Asosiasi Media Siber Indonesia

Yayasan TIFA

SINDIKASI

Didukung oleh:

ABC INTERNATIONAL DEVELOPMENT

PELINDUNGAN DATA PRIBADI DALAM JURNALISME DAN MEDIA

2024

PELINDUNGAN DATA PRIBADI DALAM JURNALISME DAN MEDIA

Didukung oleh:

2024

PELINDUNGAN DATA PRIBADI DALAM JURNALISME DAN MEDIA

Penulis: Heru Tjatur, Debora Irene C., Bayu Wardhana, Guruh Dwi Riyanto

Expert Reviewer: Bhredipta Socarana

Editor: Citra Dyah Prastuti

Tim Pendukung: Sarah Ervina, Putri Tirtasari, Muhammad Abd. Rosyid

Perancang sampul dan Tata letak: Fahrul Rozi

Diterbitkan oleh:

Asosiasi Media Siber Indonesia

Asosiasi Media Siber Indonesia (AMSI), 2024
Gedung Tempo Media,
Jl. Palmerah Barat No. 8, Jakarta Selatan 12210
Website: www.amsi.or.id
Email: info@amsi.or.id

Edisi Pertama: Mei 2024

Indonesia Media Program dilaksanakan oleh
ABC International Development dan didanai oleh Pemerintah Australia
berdasarkan Strategi Penyiaran Indo-Pasifik.

DAFTAR ISI

KATA PENGANTAR

Perkembangan industri media digital belakangan ini menuntut perusahaan media untuk membangun dan menjaga relasi yang baik dengan audiensnya. Tanpa relasi langsung dengan audiensnya, perusahaan media digital akan sangat tergantung pada platform pihak ketiga. Ketergantungan yang berlebihan dari perusahaan media pada pihak ketiga yang menguasai jalur distribusi kontennya pada pembaca akan membuat redaksi media kehilangan independensinya. Hal itu tentu tidak sehat untuk kesinambungan bisnis media digital.

Akan tetapi, relasi langsung media dengan audiensnya menuntut kesadaran perusahaan media untuk menjaga dan melindungi data pribadi penggunanya. Tak hanya kesadaran, perusahaan media harus merumuskan metode dan infrastruktur pendukung yang memadai untuk menjamin kerahasiaan data pribadi semua penggunanya. Tanpa itu, perusahaan media tak akan bisa membangun keterpercayaan publik pada layanan digitalnya. Sebuah media yang tak dipercaya tentu buruk untuk bisnis mereka ke depan.

Pada Oktober 2024, Undang Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) bakal resmi berlaku di Indonesia. Dalam menyambut momentum penting ini, Asosiasi Media Siber Indonesia (AMSI) telah melakukan survei awal untuk menguji sejauh mana pemahaman perusahaan media akan regulasi penting ini. Kami juga melakukan uji penilaian kesenjangan (*gap assessment*) terkait pemrosesan data pribadi yang diterapkan perusahaan media anggota AMSI.

Hasilnya masih jauh dari ideal. Ada variasi kesenjangan yang cukup tinggi antara regulasi dan implementasinya di lapangan. Survei AMSI juga menemukan sejumlah indikasi perlunya upaya intensif untuk menaikkan tingkat kepatuhan minimum perusahaan media terhadap UU PDP.

Dalam rangka upaya itulah, modul pelatihan ini disiapkan sebagai upaya untuk membantu program AMSI dalam meningkatkan kapasitas perusahaan media mengelola dan melindungi data pribadi penggunanya.

Secara khusus, modul pelatihan tentang Pelindungan Data Pribadi ini dirancang khusus untuk pemangku kepentingan dalam industri media digital. Modul ini akan jadi basis pelatihan yang bertujuan untuk meningkatkan kepatuhan anggota AMSI terhadap UU PDP, sebagai regulasi penting yang mengatur pemenuhan hak-hak individu atas pelindungan data pribadi.

Dengan perkembangan teknologi informasi dewasa ini dan semakin kompleksnya model bisnis industri media digital, upaya melindungi privasi dan data pribadi memang merupakan tantangan tersendiri. Justru karena itulah, standardisasi pemahaman tentang konsep privasi dan pelindungan data pribadi jadi kian krusial bagi pengelola perusahaan media, staf redaksi atau jurnalis, serta staf non-redaksi. Modul pelatihan ini dirancang untuk memberikan pengetahuan yang komprehensif dan praktis tentang hal tersebut.

Secara garis besar, modul ini mencakup beberapa materi penting, antara lain (1) pengenalan konsep privasi dan pelindungan data pribadi, termasuk memahami konsep dasar privasi dan pentingnya pelindungan data pribadi dalam konteks media digital; (2) kewajiban Perusahaan Media sebagai Pengendali Data, yang mencakup apa dan bagaimana pemrosesan data pribadi dan tanggung jawab perusahaan media dalam mengelola dan melindungi data pribadi sesuai dengan ketentuan undang-undang; dan (3) daftar periksa (*check list*) implementasi UU PDP yang berisi panduan praktis sekaligus tahapan implementasi bagi pengelola perusahaan media untuk memastikan kepatuhan terhadap UU PDP.

Modul pelatihan ini disusun secara kolaboratif oleh Asosiasi Media Siber Indonesia (AMSI), Aliansi Jurnalis Independen (AJI), Yayasan TIFA, dan Serikat Pekerja Media dan Industri Kreatif untuk Demokrasi (Sindikasi), dengan dukungan dari Indonesia Media Program yang dilaksanakan oleh ABC International Development. Kolaborasi ini bertujuan untuk memastikan materi pelatihan dalam modul ini relevan, komprehensif, dan aplikatif bagi seluruh perusahaan media anggota AMSI, termasuk di dalamnya semua awak redaksi dan staf non-redaksi perusahaan media terkait.

Kami berharap modul ini dapat menjadi alat yang efektif dalam meningkatkan pemahaman dan kemampuan praktis para pemangku kepentingan di industri media digital dalam melindungi data pribadi pengguna dan karyawannya. Dengan pelatihan ini, kami juga berharap dapat mendorong tercapainya tingkat kepatuhan minimum pelindungan data pribadi yang lebih baik di seluruh perusahaan media, demi menjaga penghormatan hak-hak privasi individu dan kepercayaan publik pada institusi media.

Terima kasih pada semua pihak yang mendukung perumusan modul pelatihan ini. Semoga modul ini memberikan manfaat yang signifikan dalam upaya kita bersama untuk melindungi data pribadi di ranah digital.

Wahyu Dhyatmika
Ketua Umum AMSI

Didukung oleh:

BAB 1

PENGANTAR PELINDUNGAN DATA PRIBADI

MODUL 1

PRIVASI DAN PELINDUNGAN DATA PRIBADI

Deskripsi: Modul ini adalah modul pertama dalam seri pelatihan PDP untuk industri media. Selain perlu memberikan pemahaman dan filosofi pelindungan data pribadi, pada modul ini juga perlu dibangun konvensi bagaimana pelatihan akan berjalan dan komitmen dalam menjalankan pelatihan dalam rangka implementasi PDP.

Tujuan: Pada sesi ini juga dimaksudkan untuk mengidentifikasi dan mengukur tingkat pemahaman, pengetahuan, serta pengalaman peserta dalam konteks PDP. Dengan mengetahui informasi tersebut, peserta dapat diminta untuk berbagi pengalaman dan pengetahuannya dalam berbagai sesi diskusi yang melibatkan peserta.

Durasi: 90 menit

Metodologi: Presentasi, diskusi dan praktikum untuk memaparkan prinsip dasar tentang privasi, individu, data pribadi, dan pelindungan data pribadi. Mengidentifikasi informasi yang memberikan identifikasi terhadap individu atau pribadi.

Pokok Bahasan

1.1 Privasi dan Data Pribadi

Sebelum menyentuh data pribadi dan pelindungan data pribadi, ada baiknya kita mulai dengan menarik mundur dengan membahas terminologi privasi atau *privacy*. Privasi sendiri berarti hak untuk tidak diganggu (*the right to be let alone*). Atau dapat diartikan sebagai "penggunaan informasi pribadi yang sesuai dalam situasi tertentu" yang tidak mengganggu atau menimbulkan kerusakan/kerugian (*harms*). Oleh karenanya, pelindungan data pribadi mengacu pada manajemen atau pengelolaan informasi tentang pribadi (*personal information*).

Mengacu dari definisi tersebut, terdapat beberapa kategori privasi yaitu: (1) privasi informasi, berkaitan dengan regulasi yang mengatur pengumpulan dan pengelolaan informasi pribadi atau data pribadi; (2) privasi komunikasi, berkaitan dengan pelindungan cara berkorespondensi, misalnya percakapan telepon, email dan bentuk lain kegiatan komunikasi; (3) privasi badani, yang berfokus ke invasi pada tubuh fisik individu, seperti uji genetika, penggeledahan badan, biometrik dan lainnya; (4) privasi teritorial, yang membatasi individu atau organisasi untuk memasuki lingkungan individu atau organisasi, seperti lingkungan rumah, ruang meeting, termasuk mengatur *video or audio surveillance,* pemeriksaan kartu identitas, dan lain sebagainya.

Selanjutnya setiap informasi terkait dengan identifikasi atau yang dapat mengidentifikasi pribadi didefinisikan dengan data pribadi dari seorang subjek data[1] atau biasanya disingkat dengan *personally identifiable information* (PII) yang selanjutnya kita akan gunakan data pribadi untuk definisi yang sama. Terdapat berbagai klasifikasi data

[1] Definisi asli data pribadi atau *personal data* dapat dilihat dalam *Article 4.1. General Data Protection Regulation* (GDPR)

pribadi, di antaranya data pribadi yang bersifat umum dan khusus sebagaimana didefinisikan dalam UU PDP yang juga mengacu pada GDPR.

UU PDP berlaku kepada setiap orang, badan publik, dan organisasi internasional yang melakukan perbuatan hukum yang diatur pada UU PDP, termasuk kegiatan pemrosesan data pribadi, apabila kegiatan tersebut (1) terjadi di wilayah hukum Negara Republik Indonesia; dan (2) di luar wilayah hukum Republik Indonesia namun memiliki akibat hukum di wilayah hukum Negara Republik Indonesia dan/atau kepada subjek data pribadi warga negara Indonesia di luar wilayah hukum Negara Republik Indonesia. Sepanjang suatu entitas melakukan kegiatan pemrosesan data pribadi warga negara Indonesia atau warga negara asing di Indonesia, maka UU PDP wajib untuk dipatuhi.

Jenis-jenis data pribadi, klasifikasi data pribadi dalam Pasal 4 Undang-Undang Nomor 27 Tahun 2022 terdiri atas (a) data pribadi umum yaitu informasi pribadi yang bersifat umum, mencakup (1) identitas lengkap, (2) jenis kelamin, (3) kebangsaan, (4) keyakinan agama, dan (5) penggunaan gabungan data individu untuk identifikasi; dan data pribadi spesifik yaitu informasi pribadi bersifat khusus atau spesifik, mencakup (1) informasi kesehatan, (2) data biometrik, (3) data genetika, (4) kehidupan/orientasi seksual, (5) pemikiran politik, (6) riwayat kejahatan, (7) data anak, (8) data keuangan, dan (9) data lain sesuai dengan ketentuan yang ada.

Perbedaan utama antara data pribadi yang bersifat umum dan spesifik terletak pada tingkat sensitivitas privasi yang terkandung di dalamnya. Data pribadi yang bersifat umum cenderung mencakup informasi yang bisa diketahui secara umum, seperti nama lengkap, jenis kelamin, kewarganegaraan, dan agama, serta kombinasi data untuk mengidentifikasi individu.

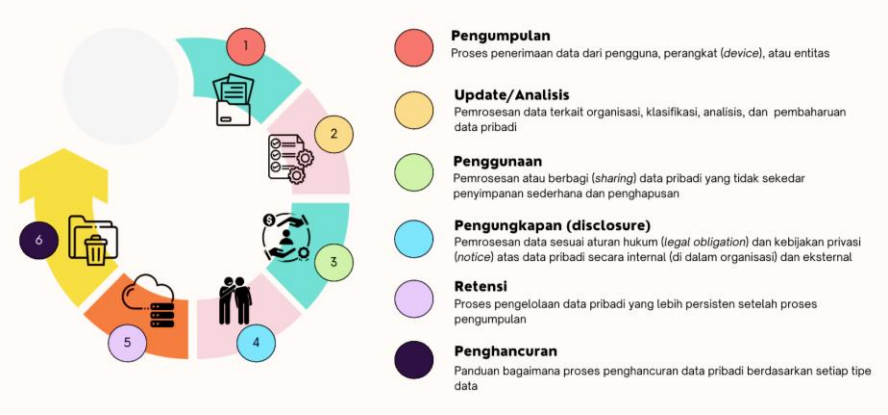
Sementara itu, data pribadi yang bersifat spesifik, seperti informasi kesehatan, biometrik, dan genetika, memiliki tingkat sensitivitas yang lebih tinggi dan berpotensi menyebabkan implikasi yang lebih serius terhadap privasi dan keamanan individu jika disalahgunakan atau bocor. Karenanya, pelindungan dan pengaturan yang lebih ketat seringkali diperlukan untuk data pribadi yang bersifat spesifik untuk memastikan bahwa potensi risiko terhadap privasi individu diminimalkan.

1.2. Pemrosesan dan Pelindungan Data Pribadi

Perusahaan Media dan seluruh bagian ekosistem industri media wajib mematuhi UU PDP karena melakukan pemrosesan data pribadi, baik data pribadi spesifik maupun non-spesifik, yang berasal dari konsumen, karyawan, dan/atau penyedia jasa (*vendor*) entitas pers dengan beragam tujuan pemrosesan data pribadi.

