas pengawas dan individu sering tidak menyadari terjadinya pelanggaran data pribadi. Hal ini menghambat subjek data untuk mengambil langkah-langkah melindungi diri mereka sendiri dari konsekuensi negatifnya. Oleh karena itu perlu diatur mekanisme penyampaian informasi pelanggaran data pribadi kepada otoritas pengawas dan ke subjek data.

- Pemberitahuan Pelanggaran kepada Otoritas Pengawas

Dalam kasus pelanggaran data pribadi, tugas dan kewajiban pengendali data adalah:

- a. setelah menyadari adanya pelanggaran data pribadi, tanpa penundaan yang tidak semestinya menyampaikan laporan pelanggaran data pribadi kepada otoritas pengawas yang berkompeten.
- b. hak ini dikecualikan jika pelanggaran data pribadi tidak mungkin mengakibatkan risiko terhadap hak dan kebebasan orang perseorangan.
- c. jika pemberitahuan kepada otoritas pengawas dilakukan penundaan harus disertai dengan alasan penundaan.
- d. materi pemberitahuan setidaknya harus:
 - (1) menjelaskan sifat dari pelanggaran data pribadi termasuk kategori dan perkiraan jumlah subjek data yang bersangkutan dan kategori serta perkiraan jumlah catatan data pribadi yang bersangkutan.
 - (2) menyampaikan/mengomunikasikan nama dan perincian kontak petugas perlindungan data atau personal kontak lain untuk mendapatkan lebih banyak informasi.
 - (3) menggambarkan kemungkinan konsekuensi dari pelanggaran data pribadi.
 - (4) menggambarkan tindakan yang diambil atau diusulkan untuk mengatasi pelanggaran data pribadi.
- e. jika tidak mungkin untuk memberikan informasi pada saat yang sama, informasi dapat diberikan secara bertahap tanpa penundaan lebih lanjut.
- f. Pengendali data harus mendokumentasikan setiap pelanggaran data pribadi, yang terdiri dari fakta yang berkaitan dengan pelanggaran data pribadi, dampaknya, dan tindakan perbaikan yang diambil. Dokumentasi itu harus memungkinkan otoritas pengawas untuk memverifikasi kepatuhan.⁸⁶

- Komunikasi dengan Pemilik Data Pribadi

Ketika pelanggaran data pribadi berpotensi mengakibatkan risiko tinggi terhadap hak dan kebebasan individu, pengendali harus mengkomunikasikan pelanggaran data pribadi kepada subjek data tanpa penundaan yang tidak semestinya. Komunikasi ke subjek data harus menjelaskan dalam bahasa

⁸⁵ EU Article 29 Data Protection Working Party, Opinion 03/2014 on Personal Data Breach Notification, 693/14/EN, WP 213, Adopted on 25 March 2014.

⁸⁶ EU General Data Protection Regulation, Article 33.

yang jelas dan menguraikan setidaknya informasi fakta yang berkaitan dengan pelanggaran data pribadi, dampaknya, dan tindakan perbaikan yang diambil.

Apabila pengendali belum mengkomunikasikan pelanggaran data pribadi ke subjek data, otoritas pengawas, setelah mempertimbangkan kemungkinan pelanggaran data pribadi yang mengakibatkan risiko tinggi, mungkin akan mengharuskan pengendali data untuk segera melakukan komunikasi.⁸⁷

D.6. Penilaian Dampak Perlindungan Data

Penilaian dampak perlindungan data pribadi atau dikenal dengan *data protection impact assessment* (DPIA) adalah proses yang dirancang untuk menggambarkan pemrosesan, menilai kebutuhan dan proporsionalitasnya, dan membantu mengelola risiko terhadap hak dan kebebasan orang perorangan, yang dihasilkan dari pemrosesan data pribadi, dengan menilai dan menentukan langkah-langkah untuk mengatasinya. DPIA adalah alat penting untuk memastikan akuntabilitas, karena membantu pengendali untuk menunjukkan bahwa langkah-langkah yang tepat telah diambil untuk memastikan kepatuhan terhadap peraturan perundang-undangan (Langkah ini merupakan proses untuk membangun dan menunjukkan kepatuhan).⁸⁸

