Kedutaan Besar
Republik Indonesia
Brussel

EDISI 2021 NO. 6

RESEARCH SERIES

EMBASSY OF THE REPUBLIC OF INDONESIA IN BRUSSELS

A Policy Brief

EU GENERAL DATA PROTECTION REGULATION (GDPR)

Kedutaan Besar Republik Indonesia di Brussel
Boulevard de la Woluwe, 38
1200 Brussels Belgium
Email: rbi@embassyofindonesia.eu
https://kemlu.go.id/brussels

A Policy Brief
EU General Data Protection Regulation (GDPR)

Penulis:

Riza Roidila Mufti, Mahasiswa pasca sarjana pada program Communication Studies: New Media and Society in Europe, Vrije Universiteit Brussel, Belgia

Pendamping:

Dara Yusilawati, Koordinator Fungsi Pensosbud
Muhamad Mufti Arkan, Atase Keuangan
Nefertiti Hindratmo, Sekretaris I Fungsi Pensosbud
Muthia Chandra, Sekretaris II Fungsi Ekonomi

Daftar Isi

Pengantar

GDPR: Saat Kontrol Perlindungan Data Pribadi Dikembalikan pada Pengguna

Mengakses laman website di Eropa dan Indonesia seolah sama, tapi ternyata berbeda. Di Eropa, setiap mengakses laman website, terutama yang bersifat komersial, pengguna selalu disuguhkan dengan pop-up box berukuran besar bertuliskan "*Manage Your Privacy", "We Value Your Privacy*" atau "*Select Your Cookie Preferences*". Pengunjung bisa melakukan pengaturan privasinya dan punya hak untuk menolak atau memberi persetujuan (*consent*) untuk *cookie* dengan berbagai tujuan dari website tersebut.

Lewat pengaturan ini, pengguna bisa menolak jika tidak ingin perilaku online mereka dimonitor untuk tujuan personalisasi iklan, *marketing* atau untuk tujuan analisis lebih lanjut. Pengguna juga bisa menolak semua permintaan *consent* untuk *cookie* yang diajukan, dan tetap bisa mengakses website tersebut.

Di Indonesia hal seperti ini tidak terjadi. Saat membuka laman e-commerce, atau laman komersial lain, pengguna tidak diberikan pilihan pengaturan privasi atas data pribadinya. Kebanyakan website memang memiliki halaman "Kebijakan Privasi" dan menjelaskan apa yang mereka lakukan terhadap data pengunjung website. Namun, permintaan akan consent tidak ditanyakan kepada pengguna website. Pengguna juga tidak bisa mengatur privasinya secara langsung di website tersebut.

Di Uni Eropa, pengguna atau pengunjung website bisa melakukan pengaturan privasinya karena efek dari pemberlakukan *General Data Protection Regulation* (GDPR). GDPR membuat individu bisa memiliki kontrol lebih atas data pribadinya dan bagaimana data pribadinya digunakan pihak lain. Negara anggota Uni Eropa wajib menyediakan satu atau lebih badan independen otoritas publik yang bertanggung jawab untuk pengawasan dan penerapan GDPR.

Regulasi ini mengatur bahwa setiap individu berhak mendapatkan informasi dengan jelas tentang apa yang dilakukan terhadap data mereka. Semua pihak yang ingin memproses data pribadi juga wajib untuk memperoleh *consent* dari pemilik data. Hal ini dilakukan untuk mendorong penggunaan dan pemrosesan data pribadi yang lebih bertanggung jawab.

Figure 1: Laman website Amazon meminta persetujuan atas pengaturan *cookie* dan memberikan pilihan pengaturan kepada pengunjung

Sebagai regulasi, GDPR secara resmi berlaku di Uni Eropa pada 25 Mei 2018 di 27 negara anggota dan negara yang masuk dalam Europe Economic Area (EEA).

GDPR disebut sebagai "The toughest data protection law in the world" karena memiliki keketatan aturan dan sanksi yang besar bagi pelanggar. GDPR juga memiliki efek ekstra teritorial karena regulasi ini berlaku bagi semua pihak di manapun berada, termasuk yang berada di luar Uni Eropa, selama mereka melakukan kegiatan-kegiatan yang berkaitan dengan pemrosesan data individu yang tinggal di kawasan UE. GDPR memaksa perusahaan untuk lebih akuntabel, transparan, bertanggung jawab pada data pribadi pengguna dan meningkatkan *cybersecurity*-nya, jika tidak mau terkena denda.

Pemberlakukan GDPR membuat UE menjadi sorotan internasional, dimana:

- UE mempertahankan sepak terjangnya sebagai *leader* dan *global trendsetter* dalam *tech regulation* dengan hadirnya GDPR yang juga banyak menjadi katalis bagi negara lain untuk menerapkan regulasi serupa.
- Selama tiga tahun penerapan, GDPR menjatuhkan sanksi kepada sejumlah raksasa teknologi mulai Google, Facebook's WhatsApp, hingga Amazon dengan denda puluhan juta euro atas pelanggaran data pribadi yang mereka lakukan.
- Pemberlakukan GDPR berhasil mengundang masyarakat untuk melaporkan pelanggaran terhadap perlindungan data pribadi. Setidaknya 59,000 aduan dilaporkan hanya dalam waktu 8 bulan diberlakukannya aturan ini.

Laporan ini akan membahas pemberlakukan GDPR di Uni Eropa. Laporan ini mengupas tentang prinsip-prinsip dasar perlindungan data pribadi, legal basis pemrosesan data pribadi, hingga bagaimana kebijakan ini berdampak pada data pribadi masyarakat, terutama dalam ruang digital Eropa.

A Gambaran Umum

1. Sebuah Perkenalan: "Apa Itu GDPR?"

Apa itu GDPR?

GDPR adalah kepanjangan dari *General Data Protection Regulation*, sebuah regulasi yang dikeluarkan oleh Uni Eropa (UE) dan mulai berlaku pada 25 Mei 2018 di negara-negara anggota UE dan juga negara di kawasan EEA. GDPR bertujuan untuk melindungi data pribadi dan privasi individu yang tinggal di kawasan UE dan EEA dalam ranah digital[1] dan mendorong penggunan dan pemrosesan data pribadi yang lebih bertanggung jawab.

GDPR memiliki **efek ekstra teritorial** yang berarti regulasi ini berlaku bagi semua pihak di manapun berada, termasuk yang berada di luar UE, selama mereka melakukan kegiatan pemrosesan data individu yang tinggal di kawasan UE dan EEA[2]. Pemrosesan data pribadi menurut GDPR adalah termasuk kegiatan pengumpulan, perekaman, pengorganisasian, penataan, penyimpanan, pengambilan, dan penggunaan data pribadi residen UE[3].

Di Eropa, GDPR dikeluarkan untuk mengganti *Data Protective Directive* 1995, yang dianggap sudah ketinggalan jaman dalam menyediakan perlindungan data privasi dan standar keamanan data di era digital.

Kenapa GDPR menjadi hukum privasi dan keamanan data pribadi paling kuat di dunia?

GDPR disebut sebagai hukum keamanan data pribadi paling ketat dan paling kuat di dunia karena keketatan, sanksi dan skala penerapannya. GDPR berlaku tidak hanya bagi perusahaan, organisasi, atau entitas lain yang berbasis di UE yang memperoses data pribadi orang di UE. Aturan ini juga berlaku bagi organisasi yang ada di luar UE yang melakukan kegiatan pemrosesan data dan menarget orang yang tinggal di wilayan UE.

Aturan ini juga memiliki sanksi dan denda yang sangat keras kepada mereka yang melakukan pelanggaran. Denda dan hukuman bagi pihak pelanggar bisa mencapai puluhan juta euro. GDPR menjadi referensi dan katalis bagi banyak negara untuk memodernisasi aturan privasi dan perlindungan data pribadi mereka seperti Brazil, India, Chili, Korea Selatan, Kenya, Taiwan bahkan Indonesia[4]. Brazil bahkan sudah memberlakukan aturan perlindungan data yang baru terinspirasi dari GDPR ini.

2. Sejarah Lahirnya GDPR

Perlindungan data pribadi dan privasi menjadi perhatian Uni Eropa sejak sejak lahirnya *European Convention on Human Rights* tahun 1950. *Convention* ini menjadi dasar bagi lahirnya aturan-aturan terkait perlidungan data pribadi dan privasi di UE hingga akhirnya terlahir GDPR. Berikut *timeline* penting hingga akhirnya GDPR terbentuk[5]:

1 https://gdpr.eu/what-is-gdpr/
2 https://gdpr.eu/companies-outside-of-europe/
3 https://gdpr-info.eu/art-4-gdpr/
4 https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1166
5 https://gdpr.eu/what-is-gdpr/

1950

European Convention on Human Rights tahun 1950 dikeluarkan. *European Convention on Human Rights* tahun 1950 menyatakan bahwa semua individu memiliki hak perlindungan terhadap kehidupan pribadinya. Hal inilah yang menjadi dasar aturan berkaitan dengan perlindungan privasi dan data pribadi.

1995

Seiring dengan kemajuan teknologi dan adanya internet, UE mengeluarkan *European Data Protection Directive*. *Directive* merupakan arahan UE kepada negara anggotanya terkait perlindungan data pribadi. *Directive* ini menetapkan standar minimum keamanan privasi dan data pribadi yang harus diturunkan negara anggota UE dalam undang-undang nasional mereka.

2000

Kemajuan internet terus berlanjut. Mayoritas institusi keuangan di UE menawarkan layanan online banking.

2006

Facebook diluncurkan. Dengan konsep menghubungkan para penggunanya yang ada di berbagai wilayah di dunia, Facebook juga memanen data para pengguna.

2011

- Pengguna internet mulai banyak mempertanyakan perlindungan data pribadi mereka di internet. Pada tahun ini, seorang pengguna Gmail menuntut Google atas tindakan *scanning* terhadap e-mailnya.

- Dua bulan setelah itu, otoritas perlindungan data di UE menyatakan bahwa UE membutuhkan aturan dengan pendekatan lebih komprehensif terkait perlindungan data pribadi. UE mulai bekerja untuk memperbaharui *European Data Protection Directive* tahun 1995.

2016

GDPR disetujui dan disahkan setelah 3 tahun proses negosiasi antara Uni Eropa dengan berbagai institusi. Negara-negara anggota, dan berbagai pihak yang akan terdampak aturan ini termasuk platform besar seperti Facebook dan Google diberi waktu untuk melakukan transisi

2018

Pada tanggal 25 Mei 2018, GDPR resmi diberlakukan setelah dua tahun masa transisi dan persiapan.

3. Tujuan Dikeluarkannya GDPR

Kenapa GDPR dirasa penting di era digital? Apa tujuan utama diterbitkannya GDPR?

Di era digital, data pribadi seseorang sebagai pengguna internet dan konsumen menjadi aset yang sangat bernilai. Pihak-pihak seperti sosial media platform, *e-commerce*, *on-demand service platform* banyak melakukan kegiatan pemrosesan data pribadi konsumen seperti mengumpulkan data dan informasi pengguna, melakukan *tracking* terhadap perilaku online pengguna, hingga memproses lebih lanjut data pengguna. Sayangnya masih banyak pengguna internet yang secara tidak sadar dan sukarela memberikan data pribadi mereka tanpa tahu bagaimana data itu akan digunakan dan diproses oleh pihak lain.

Tujuan fundamental GDPR adalah ingin melindungi hak dasar individu atas perlindungan data pribadi mereka di era digital[6] *dan menjunjung tinggi prinsip penggunaan data pribadi secara bertanggung jawab dan transparan.*

Berikut tujuan-tujuan utama yang ingin dicapai melalui GDPR:

a) Memberikan kontrol yang lebih besar kepada individu yang ada di kawasan UE atas data pribadi mereka dan bagaimana data itu digunakan dan diproses oleh pihak lain[7]. Individu memiliki hak untuk memilih bersedia atau menolak penggunaan data pribadi mereka untuk keperluan tertentu.