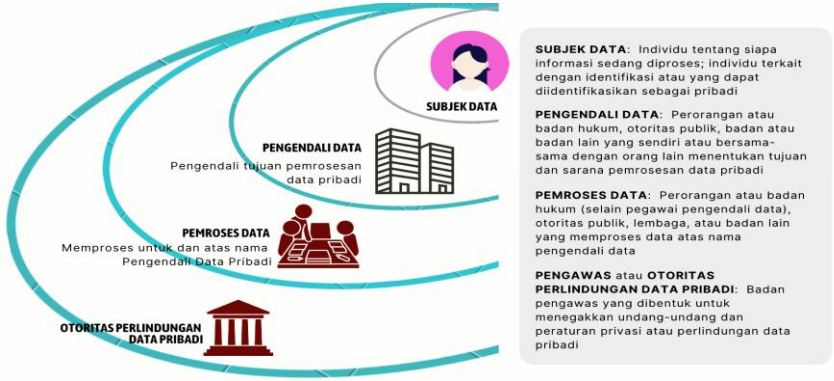
Pelindungan data pribadi bertujuan untuk membatasi pemrosesan data pribadi berdasarkan alasan yang sah dan sesuai dengan peraturan & perundangan yang berlaku. Pemrosesan data pribadi secara natural akan mengikuti proses yang selalu berulang dan akan selalu dibahas dalam pelindungan data pribadi, yaitu siklus data pribadi (*privacy information lifecycle*).

Sebagaimana diatur dalam Pasal 16, UU No. 27/2022, secara sederhana pemrosesan data pribadi berdasarkan siklus data pribadi digambarkan dalam ilustrasi berikut.



Dalam setiap tahapan siklus data pribadi, pemrosesan data melibatkan beberapa pihak, yaitu Pengendali Data (*Data Controller*) sebagaimana didefinisikan dalam Pasal 1 ayat 4, Prosesor Data Pribadi, (ayat 5), Subjek Data (ayat 6), Lembaga Penyelenggara Pelindungan Data Pribadi, atau singkatnya Otoritas Pelindungan Data Pribadi (Pasal 58, UU No. 27/2022).

Secara singkat peran pelindungan dan definisi setiap aktor dalam pemrosesan data pribadi digambarkan dalam ilustrasi berikut ini.



Kerangka kerja (*framework*) pelindungan data pribadi pada dasarnya disandarkan pada pengakuan hak pribadi, dalam hal ini setiap pemrosesan data pribadi oleh pengendali data ataupun pemroses data untuk dan atas kepentingan pengendali memperhatikan hak-hak individu sebagai subjek data. Hal ini mengatur prinsip-prinsip pemrosesan data pribadi. Pendekatan pelindungan data pribadi diformulasi dengan dasar pemikiran praktik penggunaan data pribadi yang adil (*fair information practices*) yang secara periodik dituangkan dalam panduan-panduan penggunaan.

Di Amerika Serikat proses ini ditandai dengan diterbitkannya aturan (*code*) di bidang kesehatan, pendidikan dan kesejahteraan (*welfare*) (HEW) pada 1973. *United State Fair Information Practices for Health, Education and Welfare* (US FIP HEW, 1973) menetapkan 5 prinsip yang harus dipatuhi, antara lain (1) prinsip transparansi yaitu tidak boleh ada sistem pencatatan atau *record keeping* data pribadi yang keberadaannya dirahasiakan; (2) prinsip-prinsip pemberitahuan, persetujuan dan akses dari subjek data, yaitu harus ada cara bagaimana subjek data mengetahui informasi yang ada dalam sistem & bagaimana digunakannya; (3) harus ada cara untuk mencegah pengumpulan data pribadi untuk satu tujuan digunakan atau dimungkinkan untuk tujuan lain tanpa persetujuan subjek data atau *consent*, dan (4) harus ada cara subjek data untuk memperbaiki atau menambah catatan data pribadinya. Dan prinsip yang terakhir (5) mengatur bahwa setiap organisasi yang mengelola, menggunakan, dan menyebarkan catatan data pribadi harus mampu menjamin reliabilitas data untuk tujuan yang dimaksud dan harus mengambil tindakan pencegahan yang perlu terhadap penyalahgunaan (*misuse*).

Dan pada 1980 OECD (*Organization for Economic Co-operation and Development*) menerbitkan panduan dalam *OECD Privacy Guidelines*, yang selanjutkan mengalami pengkinian pada 2013. *OECD Privacy*

Guidelines berfokus pada pertukaran data yang aman untuk keperluan bisnis. Beberapa *framework* yang juga menjadi acuan adalah *FTC Fair Information Practices Principles* (1998) dan *APEC Privacy Framework*, yang keduanya berfokus sama dengan *OECD Privacy Guidelines* yaitu memastikan pertukaran data pribadi yang aman untuk kepentingan perdagangan. Karena ini hanya bersifat panduan dan bersifat *voluntarily*, maka panduan-panduan prinsip ini tidak mengatur sanksi untuk pihak yang tidak patuh.

Secara rinci Pasal 16 Ayat 2, UU No.27/2022 mengatur 8 prinsip pemrosesan data pribadi sebagai berikut:

(1) Pengumpulan data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, dan transparan. Pembatasan Pengumpulan (*Collection Limitation*), yang mana setiap pengumpulan data pribadi harus memiliki dasar yang tak melanggar hukum/sah (*lawful*) dan dengan cara yang adil (*fair*), hanya mengumpulkan data pribadi yang relevan dengan tujuan (*limits to collection*), dan dikumpulkan dengan sepengetahuan dan persetujuan subjek data (*knowledge & consent*).

(2) Pemrosesan data pribadi dilakukan sesuai dengan tujuannya. Spesifikasi tujuan pemrosesan (*Purpose Specification*) harus dijelaskan secara menyeluruh pada saat pengumpulan atau pengambilan data pribadi, termasuk batasan-batasan penggunaannya, dan setiap ada perubahan.

(3) Pemrosesan data pribadi dilakukan dengan menjamin hak Subjek Data Pribadi, sebagaimana diatur dalam Pasal 6 s/d 13 UU No. 27/2022.

(4) Pemrosesan data pribadi dilakukan secara akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan.

Kualitas data pribadi (Data Quality), data pribadi yang diproses memenuhi kualitas data yang dibutuhkan sesuai dengan tujuan pemrosesan, antara lain akurat, lengkap dan terkini.

(5) Pemrosesan data pribadi dilakukan dengan melindungi keamanan data pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, pengubahan yang tidak sah, perusakan, dan/atau penghilangan data pribadi. Seluruh pemrosesan data pribadi dilakukan dalam lingkungan yang dilindungi oleh pengamanan yang cukup dan wajar (*reasonable*).

(6) Pemrosesan data pribadi dilakukan dengan memberitahukan tujuan dan aktivitas pemrosesan, serta kegagalan pelindungan data pribadi. Prinsip ini memastikan keterbukaan dengan membuat kebijakan yang transparan tentang pengembangan, praktik dan aturan tentang pemrosesan data pribadi; tersedia sarana untuk memastikan keberadaan data pribadi dan mewakili individu yang ada serta tujuan penggunaannya.

(7) Data Pribadi dimusnahkan dan/atau dihapus setelah masa retensi berakhir atau berdasarkan permintaan subjek data pribadi, kecuali ditentukan lain oleh peraturan perundang-undangan.

(8) Pemrosesan data pribadi dilakukan secara bertanggung jawab dan dapat dibuktikan secara jelas. Pengendali data harus bertanggung-jawab atas, dan dapat menunjukkan kepatuhan terhadap prinsip-prinsip tersebut, sebagai penjabaran dari prinsip akuntabilitas.

Dengan adanya berbagai panduan dan prinsip-prinsip pelindungan data pribadi ini, lantas bagaimana menerapkan dalam operasional pelindungan dalam satu instansi atau organisasi. Menjadi semakin menantang bila organisasi tersebut menyediakan layanannya secara digital dan dapat diakses melintasi batas wilayah hukum lain. Untuk

organisasi yang bergerak dalam wilayah hukum Indonesia, maka peraturan dan perundangan Indonesia harus menjadi panduan utama, seperti misalnya UU No. 27 2022 tentang PDP, sebagaimana diatur dalam Pasal 2.

Dan tentu saja terdapat prinsip-prinsip yang sama dalam setiap aturan dan panduan yang ada, termasuk GDPR yang berlaku di Uni Eropa. Secara sederhana ilustrasi berikut ini akan memberikan panduan prinsip yang perlu diterapkan agar implementasi pelindungan data pribadinya mematuhi aturan yang lebih luas.

1. 3. Mengapa Pelindungan Data Pribadi Penting

Pelindungan data pribadi juga merupakan bagian dari hak konstitusional setiap warga negara. Sebagaimana ditegaskan dalam Pasal 28G ayat (1) UUD 1945 yang menyatakan bahwa setiap orang memiliki hak untuk dilindungi atas diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang berada di bawah kekuasaannya. Pernyataan ini juga diakui dalam beberapa undang-undang lain,

termasuk UU No. 39/1999 tentang Hak Asasi Manusia (HAM). Oleh karena itu, untuk menghadapi tantangan masa kini, termasuk tren global pelindungan data pribadi, penting bagi Indonesia untuk mengawal Undang-Undang Pelindungan Data Pribadi (UU PDP) yang menyeluruh. Melindungi privasi berarti menjaga martabat individu, yang merupakan dasar bagi seseorang untuk dapat mengekspresikan kebebasannya dalam sebuah sistem yang demokratis.

Pelindungan data pribadi merupakan kebutuhan yang vital di era digital. Tujuan utama pelindungan data pribadi adalah memastikan informasi pribadi seseorang tidak disalahgunakan atau dieksploitasi oleh pihak yang tidak bertanggung jawab.

Data pribadi harus dilindungi karena beberapa tujuan seperti:

1) **Pengamanan dari akses tidak sah, diretas atau dicuri**: Data pribadi yang tidak dilindungi rentan terhadap serangan dunia maya oleh pihak ketiga. Ada potensi untuk mencuri informasi sensitif seperti nomor kartu kredit, informasi identifikasi, atau informasi keuangan lainnya;

2) **Mencegah penyalahgunaan oleh pihak ketiga**: Kebocoran data pribadi dapat disalahgunakan oleh beberapa pihak untuk keuntungannya sendiri, seperti pemalsuan identitas, penipuan atau bahkan pencucian uang. Penyalahgunaan ini termasuk di ***pelecehan seksual***, yaitu serangan yang bersifat pelecehan seksual, baik daring (*online*) maupun luring (*offline*), **penipuan**, **pemerasan** dan gangguan privasi lainnya.

Menurut Taksonomi Solove[2], setidaknya terdapat empat klasifikasi ancaman terhadap hak atas privasi *(privacy harms)*, yaitu ancaman yang muncul selama beberapa proses, diantaranya:

1) **Pengumpulan** (*collection*) data pribadi, misalnya interogasi dan pemantauan (*surveillance*);

2) **Penggunaan** (*use*) data pribadi, misalnya ketidakamanan (*insecurity*) infrastruktur, pengenalan (*identification*), pengumpulan atau agregasi (*aggregation*), pengecualian (*exclusion*), penggunaan kedua atau sekunder;

3) **Penyebaran** (*dissemination*), misalnya pengungkapan (*disclosure*), pemutarbalikan (*distortion*), keterpaparan (*exposure*), insiden bocornya kerahasiaan (*breach of confidentiality*), meningkatnya aksesibilitas (*increased accessibility*), pemerasan (*blackmail*), dan penggunaan identitas orang lain untuk keuntungan sendiri (*appropriation*); dan

4) **Penyerbuan** atau **invasi** (*invasion*), misalnya gangguan intrusi (*intrusion*), interferensi proses pengambilan keputusan (*decisional interference*) dan *self representation* atau gangguan representasi seseorang akibat perubahan yang dilakukan pihak lain.

Dengan semakin canggihnya teknologi kecerdasan buatan tantangan dan ancaman karena gagalnya pelindungan data pribadi menjadi semakin serius, dan potensi kerugiannya jauh lebih besar ketimbang sekedar kerugian ekonomi. Dengan memahami pentingnya melindungi data pribadi dan potensi risiko pencurian data, individu dan organisasi dapat mengambil langkah-langkah yang diperlukan

[2] Taksonomi Solove adalah panduan identifikasi dan pemilahan risiko dan bahaya akibat pelanggaran privasi seseorang. "A Taxonomy of Privacy" oleh Daniel J. Solove. https://wiki.openrightsgroup.org/wiki/A_Taxonomy_of_Privacy

untuk melindungi informasi sensitif dan melindungi diri Anda dari ancaman yang ada.

1. 4. Hak-hak Subjek Data

Data pribadi merupakan aset yang bernilai dan melekat pada setiap subjek. Oleh karena itu, pengakuan hak-hak subjek data merupakan hal penting dalam pelindungan data pribadi. Hak-hak tersebut wajib mendapat pengakuan dan pelindungan dalam peraturan perundang-undangan. Secara spesifik hak-hak subjek data diatur dalam Pasal 6 - 13 UU No 27/2022. Berikut merupakan hak-hak subjek data:

(a) **Hak atas Informasi** (*Right to Information*) Subjek data memiliki hak untuk mengetahui kapan data pribadinya akan, sedang, atau telah diproses. Dengan kata lain, subjek data berhak tahu apa yang dilakukan terhadap data pribadinya. Ini juga berarti pengumpulan data dan pemrosesan data tanpa sepengetahuan dan persetujuan eksplisit merupakan pelanggaran hak subjek data. Oleh karena itu, Pengendali data pribadi yang memiliki data pribadi wajib memberitahu subjek data tentang pelanggaran atau penyusupan apa pun dalam data mereka.

(b) **Hak Akses** (*Right to Access*) Hak untuk mengakses mencakup kemampuan untuk memaksa Pengendali data pribadi manapun yang memiliki data pribadi untuk memberikan deskripsi data yang dimilikinya, serta tujuan data tersebut akan atau sedang diproses pada subjek data. Subjek data pun berhak mengakses rincian lain mengenai pemrosesan informasi, seperti jangka waktu penyimpanan informasi, dan penerima yang menerima informasi tersebut. Hal ini harus dipenuhi dalam format yang mudah diakses, disertai penjelasan dalam bahasa yang sederhana. Hak ini eksplisit dalam Pasal 7 UU No. 27 tentang Pelindungan

Data Pribadi berbunyi, “Subjek data pribadi berhak mendapatkan akses dan memperoleh salinan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.”