Persyaratan lain yang telah diintegrasikan ke dalam kerangka kerja perlindungan data adalah bahwa penilaian dampak dilakukan sebelum memproses data pribadi. Ini sangat penting di mana ada risiko terhadap hak dan kebebasan individu, termasuk di mana pemrosesan melibatkan data pribadi yang sensitif, pengambilan keputusan otomatis, pembuatan profil, atau pemantauan ruang publik. Segala bentuk pemrosesan data cenderung menghasilkan risiko terhadap hak dan kebebasan orang perorangan. Oleh sebab itu, pengendali bertanggung jawab melakukan penilaian dampak perlindungan data. Hasil penilaian digunakan menentukan langkah-langkah yang tepat dalam pemrosesan data pribadi.⁸⁹

E. Transfer Data Internasional

Terdapat berbagai model pengaturan dan pengelolaan transfer data lintas batas (*cross border data flows*). Model Meksiko misalnya menggunakan model pemberitahuan privasi untuk disepakati antara pengendali data dan subjek data, yang akan menentukan apakah individu setuju atau tidak atas data mereka untuk ditransfer. Penerima data dalam hal ini, harus mematuhi kewajiban yang sama seperti pengendali data asli.

Model lainnya adalah yang dikembangkan di Eropa, Argentina dan Hong Kong, yang dikenal sebagai pendekatan menyeluruh, yang menegaskan bahwa setiap transfer data pribadi ke negara ketiga tidak menurunkan tingkat perlindungan hak individu atas data pribadi mereka. Di Hong Kong misalnya, dalam undang-undang perlindungan datanya dinyatakan, jika data pribadi akan ditransfer keluar Hong Kong, maka harus dipastikan terlebih dahulu bahwa yurisdiksi penerima memberikan tingkat perlindungan yang memadai, dan pengirim telah memastikan bahwa data akan dilindungi secara

⁸⁷ *Ibid.*

⁸⁸ EU Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, 17/EN WP 248 rev.01.

⁸⁹ EU General Data Protection Regulation, Recital 84.

memadai (misalnya dengan mengadopsi model kontrak klausul untuk perlindungan data), atau subjek data telah menyetujui secara tertulis.

Pendekatan tersebut pada dasarnya menekankan bahwa setiap pengungkapan atau transfer data pribadi ke entitas di negara lain diperbolehkan, jika penerima data memberikan tingkat perlindungan data pribadi, yang minimal setara dengan tingkat yang ditetapkan dalam hukum nasional pengirim. Penilaian dapat dilakukan oleh otoritas pengawas independen/Otoritas Perlindungan Data, setelah melakukan konsultasi terbuka dan penyelidikan menyeluruh.⁹⁰ Penilaian tingkat perlindungan data pribadi yang diberikan kepada negara ketiga harus mencakup secara eksplisit:

- a. Penghormatan terhadap hak asasi manusia dan kebebasan mendasar, undang-undang yang relevan, termasuk mengenai keamanan publik, pertahanan, keamanan nasional dan hukum pidana, dan akses otoritas publik ke data pribadi.
- b. Pengakuan hak-hak warga negara dan orang asing di dalam wilayah tersebut, tanpa diskriminasi berdasarkan status imigrasi.
- c. Aturan hukum, termasuk perundang-undangan nasional yang berlaku dan peraturan/peraturan profesional.
- d. Keberadaan dan berfungsinya otoritas pengawas independen secara efektif untuk memastikan kepatuhan terhadap hukum.
- e. Komitmen internasional yang telah dilakukan oleh negara ketiga atau organisasi internasional, atau kewajiban lain yang timbul dari konvensi atau instrumen yang mengikat secara hukum serta dari partisipasinya dalam sistem multilateral atau regional, khususnya terkait dengan perlindungan data pribadi.
- f. Mekanisme pengambilan keputusan harus terbuka, jelas, preskriptif, dan melibatkan konsultasi dengan aktor-aktor terkait termasuk masyarakat sipil. Selain itu, penilaian ini harus ditinjau secara berkala, untuk menyediakan mekanisme peninjauan berkala dari proses pengambilan keputusan.