   Contoh:

   - Dengan adanya GDPR, residen UE, bisa memilih untuk menolak atau mengizinkan permintaan suatu website untuk melihat dan memonitor jejak perilaku mereka di internet melalui *cookie* untuk kebutuhan analisis.
   - Dengan GDPR, pengguna internet bisa memilih untuk menolak atau menerima permintaan *consent* atas penggunaan data mereka untuk dengan tujuan personalisasi iklan dan *targeted* iklan.

b) Menyediakan aturan dan persayaratan yang mendetail kepada perusahaan, organisasi tentang bagaimana kegiatan pemrosesan data pribadi milik warga UE dilakukan secara bertanggung jawab.

c) Memastikan bahwa organisasi dan perusahaan yang melakukan kegiatan pemrosesan data residen di UE, bersifat akuntabel dan bertindak sesuai hukum saat mereka menggunakan data pribadi penggunanya.

d) GDPR juga ingin memastikan bahwa pengguna internet bisa terinformasikan tentang bagaimana data mereka dikumpulkan, disimpan, diakses, digunakan oleh pihak lain.

6 https://gdpr.eu/article-1-subject-matter-and-objectives-overview/
7 https://techcrunch.com/2018/01/20/wtf-is-gdpr/

4. Prinsip-Prinsip Penting dalam Penerapan GDPR

4.1 Prinsip-Prinsip Perlindungan Data Pribadi

Jika perusahaan, organisasi dan entitas lain melakukan kegiatan berkaitan dengan data pribadi individu yang tinggal di kawasan UE, maka mereka harus melakukannya sesuai dengan prinsip perlindungan data pribadi yang diatur dalam Pasal 5 GDPR [8 9]:

a) Sesuai hukum, adil dan transparan *(Lawfulness, fairness and transparency)*
Data pribadi harus diproses secara sah sesuai hukum, menjunjung prinsip keadilan dan transparan pada subyek data (individu yang datanya diproses).

b) Pembatasan tujuan *(Purpose limitation)*
Pemrosesan data harus dilakukan untuk tujuan yang jelas dan dijelaskan secara eksplisit pada subyek data. Pemrosesan lebih lanjut yang tidak sesuai dengan tujual awal yang diberitahukan kepada subyek data adalah tidak diperbolehkan.

c) Minimalisasi data *(Data minimization)*
Penggunaan data harus relevan, dan terbatas pada apa yang diperlukan sesuai dengan tujuan awal penggunaan data yang sudah diinfokan kepada subyek data. Data hanya boleh diproses tidak lebih dari yang dibutuhkan.

d) Akurasi *(Accuracy)*
Data harus akurat dan *up-to-date*

e) Pembatasan penyimpanan *(Storage limitation)*
Data pribadi hanya boleh disimpan selama periode waktu yang diperlukan untuk tujuan yang sudah ditentukan.

f) Integritas dan kerahasiaan *(Integrity and confidentiality)*
Pemrosesan data pribadi harus dilakukan dengan cara-cara yang bisa memastikan keamanan data, termasuk perlindungan dari pemrosesan yang tidak sah dan melanggar hukum yang bisa mengakibatkan kerugian yang tidak diinginkan. Hal ini bisa dicapai dengan menggunakan langkah-langkah keamanan teknis yang sesuai (misalnya dengan penggunaan enkripsi).

g) Akuntabel *(Accountability)*
Organisasi, perusahaan atau entitas lain yang melakukan pemrosesan data pribadi harus akuntabel dan bertanggung jawab dan bisa mendemonstrasikan bahwa mereka mematuhi prinsi-prinsip perlindungan data pribadi di atas.

4.2 Legal Basis Pemrosesan Data Pribadi

Kegiatan pemrosesan terhadap data pribadi harus dilakukan secara sah dan sesuai hukum. Untuk memenuhi keabsahan secara hukum, GDPR mengharuskan perusahaan atau organisasi untuk memiliki legal basis jika ingin melakukan pemrosesan data. Berikut 6 legal basis seperti dinyatakan dalam Pasal 6 GDPR. Pemrosesan data bisa dilakukan setidaknya, jika salah satu kondisi di bawah ini dipenuhi[10]:

a) *Consent*
Consent yang bisa diartikan sebagai izin atau persetujuan adalah elemen penting berkaitan dengan data pribadi yang wajib ada dalam pemrosesan data pribadi. Melakukan pemprosesan data pribadi pada dasarnya adalah dilarang, kecuali diizinkan oleh hukum atau jika subyek data memberikan *consent* untuk memprosesnya[11]. Dalam GDPR, *consent* harus diperoleh sebelum data dikumpulkan dan diproses. *Consent* harus diberikan secara sukarela atas kemauan

8 https://gdpr.eu/article-5-how-to-process-personal-data/
9 https://gdpr.eu/what-is-gdpr/
10 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_en
11 https://gdpr-info.eu/issues/consent/

subyek data. Permintaan akan *consent* harus disampaikan secara spesifik, jelas dan tidak ambigu.

Contoh: Sebuah website brand fashion harus meminta persetujuan pembeli/pengunjung website jika ingin mengumpulkan dan memonitor perilaku online dan preferensi pencarian pengguna di internet dengan tujuan untuk memberikan anjuran tentang produk yang mirip atau digunakan untuk menampilkan iklan di *third party* website yang berpartner dengan website brand fashion ini.

b) *Performance of Contract/Contractual Obligation.*

Pemrosesan data diperlukan sebagai bagian dari *contractual obligation* dari kedua pihak di mana subyek data menjadi pihak yang mengambil langkah atas permintaan pemrosesan data.

Contoh: Sebuah perusahaan yang menjual barang secara online, bisa memproses data pembeli untuk mengambil langkah lanjutan atas permintaan pembeli sebagai individu. Perusahaan bisa memproses nama, dan alamat pengiriman untuk melakukan pengiriman barang setelah pembeli melakukan *check-out* dan pembayaran.

c) *Legal Obligation*

Pemrosesan data diperlukan untuk pemenuhan kepatuhan kepada suatu kewajiban hukum di bawah Uni Eropa atau legislasi nasional.

Contoh: Sebuah perusahaan uang memiliki karyawan perlu menyediakan data pribadi karyawannya kepada otoritas untuk mendapatkan perlindungan jaminan sosial sesuai undang-undang.

d) *Vital Interest*

Pemrosesan diperlukan untuk pelindungi kepentingan vital dari subyek data atau individu lain. Contoh: Rumah sakit tidak perlu konsen untuk melakukan tindakan emergency bagi korban kecelakaan serius demi keselamatan korban.

e) *Public Interest*

Pemrosesan diperlukan untuk pelaksanaan tugas yang harus dilakukan untuk kepentingan publik atau dalam pelaksanaan wewenang resmi yang diberikan kepada *data controller*.

f) *Legitimate Interest*

Pemrosesan diperlukan untuk tujuan dan kepentingan yang sah yang dilakukan oleh data controller atau pihak ketiga. Pemrosesan dilakukan dengan cara yang diharapkan oleh subyek data. Pemrosesan data memiliki manfaat yang jelas, dan punya sedikit resiko melanggar privasi subyek data.

Contoh: Perusahaan atau organisasi memastikan keamanan jaringan perusahaan dengan cara memonitor penggunaan perangkat IT karyawannya. Perusahaan boleh melakukan proses monitoring untuk tujuan yang disebutkan, hanya jika metode yang paling aman dan tidak menganggu dipilih untuk menghormati hak perlindungan data dan privasi pegawainya. Misalnya dengan cara membatasi akses ke website-website tertentu.

4.3 Hak-Hak Subyek Data

Salah satu yang menjadi hal paling menarik dari GDPR adalah aturan ini memperkenalkan hak-hak baru bagi individu kaitannya dengan bagaimana mereka bisa mengontrol data mereka yang ada di internet dan penggunaan atas datanya oleh pihak lain. Di bawah GDPR individu yang datanya diproses (subyek data) dijamin haknya sesuai Pasal 12-22:

a) Hak untuk diinformasikan *(Right to be informed)*

Setiap individu yang datanya diambil, punya hak untuk tahu dan diberitahu secara jelas dan gamblang data apa yang dikumpulkan dari mereka dan apa yang perusahaan atau organisasi lakukan dengan data mereka.

b) Hak untuk akses *(Right to access)*

Setiap individu punya hak untuk mengakses datanya, mendapat *copy* dari data pribadinya yang sudah dikumpulkan oleh pihak lain seperti organisasi atau perusahaan yang melakukan pemrosesan datanya.

c) Hak untuk mengubah/memperbaiki *(The right to rectification)*

Setiap individup punya hak untuk melakukan perbaikan atau melakukan koreksi atas datanya yang dianggap kurang tepat atau kurang lengkap.

d) **Hak untuk menghapus *(The right to erasure/ Right to be forgotten)***
Setiap individu punya hak untuk datanya dihapus. Organisasi atau perusahaan harus menghormati pemintaan subyek data untuk menghapus datanya.

e) **Hak untuk membatasi pemrosesan *(The right to restrict processing)***
Setiap individu punya hak untuk membatasi pemrosesan atas data pribadinya.

f) **Hak atas portabilitas data *(The right to data portability)***
Setiap individu memiliki hak untuk mentransfer datanya dari satu *data controller* ke *data controller* atau organisasi lain di bawah kondisi tertentu.

g) **Hak untuk menolak *(The right to object)***
Individu berhak untuk menolak pemrosesan data pribadinya misalnya menolak untuk datanya diproses dengan tujuan direct marketing atau monitoring.

h) **Hak terkait dengan pengambilan keputusan dan pembuatan profil otomatis *(Rights in relation to automated decision making and profiling)***
Individu berhak untuk tidak menjadi subyek bagi keputusan yang semata-mata didasarkan pada *automatic processing* termasuk di dalamnya profiling otomatis, yang menghasilkan efek hukum kepada dirinya atau mebawa dampak signifikan kepadanya

5. Data dalam Ruang Lingkup dan Konteks GDPR

Jenis data apa saja yang diatur dalam GDPR?

GDPR hanya berlaku bagi **data pribadi**[12]. Data pribadi adalah informasi apa saja yang berkaitan dengan seorang individu hidup yang dapat secara langsung atau tidak langsung mengidentifikasi individu tersebut[13]. **Subyek data (Data subject)** adalah orang atau individu yang data pribadinya diproses. Subyek data bisa merupakan pengguna internet, pelanggan online marketplace, pengunjung website, dll.

Apa yang termasuk data pribadi?

- Nama
- Alamat tempat tinggal
- Alamat e-mail
- Nomor telepon
- Nomor ID card, Nomor paspor
- Informasi pendapatan
- IP address
- Data lokasi, *geolocation*
- Web cookies
- Dll yang bisa mengidentifikasi individu

Data pribadi juga meliputi data pribadi dalam kategori khusus seperti[14]:

- Informasi ras atau suku
- Orientasi seksual
- Political opinions
- Agama dan kepercayaan, filosofis
- Keanggotaan serikat pekera
- Data genetik
- Data Biometrik
- Medical Records

12 https://gdpr.eu/eu-gdpr-personal-data/
13 https://gdpr-info.eu/art-4-gdpr/
14 https://gdpr-info.eu/art-9-gdpr/

Apa yang dimaksud pemrosesan data *(Data processing)*?

Setiap tindakan yang dilakukan pada data pribadi, baik secara otomatis atau manual. Kegiatan pemrosesan data adalah semua kegiatan yang berhubungan dengan penggunaan data termasuk mengumpulkan, merekam, mengatur, menyusun, menggunakan, menganalisis, hingga menghapus data[15, 16, 17].