(c) **Hak Memperbaiki, Memblokir dan Menghapus** (*Rights to Rectify, Restrict, and Erasure*) Hak untuk memperbaiki memungkinkan subjek data untuk membantah segala ketidakakuratan atau kesalahan dalam informasi pribadi yang diproses, dan meminta Pengendali data pribadi yang memegang informasi pribadi segera memperbaikinya. Sejalan dengan ini, Pengendali data pribadi harus memastikan bahwa informasi baru dan informasi yang ditarik dapat diakses, dan bahwa pihak ketiga yang menerima data yang salah akan diberitahu, atas permintaan subjek data. Pasal 6 UU Pelindungan Data Pribadi menyebut, “Subjek data pribadi berhak melengkapi, mengkinikan, dan/atau memperbaiki kesalahan dan/atau ketidakakuratan data pribadi tentang dirinya sesuai dengan tujuan pemrosesan data pribadi.”

Sejalan dengan itu, subjek data juga memiliki hak untuk memblokir dan menghapus data pribadinya. Hak ini mengizinkan subjek data untuk menangguhkan, menarik atau memerintahkan pemblokiran, penghapusan, penghancuran informasi pribadinya dari sistem pengarsipan pengontrol informasi pribadi setelah ditemukan dan bukti substansial bahwa informasi pribadi tersebut tidak lengkap, tidak *update*, palsu, diperoleh secara tidak sah, digunakan untuk tujuan yang tidak sah atau tidak lagi diperlukan untuk tujuan pengumpulannya. Hal ini secara eksplisit diamanatkan dalam Pasal 8 UU PDP yang menyebut bahwa, “Subjek data pribadi berhak untuk mengakhiri pemrosesan, menghapus, dan/atau memusnahkan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan.”

(d) **Hak untuk Menolak** (*Right to Object*) Subjek data mempunyai hak untuk menolak terhadap pemrosesan data pribadi mengenai dirinya, termasuk pembuatan profil atas data pribadinya. Oleh karena itu Pengendali data pribadi tidak boleh lagi memproses data subjek tersebut. Dalam UU PDP, Pasal 11 menyebutkan, "Subjek data pribadi berhak menunda atau membatasi pemrosesan data pribadi secara sesuai dengan tujuan pemrosesan data pribadi."

(e) **Hak Portabilitas Data** (*Right to Data Portability*) Hak atas portabilitas data memungkinkan subjek data untuk memperoleh dan memindahkan, menyalin, atau mentransfer data pribadi secara elektronik untuk penggunaan lebih lanjut. Hal ini juga untuk memastikan aliran bebas informasi pribadi. Pasal 13 dalam UU PDP menyebutkan bahwa subjek data berhak mendapatkan dan/atau menggunakan data pribadi tentang dirinya dari Pengendali data pribadi dalam bentuk yang sesuai dengan struktur dan/atau format yang lazim digunakan atau dapat dibaca oleh sistem elektronik. Sementara itu, hak untuk memindahkan data menyebut "Subjek data pribadi berhak dan data pribadi tentang dirinya ke Pengendali data pribadi lainnya, sepanjang sistem yang digunakan dapat saling berkomunikasi secara aman sesuai dengan prinsip Pelindungan Data Pribadi berdasarkan Undang-Undang ini."

(f) **Hak terkait Pengambilan Keputusan Otomatis dan Pemrofilan** (*Rights related to Automated Decision Making and Profiling*), Dengan berlimpahnya data, pengendali data pribadi memiliki keuntungan untuk memprofilkan dan membuat keputusan secara otomatis, biasanya berdasarkan algoritma, atas nama efisiensi. Pembuatan profil dan pengambilan keputusan otomatis adalah praktik umum di sejumlah sektor, seperti perbankan dan keuangan, perpajakan, dan pelayanan kesehatan.

Contoh dari pemrofilan adalah ketika sebuah perusahaan perbankan menilai karakteristik nasabah (seperti usia, jenis kelamin, tinggi badan) atau mengklasifikasikan nasabah dalam suatu kategori, ini berarti nasabah sedang diprofilkan. Ketika nasabah mengajukan pinjaman. Nasabah mungkin diminta memasukkan data dan algoritma bank memberi tahu apakah nasabah akan mendapat pinjaman atau tidak dan memberikan tingkat bunga yang disarankan. Ketika pengambilan keputusan itu diambil secara otomatis berdasarkan data pribadi nasabah.

Dalam UU PDP, Pasal 10 mengatur soal subjek data yang memiliki hak untuk mengajukan keberatan atas tindakan pengambilan keputusan yang didasarkan pada pemrosesan secara otomatis, termasuk pemrofilan, yang menimbulkan akibat hukum atau berdampak signifikan pada Subjek data pribadi.

Sejumlah alasan mengapa pemrofilan dan pengambilan keputusan berisiko adalah sebagai berikut:

a. Pembuatan profil seringkali tidak transparan.
b. Subjek data bisa jadi tidak bersedia informasi pribadi mereka digunakan untuk membuat pemrofilan.
c. Subjek data mungkin tidak memahami cara kerja proses tersebut atau pengaruhnya terhadap mereka.
d. Keputusan yang diambil mungkin menimbulkan dampak buruk yang signifikan bagi sebagian orang.
e. Hanya karena analisis data menemukan adanya korelasi, bukan berarti korelasi tersebut signifikan. Karena proses ini hanya dapat membuat asumsi tentang perilaku atau karakteristik seseorang, akan selalu ada margin kesalahan dan diperlukan upaya penyeimbangan untuk mempertimbangkan risiko penggunaan hasil.

(g) **Hak atas Pemulihan yang Efektif** (*Right to an Effective Remedy*) Secara umum, hak atas pemulihan merupakan hak seseorang yang telah dilanggar hak-haknya untuk dapat menggugat pelaku dan menuntut pemulihan, umumnya melalui pengadilan. Hak itu mengatur agar pemulihan itu dapat diakses, mengikat, dapat membawa pelaku ke pengadilan, menyediakan ganti rugi, dan mencegah pelanggaran hak tersebut berulang lagi.

Dalam hal pelindungan data pribadi, dapat saja terjadi pelanggaran atas hak tersebut ketika ada kebocoran atau penyalahgunaan data. Ketika terjadi kegagalan pelindungan data pribadi, Pengendali data pribadi wajib melayangkan pemberitahuan secara tertulis paling lambat 3 x 24 jam kepada lembaga maupun subjek data. Ada kalanya kegagalan pelindungan data pribadi tersebut memiliki dampak yang merugikan subjek data, baik secara hukum maupun kerugian-kerugian lainnya. Untuk itu, ada hak atas upaya hukum yang efektif bagi subjek data jika mereka menganggap bahwa hak mereka berdasarkan UU PDP dilanggar.

(h) **Hak atas Kompensasi dan Pertanggungjawaban**, Berkaitan dengan hak di atas, subjek data yang mengalami pelanggaran data berhak untuk menerima kompensasi dan pertanggungjawaban. Dalam hal ini, subjek data harus membuktikan adanya kerugian sebagai dasar kompensasi dan pertanggungjawaban. Juga, subjek data menunjukan bahwa pengendali data, atau yang memproses data, seharusnya dapat melakukan tindakan yang dibutuhkan untuk mencegah kebocoran data tersebut.

Dalam UU PDP, hal ini diatur dalam Pasal 12 (I) yang menyebut, “Subjek data pribadi berhak menggugat dan menerima ganti rugi

atas pelanggaran pemrosesan data pribadi tentang dirinya sesuai dengan ketentuan peraturan perundang-undangan."

1. 5. Landasan Hukum Pemrosesan Data Pribadi dalam Konteks Kerja Jurnalistik dan Perusahaan Media

Sesuai kerangka-kerja dan pendekatan pelindungan data pribadi, setiap pemrosesan data pribadi bertumpu pada keterbukaan, pengakuan hak individu, dan mengikuti aturan serta hukum yang berlaku. Secara rinci berikut ini adalah beberapa landasan pemrosesan data pribadi pada konteks media dan kerja jurnalistik:

Persetujuan (*consent*) subjek data adalah prinsip inti dari pelindungan data pribadi. Landasan ini memungkinkan subjek data menetapkan kapan data pribadi mereka dapat diproses. Hal ini berkaitan pula dengan pelaksanaan hak-hak dasar otonomi dan penentuan nasib sendiri.

Prinsip-prinsip pelindungan data pribadi akan menjadi bermakna ketika subjek data telah mendapatkan penjelasan (*notice*) tentang kebijakan privasi (*privacy policy/notice*) perusahaan dan hak-hak subjek data sehubungan dengan kebijakan itu. Oleh karenanya, kebijakan privasi memiliki peran yang sangat penting dalam pendekatan 'pemberitahuan' dan 'persetujuan' demi melindungi privasi subjek data.

Persetujuan subjek data harus diberikan secara bebas (*freely given/voluntary*), spesifik, berdasarkan informasi yang memadai (*informed*) dan tidak ambigu. Implikasinya, subjek data memiliki hak untuk menarik persetujuannya kapan pun.

Persetujuan dapat diberikan dalam bentuk pernyataan lisan, tertulis, termasuk dengan cara elektronik (*online*). Dalam praktik, untuk

menghindari ambiguitas '*consent*', diperlukan tindakan afirmatif yang jelas dari subjek data, seperti mencentang kotak yang digunakan saat mengunjungi situs web.

Selanjutnya, untuk memastikan prinsip sukarela (*voluntary*) pemberian persetujuan ('*consent*'), persetujuan harus dinyatakan tidak sah ketika terdapat ketidakseimbangan kuasa yang jelas antara subjek data dan pengendali data. Situasi ketidakseimbangan dapat muncul dalam situasi tertentu, misalnya jika pengendali adalah otoritas publik. Meski demikian, eksistensi situasi ketidakseimbangan dalam pemberian '*consent*' harus diidentifikasi berdasarkan kasus per kasus.

Ada larangan mengaitkan pelaksanaan kewajiban kontraktual (*performance of a contract*) dengan persetujuan untuk melakukan pemrosesan data yang tidak diperlukan. Kemudian, pengendali data wajib memastikan bahwa pemberian persetujuan (*consent*) berdasarkan informasi yang cukup (*informed consent*) mengenai setidaknya identitas pengendali data, tujuan pemrosesan data pribadi, dan informasi yang diperlukan lainnya. Persetujuan subjek data haruslah sesuai dengan situasi pemrosesan data yang spesifik, atau dengan kata lain bentuk otorisasi umum tidak diperbolehkan.

Contoh: Perusahaan media sosial mengumpulkan data pribadi penggunanya untuk melakukan bisnis periklanan berdasarkan minat penggunanya. Dalam situasi ini, perusahaan media sosial harus mendapatkan persetujuan dari penggunanya untuk pemrosesan data pribadi untuk tujuan penargetan iklan di platform media sosialnya.

Pelaksanaan Tugas dalam rangka Kepentingan Umum, Pemrosesan data pribadi dapat dilakukan untuk tujuan pelaksanaan kewajiban hukum berdasarkan perundang-undangan yang dimiliki oleh pengendali data.

Contoh: Suatu perusahaan mengumpulkan data pribadi pekerjanya untuk tujuan pelaporan perpajakan. Dalam situasi ini, perusahaan dapat melakukan pemrosesan data pribadi pekerjanya berdasarkan kewajiban hukum perusahaan untuk melakukan pelaporan pajak.

Pemenuhan Kewajiban Perjanjian, Pemrosesan data pribadi dapat dilakukan jika dibutuhkan guna pelaksanaan kontrak. Subjek data merupakan salah satu pihak, atau dibutuhkan guna mengambil langkah-langkah yang diperlukan sesuai dengan kehendak subjek data sebelum suatu kontrak berlaku secara sah.

Contoh: Perusahaan *e-commerce* mengumpulkan data pribadi penggunanya untuk mengirimkan barang pesanan pembeli di *platform e-commerce*-nya. Dalam situasi ini, perusahaan *e-commerce* dapat melakukan pemrosesan data pribadi konsumen berdasarkan pelaksanaan kontrak jual-beli antara penjual dan pembeli.

Pemenuhan Kewajiban Hukum, Pasal 20 ayat (2) huruf c menyatakan "pemrosesan data pribadi untuk pemenuhan kewajiban hukum oleh pengendali data sesuai ketentuan peraturan perundang-undangan." Artinya, meskipun tanpa persetujuan eksplisit dari subjek data, pengendali data pribadi dapat melakukan pemrosesan data pribadi sepanjang ada kewajiban hukum sesuai ketentuan peraturan perundang-undangan. Sebagai contoh adalah terkait pemrosesan data kependudukan, registrasi dan aktivasi telepon seluler, data terkait kesehatan yang dilaksanakan sebagai pemenuhan amanat peraturan perundang-undangan.

Pemenuhan Kepentingan Sah lainnya, Pemrosesan data pribadi dapat dilakukan jika dibutuhkan untuk kepentingan yang sah yang dimiliki oleh pengendali data atau pihak ketiga kecuali dalam kondisi di mana kepentingan yang sah tersebut akan menimbulkan dampak

yang signifikan bagi kepentingan, serta hak dan kebebasan mendasar yang dimiliki subjek data.

Umumnya, untuk membantu pengendali data melakukan analisa apakah pihaknya dapat menggunakan kepentingan yang sah sebagai dasar pemrosesan data pribadi, pengendali data dapat mengaplikasikan syarat 3 tahap: uji tujuan, kebutuhan dan keseimbangan.

Contoh: Perusahaan *e-commerce* mendeteksi serangan '*denial of service*' dan serangan yang menyebabkan akses tidak sah terhadap sistem elektronik. Dalam situasi ini, pengendali dapat melakukan tindakan pengamanan data pribadi yang melingkupi pemrosesan data pribadi konsumen berdasarkan kepentina dimaksud dalam Pasal 8, Pasal 9, Pasal 10 ayat (1), Pasal 11, dan Pasal 13 ayat (1) dan ayat (2) dikecualikan untuk kepentingan:

1. pertahanan dan keamanan nasional;
2. proses penegakan hukum;
3. kepentingan umum dalam rangka penyelenggaraan negara;
4. pengawasan sektor jasa keuangan, moneter, sistem pembayaran, dan stabilitas sistem keuangan yang dilakukan dalam rangka penyelenggaraan negara; atau
5. statistik dan penelitian ilmiah.