Jika penilaian kecukupan tidak dapat dilakukan, pengendali atau prosesor data harus mengambil langkah-langkah untuk mengkompensasi kurangnya perlindungan data, memastikan bahwa perlindungan yang sesuai ada dan dapat diberlakukan untuk melindungi data

Namun demikian pengecualian terhadap ketentuan pengiriman data internasional dapat dilakukan berdasarkan sejumlah alasan: (i) kerja sama hukum internasional antara badan intelijen dan lembaga penyelidikan; (ii) keselamatan subjek data atau pihak ketiga; (iii) berdasarkan komitmen dari kesepakatan kerja sama internasional, ini misalnya yang dilakukan antara Uni Eropa dengan Amerika Serikat, dengan diterapkannya EU-US Privacy Shield, yang pada intinya menyatakan bahwa ketika data pribadi akan ditransfer pengendali data ke Amerika Serikat, akan diterapkan mekanisme perlindungan data yang sama dengan di Eropa; dan (iv) merupakan pelaksanaan dari kebijakan publik atau perintah dari lembaga berwenang.

⁹⁰ Privacy International, *The Keys to Data Protection... Op.Cit.*, hlm. 80.

PROFIL ELSAM

Lembaga Studi dan Advokasi Masyarakat (ELSAM) atau Institute for Policy Research and Advocacy, adalah sebuah organisasi hak asasi manusia, yang berdiri di Jakarta, sejak Agustus 1993. Tujuannya turut berpartisipasi dalam usaha menumbuhkembangkan, memajukan dan melindungi hak-hak sipil dan politik serta hak-hak asasi manusia pada umumnya –sebagaimana diamanatkan oleh UUD 1945 dan Deklarasi Universal Hak Asasi Manusia. Sejak awal, semangat perjuangan ELSAM adalah membangun tatanan politik demokratis di Indonesia melalui pemberdayaan masyarakat sipil melalui kegiatan penelitian, advokasi dan promosi hak asasi manusia.

Saat ini ELSAM memiliki tiga kegiatan utama, yang terdiri atas: (1) pengarusutamaan hak asasi manusia dalam pengambilan kebijakan; (2) studi dan produksi pengetahuan hak asasi untuk mendukung advokasi kebijakan; dan (3) Pendidikan Hak Asasi Manusia.

Dalam kegiatan pengarusutamaan hak asasi manusia dalam pengambilan kebijakan, ELSAM secara terus-menerus mendorong pengintegrasian prinsip-prinsip hak asasi manusia dalam setiap proses pembentukan kebijakan, seperti: (i) Memberikan masukan dan rekomendasi bagi lembaga legislatif dan pemerintah; (ii) Menyusun catatan kritis melalui berbagai policy brief atas suatu rancangan kebijakan; (iii) Monitoring pelaksanaan fungsi legislasi; (iv) Menyediakan pendampingan teknis keahlian bagi lembaga-lembaga pemerintah; dan (v) Melakukan berbagai kemitraan strategis dengan berbagai lembaga.

Berikutnya pada kegiatan studi dan produksi pengetahuan hak asasi untuk mendukung advokasi kebijakan, ELSAM melakukan berbagai penelitian dan produksi pengetahuan untuk mendorong pembentukan kebijakan berbasis bukti (*evidence based policies*), dengan pendekatan hak asasi manusia (*human rights based approach*). Fokus-fokus studi ELSAM antara lain:

- Bisnis dan hak asasi manusia: Mengkaji dampak operasi korporasi terhadap hak asasi, termasuk mendorong lahirnya berbagai kebijakan untuk mengaplikasikan UN Guiding Principles on Business and Human Rights.
- Internet dan hak asasi manusia: Meneliti mengenai implikasi kemajuan teknologi informasi dan komunikasi terhadap perlindungan hak asasi, termasuk isu tatakelola internet, kebijakan konten, perlindungan data pribadi, keamanan siber, dan respon terhadap berbagai perkembangan terbaru inovasi teknologi (*fintech, e-commerce, big data, artificial intelligence*).
- Perlindungan kebebasan sipil: ELSAM ingin memastikan penghormatan dan perlindungan terhadap kebebasan sipil di Indonesia melalui berbagai kegiatan studi dan advokasi kebijakan, khususnya yang terkait dengan kebebasan berekspresi, kebebasan berkumpul/berorganisasi, kebebasan beragama, termasuk respon terhadap makin maraknya praktik-praktik intoleransi.
- Penyelesaian pelanggaran HAM masa lalu: ELSAM secara intensif mempromosikan pengadopsian pendekatan keadilan transisional untuk menyelesaikan berbagai kasus pelanggaran HAM yang berat di masa lalu. Tujuannya untuk memastikan keadilan dan pemulihan bagi korbannya, serta mencegah keberulangan.