GDPR hanya berlaku untuk data pribadi yang diproses dengan salah satu dari 2 cara berikut ini[18]:

- Data pribadi diproses seluruhnya atau sebagian dengan cara otomatis atau secara otomat (*automated*) atau informasi dalam bentuk elektronik
- Data pribadi yang diproses secara non-otomatik yang merupakan bagian dari sistem pengarsipan atau catatan tertulis dalam sistem pengarsipan yang manual

Dalam kondisi apa data pribadi boleh dan sah untuk diproses menurut GDPR?

Perusahaan, organisasi, atau entitas yang bersifat profesional dan komersial wajib mematuhi beberapa aturan kunci di bawah ini jika ingin memproses data pribadi pengguna. Berikut aturan-aturan kunci GDPR dalam pemrosesan data pribadi [19,20,21]:

- Data pribadi harus diproses secara sah sesuai hukum, transparan dan memastikan adanya keadilan terhadap individu yang data pribadinya diproses. ***(lawfulness, fair and transparent)***
- Harus ada tujuan khusus untuk bisa memproses data. Perusahaan, organisasi atau entitas yang memproses data harus menjelaskan tujuan tersebut secara gamblang kepada individu saat melakukan pengumpulan data pribadi mereka. Perusahaan, organisasi tidak bisa menggunakan data pribadi untuk tujuan yang tida ditentukan ***(Purpose limitation).***
- Penggunaan data pribadi harus relevan, dan terbatas pada apa yang diperlukan sehubungan dengan tujuan awal penggunaan data yang sudah dinyatakan secara eksplisit kepada pemilik data. Data hanya boleh diproses tidak lebih dari yang dibutuhkan ***(Data minimization).***
- Perusahaan, organisasi atau entitas lain yang memproses data harus memastikan bahwa data pribadi akurat dan paling *up to date*, dengan juga memperhatikan tujuan pemrosesannya. Mereka juga harus mengoreksi tidak akurat ***(accuracy)***
- Perusahaan, organisasi atau entitas yang menggunakan data pribadi tidak bisa lagi menggunakan data pribadi untuk tujuan lain yang tidak sesuai dengan tujuan semula ***(compatible)***
- Perusahaan, organisasi atau entitas yang menggunakan data pribadi harus memastikan bahwa data pribadi disimpan tidak lebih dari yang diperlukan untuk tujuan pengumpulan. Data pribadi hanya boleh disimpan selama deiperlukan untuk tujuan yang sudah ditentukan ***(storage limitation)***
- Perusahaan, organisasi atau entitas yang menggunakan data pribadi harus memasang pengamanan teknis dan organisasional yang layak yang bisa memastikan keamanan dari data pribadi. Termasuk pengamanan teknis untuk memastikan perlindungan terhadap pemrosesan yang tidak sah dan melanggar hukum, kerusahan atau kehancuran data yang tidak sengaja dengan teknologi yang layak ***(integrity and confidentiality)***
- Perusahaan, organisasi atau entitas yang menggunakan data bertanggung jawab untuk bisa mendemonstrasikan bahwa mereka mematuhi prinsi-prinsip perlindungan data pribadi di atas ***(accountability).***

15 https://gdpr.eu/what-is-gdpr/
16 https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en
17 https://gdpr-info.eu/art-4-gdpr/
18 https://gdpr.eu/article-2-processing-personal-data-by-automated-means-or-by-filling-system/
19 https://gdpr.eu/eu-gdpr-personal-data/
20 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_en
21 https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm

Siapa yang melakukan pemrosesan data pribadi?

Selama pemrosesan, data pribadi bisa ditangani oleh berbagai perusahaan dan organisasi. Dalam siklus pemrosesan ini ada dua pelaku utama yang menangani data pribadi:

1) **Pengontrol Data *(Data Controller)***
   Pihak yang memutuskan mengapa dan bagaimana data pribadi akan diproses. Pemilik atau karyawan di perusahaan atau organisasi lain yang menangani data pribadi milik subyek data adalah *data controller*. Contoh: Facebook merupakan *data controller* bagi semua data penggunanya.

2) **Pemroses Data *(Data Processor)***
   Pihak ketiga yang memproses data pribadi atas nama *data controller.* GDPR memiliki aturan khusus untuk pihak ketiga ini.

Contoh-contoh kegiatan data processing:

- Menyimpan IP address atau MAC address
- Mengakses database kontak yang berisi data pribadi
- Mengirim email promosi juga merupakan bentuk dari pemrosesan data
- Melakukan *behaviour monitoring* atas perilaku online dan preferensi seseorang

6. Ruang Lingkup dan Skala Penerapan GDPR (Teritorial Scope)

Berlaku pada siapa sajakah aturan dalam GDPR?

GDPR berlaku bagi semua organisasi, perusahaan atau entitas dalam bentuk lain yang melakukan pemrosesan data pribadi orang yang tinggal di UE[22]. GDPR hanya berlaku organisasi yang terlibat dalam "**aktivitas profesional atau komersial**"[23].

Dalam cakupan teritorial, GDPR otomatis berlaku pada semua oganisasi, perusahaan yang berada di UE. GDPR juga memiliki **efek ekstra teritorial**. Artinya aturan juga berlaku bagi semua pihak di manapun berada, bahkan yang ada di luar UE sekalipun, selama mereka melakukan kegiatan-kegiatan pemrosesan data pribadi milik residen UE maka mereka harus patuh kepada GDPR.

Menurut Pasal 3 GDPR, terkait ruang lingkup teritorial, berikut pihak-pihak yang wajib patuh terhadap GDPR [24, 25]:

1) Organisasi, perusahaan atau entitas lain (*data contoller*) yang berbasis di UE dan melakukan pemrosesan data pribadi residen UE. Hal ini terlepas di mana pemrosesan data dilakukan di dalam kawasan UE atau di luar UE.
   Contoh: Sebuah *food delivery apps* berbasis di UE, mengharuskan pengguna untuk mendaftar dan mengisi data mereka sebelum dapat menggunakan aplikasi tersebut, maka perusahaan ini wajib patuh dengan aturan GDPR.

2) Perusahaan, institusi atau organisasi non-UE yang berada di luar UE tetap diharuskan untuk tunduk dalam aturan ini jika mereka:

22 https://gdpr.eu/what-is-gdpr/
23 https://gdpr.eu/companies-outside-of-europe/
24 https://gdpr.eu/article-3-requirements-of-handling-personal-data-of-subjects-in-the-union/

a) Menawarkan barang dan jasa pada residen UE
Contoh: Perusahaan di Amerika Serikat yang menarget pasar Jerman, dan membuat iklan yang menyasar konsumen Jerman dengan menawarkan produk mereka dengan harga dalam Euro, maka wajib untuk patuh tehadap GDPR.

b) Memonitor perilaku orang yang tinggal di kawasan UE
Contoh: Jika sebuah perusahaan di luar UE menggunakan web tools yang membuat perusahaan ini bisa memonitor *cookies* atau IP addresses dari pengunjung website yang berasal dari UE, maka perusahaan ini juga masuk dalam ranah GDPR.

3) GDPR berlaku bagi kegiatan pemprosesan data yang dilakukan oleh *data controller* yang tidak berada di kawasan EU, namun di tempat di mana hukum di negara anggota UE berlaku karena berdasarkan hukum internasional.

Pengecualian dalam Penerapan GDPR

Ada beberapa pengecualian penting yang harus diperhatikan dalam penerapan GDPR, berikut di bawah ini[26]:

1. **Aktivitas yang sangat personal dan aktivitas rumah tangga.**
   Contoh: Saat kita mengumpulkan alamat e-mail teman-teman kita dengan tujuan untuk mengundang mereka ke pesta atau piknik bersama, kita tidak masuk dalam kategori wajib tunduk terhadap GDPR. Hal ini kembali pada dasar bahwa GDPR hanya berlaku bagi organisasi yang terlibat aktivitas profesional atau komersial.
2. **Sejumlah pembebasan kewajiban bagi UKM, namun hanya dengan kondisi tertentu**
   Implementasi GDPR tidak melihat besar kecilnya entitas, tapi melihat jenis kegiatan yang dilakukan. Jika perusahaan, terlepas dari ukurannya, memiliki bisnis dimana pemrosesan data merupakan bagian utama dari bisnisnya, dan bisa menimbulkan resiko terhadap data pribadi individu, maka mereka tetap wajib patuh terhadap GDPR tanpa pengecualian. **Beberapa kewajiban GDPR bisa dibebaskan bagi UKM atau perusahaan kecil jika:**

   - Perusahaan dengan jumlah karyawan kurang dari 250 orang, tidak diwajibkan untuk menyimpan *record* dari aktivitas pemrosesan datanya. Kecuali jika pemrosesan data adalah kegiatan utama mereka dan kegiatan mereka beresiko bagi data pribadi individu maka tetap wajib patuh kepada GDPR[27]
   - UKM tidak perlu menunjuk / mengangkat *Data Protection Officer* jika pemrosesan data pribadi tidak menjadi bagian utama dari bisnis mereka dan aktivitas yang dilakukan tidak beresiko besar pada individu.

7. Badan Otoritas Pelaksana dan Pengawas GDPR dan Mekanisme Kerjanya

Sebagai regulasi UE, GDPR otomatis berlaku di 27 negara anggota UE. Pelaksanaan GDPR dikawal ketat oleh *European Data Protection Board (EDPB)*, yang sengaja dibentuk khusus pengawal pelaksanaan GDPR di tingkat UE. Sementara itu penerapan dan pengawasan di masing-masing negara dikawal oleh *Data Protection Authotries/ Supervisory Authorities*. EDPB bekerja sama dengan DPA dalam mengawal penarapan GDPR. Berikut secara detail badan-badan yang memiliki peran penting dalam pelaksanaan GDPR:

26 https://gdpr.eu/companies-outside-of-europe/
27 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-rules-apply-smes_en

1. Otoritas Pengawas *(Supervisory Authorities / Data Protection Authorities)*

Sesuai dengan bunyi GDPR Pasal 51, setiap negara anggota UE wajib menyediakan satu atau lebih badan independen otoritas publik yang bertanggung jawab untuk pengawasan dan penerapan GDPR, menyikapi jika ada pelaporan tindakan pelanggaran, hingga menjatuhkan sanksi untuk kasus pelanggaran regulasi[28]. Dalam konteks GDPR, *Supervisory Authorities* disebut juga *Data Protection Authorities* (DPA).

DPA merupakan badan yang penting untuk pengawasan dan penerapan GDPR di masing-masing negara. Sebagai otoritas DPA menjadi jujugan jika ada pertanyaan terkait GDPR atau aduan pelanggaran di negara-negara UE. Dalam Pasal 31 GDPR disebutkan bahwa *data controller* dan *data processor* pribadi harus kooperatif dengan DPA dalam melakukan kegiatan mereka.