1. 6. Kewajiban Pengendali dan Prosesor Data

Selama menjalankan fungsi pengendalian dan pemrosesan, pengendali data dan pemroses data pribadi berkewajiban, UU No. 27/2022 tentang Pelindungan Data Pribadi:

(a) Pengendali data pribadi, di antaranya, wajib menunjukkan bukti persetujuan yang telah diberikan subjek data pribadi saat melakukan pemrosesan data pribadi, wajib menjaga kerahasiaan data pribadi, dan wajib mencegah data pribadi diakses secara tidak sah (Pasal 20 s.d. Pasal 50).

(b) Prosesor data pribadi, antara lain, wajib melakukan pemrosesan data pribadi berdasarkan perintah pengendali data pribadi, wajib mendapatkan persetujuan tertulis dari pengendali data pribadi sebelum melibatkan prosesor data pribadi lain (Pasal 51 s.d. Pasal 52).

(c) Pengendali data pribadi dan prosesor data pribadi wajib menunjuk pejabat atau petugas yang melaksanakan fungsi pelindungan data pribadi dalam hal (Pasal 53 ayat (1)):

1. pemrosesan data pribadi untuk kepentingan pelayanan publik;
2. kegiatan inti pengendali data pribadi memiliki sifat, ruang lingkup, dan/atau tujuan yang memerlukan pemantauan secara teratur dan sistematis atas data pribadi dengan skala besar; dan
3. kegiatan inti pengendali data pribadi terdiri dari pemrosesan data pribadi dalam skala besar untuk data pribadi yang bersifat spesifik dan/atau data pribadi yang berkaitan dengan tindak pidana.

Kewajiban pengendali dan pemroses data pribadi akan dibahas dengan lebih detail pada bagian Pelindungan Data Pribadi untuk Perusahaan Media, karena dalam ekosistem industri media digital tanggungjawab untuk menegakkan pelindungan data pribadi akan berada pada perusahaan media sebagai pengendali atau pengendali bersangan yang sah.

1. 7. Pengecualian Pemenuhan Hak-hak Subjek Data

Ada pengecualian dalam penerapan pasal-pasal tersebut. Setiap individu tetap dikenakan kewajiban terhadap, terutama, kepentingan proses penegakan dan kepentingan publik.

Dalam Pasal 15 ayat (1) disebutkan: Hak-hak Subjek Data Pribadi sebagaimama data pribadi.

Praktikum: Dalam industri media memahami audiens adalah langkah penting untuk memahami topik dan pola konsumsi informasinya, cobalah identifikasi jenis data pribadi apa yang akan dikumpulkan dan diproses oleh perusahaan media, dan jelaskan risiko yang mungkin dihadapi oleh subjek data, jika terjadi insiden kegagalan pelindungan data pribadi.

Didukung oleh:

BAB 2

PDP UNTUK PERUSAHAAN/ORGANISASI PENGELOLA MEDIA

MODUL 2

PDP UNTUK PERUSAHAAN/ ORGANISASI PENGELOLA MEDIA

2.0. Pengantar

Media sebagai badan usaha yang produknya adalah informasi, mengelola dua informasi penting, yaitu informasi terkait materi yang ditransaksikan, dalam hal ini dipublikasi sebagai produk & layanan (*created value*) dan informasi terkait pihak yang mendapatkan manfaat (target pengguna) dari materi tersebut dan mitra usaha.

Dalam konteks jurnalisme, media adalah elemen penting dalam pelaksanaan fungsi kebebasan berekspresi dalam berdemokrasi. Dalam melaksanakan fungsi ini, acapkali media berhadapan dengan tantangan pemenuhan hak perlindungan atas privasi manakala informasi yang menjadi hak publik bersifat atau mengandung informasi pribadi. Oleh karenanya adalah sangat penting, media menemukan kesetimbangan antara pemenuhan hak publik atas informasi dan pemenuhan perlindungan hak atas privasi.

Perusahaan (atau organisasi) media sebagai pengendali data (*data controller*) melakukan penyeimbangan di atas berdasarkan prinsip persetujuan publikasi/pemrosesan informasi pribadi dan batasan-batasan proporsional kepentingan publik. Prinsip-prinsip ini tentu saja mengacu

pada landasan pemrosesan data pribadi sebagaimana dibahas dalam Bagian 1.5 sebelumnya tentang Landasan Pemrosesan Data Pribadi. Dalam hal pemrosesan informasi pribadi untuk memenuhi kepentingan publik, batasan-batasan tersebut terkait dengan hal-hal yang mempengaruhi, menarik perhatian, dan berdampak pada publik, bisa dalam bentuk elemen-elemen informasi yang dapat dipublikasikan.

Penyeimbangan kepentingan itu penting dalam rangka melaksanakan fungsi jurnalistik, dan mengatasi tantangan klausul perlindungan hak privasi dan kepentingan publik (kebebasan berekspresi), seperti isu defamasi dalam Revisi UU ITE No. 16/2016 dan hak penghapusan informasi yang tidak relevan (dalam konteks *the right to be forgotten*) dalam publikasi jurnalistik. Kemudian, klausul pemrosesan data pribadi untuk kepentingan publik yang dibatasi dalam penyelenggaran negara, dan ini akan menimbulkan tantangan dan risiko, karena klausul jurnalisme tidak ditempatkan sebagai bagian dari kepentingan publik.

Pada kutub yang lain, perusahaan media pun mengelola informasi pribadi terkait pengguna atau audiens media, yang mana dinamika pengelolaannya tidak kalah pentingnya. Karena dalam pengelolaan usaha media digital, audiens menjadi salah satu faktor penting dalam keberlangsungan usaha penerbitan media.

Kebutuhan mengenali audiens menjadi salah satu faktor penting dalam rencana dan strategi pengembangan aspek komersial penerbitan media, yang secara khusus akan mempengaruhi valuasi bisnisnya. Valuasi terbesar badan usaha penerbitan atau media digital bersumber pada pengguna atau audiens (*users*) media yang bersangkutan. Semakin besar audiens atau pengguna sebuah usaha penerbitan media, semakin besar pula valuasinya, karena potensi transaksi komersial yang terjadi juga menjadi semakin besar. Realisasi potensi transaksi komersial tersebut makin besar, manakala pelaku usahanya mampu mengenali audiensnya. Setiap penggal informasi yang mengidentifikasi audiens adalah data

pribadi. Melindungi data pribadi, dalam hal ini adalah data pribadi audiens, berarti melindungi aset dan valuasi badan usaha media.

Proses mengenali audiens ini melibatkan sebuah proses berulang yang disebut sebagai siklus data pribadi (*privacy information lifecycle*), sebagaimana telah disinggung pada Bab 1, tentang Pengantar Data Pribadi dan Pelindungan Data Pribadi. Bagaimana siklus data pribadi berjalan bergantung pada model bisnis perusahaan media yang ada. Tiga model bisnis paling sederhana sebuah usaha penerbitan media digital adalah:

(1) Semua layanan disediakan secara cuma-cuma atau gratis, dan layanan yang ada dibiayai dari pendapatan periklanan. Umumnya upaya pengenalan audiens sangat minimum dan mengandalkan layanan pihak ketiga untuk melakukan pengenalan penggunanya. Aktivitas pemrosesan data pribadi sangat ringan, sampai tidak mengenali penggunanya secara spesifik.

(2). Pada ekstrim yang lain, penerbitan dengan model berlangganan atau berbayar, sehingga semua layanan yang diberikan menuntut pembayaran premi atau biaya berlangganan. Sistem penerbitan melakukan pencatatan siapa yang mendaftar sebagai pengguna dan akan selalu memeriksa setiap akses apakah pengguna tersebut masih memiliki hak mengakses layanan sampai masa berlangganannya berakhir. Implikasi model bisnis kedua ini, setiap pengguna yang mengakses tercatat dan harus teridentifikasi dan *authenticated* atau terbukti identitasnya. Meskipun sederhana prosesnya, sebagian besar tahapan siklus data pribadi terlampaui sampai penghancuran data pribadi, bilamana pengguna memutuskan untuk tidak lanjut berlangganan.

(3) Sementara pada model bisnis ketiga adalah campuran dari model bisnis pertama dan kedua, yaitu penerbitan media digital yang pendanaannya bertumpu pada model berlangganan untuk informasi yang bersifat premium, tetapi juga ditopang oleh bisnis periklanan yang

bertumpu terutama pada layanan yang diberikan secara cuma-cuma. Pemrosesan data pribadi menjadi semakin dalam. Pada satu sisi pengelola usaha melalui sistem elektronik melakukan pendataan setiap audiens yang menjadi pelanggan agar bisa mengidentifikasi dan membuktikan identitasnya bahwa seorang pengakses layanan adalah pelanggan. Selanjutnya pada sisi model bisnis layanan cuma-cuma informasi perilaku (*behaviour*) dan preferensi pelanggan terhadap isu-isu terkait menjadi senjata untuk menyukseskan transaksi komersial berbasis penawaran-penawaran melalui model bisnis periklanan. Kombinasi dua data pribadi ini akan menjadi senjata yang ampuh untuk berbagai model bisnis turunan, yang bisa jadi disediakan oleh mitra-mitra bisnis.

Berbagai model bisnis turunan ini melibatkan pengolahan data pribadi yang komplek dan tidak saja dilakukan secara internal tetapi juga melibatkan pihak lain sebagai pemroses data pribadi pelanggan media tersebut.

Setiap upaya untuk melindungi data pribadi setiap subjek data yang terlibat dalam proses bisnis akan menguatkan fondasi pengembangan usaha ke depan. Oleh karenanya perusahaan media paling tidak memiliki kewajiban:

2.0.1. Tanggung Jawab dan Kepatuhan pada Aturan Pemrosesan Data Pribadi

Perusahaan media berkewajiban memastikan kepatuhan (*compliance*) pada setiap aturan dan landasan hukum dan prinsip pemrosesan data pribadi sebagaimana tertuang dalam UU No. 27/2022 Pasal 16 & Pasal 20, dan pasal-pasal yang mengatur kewajiban pengendali dan pemroses data pribadi (1. 7. Kewajiban Pengendali dan Prosesor Data)

Secara sederhana tanggungjawab dan kepatuhan perusahaan media sebagai pihak yang terlibat dalam pemrosesan dan pengelolaan data pribadi digambarkan sebagai berikut:

 Pengendali Data Pribadi	 Pengendali Bersama Data Pribadi	 Pemroses Data Pribadi
Implementasi prosedur organisasi dan teknis untuk menjamin kepatuhan perundangan. Memastikan pelaksanaan prinsip pelindungan data dalam pemrosesan data pribadi. Mematuhi pedoman perilaku pelindungan data pribadi. Menerapkan pendekatan *privacy by design* dan *privacy by default* dalam setiap tahapan pemrosesan data pribadi. Memastikan implementasi sistem pengamanan (*security system*) yang cukup dalam pemrosesan data pribadi. Menunjuk dan memastikan adanya petugas Pelindungan Data Pribadi (*Data Protection Officer* - DPO).	Secara transparan menentukan tanggung jawab masing-masing untuk memenuhi kepatuhan terhadap UU PDP. Pengaturan mekanisme bersama yang mencerminkan peran dan hubungan masing-masing pengendali data ketika berhadapan dengan subjek data. Subjek data dapat menggunakan haknya untuk masing-masing pengendali data.	Bertindak berdasarkan perintah tertulis dari pengendali data, kecuali atas perintah perundang-undangan. Atas perintah pengendali data, menerapkan langkah-langkah teknis dan organisasi yang tepat. Penunjukan sub-pemroses atas persetujuan pengendali data. Membantu pengendali data melakukan langkah-langkah teknis dan organisasi untuk memenuhi kewajiban pengendali, termasuk pemenuhan hak subjek data, penerapan sistem keamanan, dan kewajiban yang lain. Memastikan adanya petugas Pelindungan Data Pribadi (*Data Protection Officer* - DPO).

2.0.2. Memastikan Keamanan Pemrosesan Data Pribadi

Perusahaan atau organisasi pengelola media wajib memastikan mengambil langkah-langkah yang perlu baik secara teknis atau organisasi untuk menjamin keamanan dalam pemrosesan data pribadi. Langkah-langkah pengamanan ini mencakup pengamanan secara fisik (*physical security measure*), kebijakan-kebijakan menyangkut klasifikasi, skema penyimpanan, retensi dan penghapusan/penghancuran data, untuk menjamin kerahasiaan, integritas dan ketersediaan data yang menjadi subjek pengamanan.

Dalam UU No. 27/2022 PDP, kewajiban pengamanan data pribadi ini diatur dalam Pasal 35, dengan membebankan kewajiban pada pengendali data untuk menyusun dan menerapkan langkah teknis operasional, serta menentukan tingkat keamanan data sesuai sifat dan risikonya. Kewajiban untuk melakukan pengawasan terhadap semua pihak yang terlibat dalam pemrosesan data pribadi tertuang dalam Pasal 36, dan melindungi dari pemrosesan data & mencegah akses data yang tidak sah dalam Pasal 37.

2.0.3. Melakukan Pencatatan Kegiatan Pemrosesan Data Pribadi (*Record of Processing Activities* - RoPA)

Pasal 31 UU No. 27/2022 PDP memandatkan pengendali data melakukan perekaman atau pencatatan terhadap seluruh kegiatan pemrosesan data pribadi. Perusahaan atau organisasi pengelola media wajib menyimpan catatan kegiatan pemrosesan data sebagai bentuk kepatuhan terhadap peraturan.