Kemudian sebagai bagian dari upaya promosi dan penguatan kapasitas pemangku kepentingan, ELSAM terus menyelenggarakan berbagai pendidikan hak asasi manusia, melalui unit khusus pelatihannya. Pendidikan ini seperti Kursus HAM untuk Pengacara; Penyelenggaraan pelatihan dengan topik-topik khusus, seperti penanganan kasus HAM yang berat, kursus hak asasi manusia bagi aparat penegak hukum; dan Pelatihan untuk mempromosikan penggunaan pendekatan berbasis hak, bagi pengambil kebijakan, dan sektor bisnis, termasuk di dalamnya pelatihan bisnis dan hak asasi manusia, serta pelatihan yang terkait dengan perlindungan data pribadi.

Alamat:

Jl. Siaga II No. 31, Pasar Minggu, Jakarta 12510 INDONESIA

Telepon: (+62 21) 797 2662; Telefax: (+62 21) 7919 2519

Email: office@elsam.or.id; Website: www.elsam.or.id

Twitter: [@elsamnews](https://twitter.com/elsamnews), [@elsamlibrary](https://twitter.com/elsamlibrary); Facebook: [@elsamjkt](https://facebook.com/elsamjkt)



Revolusi digital telah menciptakan sebuah inovasi baru dalam kapasitas untuk memperoleh, menyimpan, memanipulasi dan mentransmisikan volume data secara nyata (*real time*), luas dan kompleks. Oleh karenanya revolusi digital seringkali dianggap identik dengan revolusi data. Perkembangan tersebut telah mendorong pengumpulan berbagai data, tidak lagi tergantung pada pertimbangan data apa yang mungkin berguna di masa depan. Perlindungan data pribadi sendiri merupakan aspek dinamis yang akan terus berhadapan dan dipengaruhi oleh kemajuan dan inovasi teknologi serta praktik bisnis. Salah satu faktor munculnya kejahatan dan penggunaan data pribadi secara melawan hukum disebabkan oleh perkembangan teknologi, Informasi, dan komunikasi. Saat ini, teknologi, Informasi, dan komunikasi telah merambah hampir semua aspek kehidupan dan mengubah perilaku kehidupan masyarakat menuju interaksi masyarakat berbasis elektronik dan internet. Pemanfaatan teknologi informasi, media, dan komunikasi telah mengubah baik perilaku

masyarakat maupun peradaban manusia secara global dan menyebabkan interaksi antar-manusia menjadi tanpa batas (*borderless*). Oleh karena itu, hukum perlindungan data harus dikerangkakkan secara tepat untuk mencegah penyalahgunaan atau kesalahan penanganan data. Tegasnya, bila peningkatan massif dalam pengumpulan data ini tidak dilakukan dalam kerangka penghormatan hak, maka mau tidak mau proses dan tujuannya akan digunakan dengan cara yang mengesampingkan hak-hak—privasi masyarakat.

Alamat:

Jl. Siaga II No. 31, Pasar Minggu, Jakarta 12510 INDONESIA

Tel.: (+62 21) 797 2662, Fax.: (+62 21) 7919 2519

Email: office@elsam.or.id, Website: www.elsam.or.id

Twitter: [@elsamnews](https://twitter.com/elsamnews), [@elsamlibrary](https://twitter.com/elsamlibrary)

Facebook: [@elsamjkt](https://www.facebook.com/elsamjkt) | Instagram: [@elsamnews](https://www.instagram.com/elsamnews)