Berikut di bawah ini daftar *Data Protection Authorities* di setiap negara di UE dan EEA[29]

Negara	Data Protection Authorities
Austria	Österreichische Datenschutzbehörde
Belgia	Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)
Bulgaria	Commission for Personal Data Protection
Kroasia	Croatian Personal Data Protection Agency
Siprus	Commissioner for Personal Data Protection
Republik Ceko	Office for Personal Data Protection
Denmark	datatilsynet
Estonia	Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)
Finlandia	Office of Data Protection Ombudsman
France	Commission Nationale de l'Informatique et des Libertes
Jerman	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Yunani	Hellenic Data Protection Authority
Hungaria	Hungarian National Authority for Data Protection and Freedom of Information
Irlandia	Data Protection Comission
Italia	Garante per la protezione dei dati personali
Latvia	Data State Inspectorate
Lithuania	State Data Protection Inspectorate
Luxembourg	Commission Nationale pour la Protection des Données
Malta	Office of the Information and Data Protection Commissioner
Belanda	Autoriteit Persoonsgegevens
Polandia	Urząd Ochrony Danych Osobowych (Personal Data Protection Office)
Portugal	Comissão Nacional de Proteção de Dados - CNPD
Romania	The National Supervisory Authority for Personal Data Processing
Slovakia	Office for Personal Data Protection of the Slovak Republic
Slovenia	Information Commissioner of the Republic of Slovenia
Spanyol	Agencia Española de Protección de Datos (AEPD)
Swedia	Integritetsskyddsmyndigheten

28 https://gdpr-info.eu/art-51-gdpr/
29 https://edpb.europa.eu/about-edpb/about-edpb/members_en#member-ie

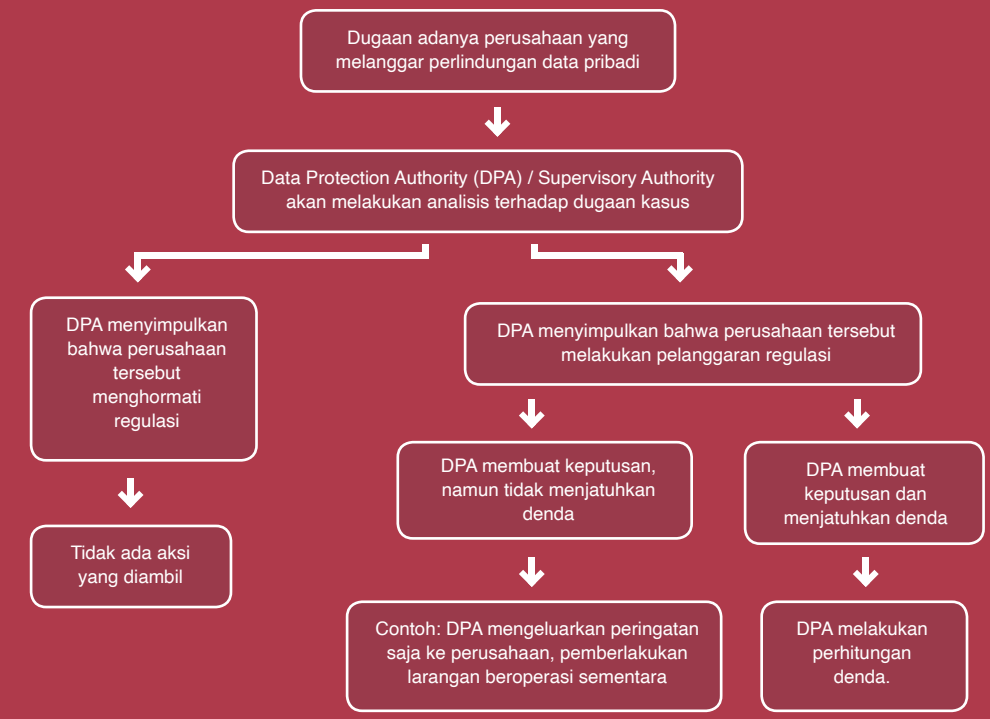
Berikut peran dan tugas *Data Protection Authorities* di masing-masing negara[30,31]:

a) Melakukan monitoring terhadap penerapan GDPR
b) Menginformasikan dan meningkatan kesadaran publik tentang hak dan resiko dalam kaitannya dengan perlindungan data pribadi di bawah GDPR
c) Meningkatatkan kesadaran *data controller* dan *data processor* tentang kewajiban mereka dalam menanangi data pribadi milik orang di bawah GDPR
d) Bekerja sama dengan sesama badan otoritas pengawas GDPR di masing-masing negara UE dan *European Data Protection Board*
e) Menangani pengaduan terhadap laporan pelanggaran GDPR dan melakukan investigasi atas pengaduan tersebut
f) Menyediakan saran dari ahli tentang isu perlindungan data pribadi
g) Menjadi kontak poin utama jika ada pertanyaan terkait perlindungan data pribadi di setiap negara anggota.

Kewenengan *Data Protection Authorities* dalam penerapan aturan GDPR:

a) Kewenangan untuk melakukan investigasi, tindakan korektif dan kepenasehatan (Pasal 58)
b) Kewenangan untuk menjatuhkan denda pada data controllers dan processors (Pasal 83)

Mekanisme Pengawasan dan Pemberian Sanksi Oleh DPA



Source: https://ec.europa.eu/info/sites/default/files/data-protection-factsheet-role-edpb_en.pdf

30 https://uk.practicallaw.thomsonreuters.com/w-014-8205?transitionType=Default&contextData=(sc.Default)&firstPage=true
31 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-role-data-protection-authority_en

2. *European Data Protection Board* (EDPB) [32 33 34 35]

European Data Protection Board (EDPB) adalah sebuah badan independen yang sengaja dibuat oleh GDPR untuk mengawal konsistensi pelaksanaan aturan ini di negara-negara UE. Berkantor di Brussels, EDPB terdiri dari perwakilan DPA dari masing-masing negara anggota dan *European Data Protection Supervisor* (EDPS). EDPB memegang beberapa peranan krusial sebagai berikut:

a) Menyediakan arahan dasar tentang GDPR termasuk pedoman, rekomendasi dan best practice untuk mempromosikan pemahaman yang seragam tentang GDPR
b) Memastikan pelaksanaan GDPR di seluruh negara-negara Uni Eropa dapat dilakukan secara seragam dan konsisten.
c) Memastikan kerja sama yang efektif bagi sesama *Data Protection Authotirities* (DPA) di masing-masing negara anggota.
d) Mengeluarkan atau menerbitkan pedoman-pedoman lanjutan tentang konsep utama dan interpretasi mengenai GDPR secara berkala
e) Mengatur dengan keputusan yang mengikat dalam sengketa terkait *cross-border processing* dan memastikan adanya keseragaman dalam pelaksanaan aturan EU untuk menghindari terjadinya kasus yang serupa tapi berpotensi ditangani secara berbeda di negara.

8. Pihak-Pihak yang Terdampak dengan Penerapan GDPR

Secara garis besar, penerapan GDPR berdampak pada siapa saja?

- **Semua individu yang berada di Uni Eropa**. Semua individu yang menjadi subyek data, atau orang yang datanya diproses pihak lain terdampak oleh GDPR. Mereka bisa siapa saja mulai pengguna *e-commerce*, pengguna sosial media, pengunjung website berita, pengguna aplikasi *food delivery*, atau pengguna internet secara umum bisa terdampak.
- **Semua organisasi, bisnis, perusahaan, otoritas publik, dan entitas lainnya**, di manapun mereka berada, yang terlibat dalam aktivitas profesional atau komersial dan melakukan kegiatan pemrosesan data pribadi orang lain juga terdampak GDPR[36].

Pihak manakah atau industri apakah yang paling terdampak dengan penerapan GDPR?

Industri yang paling terdampak dan harus patuh dengan GDPR adalah industri yang bisnis utamanya adalah pemrosesan data pribadi dan yang memproses data pribadi pengguna dengan jumlah yang masif dan besar. Berikut ini pihak-pihak yang terdampak keras oleh GDPR [37,38,39,40]:

1. ***Tech Company***
   Google, Facebook, Amazon, Apple dan **perusahaan teknologi raksasa** lainnya. Perusahaan teknologi seperti **Google, Facebook, Amazon, Apple** dan perusahaan teknologi raksasa lainnya sudah pasti harus mematuhi aturan GDPR. Perusahaan teknologi raksasa seperti ini mengumpulkan data pengguna dan memprosesnya dalam jumlah besar. Model bisnis dari perusahaan teknologi inipun juga sangat ditopang oleh data pengguna.

32 https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en
33 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_en
34 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e5663-1-1
35 https://ec.europa.eu/info/sites/default/files/data-protection-factsheet-role-edpb_en.pdf
36 https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you
37 Idem
38 https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html
39 https://cloudtweaks.com/2018/05/5-industries-most-affected-gdpr/
40 https://www.ns-businesshub.com/transport/gdpr-sectors-not-expected-affected/

2. **Sosial media dan komunitas online**
   Semua platform sosial media dan platform komunitas online mulai dari Twitter, TikTok, Facebook, Instagram, YouTube, Reddit, dll wajib untuk patuh pada GDPR. Platform seperti ini juga mengumpulkan dan memproses banyak data pengguna. Saat pengguna sosial media atau komunitas online ingin *sign-up* pada platform ini setiap pengguna harus menyertakan data pribadi mereka seperti, nama, tanggal kelahiran, alamat e-mail, hingga nomor telepon.

3. ***E-commerce, online retailer, online business***
   Semua platform *e-commerce*, dan *online business* juga wajib patuh dengan GDPR. Amazon, Bol.com, Zalando, dan semua *online retailers* yang menawarkan produknya atau jasanya pada pengguna secara online dan melakukan pemrosesan data pengguna wakjib patuh pada GDPR. Brand komestik, fashion, footwear yang memiliki layanan online untuk pembelinya lewat website juga harus patuh dengan aturan GDPR.

4. **Penyedia layanan *on-demand***
   Penyedia layanan *on-demand service* mulai *ride hailing service* seperti Uber, sampai *food delivery service* seperti Deliveroo dan UberEats juga wajib patuh dengan aturan GDPR.

5. ***Online/Digital Financial Service and Banking***
   Perbankan digital dan layanan keuangan seperti fintech wajib patuh dengan GDPR karena mereka mengumpulkan dan memproses data pengguna.

6. ***Medical and Healthcare***
   Industri medis dan kesehatan juga menjadi pihak yang harus patuh dengan aturan GDPR. Di era teknologi ini, industri kesehatan juga *go online* seperti aplikasi layanan telemedicine dan rumah sakit yang menawarkan layanan online dan menyimpan data pasien melalui cloud system dan sebagainya. Hal ini membuat banyak pemain di sektor medis dan kesehatan harus patuh dengan GDPR.

7. ***Logistics Service***
   Layanan logistik, terutama layanan pengiriman barang pada pelanggan adalah sektor yang juga terdampak penerapan GDPR. Layanan logistik dan kurir mengumpulkan data pribadi pengguna dalam melakukan misi pengiriman sehari-hari termasuk mengumpulkan informasi kontak dan alamat pengguna[41]. Perusahaan-perusahaan pengiriman barang atau kurir yang beroperasi di UE seperti Bpost, DPD hinggal DHL sudah menerapkan GDPR.

8. ***Media Organization (News Website)***
   GDPR juga berdampak pada media organisasi yang memiliki website berita seperti The Brussels Times dan Le Soir . Aturan ini juga berlaku bagi website berita lainnya di luar UE yang juga men-track data pengunjung wesbite yang berasal dari UE seperti website *The New York Times, The Washington Post* dan lainnya. Saat kita menjadi pengunjung website berita, data kita terkadang juga dikumpulkan oleh media yang bersangkutan saat kita *sign-up* dan *login* ke laman berita. Data dikumpulkan dengan berbagai tujuan seperti untuk analisis atau untuk targeted marketing.

9. **Otoritas publik, layanan publik**
   Sektor publik, yang menyediakan layanan publik dan otoritas publik juga menjadi sektor yang terdampak GDPR. Institusi pemerintah, mulai dari nasional, dan tingkat lokal juga wajib patuh GDPR. Sektor publik banyak menagani data-data pribadi milik residen. Commune atau Municipality di Belgia misalnya yang menangani data pribadi orang yang tinggal di setiap area administrasi commune tersebut juga wajib patuh kepada GDPR.

41 https://lot.dhl.com/data-protection-and-its-legal-implications-on-logistics/

10. Sekolah dan Universitas

GDPR sudah pasti berdampak pada institusi pendidikan seperti univesitas dan sekolah yang juga banyak meng-handle data-data milik siswanya. Tidak hanya yang ada di Uni Eropa, yang di luar Uni Eropa pun wajib tunduk pada aturan GDPR jika mereka memegang data pelajar atau mahasiswa dari Uni Eropa. Universitas di United States misalnya, yang menerima mahasiswa internasional dari Uni Eropa harus pastuh dalam aturan ini. Saat calon siswa dari Uni Eropa akan masuk ke universitas di US, mereka harus mengisi formulir online tentang data mereka maka data mereka harus dilindungan di bawah GDPR[42, 43].