Melalui catatan tersebut, otoritas pengawas melakukan pemantauan keabsahan pemrosesan data. Meskipun UU PDP belum menjelaskan

kriteria RoPA. RPP UU PDP saat ini telah mengatur ketentuan RoPA, untuk disimpan dalam bentuk tertulis secara elektronik atau non-elektronik dan mengandung informasi sebagai berikut: (1) nama dan detail kontak pengendali data pribadi, pengendali data pribadi bersama, dan/atau prosesor data pribadi; (2) kontak pejabat pelindungan data pribadi; (3) sumber pengumpulan dan tujuan pengiriman data pribadi; (4) dasar pemrosesan data pribadi; (5) tujuan pemrosesan data pribadi; (6) jenis data pribadi; (7) kategori subjek data pribadi; (8) pihak selain pengendali data pribadi yang dapat mengakses data pribadi; (9) pemenuhan hak subjek data pribadi; pemetaan aliran data pribadi; (10) masa retensi; dan (11) langkah teknis dan organisasi dalam rangka pengamanan data pribadi.

2.0.4. Kewajiban Menjaga Kerahasiaan Data Pribadi

Berbeda dengan kewajiban menjaga keamanan, menjaga kerahasiaan data pribadi mensyaratkan kepatuhan terhadap peraturan dan perundangan pelindungan data pribadi, yang mencakup pelindungan terhadap perangkat dan infrastruktur setiap pemrosesan data pribadi, termasuk di dalamnya adalah proses data transfer.

Pada konteks kontrak pemrosesan data pribadi, kewajiban kerahasiaan dimuat dalam setiap kontrak antara pengendali dan pemroses data pribadi. Dan kedua belah pihak berkewajiban untuk menurunkan kewajiban hukum kerahasiaan itu ke dalam klausul kontrak kerja dengan staf mereka. Pasal 36, UU No. 27/2022 PDP mengatur kewajiban untuk melindungi kerahasiaan ini.

2.0.5. Kewajiban Memberi Pemberitahuan atas Pelanggaran Pelindungan (*data breach*) dan Kegagalan Pelindungan Data Pribadi berdasarkan UU PDP

Pelanggaran pelindungan data adalah pelanggaran keamanan yang menyebabkan kerusakan, kehilangan, pemusnahan, perubahan, pengungkapan atau akses tidak sah terhadap data pribadi yang dikirim, diproses atau disimpan. Pelanggaran ini dapat dikategorikan menjadi tiga kelompok, yaitu pelanggaran kerahasiaan (*confidentiality breach*), integritas (*integrity breach*) dan ketersediaan (*availability breach*).

Kewajiban pemberitahuan terhadap pelanggaran ini bergantung pada tingkat risiko yang ditimbulkan, dimulai dari tidak wajib melakukan pemberitahuan jika pelanggaran dapat langsung diatasi dengan dampak tidak berisiko sampai berisiko minimum; pemberitahuan kepada otoritas pelindungan data, dengan pertimbangan besaran pelanggaran dan risiko serius; sampai pada kewajiban melakukan pemberitahuan kepada subjek data, ketika pelanggaran membawa dampak serius bagi subjek data. Pemberitahuan memuat informasi dampak dan tindakan perbaikan yang diambil. Jangka waktu pemberitahuan umumnya menekankan pada prinsip tanpa penundaan (*without undue delayed*), yang umumnya 3x24 jam.

Sementara insiden kegagalan pelindungan data pribadi sesuai UU No. 27/2022 tentang PDP Pasal 46, pengendali data wajib melakukan pemberitahuan paling lambat 3X24 jam secara tertulis kepada subjek data dan otoritas pelindungan data pribadi.

Pemberitahuan itu memuat: data pribadi yang terungkap, kapan & bagaimana data insiden terjadi, dan upaya penanganan dan pemulihan atas terungkapnya data pribadi tersebut. Dalam hal kegagalan pelindungan data pribadi mengganggu pelayanan publik dan/atau

berdampak serius terhadap kepentingan masyarakat, pengendali data wajib memberitahukan kepada masyarakat mengenai kegagalan pelindungan data tersebut.

Secara detail langkah dan tahapan yang perlu dilakukan dalam merespon terjadi insiden kegagalan pelindungan data pribadi atau *data breach* dibahas detail pada Modul 2.4.

2.0.6. Kewajiban Melakukan Penilaian Dampak Pelindungan Data Pribadi (*Data Protection Impact Assessment* - DPIA)

Kewajiban melakukan prosedur penilaian dampak pemrosesan data pribadi yang mempunyai risiko tinggi, meliputi pengambilan keputusan secara otomatis yang memiliki akibat hukum atau dampak yang signifikan terhadap subjek data, pemrosesan atas data yang bersifat spesifik, pemrosesan data dalam skala besar (*big data*), pemrosesan data untuk kegiatan evaluasi, penskoran, atau pemantauan yang sistematis terhadap subjek data pribadi, pemrosesan data untuk kegiatan pencocokan atau penggabungan sekelompok data, penggunaan teknologi baru dalam pemrosesan data, dan/atau, pemrosesan data yang membatasi pelaksanaan hak subjek data pribadi.

Dengan DPIA, pengendali data dan pemroses data dapat menilai dan mengambil langkah untuk mengatasi dampak dan risiko pemrosesan data. Melalui DPIA juga, pengendali data memastikan akuntabilitas dengan menunjukkan langkah-langkah yang telah diambil untuk memastikan kepatuhan terhadap peraturan perundang-undangan. Pasal 34 UU No. 27/2022 PDP mengatur kewajiban untuk melakukan DPIA.

2.0.7. Kewajiban Menunjuk Pejabat Pelindungan Data Pribadi *Data Protection Officer* (DPO)

Sesuai perintah Pasal 53 UU No. 27/2022 tentang PDP, pengendali data pribadi dan prosesor data pribadi wajib menunjuk pejabat atau petugas yang melaksanakan fungsi pelindungan data pribadi, apabila (a) pemrosesan data pribadi untuk kepentingan pelayanan publik; (b) kegiatan inti pengendali data bersifat, ruang lingkup, dan/atau tujuan yang memerlukan pemantauan secara teratur dan sistematis atas data pribadi dengan skala besar; dan (c) kegiatan inti pengendali data terdiri dari pemrosesan data dalam skala besar untuk data pribadi yang bersifat spesifik dan/atau yang berkaitan dengan tindak pidana.

Penunjukan pejabat pelindungan data pribadi (DPO) harus didasarkan pada profesionalitas, pengetahuan mengenai hukum, praktik pelindungan data pribadi, dan kemampuan untuk memenuhi tugas-tugasnya.

Secara umum DPO pelaksana operasional implementasi pelindungan data dan strategi privasi data dalam satu organisasi (publik atau swasta). DPO bertugas memfasilitasi budaya pelindungan data di seluruh pengendali atau pemroses data, dan memastikan kepatuhan terhadap hukum pelindungan data, memberikan saran/masukan terkait DPIA, berkoordinasi dan bertindak sebagai narahubung terkait pemrosesan data. Oleh karenanya, DPO berhak memiliki akses ke semua sumberdaya yang diperlukan dalam melaksanakan tugas.

Pejabat atau petugas yang melaksanakan fungsi pelindungan data pribadi (DPO) dapat berasal dari dalam dan/atau luar pengendali atau prosesor data pribadi.

2.0.8. Ancaman Sanksi bagi Pengendali dan Pemroses Data Pribadi

Gagal menjalankan kewajiban pelindungan sebagaimana diamanatkan oleh UU No. 27/2022 tentang PDP, pengendali dan pemroses data pribadi diancam sanksi, mulai dari sanksi dan denda administratif sebagai diatur dalam Pasal 57, sampai dengan pidana (Pasal 67-73), sebagai implikasi ketentuan larangan.

Sanksi administratif dikenakan pada pelanggaran sejumlah pasal terkait kepatuhan dalam bentuk peringatan tertulis, penghentian sementara pemrosesan, penghapusan/pemusnahan data, dan/atau denda administratif. Denda administratif dikenakan maksimum 2% dari total pendapatan/penerimaan tahunan, dengan demikian sanksi ini hanya dapat diterapkan pada pengendali data yang berasal dari korporasi.

Sementara itu, pengendali data dari sektor publik hanya dapat dikenakan sanksi administratif ketika mereka melakukan pelanggaran dalam pemrosesan data. Sanksi administratif akan ditegakkan oleh lembaga atau otoritas pelindungan data pribadi (Pasal 57 ayat 4).

Pelanggaran ketentuan Pasal 65-70, dikenakan sanksi pidana terhadap orang-perseorangan (termasuk korporasi). Melanggar larangan memperoleh atau mengumpulkan data pribadi secara melanggar hukum yang merugikan subjek data (Pasal 65 ayat 1) dan menggunakan data pribadi yang bukan miliknya (Pasal 65 ayat 3) dipidana penjara selama 5 tahun dan/atau denda Rp 5miliar. Sementara pelanggaran dengan sengaja mengungkapkan data pribadi yang bukan miliknya (Pasal 65 ayat 2) dipidana penjara 4 tahun dan/atau denda Rp 4miliar.

Modul 2.1: Pengumpulan Data Pribadi dan Praktik Penggunaan Data Pribadi yang Adil

Deskripsi: Memberikan penjelasan bagaimana tahap pengumpulan data pribadi dalam pemrosesan data pribadi melalui kerangka praktik penggunaan data pribadi yang adil (*fair information practices*), prasyarat dan kewajiban legal dan teknis atas proses yang sedang dijalankan.

Tujuan: Peserta pelatihan mampu mengidentifikasi jenis data pribadi dan praktik pengumpulan data pribadi

Durasi: 90 menit

Metodologi: Presentas, diskusi dan praktikum identifikasi dan analisis regulasi yang diperlukan dalam proses pengumpulan data pribadi.

Pokok Bahasan

Dalam kerangka pelindungan data pribadi, setiap tahapan pemrosesan yang dilalui dalam siklus harus mengikuti kerangka praktik penggunaan data yang adil (*fair information practices*[3]). Panduan umum ini meliputi aspek pengakuan terhadap hak individu (*rights of individuals*) sebagai subjek data, siklus data pribadi (*privacy information lifecycle*), pengendalian dan pengelolaan data (*controls of information*) yang menyangkut aspek keamanan dan kualitas data, manajemen pengelolaan data yang menyangkut aspek proses administrasi, pemantauan dan penegakan kebijakan pengelolaan data pribadi.

[3] Bersumber dari US Fair Information Practices (HEW, 1973) & OECD Guideline

Prinsip pengakuan terhadap hak individu dalam pemrosesan data pribadi adalah pemberitahuan (*notices*) kepada pengguna sebagai subjek data tentang objek data pribadi yang diproses, dalam hal ini dikumpulkan sebagai tahapan pertama pada siklus data pribadi, dan maksud & tujuan pemrosesan data tersebut. Di dalam praktik, pemberitahuan ini digabungkan dengan janji (*promises*) pemroses data, dalam hal ini adalah wali atau pengendali data (*data controller*) terhadap aspek tujuan pemrosesan dan pengelolaannya, termasuk di dalamnya adalah aspek keamanan & kualitas data, dan umumnya dituangkan dalam bentuk kebijakan privasi untuk pengguna layanan.

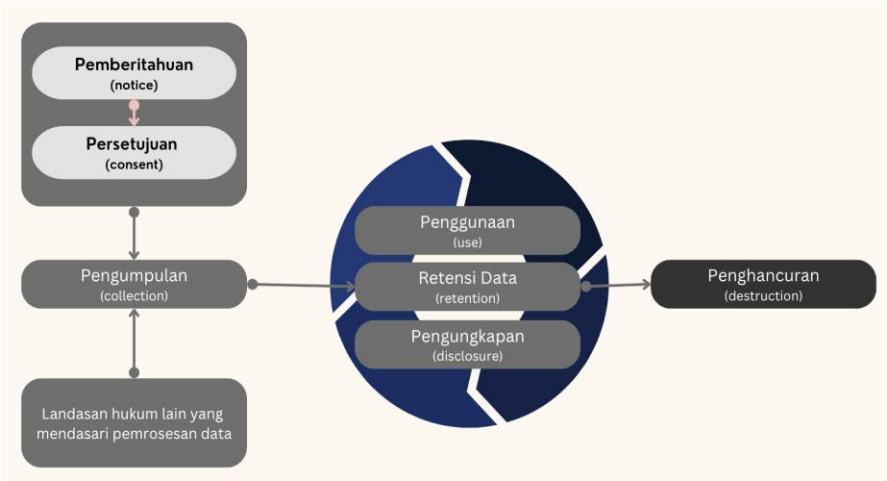
Kebijakan privasi di atas adalah pemberitahuan (*notices*) atau pernyataan (*statement*) tentang materi, maksud & tujuan pemrosesan data pribadi dan janji/kewajiban yang akan dilakukan oleh pengendali terhadap data yang diproses. Karena pernyataan privasi (*privacy notices/statements*) adalah komunikasi ke subjek data, maka pernyatan tersebut perlu disediakan di awal tahapan pemrosesan dan dapat berubah sejalan perkembangan, jelas & mudah diakses, akurat & lengkap, dan menggunakan bahasa yang mudah dibaca awam.

2.1.1 Jenis-jenis dan Bentuk-bentuk Pengumpulan Data Pribadi

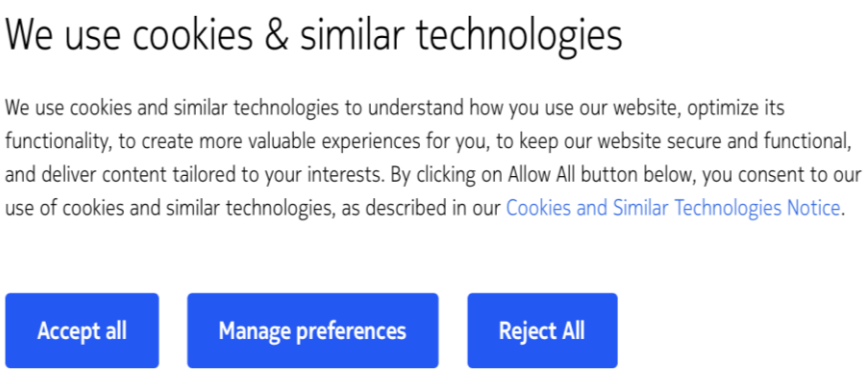
Berdasarkan skenario tiga model bisnis yang dijadikan teladan dalam pengelolaan pelindungan data pribadi, terdapat dua kelompok data pribadi yang diproses, yaitu (1) data pribadi terkait penanda individu (*personal identifier*) dan (2) data pribadi yang menunjukkan preferensi. Berdasarkan UU No 27 Th. 2022 pasal 4, kedua kelompok data pribadi tersebut bersifat data umum, yang secara sendiri-sendiri atau gabungan digunakan untuk mengidentifikasi individu. Pada beberapa model bisnis yang lebih komplek, layanan membutuhkan pemrosesan data pribadi yang bersifat khusus, misalnya terkait proses pembayaran layanan akan memproses data rekening keuangan.

Metode pengumpulan data pribadi dapat dilakukan secara aktif, dalam hal ini subjek data secara aktif memberikan datanya kepada pengendali atau wali data, atau secara pasif melalui pengamatan (*surveillance*). Setiap jenis data yang dikumpulkan, pengendali data wajib memberikan penjelasan landasan hukum dan rasional dibalik pengumpulan data tersebut. Idealnya setiap pengumpulan data mempunyai landasan hukum tertinggi, tetapi acapkali hal ini tak terpenuhi sehingga pemrosesan ini hanya berdasarkan persetujuan. Tantangan terbesar dengan persetujuan (*consent*) adalah apabila subject data mencabut persetujuannya. Pencabutan itu secara legal mewajibkan pengendali atau wali data untuk mencabut dan menghancurkan semua informasi yang dikumpulkan dan dikelola terkait subjek data. Proses menjadi lebih menantang bila pemrosesan data turunan melibatkan pihak pemroses data di luar institusi pengendali data.

Secara sederhana prinsip dasar pemrosesan data mengacu pada siklus data pribadi dijelaskan dalam diagram berikut ini.



Informasi Penanda (*identifier*) dan *Cookies*, bentuk pemrosesan dan jenis data paling sederhana yang diproses dalam tahap ini adalah pemberian penanda (*identifier*) yang disimpan dalam peramban (*browser*) pada perangkat pengguna yang dikenal dengan nama *cookies*. Karena informasi penanda ini memungkinkan penyedia layanan mengenali individu pengguna, maka informasi ini termasuk data pribadi. Oleh karenanya berdasarkan GDPR (*General Data Protection Regulation*) yang berlaku di Uni Eropa, pengguna harus memberikan persetujuan untuk sebelum penyedia layanan meletakkan informasi penanda dalam bentuk *cookie* di dalam



peramban pengguna, dan memberikan fasilitas untuk mengelola informasi penanda apa saja yang dapat diletakkan dalam perangkat pengguna sebagai subjek data. Tangkapan layar berikut ini memberikan contoh bagaimana persetujuan (*consent*) sebagai landasan hukum digunakan untuk melakukan pemrosesan data pribadi.

Umumnya setelah menempatkan penanda, penyedia layanan akan menggunakan penanda tersebut mencatat aktivitas pengguna atau subjek data dalam interaksi platform pemenuhan layanan. Dalam berbagai pengumpulan dan pemrosesan data aktivitas penggunaan seringkali melibatkan pemroses eksternal, misalnya untuk kebutuhan analisis data penggunaan dan profil pengguna melibatkan penyedia layanan seperti Google Analytic, Chartbeat atau penyedia Platform Data Pelanggan (*customer data platform*).

Fasilitas registrasi, autentikasi dan fasilitas pengaturan akun, Pada perusahaan media digital dengan model bisnis yang lebih komplek, pengumpulan elemen data (*data point*) menjadi lebih banyak dan menyediakan fasilitas mandiri mengelola data pribadi, seperti formulir pendaftaran, fasilitas autentikasi untuk membuktikan identitasnya, sampai yang lebih canggih dengan menyediakan fasilitas pengelolaan data profil pengguna.

Proses pengumpulan data secara aktif ini dapat dilakukan sekaligus dalam satu waktu, atau secara berkala menggunakan berbagai pendekatan untuk mendapatkan kelengkapan data yang mampu memberikan gambaran audiens media digital yang bersangkutan, misalnya gambaran sosiodemografi. Gambaran ini penting bagi bisnis untuk memaksimalkan realisasi potensi transaksi komersial yang akan membiayai seluruh proses bisnis, baik editorial proses maupun komersial proses.

Penggunaan ulang dan data dari pihak ketiga, Mekanisme lain yang bisa dilakukan dalam pengumpulan data pribadi adalah menggunakan ulang (*repurposing*) data pribadi dan data yang bersumber dari mitra atau *third party data*.

Untuk memberikan gambaran bagaimana mekanisme penggunaan ulang (*repurposing*), anggaplah sebuah media digital bekerja sama

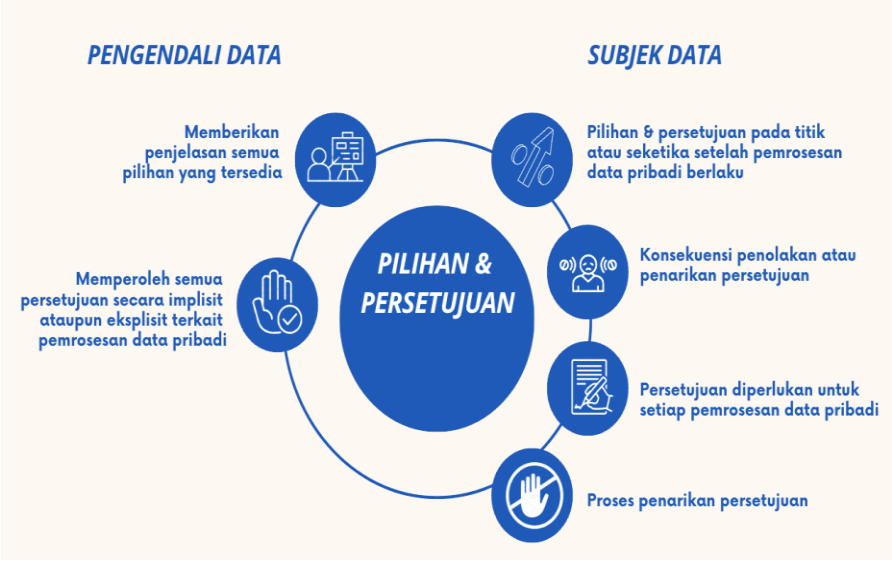
dengan sebuah produk, misalnya otomotif. Kegiatan ini (sebagai contoh produk otomotif) menawarkan pembelian dengan harga diskon spesial dan kegiatan uji kendarai produknya. Dalam rangka kegiatan tersebut, media membangun sebuah situs kecil (*microsite*) yang berisi fasilitas pendaftaran untuk mengikuti kegiatan ini dengan semua elemen data (*data point*) pribadi yang relevan. Pada kegiatan itu, bila media tersebut menggunakan data yang dikumpulkan dalam kegiatan ini untuk pengkinian data yang mereka simpan atau untuk kegiatan promosi lain, proses ini disebut penggunaan ulang (*repurposing*).

Sementara untuk data yang bersumber dari mitra bisnis atau pihak ketiga bisa terjadi dengan berbagai alasan dan mekanisme. Sebagai contoh, untuk melengkapi layanan media pada sistem layanan elektronik belanja daring bekerja sama dengan layanan media digital agar mendapatkan akses khusus bagi penggunanya. Dalam rangka pemenuhan kontrak layanan tersebut, maka pada saat pengguna layanan belanja daring mengakses layanan media data pribadi pengguna tersebut akan ditransfer ke sistem elektronik media, sehingga pengguna yang bersangkutan dikenali dan mendapatkan layanan yang layak sebagaimana dijanjikan. Proses transfer menangkap data pribadi dari pihak ketiga (layanan belanja daring) ke sistem elektronik media digital inilah yang dikategorikan sebagai pengumpulan data pribadi dari pihak ketiga.

Landasan dasar pengumpulan, Untuk setiap jenis pengumpulan data pribadi, subjek data mempunyai hak untuk mengetahui mengapa data pribadi tersebut diproses. Oleh karenanya pengelola media digital sebagai pengendali atau wali data berkewajiban untuk menjelaskan secara detail alasan mengapa & bagaimana pemrosesan data dilakukan dalam pemberitahuan (*notices*), dan mendapatkan persetujuan (*consent*) atau mendasarkannya dari dasar hukum lain yang lebih kuat, misalnya berdasarkan kontrak pemenuhan layanan

(*performance of a contract*), kepatuhan terhadap hukum atau undang-undang tertentu (*compliance with legal obligation*), pemenuhan terhadap kepentingan umum (*public interest*) atau kepentingan pokok subjek data (*vital interest of data subject*). Secara terinci hal ini dijelaskan pada 1. 5. *Landasan Hukum Pemrosesan Data Pribadi dalam Konteks Kerja Jurnalistik dan Perusahaan Media*.

Pengambilan persetujuan (*consent*) harus dilakukan pada titik di mana data pribadi diproses, atau seketika setelah dampak pemrosesan itu terjadi. Dalam proses tersebut, pengendali data harus memberikan penjelasan tentang pilihan yang tersedia, konsekuensi bila subjek data menolak atau menarik persetujuannya, dan bagaimana proses penarikan persetujuan tersebut dilakukan. Proses pengambilan persetujuan ini harus dilakukan pada setiap titik pengambilan atau penggunaan ulang data pribadi.



Praktikum

Anggaplah Anda mendapatkan tugas mendirikan sebuah publikasi media digital yang berfokus pada publikasi hasil perjalanan wisata. Selain mempublikasi informasi dari tim redaksi, juga membuka publikasi pengalaman pengguna, sebagai mitra publikasi. Selain itu, sebagai salah satu model bisnis, perusahaan media ini bermitra dengan biro perjalanan daring menyediakan akomodasi dan transportasi. Coba identifikasi bagaimana pemrosesan data, pada tahap ini adalah tahapan pengumpulan data, dan hal-hal apa yang perlu diatur dalam proses pemberitahuan dan pengambilan persetujuan untuk seluruh pemrosesan data pribadi semua aktor yang terlibat.

Modul 2.2: Penggunaan, Pengungkapan, Retensi dan Penghancuran dalam Pengelolaan Data Pribadi

Deskripsi: Memberikan penjelasan bagaimana pemrosesan data dilakukan dan mengklasifikasikan aktivitasnya dalam siklus data pribadi agar perusahaan media dapat menciptakan kerangka kerja pelindungan data pribadi.

Tujuan: Peserta pelatihan mendapatkan pemahahaman pemrosesan data dalam siklus data pribadi

Durasi: 90 menit

Metodologi: Presentasi & diskusi, dan praktikum identifikasi dan analisis regulasi yang diperlukan dalam proses penggunaan, pengungkapan dan pengelolaan data pribadi.

Pokok Bahasan

Setelah data pribadi dikumpulkan dan disimpan sedemikian rupa sehingga keseluruhan data pribadi siap diproses lebih lanjut. Secara definisi penggunaan data pribadi adalah pemrosesan data untuk tujuan tertentu yang tidak sekedar proses penyimpanan dan penghapusan. Pertanyaan berikutnya adalah bagaimana data pribadi tersebut akan digunakan perusahaan media?

Apapun tujuan pemrosesannya, berdasarkan prinsip praktik penggunaan informasi yang adil (*fair information practices*) dan pengakuan hak individu, setiap tujuan pemrosesan data harus mendapatkan persetujuan subjek data. Implikasinya, semua tujuan pemrosesan harus sudah dijelaskan dalam pemberitahuan (*notices*), bisa dalam bentuk kebijakan privasi (*privacy policy/notice*), sehingga telah mendapatkan persetujuan (*consent*) pada saat data tersebut diperoleh atau dikumpulkan.

Siklus Data Pribadi: Penggunaan (*use*), Mengacu model bisnis dasar di awal, ada beberapa tujuan pemrosesan yang akan kita bahas bagaimana seyogyanya dilakukan dan implikasi legal yang harus diantisipasi. Kelompok tujuan pertama dan sangat mendasar adalah untuk pemantauan kinerja internal media. Termasuk di dalam kelompok ini kinerja individu setiap staf redaksi dan kinerja isu-isu yang dipublikasikan. Tujuan berikutnya akan terkait pemrofilan pengguna dalam bentuk profil sosiodemografi, terkait parameter demografi, ekonomi dan preferensi sosial pengguna. Informasi ini akan membantu perusahaan untuk meningkatkan kinerja publikasi (*traffic & usage*) dan mengembangkan aspek komersial.

Agar mendapatkan hasil analisis kinerja sederhana, seperti impresi setiap artikel yang diproduksi, sistem publikasi perlu mencatat setiap akses yang dilakukan oleh pengguna, Proses ini secara teknis

dinamakan proses *logging*. Analis akan melakukan agregasi dan klasifikasi data berdasarkan parameter tertentu, misalnya judul artikel dan penulis, rata-rata konsumsi artikel setiap kunjungan pengguna, total kunjungan pengguna, waktu setiap kunjungan, dan klasifikasi-klasifikasi lain yang diperlukan.

Sampai di sini, pertanyaannya adalah di mana data pribadi terlibat agar *framework* pelindungan data pribadi dapat diterapkan. Untuk mendapatkan data yang akurat dan granular, proses logging melibatkan penanda pengguna sebagai subjek data, baik penanda yang bersifat acak, untuk platform publikasi tanpa registrasi pengguna, atau penanda yang diambil dari proses registrasi dan autentikasi pengguna. Elemen data pribadi yang terlibat dalam proses analisis ini memandatkan implementasi *framework* pelindungan data pribadi. Aktivitas ini secara khusus penggunaan/pemrosesan informasi yang adil diatur dalam Pasal 27 & 28 UU No. 27/2022, yang mengamanatkan prinsip pemrosesan sesuai tujuan yang disepakati secara terbatas & spesifik yang legal, transparan dan adil.