11. Dan lain-lain

Apakah GDPR juga berdampak pada *small and medium-sized enterprises* (SME) atau UKM?

Ya[44]. Jika ada perusahaan yang merupakan UKM dan melakukan kegiatan pemrosesan data pribadi pengguna atau pelanggan, mereka tetap harus patuh terhadap aturan GDPR. Implementasi regulasi data pribadi tidak bergantung pada besar kecilnya perusahaan atau organisasi, tapi bergantung pada natur aktivitas yang dilakukan. Jika dalam kegiatannya mereka melakukan pemrosesan data pribadi sudah pasti mereka wajib patuh dengan GDPR.

Namun, dalam konteks UKM, jika pemrosesan data pribadi tidak menjadi bagian dari core bisnis suatu UKM, dan aktivitas yang dilakukan tidak menimbulkan resiko besar bagi data pribadi individu maka beberapa kewajiban dalam GDPR tidak perlu dilakukan. Pengecualian yang bisa didapatkan[45]:

- UKM dengan karyawan kurang dari 250 orang dibebaskan dari kewajiban *record-keeping* pemrosesan data, kecuali jika pemrosesan data pribadi adalah aktivitas regular dan utama mereka dan kegiatan yang dilakukan bisa menimbukan resiko atau ancaman terhadap data pribadi individu at au menyangkut data sensitif.

Bagaimana jika GDPR diterapkan di Indonesia?

Jika aturan tentang perlindungan data pribadi yang serupa dengan GDPR diterapkan di Indonesia, maka Google, Facebook, Instagram, YouTube dan perusahaan teknologi lainnya yang beroperasi di Indonesia seperti perusahaan transportasi online, *e-commerce* dan perusahaan *travel online* sudah pasti harus patuh dengan aturan ini di Indonesia. Perusahaan-perusahaan di atas mengumpulkan data pengguna dan melakukan pemrosesan data pengguna dalam jumlah yang besar dan masif. Aplikasi penyedia layanan digital perbankan, dan aplikasi pijaman *online* juga sudah pasti juga harus patuh dengan aturan ini karena layanan finansial juga banyak mengumpulkan data pribadi pengguna. Institusi milik pemerintah mulai dari kementerian sampai dinas yang ada di daerah juga wajib patuh dengan aturan perlindungan data pribadi apalagi jika mereka banyak menangani data dari warga seperti dinas kependudukan dan catatan sipil.

42 https://www.stonegroup.co.uk/insights/how-will-gdpr-affect-schools/
43 https://moderncampus.com/blog/gdpr-and-higher-education.html
44 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-rules-apply-smes_en
45 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-rules-apply-smes_en

9. Kewajiban yang Harus Dilakukan Perusahaan/Organisasi terkait GDPR

Apa saja kewajiban yang harus dilakukan perusahaan atau organisasi terkait GDPR?

a) Perusahaan, organisasi atau entitas lainnya yang melakukan kegiatan pemrosesan data pribadi wajib mematuhi semua prinsip-prinsip perlindungan data pribadi seperti dijabarkan pada Pasal 5 yang sudah dijelaskan dalam laporan ini mengenai prinsip-prinsip perlindungan pribadi.
b) Perusahaan, organisasi wajib melakukan pemrosesan data secara sah dan sesuai hukum *(lawfullness of processing)* seperti dijabarkan pada Pasal 6. Untuk memproses data secara sah, perusahaan atau organisasi wajib memiliki salah satu dari legal basis pemrosesan data pribadi yang sudah dijelaskan dalam laporan ini sebelumnya.
c) Perusahaan wajib memahami dan menghormati hak-hak individu yang datanya diproses (subyek data) dan mengikuti aturan GDPR untuk melakukan pemenuhan terhadap hak-hak tersebut. Hal ini untuk menghindari pelanggaran karena melanggar hak-hak subyek data
d) Perusahaan juga wajib bertanggung jawab untuk membuktikan atau mendemonstrasikan kepatuhannya terhadap GDPR.
e) Di bawah kondisi tertentu GDPR mewajibkan perusahaan atau organisasi menunjuk orang untuk menjadi *Data Protection Officer* (DPO). DPO memiliki tugas untuk mengawasi kepatuhan organisasi atau perusahaan terhadap GDPR. DPO juga diharuskan memiliki pengetahuan akan undang-undang dan praktik perlindungan data pribadi. Namun tidak semua organisasi atau perusahaan harus memiliki DPO. Kewajiban memiliki DPO hanya diwajibkan untuk perusahaan atau organisasi yang memenuhi satu atau kriteria di bawah ini[46]:

- **Otoritas publik *(Public Authority)***
  Jika pemrosesan data pribadi dilakukan oleh badan publik atau otoritas publik maka wajib hukumnya menunjuk DPO, dengan pengecualian diberikan kepada pengadilan atau otoritas yuridisial independen lain.
- **Melakukan monitoring data secara berkala dengan skala besar**
  Perusahaan atau organisai wajib memiliki DPO jika pemrosesan data pribadi yang mereka lakukan adalah aktivitas inti organisasi tersebut yang secara reguler dan sistematis dilakukan mengamati subyek data dalam skal besar. Contoh: *tech giant company* seperti Facebook wajib memiliki DPO untuk memastikan kepatuhannya terhadap GDPR
- **Memproses *special data categories* dengan skala besar**
  Perusahaan atau organisasi yang melakukan pemrosesan terhadap data khusus tertentu yang dilakukan dalam skala besar dan hal itu menjadi aktivitas inti dari perusahaan. Atau organisasi tersebur. Special data categories atau data khusus tertentu menurut GDPR adalah data tentang ras dan suku, political opinion, agama dan kepercayaan, keanggotaan serikat pekerja, data genetik, data biometrik, dan informasi tentang orientasi seksual seseorang.

46 https://gdpr.eu/data-protection-officer/

10. Sanksi dan Denda terhadap Pelanggaran GDPR

GDPR berlaku bagi semua jenis organisasi dan bisnis, mulai dari perusahaan besar dan multi-national hingga perusahaan dengan skala lebih kecil. Sanksi dengan ancaman denda yang signifikan bisa melanda siapapun pihak yang tidak patuh terhadap GDPR terlepas dari besar kecilnya organisasi.

Bagaimana menetapkan denda pada pelanggar GDPR?

Pemberian denda administratif kepada pihak yang melanggar ketentuan GDPR tergantung pada masing-masing kasus. Di bawah GDPR, denda ditentukan oleh *Data Protection Regulator* di setiap negara annggota UE[47]. Otoritas tersebut akan mememutuskan berat tidaknya pelanggaran yang dilakukan dan hukumannya.

Jika regulator menyatakan bahwa sebuah organisasi atau perusahaan telah melakukan beberapa kali pelanggaran GDPR, maka mereka hanya akan dihukum untuk kesalahan yang paling parah dengan pertimbangan bahwa pelanggaran kecil lainnya adalah bagian dari pelanggaran besar.

Jadi bagaimana cara menetapkan denda GDPR? Berikut 10 kriteria yang dinilai untuk menentukan denda:

1. **Gravitasi dan natur *(Gravity and nature)*** - Gambaran keseluruhan dari pelanggaran yang dilakukan. Di sini otoritas akan melihat pelanggaran apa yang terjadi, bagaimana hal itu bisa terjadi, mengapa itu terjadi, jumlah orang yang terdampak, kerusakan yang diderita oleh orang yang terdampak, berapa lama waktu yang dibutuhkan untuk menyelsaikan masalah.

2. **Niat *(Intention)*** - Melihat apakah pelanggaran yang terjadi adalah sengaja atau tidak sengaja dan merupakan hasil dari kelalaian.

3. **Mitigasi *(Mitigation)*** - Melihat apakah organisasi atau perusahaan yang melakukan pelanggaran melakukan sesuatu untuk memitigasi terjadinya kerusakan yang diderita oleh pihak yang terdampak pelanggaran.

4. **Langkah pencegahan *(Precautionary measures)*** - Melihat sejauh apa persiapan teknis dan persiapan yang dimiliki organisasi atau perusahaan sebelumnya untuk bisa mentaati GDPR

5. **Catatan Sejarah *(History)*** - Melihat kemungkinan pelanggaran yang dilakukan sebelumnya, termasuk pelanggaran yang dilakukan di bawah *data Protection Directive* dan bagaimana kepatuhan terhadap tindakan korektif di bawah GDPR

6. **Kerjasama *(Cooperation)*** - Melihat apakah perusahaan atau organisasi yang melakukan pelanggaran kooperatif dengan otoritas pengawas untuk berusaha menemukan dan memperbaiki pelanggaran yang terjadi.

7. **Kategoti Data *(Data Category)*** - Tipe personal data apa yang terdampak oleh pelanggaran

8. **Pemberitahuan *(Notification)*** - Melihat apakah perusahaan, organisasi atau pihak ketiga yang melakukan pelanggaran secara proaktif melaporkan adanya elanggaran kepada otoritas pengawas.

9. **Sertifikasi *(Certification)*** - Melihat apakah organisasi atau perusahaan yang melakukan pelanggaran telah mengikuti kode etik yang disetujui atau disepakati sebelumnya.

10. **Faktor yang memberatkan atau meringankan *(Aggravating/Mitigating Factors)*** - Isu lain yang muncul akibat kasus pelanggaran tersebut, termasuk akan dilihat adalah keuntungan finansial yang didapat atau kerugian yang dihindari sebagai akibat dari pelanggaran tersebut.

47 https://gdpr.eu/article-83-conditions-for-imposing-administrative-fines/

Seberapa besar denda bagi pelanggaran GDPR?

GDPR menyatakan secara eksplisit bahwa sejumlah pelanggaran memiliki tingkat pelanggaran yang lebih parah dari lainnya dan hal itu membuat dendapun berbeda-beda. Ada dua tingkat denda atas pelanggaran GDPR yaitu[48]:

1. **Pelanggaran yang tidak terlalu parah**
   Pelanggaran yang tidak terlalu parah dapat mengakibatkan denda hingga **€10 juta atau sebesar 2%** dari pendapatan global tahunan perusahaan dari tahun keuangan sebelumnya, berapapun jumlah yang lebih tinggi. Termasuk pelanggaran pada pasal-pasal yang mengatur hal-hal di bawah ini:

   a) **Mengatur tentang *controller* dan *processor***
   Data controller dan *data processor* harus patuh terhadap aturan yang mengatur perlindungan data pribadi dalam melakukan pemprosesan data. Sebagai sebuah organisasi yang melakukan pengumpulan data pribadi pengguna dan mengolahnya, mereka harus memahami pasal Pasal 8, 11, 25-39, 42, dan 43.

   b) **Mengatur tentang *certification bodies***
   Badan terakreditasi yang bertanggung jawab atas sertifikasi terhadap organisasi harus melakukan tindakan evaluasi dan penilaian kerja tanpa bias melalui proses yang transparan. Lihat Pasal 42 dan 43.

   c) **Mengatur tentang *monitoring bodies***
   Badan yang dibuat untuk memiliki level keahlian yang sesuai harus mendemonstrasikan independensi dan mengikuti prosedur yang ada dalam menangani komplain atau pelanggaran yang dilaporkan secara transparan dan tidak memihak atau

2. **Pelanggaran serius**
   Pelanggaran serius adalah pelanggaran melawan prinsip-prinsip perlindungan data pribadi dan hak-hak subyek. Ini bisa berdampak pada denda hingga **€20 juta atau 4%** dari pendapatan global perusahaan tahunan dari tahun keuangan sebelumnya, berapapun jumlah yang lebih tinggi. Denda serius diberikan untuk pelanggaran hal-hal di bawah ini:

   a) **Prinsip-prinsip dasar pemrosesan data pribadi (Pasal 5,6 dan 9).**
   Sesuai dengan aturan GDPR, pemrosesan data pribadi harus dilakukan sesuai hukum, adil dan transparan. Data pribadi dikumpulkan untuk tujuan yang jelas, dijaga akurasinya dan diproses sesuai dengan tata cara yang diatur dalam GDPR untuk memastikan keamanannya. Organisasi atau perusahaan hanya boleh memproses data pribadi jika mereka memenuhi 6 dasar hukum dalam pemprosesan data seperti tertua pada GDPR Pasal 6[49].

   b) **Status persetujuan atau *the conditions for consent* (Pasal 7)**
   Saat organisasi atau perusahaan melakukan pemrosesan data dengan dasar telah mendapat persetujuan atau *consent* dari pemilik data, maka orhanisasi tersebut perlu memiliki dokumetasi untuk membuktikannya.

   c) **Hak Subyek Data (Pasal 12-22)**
   Individu pemilik data pribadi memiliki hak untuk tahu data apa dari dirinya yang dikumpulkan oleh organisasi atau perusahaan dan apa yang mereka lakukan terhadap datanya. Setiap individu juga memiliki hak untuk mendapatkan copy dari data yang telah dikumpulkan, untuk mengoreksi datanya, dan di beberapa kasus juga berhak agar datanya bisa dihapus.