Kebutuhan implementasi *framework* tersebut perlu mendapat perhatian lebih karena untuk alasan kredibilitas, hasil analisis kinerja media perlu dihasilkan oleh pihak ketiga yang netral. Penyedia layanan analisis web (*web analytic services*), seperti *Google Analytics*, *Adobe Sitecatalyst*, *Chartbeat* atau yang lain, beroperasi di luar yurisdiksi NKRI. Berdasarkan UU PDP Pasal 56 memungkinkan pengendali data melakukan transfer data ke luar negeri dengan syarat negara tujuan telah memiliki regulasi pelindungan data pribadi yang setara. Hal ini sejalan dengan prinsip kesetaraan atau kecukupan (*adequacy*) untuk transfer data lintas batas (*cross border data transfer*) dalam GDPR. Oleh karena penjelasan pemrosesan data ini harus dimasukkan dalam klausul pemberitahuan (*notice*) yang termuat dalam Kebijakan Privasi (*Privacy Policy/Notice*) yang dirujuk pada proses pengambilan persetujuan (*consent*) subjek data.

Dengan proses serupa, data penggunaan media selanjutnya diproses dari sudut pandang pengguna media. Dipadukan dengan data demografi dan data ekonomi yang dikumpulkan, analisis data konsumsi media akan membangun peta pergerakan-pergerakan segmentasi pengguna media yang bersangkutan. Berdasarkan segmentasi inilah, dapat berupa demografi, geografi, psikografi, perilaku (*behavioural*), selanjutnya keputusan bisnis didasarkan. Misalnya, setiap segmen akan mendapatkan penawaran yang berbeda terkait topik artikel setelah mengkonsumsi sebuah artikel dan penawaran produk yang sesuai dengan segmentasi untuk meningkatkan kinerja penawaran bisnis, iklan atau produk komersial lainnya.

Proses penggunaan data di atas termasuk juga proses pake bersama data pribadi terkait dengan segmentasi. Mitra pake bersama paling sederhana adalah untuk tujuan penyediaan periklanan atau penawaran komersial yang paling sesuai dengan profil atau segmen pengguna terkait. Umumnya, dengan tujuan periklanan mitra pake bersamanya adalah *ads network* atau penyedia *demand side platform* (DSP), misalnya Google AdX, AdSense, MGID dan jaringan periklanan lainnya.

Untuk kebutuhan analisis pengguna yang lebih terintegrasi demi mendapatkan sudut pandang pengguna secara menyeluruh atau sudut pandang 360^0, maka data pengguna dikirimkan ke penyedia layanan platform analisis data pelanggan (*customer data platform*). Karena sifat dan ketersediaan layanan analisis dan platform periklanan komersial umumnya bersifat eksternal dan bergerak atar yurisdiksi hukum negara, maka diperlukan langkah antisipasi yang sama dengan pemrosesan untuk statistik kinerja penerbitan di atas.

Siklus Data Pribadi: Pengungkapan (*disclosure*), Pengungkapan data pribadi adalah proses yang membuat dapat diaksesnya data pribadi oleh pihak ketiga, baik individu atau organisasi. Apakah pengendali atau wali data dapat melakukan pemrosesan itu? Jawabannya, bisa dengan syarat, antara lain: prosesnya mendapatkan persetujuan (*consent*) dari subjek data, tujuan pengungkapan data ini adalah penggunaan ulang (*repurposing*) yang sangat relevan dengan tujuan utama pengumpulan data atau, dalam kondisi data pribadi yang bersifat khusus atau sensitif tujuan keduanya terkait langsung dengan tujuan utama pengumpulan data, atau pengungkapan data pribadi ini diperlukan dan diotorisasi oleh pelaksana kekuatan hukum yang berlaku.

Di dalam proses pengungkapan data pribadi, sedapat mungkin menggunakan prinsip minimisasi data, artinya data yang diungkapkan (*disclosed*) seminimum mungkin sejauh mencukupi proses pengungkapan yang dimandatkan. Salah satu contoh pengungkapan data pribadi dalam penggunaan layanan SSO atau *single signed-on*. Prosesnya diberikan setelah subjek data atau pemilik akun SSO memberikan persetujuan (*consent*) atas proses autentikasi SSO, dan data yang dikirimkan oleh penyedia SSO adalah nama pengguna dan nomor penanda (*nomor identifier*).

Kewajiban untuk melakukan langkah pengamanan data pribadi dalam pemrosesan ini diatur Pasal 35 & 36, termasuk menetapkan langkah-langkah teknis dan prosedural untuk memastikan tingkat keamanan yang tinggi dalam pemrosesan data pribadi, antara lain: (1) minimisasi data, (2) anonimasi, (3) pseudonimasi, (4) enkripsi data, (5) memastikan keamanan sistem dan layanan pemrosesan, (6) menjaga kerahasiaan, integritas, dan ketersediaan layanan, (7) ketersediaan layanan pemulihan akses data pribadi, dan langkah-langkah yang diperlukan lainnya untuk memastikan keamanan data pribadi. Secara sederhana pengendali data berkewajiban mengimplementasikan

teknologi yang diperlukan untuk meningkatkan pelindungan data pribadi (*privacy enhancing technology*).

Siklus Data Pribadi: Retensi, Dalam GDPR yang digunakan sebagai salah satu acuan UU No. 27/2022 retensi adalah kunci prinsip pembatasan penyimpanan data pribadi, yang menyatakan bahwa data pribadi tidak boleh disimpan melebihi waktu yang diperlukan untuk pemrosesan data.

"Melebihi waktu yang diperlukan" tidak menunjuk berapa lama waktu, sehingga justifikasi jangka waktu penyimpanan akan bergantung pada jenis pemrosesan data dan industri. Penetapan jangka waktu penyimpanan ini harus berdasarkan justifikasi yang tepat dan terdokumentasi dengan baik. Sebagai contoh data langganan media digital berbayar, informasi terkait langganan pengguna yang bersangkutan disimpan selama masa langganan berlaku atau pengguna menyatakan berhenti berlangganan dan mencabut semua persetujuan penggunaan datanya. Mekanisme yang sama harus diturunkan untuk proses yang dialihkan ke data pemroses pihak ketiga.

Siklus Data Pribadi: Penghancuran (*destruction*), Penghancuran atau pemusnahan catatan data pribadi diatur dalam Pasal 42, 43, 44, dan 45 UU PDP. Pasal-pasal itu mengatur tahapan siklus data pribadi dengan 3 terminologi, yaitu menghentikan pemrosesan data dalam Pasal 42 berdasarkan (1) telah tercapainya masa retensi pengelolaan data pribadi, (2) tujuan pemrosesan data pribadi telah tercapai, (3) permintaan subjek data; menghapus catatan data pribadi berdasarkan (1) data pribadi tidak lagi diperlukan untuk pencapaian tujuan pemrosesan, (2) pencabutan persetujuan (*consent*) pemrosesan data, (3) permintaan dari subjek data pribadi, (4) data pribadi diperoleh atau diproses dengan cara melawan hukum; dan yang terakhir

terminologi pemusnahan data pribadi berdasarkan (1) telah habis masa retensi dan berstatus dimusnahkan dalam jadwal retensi, (2) permintaan subjek data pribadi, (3) tidak terkait penyelesaian proses hukum suatu perkara, dan (4) data pribadi diperoleh atau diproses dengan cara melawan hukum.

Dalam menjalankan ketentuan UU di atas, perusahaan media harus menetapkan mekanisme dan prosedur kapan dan bagaimana proses penghancuran data dilakukan. Termasuk di dalamnya panduan teknis penghancuran dan prosedur standar bagaimana menjalankan prosesnya. Hal ini penting agar menghindari atau mengelola risiko yang mungkin terjadi, yaitu (1) mempertahankan data yang tak diperlukan, (2) mengelola dan mempertahankan data pribadi melampaui jangka waktu yang diijinkan, dan (3) menghancurkan data pribadi secara sebelum waktu retensinya habis (*premature*).

Berikut ini adalah beberapa studi kasus-kasus hukum terkait pemrosesan dalam tahapan siklus data pribadi:

Penggunaan (*use*)	**Pengungkapan (*disclosure*)**
Kasus: Hearst Communication (1/08/2018) oleh Pengadilan Distrik Manhattan AS Hearst didakwa melanggar UU Privasi Michigan, karena dituduh menjual informasi personal pelanggan majalah yang dikelolanya ke perusahaan data analisis dan menawarkan data profil yang diperkuat (*enhanced*) kepada pihak	Kasus: EmblemHealth, Group Health Inc. (6/03/2008) oleh Kejaksaan (DA) New York Kejaksaan (DA) New York berhasil mencapai penyelesaian kasus pengungkapan (*accidental disclosure*) oleh penyedia layanan kesehatan EmblemHealth dan anak

ketiga menggunakan informasi dari perusahaan data analisis tersebut. Data yang dijual mencakup data usia, ras, agama, tingkat penghasilan, donasi, status kesehatan, dan kebiasaan belanja. Hearst menolak dakwaan tetapi setuju untuk membayar denda penyelesaian senilai AS$50 juta untuk menghindari tuntutan lebih jauh. Sumber Reuter: https://www.reuters.com/article/idUSKBN1K234M/	usahanya Group Health Inc. 81.122 Nomor Jaminan Sosial. EmblemHealth setuju membayar denda AS$575.000 dan melakukan rencana perbaikan (*corrective action plan*) karena menampilkan nomor jaminan sosial pada setiap label surat saat mengirim polis asuransi.
Retensi	**Penghancuran (*destruction*)**
Kasus: Social Metric (27/10/2017) oleh Personal Data Protection Commision (PDPC) Singapore Social Metric membuat situs web untuk menjalankan *Social Marketing Campaign* untuk dan atas nama kliennya. Akan tetapi Social Metric gagal untuk menghapus situs web dari internet meskipun masa kegiatan kampanye tersebut sudah habis. Komplain dilayangkan ke PDPC Singapore dengan alasan	Kasus: Dokter Gigi di Indianapolis (2015) oleh Kejaksaan (DA) Indiana AS Seorang mantan dokter gigi yang telah dicabut izinnya didakwa melanggar UU federal dan Negara Bagian tentang Privasi karena membuang 60 kardus catatan medis pasien di tempat sampah di Indianapolis. Mantan dokter

pengungkapan data ilegal (*unauthorized disclosure*). Denda SG$18.000 dan peringatan dilayangkan karena membiarkan data pribadi terekspos di internet tanpa pelindungan URL, dan juga atas kegagalan untuk menghapus data pribadi pelanggan kliennya ketika sudah tidak diperlukan secara legal dan bisnis.	gigi setuju dengan keputusan persetujuan (*consent decree*) dan didenda AS$12.000

Praktikum

Berdasarkan contoh sebelumnya, sebagai perusahaan media yang mencoba memanfaatkan data penggunaan dan data pelanggan berbayar (*subscriber*) & pelanggan tak berbayar untuk mengelola kinerja publikasi dan upaya penemuan model bisnis yang baik baik untuk meningkatkan potensi penerimaan perusahaan dari biaya berlangganan dan iklan dari *ads networks*. Cobalah petakan data pribadi yang diproses dan apa implikasi dari setiap jenis pemrosesan datanya.

Modul 2.3: Kerangka Kerja (*framework*) Pelindungan Data Pribadi

Deskripsi: Pelindungan data pribadi membutuhkan kebijakan yang mengatur bagaimana teknologi diimplementasikan dan bagaimana prosedur pengelolaan dan pemrosesan data di setiap unit kerja perusahaan media.

Tujuan: Peserta pelatihan mendapatkan pemahaman bagaimana mengimplementasikan kerangka kerja (*framework*) pelindungan data pribadi

Durasi: 90 menit

Metodologi: Presentasi, diskusi dan praktikum identifikasi dan analisis regulasi yang diperlukan dalam proses penggunaan, pengungkapan dan pengelolaan data pribadi.

Pokok Bahasan

Dua pendekatan yang biasa digunakan sebagai landasan pengembangan kebijakan dan prosedur pengaturan privasi di dalam organisasi adalah pendekatan *Privacy by Designed* (PbD) dan *Privacy Risk Models and Framework*. PbD adalah pendekatan yang secara proaktif memasukkan dan menggabungkan aspek privasi ke dalam setiap tingkatan operasi secara organik, ketimbang melihatnya sebagai *trade-off* atau menambahkannya ke dalam sebuah sistem, produk, layanan atau proses setelah semuanya dibangun.

Tujuh prinsip PbD memberikan panduan bagaimana mengembangkan sebuah sistem, produk, layanan atau proses yang (1) memasukkan aspek pelindungan privasi secara proaktif dan preventif, (2) menetapkan privasi sebagai setelan standar (*default*), (3) privasi ditanamkan (*embedded*) dalam sistem, (4) berfungsi secara penuh dan memberikan nilai positif dan bukan *trade-off*, (5) terproteksi utuh dalam siklus data pribadi (*end-to-end protection*), (6) setiap prosesnya terimplementasi jelas (*visible*) dan transparan, (7) menghormati privasi pengguna.

Selanjutnya *Privacy Risk Model and Framework* memberikan panduan kerangka bekerja berdasar risiko yang mungkin diterima oleh subjek data akibat privasinya dilanggar. Model risiko privasi mendasarkan pada dua model dasar yaitu model kepatuhan (*compliance model*), yaitu setiap pemrosesan data pribadi harus memenuhi persyaratan dan larangan hukum, dan prinsip penggunaan informasi yang adil (*fair information privacy practice principle or FIPP*) yang telah sebagian disinggung dalam modul sebelumnya tentang pemrosesan data pribadi dalam siklus data pribadi (*privacy information lifecycle*).

<table>
<tr><th colspan="2">Hak-hak Individual (Individual Rights)</th></tr>
<tr><td colspan="2">Pemberitahuan (notice)</td></tr>
<tr><td>Memberitahukan tentang kebijakan dan prosedur pelindungan privasi

Mengidentifikasi tujuan setiap pemrosesan data pribadi (pengumpulan, penggunaan, penyimpanan/retensi, dan pengungkapan)</td><td>Kebijakan Privasi (Privacy Policy): adalah pengumuman atau komunikasi internal terkait kebijakan tentang pelindungan privasi.