48 https://gdpr.eu/fines/
49 https://gdpr.eu/article-6-how-to-process-personal-data-legally/

d) ***Transfer Data*** **kepada Organisasi Internasional atau Penerima di negara Ketiga (Pasal 44-49)**
Sebelum organisasi atau pihak *data controller* menstransfer data pribadi siapapun ke negara ketiga atau organisasi internasional lainnya, *European Commission* harus menentukan bahwa negara ketiga atau organisasi interasional yang menjadi pihak ketiga itu memiliki tingkat perlindungan data pribadi yang memadai. Proses transfer sendiri harus dilindungi hukum.

Denda juga bisa diberikan pada tipe pelanggaran di bawah ini[50]:

a) Pelanggaran apa saja terhadap hukum di negara anggota.
GDPR menjamin negara anggota UE memiliki kemampuan untuk mengesahkan hukum perlindungan data pribadi tambahan di negaranya selama itu sesuai dengan GDPR. Semua jenis pelanggaran terhadap hukum nasional yang diterapkan oleh negara anggota ini juga bisa dikenakan denda GDPR.

b) Tidak patuh terhadap permintaan otoritas pengawas GDPR
Jika ada organisasi atau perusahaan yang gagal untuk mematuhi permintaan dari badan pengawas GDPR, mereka bisa menghadapi denda besar, terlepas dari apa pelanggaran awal yang mereka lakukan.

Dalam tiga tahun pemberlakuan GDPR, berapakah denda terbesar yang pernah dijatuhkan oleh regulator dan kepada siapa saja?

Sejak diterapkan tahun 2018 lalu, aturan ini menjatuhkan denda kepada banyak pihak dalam kasus berbeda-beda. Berikut beberapa kasus denda besar GDPR[51]:

1. **Google - €50 juta**
Google adalah raksasa teknologi pertama yang dijatuhi denda GDPR yang sangat besar yaitu €50 juta di tahun 2019. Denda dijatuhkan oleh regulator Perancis yang menyatakan bahwa Google gagal membuat *statement* tentang pemrosesan data konsumennya mudah diakses oleh pengguna. Google juga dinyatakan bersalah karena tidak meminta *consent* untuk memanfaatkan data pengguna untuk keperluan *targeted advertising campaign.*

2. **H&M - €35,5 juta**
Perusahaan pakaian H&M dikenai denda €35,5 juta oleh regulator Jerman karena terbukti secara rahasia sudah bersalah melakukan *monitoring* kepada ratusan karyawannya tanpa sepengetahuan mereka. Karyawan H&M diwajibkan untuk menghadiri sebuah pertemuan dengan staf senior sebagai gantinya jika mereka mengambil libur atau izin sakit. Pertemuan itu direkam dan bisa diakses oleh manajer H&M tanpa sepengetahuan staf.

3. **Tim (Telecom Italia) - €27,8 juta**
Pada awal 2020, otoritas perlindungan data Italia menjatuhkan denda sebesar €27,8 juta kepada perusahaan telekomunikasi Tim (sebelumnya Telecom Italia). Denda dijatuhkan setelah adanya banyak komplain dari konsumen tentang adanya banyak telepon-telepon promosi dan *marketing* tanpa dimintai *consent* terlebih dahulu. Seorang pengguna bahkan melaporkan telah mendapat 155 telepon promosi yang tidak diinginkan.

4. **British Airways - £20 juta**
British Airways dijatuhi denda £20 juta pada tahun 2020 setelah gagal memberika *online security* kepada pengguna website mereka. Pengguna website British Airways diarahkan ke situs penipuan yang mengakibatkan bisa mengakses data pribadi dari 400,000 pengunjung website British Airways. Data-data pribadi yang diambil termasuk detail *login* dan pemesanan pesawat, nama, alamat, hingga informasi kartu kredit pengguna.

50 https://gdpr.eu/fines/
51 https://www.bbc.com/news/technology-57011639

Jika GDPR Diterapkan di Indonesia, Siapa Berpotensi Terkena Denda?

Jika GDPR diterapkan di Indonesia, banyak pihak-pihak yang berpotensi dijatuhi denda atas kelalaiannya dalam memastikan keamanan data pribadi pengguna atau atas pelanggaran terhadap data pribadi penggunanya. Dalam kasus kebocoran data yang terjadi pada salah satu toko online tahun 2020, dalam aturan GDPR, toko online tersebut bisa terancam hukuman denda besar mengingat hacker mampu mengakses password, nama, alamat email hingga informasi login pengguna.[52]

Salah satu perusahaan penerbangan juga berpotensi menghadapi denda dalam kasus bocornya data 7.8 juta penumpang anak perusahaannya, dimana sebanyak 156,000 di antaranya merupakan data pengguna Indonesia.[53]

11. *Data Breach* Dalam GDPR

Personal data breach atau pelanggaran terhadap data pribadi adalah hal yang ingin dicegah oleh GDPR. *Data breach* data pribadi adalah kondisi di mana keamanan data pribadi pengguna seseorang terancam dan dalam berbagai kasus data pribadi pengguna juga terekspose[54]. Aturan GDPR terkait pelanggaran data pribadi diatur dalam Pasal 33 dan Pasal 34 GDPR.

Menurut aturan GDPR apa yang harus dilakukan saat terjadi data breach?

1. **Pemberitahuan kepada Otoritas Pengawas *(Supervisory Authorities/Data Protection Authorities)***
   Pasal 33 mengatur persyaratan pelaporan kepada Otoritas Pengawas yang harus dilakukan pihak organisasi, perusahaan atau entitas lain yang menangani pemrosesan data pribadi. Berikut aturannya[55]:

a) *Data controller* tanpa menunda harus memberi notifikasi kepada *supervisory authotories* atau *data protection authorities,* tidak lebih dari 72 jam setelah mereka sadar adanya *data breach*. Jika pelaporan dilakukan dalam waktu lebih dari 72 jam, *data controller* wajib memberikan penyebab kenapa ada keterlambatan pelaporan.
b) *Data processor* harus memberi notifikasi terhadap *data controller* tanpa ditunda-tunda setelah menyedari adanya *data breach*.
c) Pemberitahuan atau pelaporan akan adanya *data breach* harus dilakukan dengan:

- Menjelaskan secara gamblang tentang *data breach* yang terjadi termasuk kategori pelanggaran dan perkiaran jumlah subyek data (pemilik data) yang terdampak serta perkiraan jumah data pribadinya.
- Menjelaskan kemungkinan konsekuensi atas pelanggaran yang terjadi.
- Menjelaskan tindakan-tindakan yang diambil atau ajukan untuk mengatasi *data breach* ini atau mengurasi dampak negatifnya.

52 https://tekno.kompas.com/read/2020/05/03/03330087/kebocoran-data-15-juta-pengguna-pengakuan-tokopedia-dan-analisis-ahli?page=all
53 https://www.cnnindonesia.com/teknologi/20190926200343-185-434426/kemenkominfo-156-ribu-wni-terimbas-kebocoran-data-lion-air
54 https://www.i-scoop.eu/gdpr/personal-data-breach-notification/
55 https://gdpr-info.eu/art-33-gdpr/

- Mengkomunikasikan nama dan kontak petugas perlindungan data (*Data protection officer*) di mana informasi lebih lanjut bisa diperoleh.

d) Informasi terkait *data breach* bisa diberikan secara bertahap, asalkan tanpa penundaan yang tidak perlu.
e) *Data controller* harus mendokumentasikan setiap data brecah yang terjadi, menyajikan fakta-fakta yang berkaitan tentang data breach tersebut, dampaknya dan tindakan perbaikan yang dilakukan. Dokumentasi digunakan oleh *supervisory authorities* untuk memeriksa dan mengevaluasi kapatuhan terhadap GDPR.

2. Pemberitahuan kepada individu atau subyek data yang terdampak

Pasal 34 mengatur persyaratan bagaimana mengkomunikasikan kepada individu atau subyek data yang terdampak. Berikut peraturannya:

a) *Data controller* harus mengkomunikasikan tanpa penundaan tentang kejadian *data breach* tersebut ke individu yang datanya diproses (subyek data) saat pelanggaran berpotensi besar mengakibatkan resiko tinggi kepada hak dan kebebasan individu.
b) Komunikasi atau pemeritahuan kepada subyek data harus dilakukan secara jelas, sederhana tapi lengkap tentang apa yang terjadi berikut dengan konsekuensi dan langkah yang sudah diambil untuk mengatasinya.
c) Komunikasi kepada subyek data tidak perlu dilakukan jika salah satu dari kondisi di bawah ini terpenuhi:

- Jika *data controller* telah menerapkan langkah-langkah perlindungan teknis dan organisasional yang sesuai di mana langkah-langkah tersebut dilakukan pada data pribadi yang terkena *data breach*. Contohnya: Enkripsi
- Jika *data controller* telah mengambil langkah-langkah selanjutnya untuk memastikan bahwa resiko tinggi terhadap kekebasan subyek data tidak mungkin lagi terjadi
- Akan melibatkan upaya yang tidak proporsional. Dalam kasus ini komunikasi publik akan dipilih di mana subyek data diinformasikan dengan cara yang sama efektifnya.

- Jika *data controller* belum mengkomunikasikan tentang pelanggaran data pribadi kepada subyek data, otoritas pengawas, setelah mempertibangkan adanya pelanggaran dengan resiko tinggi, bisa meminta kepada *data controller* untuk mengkomunikasikan kepada subyek data. Otoritas pengawas juga bisa memutuskan apakah *data controller* memenuhii syarat untuk tidak perlu melakukan komunikasi kepada subyek data.

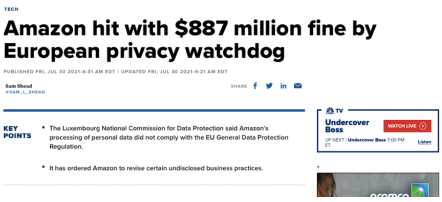
Sejumlah contoh kasus *data breach* dan sanksinya

1. WhatsApp didenda US$267 juta akibat kasus *data breach* di Irlandia

Aplikasi pesan instan miliki Facebook, WhatsApp dijatuhi denda sebesar US$267 juta oleh Otoritas Perlindungan Data di Irlandia atas pelanggaran terhadap GDPR. WhatsApp dijatuhi denda setelah terbukti tidak transparan tentang bagaimana mereka menggunakan data yang dikumpulkan dari pengguna WhatsApp. *Regulator* mengatakan bahwa WhatsApp tidak bersikap jelas dengan pengguna tentang bagaimana mereka membagikan data kepada Facebook's *platform* lainnya seperti Instagram dan Facebook sendiri [56,57].


Facebook's WhatsApp is fined for breaking the E.U.'s data privacy law.

2. Amazon didenda US$ 887 juta akibat pelanggaran data di Luxembourg[58]


TECH

Amazon hit with $887 million fine by European privacy watchdog

PUBLISHED FRI, JUL 30 2021-8:31 AM EDT | UPDATED FRI, JUL 30 2021-9:21 AM EDT

Sam Shead

SHARE

KEY POINTS

- The Luxembourg National Commission for Data Protection said Amazon's processing of personal data did not comply with the EU General Data Protection Regulation.
- It has ordered Amazon to revise certain undisclosed business practices.

TV
Undercover Boss
WATCH LIVE
UP NEXT | Undercover Boss 7:00 PM ET
Listen

Otoritas Luksemburg menjatuhi denda sebesar US$ 887 juta. Komisi nasional Luksemburg untuk perlindungan data pribadi mengatakan bahwa *e-commerce giant* Amazon tidak mematuhi aturan pemrosesan data pribadi sesuai GDPR.

3. Facebook dijatuhi denda sebesar £500,000 akibat *data breach* di kasus Cambridge Analytica[59]

Salah satu kasus yang terkenal mengenai *data breach* adalah kasus Facebook yang dijatuhi denda sebesar £500,000 setelah melakukan *data breach* dalam skandal *Cambridge Analytica*. *The Information Commissioner* (ICO) di Inggris menyatakan Facebook terbukti telah melakukan dua pelanggaran berat terhadap data pengguna yaitu gagal menjaga keamanan data penguna dan gagal bersikap transparan atas bagaimana data di pengguna Facebook juga digunakan pihak ketiga. ICO mengatakan bahwa Facebook hanya bisa dijatuhi denda sebesar £500,000 karena adanya batas denda £500.000 yang ditetapkan oleh *Data Protection Act 1998.* ICO mengatakan karena waktu pelanggaran yang dilakukan Facebook adalah sebelum GDPR diberlakukan pada Mei 2018, Facebook tidak bisa didenda dengan aturan GDPR. ICO mengatakan dalam aturan GDPR Facebook bisa dikenai denda lebih besar yaitu hingga £ 1,4 miliar atau 4% dari pendapatan globalnya.


Facebook fined for data breaches in Cambridge Analytica scandal

Firm fined £500,000 for lack of transparency and failing to protect users' information

▲ Facebook's co-founder, chairman and chief executive, Mark Zuckerberg, prepares to testify before Congress about Cambridge Analytica. Photograph: Chip Somodevilla/Getty Images

Facebook is to be fined £500,000, the maximum amount possible, for its part in the Cambridge Analytica scandal, the information commissioner has announced.

56 https://www.nytimes.com/2021/09/02/business/facebook-whatsapp-privacy-fine.html
57 https://techcrunch.com/2021/09/02/whatsapp-faces-267m-fine-for-breaching-europes-gdpr/
58 https://www.cnbc.com/2021/07/30/amazon-hit-with-fine-by-eu-privacy-watchdog-.html
59 https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal

12. Keuntungan dan Kerugian Bagi Individu Atas Penerapan GDPR

Keuntungan bagi individu sebagai seorang subyek data [60,61,62] :

a) Residen UE memiliki kontrol lebih besar atas data pribadinya sendiri dan bagaimana data pribadi digunakan atau diproses pihak lain. Individu bisa memilih untuk memberi atau menolak *consent* penggunaan data pribadi mereka untuk kepentingan tertentu termasuk kepentingan *marketing* dan *advertising*.

b) GDPR meningkatan transparansi dan akuntabilitas penggunaan data pribadi individual oleh pihak lain dan memberikan hak-hak kepada individu atas datanya.

c) Residen UE menjadi lebih sadar akan hak-hak mereka terkait perlindungan data pribadi seperti hak untuk akses data dan mendapatkan copy atas data mereka, hak untuk menolak, hak untuk terinformasikan tentang penggunaan data, hak untuk membatasi penggunaan data, hingga hak untuk melakukan koreksi atau perbaikan data.

d) Meningkatkan *cybersecurity*. Individu menjadi lebih terlindungi dari pelanggaran-pelanggaran terhadap data pribadi mereka di era digital termasuk *data breach* yang bisa mengancam kekebasan mereka.

e) Individu di UE memiliki hak untuk membuat pengaduan kepada *Data Protection Authority* dan mencari keadilan atas pelanggaran data pribadi yang berdampak buruk pada mereka.

f) GDPR membantu individu untuk mengambil peran aktif dengan penggunaan data pribadi mereka di era digital.

Kerugian bagi individu:

a) Terlepas dari peningkatan *cybersecurity* terhadap data pribadi, bagi sebagian orang, adanya GDPR membuat kegiatan mengakses laman online menjadi tidak sesederhana dahulu. Setiap membuka website di internet, mulai dari website berita, e-commerce, dan lainnya, residen UE dihadapkan dengan *pop-up box* “Pengaturan Privasi” di mana user diminta untuk memberi atau menolak *consent* untuk pemrosesan datanya untuk berbagai tujuan.

b) Individu sempat kesulitan mengakses beberapa website luar kawasan UE dari wilayah UE. Beberapa saat setelah GDPR diberlakukan, orang yang tinggal di Kawasan UE kesulitan mengakses banyak website media Amerika Serikat.

60 https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1166
61 https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/?sh=2f5e0f7694ad
62 https://www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you

13. Keuntungan dan Kerugian Bagi Perusahaan/Organisasi Atas Penerapan GDPR

Keuntungan penerapan GDPR untuk perusahaan atau organisasi [63,64]:

a) Dunia bisnis termasuk UMKM memiliki standarisasi aturan yang sama tentang perlindungan data pengguna. Semua bisnis terikat oleh aturan yang sama dan mendapat manfaat dari peluang yang sama, terlepas dari apakah mereka berbasis di UE atau tidak.

b) Membantu terciptanya level *playing field* antara bisnis lokal dengan pemain di luar UE yang beroperasi atau menyasar pasar UE.

c) Dapat meningkatkan sistem *cybersecurity* perusahaan. Lewat aturannya, GDPR memaksa perusahaan atau organisasi untuk meningkatkan dan mengevaluasi kembali kemanan siber mereka, meningkatkan infrastruktur IT mereka, dan membangun pelindungan data pribadi yang lebih sehat.

d) GDPR juga memaksa perusahaan untuk memiliki manejemen data yang lebih baik. GDPR membuat perusahaan atau organisasi bisa meminimalisasi data yang dikumpulkan, mengatur penyimpanan data secara lebih baik dan melakukan audit terhadap data yang mereka punya.

e) Meningkatkan *customer loyality*. GDPR memungkinkan pengguna internet untuk bisa menghabiskan waktu di website yang mereka sukai tanpa banyak terganggu dengan iklan yang terlalu banyak dari pengiklan. Dalam aturannya GDPR, *customer* bisa memilih untuk menolak, membatasi atau menyetujui. Hal ini bisa meningkatkan *customer loyality*.

f) Strategi *marketing* bisa lebih efektif. Dengan GDPR, data yang dikumpulkan perusahaan atau bisnis akan lebih ramping dan akurat. Di bawah GDPR, *customer* hanya akan menyetujui *consent* terkait pelacakan perefrensi produk dan perefrensi iklan tertentu misalnya jika mereka memang menginginkan. Hal itu berarti, bisnis berpotensi untuk mendapatkan data yang lebih akurat dan ramping tentang konsumen mana yang memiliki ketertarikan lebih kepada produknya.

Kerugian penerapan GDPR untuk perusahaan dan organisasi[65,66,67,68,69]:

a) Ancaman denda bisa mengancam organisasi atau perusahaan jika melakukan pelanggaran GDPR. Di Eropa, denda besar sering dijatuhkan pada perusahaan teknologi raksasa karena pelanggarannya yang masif dan berskala besar. Pada tahun 2021, Uni Eropa mengenakan €1 miliar denda dari Juli hingga September. Denda ini bukan berasal dari banyak pelanggaran tapi pelanggaran dari sedikit perusahaan besar.

b) Perusahaan dan organisasi tidak jarang harus mengeluarkan *cost of compliance* untuk investasi agar bisa memenuhi semua aturan GDPR. Misalnya untuk meningkatkan keamanan teknis sistem mereka, *training staff* terkait GDPR, mempekerjakan lebih banyak orang untuk memastikan *compliance*, sampai untuk menunjuk *Data Protection Officer* (meski ini tidak berlaku pada semua organisasi/ perusahaan).

63 https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1166
64 https://www.forbes.com/sites/forbestechcouncil/2018/03/29/five-benefits-gdpr-compliance-will-bring-to-your-business/
65 https://www.businesseurope.eu/sites/buseur/files/media/position_papers/internal_market/2019-11-29_be_gdpr_review.pdf
66 https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/?sh=2f5e0f7694ad
67 https://www.brusselstimes.com/economics/187915/gdpr-fines-for-third-quarter-almost-e1-billion/
68 https://www.brusselstimes.com/economics/187915/gdpr-fines-for-third-quarter-almost-e1-billion/
69 https://www.timedatasecurity.com/blogs/the-positive-and-negative-implications-of-gdpr-in-the-workplace

c) *StartUp* kecil dan SME mengalami situasi yang lebih berat untuk memastikan kepatuhan terhadap GDPR. Banyak dari SME dan StartUp kecil yang kurang siap untuk bisa *compliance* dengan semua GDPR karena keterbatasan dana dan *resources*. Bagi perusahaan teknologi besar seperti Facebook, Google, Amazon yang memiliki dana besar dan *resource* besar, akan lebih cepat dalam beradaptasi dengan GDPR.

d) Proses persiapan untuk mematuhi GDPR membuat perusahaan-perusahaan kecil harus memangkas biaya di area lain untuk dialokasikan ke langkah-langkah persiapan untuk patuh terhadap GDPR.

e) Organisasi atau perusahaan harus meluangkan waktu untuk benar-benar memahami dan mempelajari GDPR apabila ingin memastikan kepatuhan mereka untuk menghindari denda. Perubahan aturan terkait perlindungan data pribadi dan privasi yang diperkenalkan oleh GDPR ikut merubah banyak prosedur dan birokrasi pemrosesan data pengguna yang menyebabkan adanya *changing operation.*

f) Pada saat GDPR pertama kali diberlakukan pada 2018 lalu, sebanyak kurang lebih 1,000 website berita US tidak bisa diakses dari Uni Eropa karena mereka belum bisa memenuhi aturan GDPR. Daripada terkena ancaman denda, banyak website berita asal US yang memilih untuk melakukan *blocking* terhadap pengunjung website dari UE

14. Tantangan Penerapan GDPR

Sebagai aturan baru, tentu penerapan GDPR menemui sejumlah tantangan dalam penerapannya. Berikut sejumlah tantangan di bawah ini:

a) Kesiapan untuk adopsi banyak aturan baru GDPR

GDPR memuat banyak persyaratan dan aturan yang masih belum familiar bagi banyak pihak. Hal itu membuat proses adopsi dan kesiapan organisasi atau perusahaan terhadap GDPR menjadi tantangan tersendiri pada saat awal GDPR diterapkan. Kurang dari 11 bulan sebelum diimplementasikan, hanya 8% pelaku bisnis di Uni eropa yang benar-benar siap mengimplimentasikan GDPR[70]. Sementara itu 28% mengatakan tidak familiar, dan 52% mengatakan bahwa GDPR terlalu kompleks untuk UKM.

b) Masih banyak pelaku bisnis yang belum *compliance* karena rendahnya pemahaman dan *awareness*[71]

Kurang dari 1 tahun setelah GDPR dikeluarkan, masih banyak perusahaan khususnya yang berskala kecil masih memiliki kendala untuk memenuhi semua aturan GDPR. Aturan GDPR masih dirasa kompleks bagi banyak pihak. Banyak pelaku bisnis yang masih bingung tentang konsep *data security*, hingga *legal basis*. Rendahnya pemahaman dan kesadaran akan perlindungan data pribadi dan apa saja prinsip pemrosesannya di sejumlah negara juga menjadi tantangan tersendiri penerapan aturan ini[72]

70 https://www.prnewswire.com/news-releases/92-of-european-businesses-are-unprepared-for-gdpr-658099083.html
71 https://gdpr.eu/six-months-gdpr-what-do-we-know/
72 https://www2.deloitte.com/content/dam/Deloitte/ce/Documents/legal/ce-deloitte-the-gdpr-six-months-after- implementation-report-1.pdf?nc=1

c) Adanya *cost of compliance* menjadi tantangan berat bagi bisnis kecil[73]

Aturan GDPR menjadi pekerjaan rumah besar yang membutuhkan investasi bagi perusahaan baik besar atau kecil untuk memastikan bahwa prosedur yang mereka lakukan patuh kepada GDPR. Bagi, bisnis kecil tantangan yang dirasakan sangat berat, palagi bagi UMKM yang sebenarnya tidak melibatkan pemrosesan data dengan skala besar dan tidak beresiko tinggi. Survei yang dilakukan tahun 2019, menemukan bahwa bisnis kecil mengeluarkan investasi yang tidak sedikit mulai dari €1,000 hingga €50,000 dalam usahanya untuk GDPR *compliance*. Hal itu digunakan di antaranya untuk meng-*hire* konsultan dan ahli teknologi.

d) *Regulator* yang kewalahan

Di sejumlah besar negara-negara UE, *regulator* yang kewalahan karena kurang cukupnya staf dalam menangani GDPR *compliance* dan pertanyaan publik juga menjadi tantangan tersendiri. *Regulator* kewalahan menghadapi pertanyaan dari pihak seperti dari perusahaan dan organisasi, dan menerima laporan dari publik. Kurangnya *regulator*, juga membuat proses diseminasi informasi kepada publik menjadi tantangan tersediri. *Regulator* harus menangani banyaknya rumor atau miskonsepsi yang salah terkait GDPR yang beredar di publik karena banyak orang yang salah menafsirkan bagaimana GDPR berlaku bagi kehidupan sehari-hari[74]

e) Harmonisasi aturan GDPR dengan *national law*

Dalam konteks Uni Eropa, tantangan penerapan GDPR adalah harmonisasi antara aturan GDPR dengan *national law* di negara-negara anggota. Belum semua hukum nasional termasuk yang sifatnya sektoral di masing-masing negara anggota selaras dengan GDPR[75]. Memastikan legislasi nasional bisa selaras dengan aturan GDPR masih menjadi PR bagi penerapan aturan ini[76].

73 https://gdpr.eu/2019-small-business-survey/
74 https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html
75 https://www.businesseurope.eu/sites/buseur/files/media/position_papers/internal_market/2019-11-29_be_gdpr_review.pdf
76 https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1166

B GDPR Bagi Indonesia

1. GDPR Bagi Indonesia, Kesempatan Atau Ancaman?

Perlindungan data pribadi yang lebih ketat sangat diperlukan di era digital, di mana semakin banyak orang yang mempercayakan data pribadinya pada banyak aplikasi digital, *platform* media sosial, *platfom e-commerce* hingga aplikasi keuangan digital.

Sayangnya, di Indonesia banyak orang yang masih tidak tahu-menahu apa yang dilakukan pihak lain terhadap data pribadinya dan tidak punya kontrol atas datanya sendiri yang dikumpulkan dan diproses oleh pihak lain dalam dunia digital.

Indonesia saat ini dalam kondisi "*emergency*" untuk memiliki perundang-undangan perlindungan data pribadi yang lebih komprehensif dan kuat dan bisa memberikan perlindungan maksimal bagi data pribadi individu. Saat ini semakin banyak kasus pelanggaran data pribadi, mulai dari penyalahgunaan data pribadi oleh aplikasi pijaman online, kasus *data breach e-commerce online*, kebocoran data pengguna e-Hac, hingga kasus *personal data transfer* yang dilakukan oleh sesama aplikasi pijaman online tanpa *consent* pemilik data pribadi. Di saat seperti ini, individu menjadi pihak yang tidak berdaya dan hanya bisa berpasrah karena belum ada aturan perlindungan data pribadi yang komprehensif.

Saat ini regulasi di Indonesia yang menyinggung soal data pribadi masih bersifat sektoral yaitu disebut dalam Undang-Undang Perbankan, Telekomunikasi, Administrasi Kependudukan. Undang-undang sektoral lemah karena tidak bisa mencakup semua kasus. Perlindungan data pribadi di ranah eletronik juga pernah diturunkan lewat Peraturan Menteri Kominfo Nomor 20 tahun 2016[77]. Sayangnya peraturan-peraturan di dalamnya yang belum mendetail, belum komprehensif dan belum bisa memberikan individu hak dan kontrol atas data pribadinya sendiri.

Pelaporan dan penanganan atas kasus pelanggaran data juga masih diatasi oleh polisi. Sementara itu, ancaman denda administratif yang ketat atas kasus-kasus pelanggaran data pribadi juga belum diatur secara spesifik.

GDPR Bisa Memberikan Referensi Ihwal Peraturan Perlindungan Data Pribadi di Indonesia

GDPR yang diterapkan oleh Uni Eropa bisa menjadi referensi bagi Indonesia untuk menerapkan aturan terkait perlindungan data pribadi. Indonesia bisa belajar dari GDPR tentang sejumlah poin penting seperti tentang prinsip-prinsip apa saja yang penting untuk dipatuhi dalam pemrosesan data pribadi, hak-hak apa saja yang harusnya dimiliki individu atas data pribadinya, dan beberapa *legal basis* yang harus ada sebagai dasar pemrosesan data pribadi, hingga aturan detail soal kewajiban yang harus dilakukan *data controller* dan *processor.*

77 https://kominfo.go.id/content/detail/35104/ruu-pdp-jamin-perlindungan-data-pribadi-yang-progresif-dan- komprehensif/0/berita_satker

2. Keuntungan dan Tantangan Penerapan Aturan Serupa di Indonesia

Keuntungan Jika GDPR Diterapkan di Indonesia:

a) Setiap individu akan bisa memiliki kontrol terhadap data pribadinya sendiri di ranah digital kaitannya dengan bagaimana data itu digunakan dan diproses pihak lain. Individu bisa memiliki pilihan dan hak penuh untuk menolak atau menerima *consent* penggunaan data pribadinya untuk tujuan tertentu.

b) Pengguna aplikasi digital, pengguna internet bisa lebih terlindungi dari ancaman pelanggaran terhadap data pribadi mereka karena *cybersecurity* meningkat.

c) Kasus penyalahgunaan data dan kebocoran data pribadi bisa ditekan.

d) Publik bisa melakukan pengaduan atau komplain kepada otoritas yang tepat tentang pelanggaran data pribadi yang dialaminya dan mendapat penanganan jelas karena sudah ada payung hukum yang komprehensif.

e) Perusahaan teknologi bisa dipaksa untuk lebih akuntabel, transparan dan bertanggung jawab dalam melakukan pemrosesan data pengguna dan tidak semena-mena dalam menggunakan data pribadi pengguna untuk kepentingannya.

Kemungkinan Tantangan yang Bisa Terjadi

a) Adopsi aturan baru sudah pasti akan membutuhkan waktu dan memerlukan banyak sosialisasi untuk memberikan pemahaman kepada semua pihak, terutama kepada organisasi, perusahaan, atau entitas lain yang melakukan kegiatan pemrosesan data pribadi. Menumbuhkan kesadaran dan pemahaman yang benar biasanya menantang dilakukan di Indonesia.

b) Penyediaan otoritas pengawas yang kompeten dengan jumlah yang cukup juga bisa menjadi tantangan tersendiri untuk pemberlakuan aturan ini di Indonesia. Pengawasan aturan perlindungan data pribadi baiknya dilakukan oleh otoritas tersendiri yang memang sengaja dibentuk untuk pengawasan perlindungan data pribadi.

c) Memastikan kepatuhan dan melakukan pengawasan bisa jadi hal yang menantang di Indonesia.

d) Akan banyak pihak yang gagal dalam memenuhi kepatuhan terhadap aturan perlindungan data pribasi, terutama perusahaan yang lebih kecil atau startup karena tidak memiliki kapabilitas yang cukup dari segi dana dan sumber daya manusia.

C Kesimpulan dan Rekomendasi

1. Kesimpulan

Penerapan GDPR selama tiga tahun di kawasan Uni Eropa, menunjukkan bahwa regulasi ini berpihak pada individu dan perlindungan data pribadinya di ranah digital. Di bawah GDPR, setiap individu yang tinggal di Uni Eropa memiliki suara dan kontrol atas penggunaan data pribadinya di dunia digital oleh pihak lain. Individu bisa memberi persetujuan, menolak, membatasi penggunaan dan pemrosesan data pribadinya oleh pihak lain. Lewat prinsip-prinsip perlindungan data pribadi, prinsip pemrosesan data, dan beberapa *legal basis* yang diperkenalkan aturan ini, pemprosesan data pribadi pengguna menjadi lebih bertanggung jawab. Setiap pelanggaran atas data pribadi pengguna juga bisa dikenakan sanksi.

Namun, di sini lain, aturan ini membawa tantangan tersendiri bagi organisasi, perusahaan, terutama yang pelaku bisnis yang kegiatan utamanya berkutat pada pemrosesan data pengguna untuk mencapai tingkat kepatuhan yang baik pada regulasi ini. Pemberlakukan aturan ini juga membutuhkan proses sosialisasi yang berkala ke publik dan semua pihak yang terlibat agar dicapai pemahaman yang seragam atas perlindungan data pribadi. Secara umum, GDPR membuat penggunaan data pribadi di Uni Eropa lebih bertanggung jawab dan melindungi masyarakat.

2. Rekomendasi

a. GDPR bisa menjadi referensi poin bagi Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP) di Indonesia. Prinsip-prinsip perlindungan data pribadi, prinsip pemrosesan data pribadi dan legal basis pemrosesan data yang diperkenalkan GDPR bisa menjadi referensi Indonesia untuk menciptakan perlindungan data pribadi bagi warga.

b. Jika Indonesia memiliki undang-undang perlindungan data pribadi, undang-undang tersebut harus memiliki cakupan penerapan yang jelas; kepada siapa aturan ini mengikat, kegiatan-kegiatan seperti apa yang diatur dalam aturan ini, adakah pengecualian kewajiban tertentu dan dalam kondisi apa pengecualian bisa dilakukan, bagaimana mekanismenya, semua harus jelas diatur. Hal ini agar tidak menimbulkan kebingungan dalam implementasinya.

c. Dalam penerapan di Eropa, GDPR berlaku secara merata kepada semua pihak tanpa memandang ukuran besar kecilnya entitas. Hanya ada beberapa pengecualian yang diberlakukan dalam kondisi tertentu. Di Indonesia, hal ini mungkin bisa dikaji kembali. Dalam penerapan di Uni Eropa, terbukti *startup* kecil dan usaha kecil banyak yang mengalami kesulitan dalam mengadopsi aturan ini.

d. Jika aturan perlindungan data pribadi diterapkan di Indonesia, pembetukan badan publik untuk mengawal persiapan dan penerapan aturan ini diperlukan. Badan publik ini bisa mengambil peran dalam proses edukasi, dan sosialiasi secara berkala untuk memastikan adanya keseragaman pemahaman semua pihak pada kebijakan ini.

e. Jika diterapkan, maka Indonesia juga perlu untuk melakukan program-program sosialisasi untuk meningkatan kesadaran masyarakat akan pentingnya data pribadi terutama di ranah digital. Aturan seperti GDPR akan efektif jika masyarakatnya juga memiliki kesadaran akan privasi dan data pribadi mereka, sehingga mereka bisa memanfaatkan *tools* yang disediakan oleh regulasi ini untuk melindungi data pribadi dan privasinya.

Notes

Embassy of
the Republic of Indonesia
in Brussels

www.kemlu.go.id/brussels