Pernyataan Privasi (Privacy Statement/Notice) adalah pengumuman yang dikomunikasikan ke subjek data:
Tersedia sejak awal pemrosesan data pribadi, dan dalam beberapa kasus mengalami pengkinian secara berkala
Jelas dan mudah ditemukan (mencolok)
Akurat dan lengkap
Mudah dibaca dan dipahami pengguna awam</td></tr>
</table>

Pilihan & Persetujuan (*choice & consent*)	
Menjelaskan dan menyediakan pilihan yang bagi individu Mendapatkan persetujuan secara implisit atau eksplisit terkait pemrosesan data pribadi (pengumpulan, penggunaan, retensi dan pengungkapan)	• Pilihan & persetujuan pada titik atau seketika setelah pemrosesan data pribadi berlaku • Konsekuensi penolakan atau penarikan persetujuan • Persetujuan diperlukan untuk setiap pemrosesan data pribadi • Proses penarikan persetujuan
Akses Subjek Data (*data subject access*)	
Menyediakan akses terhadap data pribadi kepada individu untuk melakukan telaah (*review*) dan pengkinian data	• Konfirmasi identitas individu • Memahami format, jangka waktu dan biaya pengelolaan data pribadi • Proses penolakan akses, termasuk alasannya • Pengkinian dan ralat data pribadi • Pernyataan ketidaksetujuan • Eskalasi keluhan dan perselisihan
Pengendalian informasi (*Control of Information*)	
Keamanan Informasi (*information security*)	
Menggunakan tindakan yang	• Penilaian risiko

wajar untuk melindungi informasi pribadi dari akses, penggunaan, pengungkapan, modifikasi, dan penghancuran yang tidak sah	• Program keamanan informasi • Melindungi secara fisik, administratif dan teknis dengan efektif, wajar atau masuk akal, dan memadai
Kualitas Data (*Data Quality*)	
Menjaga akurasi, kelengkapan, dan relevansi data pribadi sesuai dengan tujuan yang ditetapkan dan dinyatakan pada pernyataan kebijakan privasi organisasi	• Akurasi dan kelengkapan • Relevansi dan ketepatan waktu
Siklus Data Pribadi (*privacy information lifecycle*)	
Pengumpulan (*Collection*)	
Menyediakan sarana untuk melakukan pengumpulan data pribadi, baik secara aktif atau pasif Menjelaskan dasar pengumpulan data pribadi, misalnya pemenuhan kewajiban hukum, kontrak kinerja, dll.	• Persetujuan (*consent*) secara eksplisit atau implisit • Pemberitahuan (*notice*) • Metode pengumpulan: langsung (*first party data*), pemantauan (*surveillance*), penggunaan ulang data (*repurposing*), dan data yang bersumber dari pihak ketiga
Penggunaan (*Use*)	
Memberikan penjelasan bagaimana data pribadi akan dimanfaatkan atau diproses di	• Pakai bersama (*sharing*) & pencocokan (*matching*) data pribadi

luar proses penyimpanan dan penghapusan (*deletion*).	• Pemantauan kinerja (*performance monitoring*) • Dan penggunaan turunan lain yang berdasarkan pemrosesan data pribadi
Pengungkapan (*Disclosure*)	
Memberikan penjelasan bagaimana data pribadi dapat diungkapkan/dibuka: kapan, bagaimana, dan atas dasar apa.	• Pemenuhan Undang-undang dan hukum yang berlaku (*law & regulation*) • Diumumkan & diatur dalam oleh Kebijakan/Pernyataan Privasi (*privacy notice*) • Biasanya untuk tujuan penggunaan ulang data pribadi (*repurposing of data*) • Mengikuti prinsip minimasi data (*data minimisation*) • Pengungkapan internal vs eksternal
Retensi (*Retention*)	
Melakukan penyimpanan dan menjaga data pribadi dalam jangka waktu tertentu (retensi) dengan teknologi & standar yang berlaku	• Jangka waktu tertentu sesuai kebutuhan tujuan pemrosesan • Mematuhi aturan hukum dan standar teknologi yang berlaku • Kebijakan & prosedur retensi

Penghancuran (*Destruction*)	
Menetapkan mekanisme dan prosedur bagaimana dan kapan data pribadi yang diproses organisasi dihancurkan	• Menyimpan dan mengelola data pribadi yang tidak diperlukan dalam pemrosesan • Menyimpan data pribadi lewat dari waktu yang diijinkan • Menghancurkan data pribadi terlalu cepat (*premature*)
Pengelolaan dan Administrasi (*management & administration*)	
Mendefinisikan, mendokumentasikan, mengkomunikasikan, dan memberikan pembebanan akuntabilitas pada semua kebijakan dan prosedur privasi	• Tanggung jawab dan akuntabilitas • Kebijakan dan prosedur privasi konsisten dengan hukum dan regulasi • Komitmen yang konsisten dengan kebijakan & prosedur privasi • Menyediakan sumberdaya pendukung • Menyediakan personil dengan kualifikasi yang diperlukan • Mengelola perubahan-perubahan lingkungan bisnis dan aturan yang menaunginya

Prinsip, aspek, dan proses penggunaan data pribadi yang adil selanjutnya akan ditimbang risiko dan nilai-nilai (*values*) yang diturunkan dari berbagai teori/analisis agar meminimalkan risiko

yang diterima subjek data. Beberapa teori dan analisis yang digunakan dalam implementasi pelindungan data pribadi, misalnya *Calo's Harm Dimensions Model* dan *Nissenbaum's Contextual Integrity Model, NIIST Framework,* dan *Value Sensitive Design Model*. Beberapa teori dan model bersifat industri spesifik, maka gunakan teori dan model pendekatan yang sesuai dengan industri di mana implementasi PDP dilakukan.

Sebagai ilustrasi bagaimana pendekatan-pendekatan di atas bermain dalam upaya pelindungan data pribadi, ambil contoh pengembangan formulir pendaftaran (*sign up form*) pengguna sebuah layanan media digital. Analisis dan perencanaan proses pengembangan layanan dengan meletakkan aspek pelindungan data pribadi sebagai aspek utama mengikuti pendekatan *privacy by design* (PbD), *privacy by default*, dan prinsip penggunaan data pribadi yang adil (FIPP), sehingga menghasilkan ringkasan sebagai berikut:

Tujuan (*Goal*)	**Penjelasan**
Formulir pendaftaran bagi pengguna untuk mendapatkan layanan lebih personal Fasilitas autentikasi Halaman pengelolaan data profil	Halaman profil memberikan akses untuk memenuhi hak akses subjek data untuk menelaah dan pengkinian data
Data pribadi yang dikumpulkan	
Nama (teks, maks 40 huruf) Kata kunci: (alfanumerik, *case sensitive*, 10 - 20 huruf)	Mempertimbangkan prinsip minimisasi data untuk mencapai tujuan pemrosesan data dan

Alamat email Data penggunaan	mitigasi aspek risiko kepada subjek data
Pemangku kepentingan (*stakeholders*)	
Pengguna Tim Layanan Pelanggan Tim Komersial/Bisnis Tim Layanan Teknologi Informasi Tim Redaksi Dewan Direksi (*Board of Directors*)	Setiap pemangku kepentingan memiliki kepentingan dan tanggungjawab yang berbeda dalam pemrosesan data pribadi. Dengan mengidentifikasi setiap pihak akan membantu menciptakan kebijakan dan standar alur proses terkait peran dan tanggung jawabnya.
Rencana Pengamanan Teknis (*technical resources*)	
Implementasi TLS (transport layer security) dalam komunikasi melalui protokol https Penyimpan melalui RDBMS MySQL ver 8 dengan implementasi hashing pada field kata kunci (password) dan pembatasan akses berdasarkan tipe pengguna yg digunakan aplikasi Pengelolaan penyimpanan data mengikuti kebijakan rotasi penyimpanan dan logging Menambahkan penanda unik	Didasarkan pada prinsip *Cybersecurity framework*. Secara khusus untuk aplikasi berbasis web, dapat juga mengacu pada *best practice guide* dari OWASP (*The Open Worldwide Application Security Project*)

(unique identifier) untuk menggantikan (pseudonymisation) dalam proses pemrosesan data pribadi selanjutnya Memastikan bahwa pemroses data eksternal memenuhi kebutuhan pengamanan data pribadi saat memproses data penggunaan media (*media usage*)	
Pemberitahuan dan persetujuan (*notice & consent*)	
Membuat Kebijakan Privasi sebagai penjelasan dan komunikasi bagaimana data pribadi akan digunakan Memastikan bahwa pemroses data pribadi eksternal, dalam hal ini penyedia layanan analisa data, memiliki kebijakan privasi yang tidak bertentangan dengan prinsip pelindungan data peribadi Penjelasan langsung dalam formulir registrasi dan pilihan-pilihan yang tersedia, termasuk implikasi pendaftaran dan penolakan pendaftaran pengguna terkait layanan yang diberikan dan pemrosesan data pribadi yang akan melibatkan pemroses eksternal dalam hal ini penyedia layanan analisis data. Kebijakan privasi yang memerlukan persetujuan (*consent*) terkait pengumpulan data pribadi	Berdasarkan prinsip penggunaan data pribadi yang adil (FIPP) terkait pengakuan hak individu.

Kebijakan Privasi dan Standar Prosedur Pengelolaan Data Pribadi	
Menetapkan bagian organisasi yang bertanggungjawab mengelola data pendaftaran, misalnya Tim Layanan Pelanggan, dan menciptakan alur kerja dan otoritasnya dalam rangka pembatasan akses tim pengelola. Aplikasi dan sistem pengelolaan menyiapkan layanan logging untuk mencatat setiap pemrosesan yang terjadi pada setiap titik data pribadi Menciptakan alur kerja dan batasan akses untuk tim lain yang mungkin mengakses data pribadi yang dikelola dan hasil turunannya. Menciptakan alur kerja pengelolaan infrastruktur layanan dan penyimpanan, misalnya proses backup data dan retensinya, rotasi *file log* akses, dan proses lain yang diperlukan oleh tim teknologi	Berdasarkan prinsip penggunaan data pribadi yang adil (FIPP) terkait pengakuan hak individu. Analisis risiko data subjek berdasarkan model *Calo's Harm Dimensions* dan *Nissenbaum's Contextual Integrity*.

Dengan demikian proses pengembangan aplikasi untuk memfasilitasi pemrosesan data pribadi dapat dilakukan dan dapat mengikuti proses yang dikenal sebagai SDLC atau *software development lifecycle*.

Setelah selesai, kemudian Tim Bisnis membutuhkan pemrosesan data pribadi lainnya untuk memenuhi kontrak kerjasama dengan sebuah perusahaan distribusi produk otomotif. Mereka sepakat untuk melaksanakan kampanye penjualan produk otomotif dengan harga diskon yang diawali dengan kegiatan uji kendari produk.

Kegiatan ini menyasar audiens media yang telah terdaftar sebagai pengguna. Implikasi dari kerjasama ini adalah perlu menambahkan pengumpulan data pribadi untuk melengkapi data pribadi yang telah diproses sebelumnya. Setelah melakukan pembicaraan dengan mitra kerjasama, akhirnya disepakati agar mengikuti program uji kendarai dan diskon khusus, pengguna harus memberikan data alamat, pekerjaan, tingkat penghasilan dan surat ijin mengemudi yang dimiliki. Perubahan apakah yang diperlukan untuk melaksanakan kegiatan tersebut dan masih mematuhi prinsip pelindungan data pribadi.

Tujuan (*Goal*)	**Penjelasan**
Formulir pendaftaran program kampanye penjualan dan uji kendarai bagi pengguna setelah melakukan proses autentikasi pengguna.	
Data pribadi tambahan yang dikumpulkan	
Alamat: text Pekerjaan Penghasilan Jenis & Nomor SIM	Mempertimbangkan prinsip minimisasi data untuk mencapai tujuan pemrosesan data dan mitigasi aspek risiko kepada subjek data.

Pemangku kepentingan (*stakeholders*)	
Pengguna **Mitra Kerjasama (pihak ketiga)** Tim Layanan Pelanggan Tim Komersial/Bisnis Tim Layanan Teknologi Informasi Tim Redaksi Dewan Direksi (*Board of Directors*)	Setiap pemangku kepentingan memiliki kepentingan dan tanggungjawab yang berbeda dalam pemrosesan data pribadi. Dengan mengidentifikasi setiap pihak akan membantu menciptakan kebijakan dan standar alur proses terkait peran dan tanggung jawabnya.
Rencana Pengamanan Teknis (*technical resources*)	
Implementasi TLS (*transport layer security*) dalam komunikasi melalui protokol https. Penyimpan melalui RDBMS MySQL ver 8 dengan implementasi *hashing* pada *field* kata kunci (*password*) dan pembatasan akses berdasarkan tipe pengguna yang digunakan aplikasi. Pengelolaan penyimpanan data mengikuti kebijakan rotasi penyimpanan dan *logging*. Menambahkan penanda unik (*unique identifier*) untuk menggantikan (*pseudonymisation*) dalam proses pemrosesan data pribadi selanjutnya. Memastikan bahwa pemroses data	Didasarkan pada prinsip *Cybersecurity framework*. Secara khusus untuk aplikasi berbasis web, dapat juga mengacu pada *best practice guide* dari OWASP (*The Open Worldwide Application Security Project*). **Mitra program sebagai pihak ketiga yang menerima manfaat pengungkapan (*disclosure*) harus memenuhi kebutuhan pengamanan minimum**

eksternal memenuhi kebutuhan pengamanan data pribadi saat memproses data penggunaan media (*media usage*).	**yang cukup (*adequacy*).**
Pemberitahuan dan persetujuan (*notice & consent*)	
Membuat ***Update*** Kebijakan Privasi sebagai penjelasan dan komunikasi bagaimana data pribadi akan digunakan, untuk penambahan data pribadi yang diproses. Memastikan bahwa pemroses data pribadi eksternal, dalam hal ini penyedia layanan analisa data, memiliki kebijakan privasi yang tidak bertentangan dengan prinsip pelindungan data pribadi. Penjelasan langsung dalam formulir registrasi dan pilihan-pilihan yang tersedia, termasuk implikasi pendaftaran, penolakan pendaftaran pengguna terkait layanan yang diberikan dan pemrosesan data pribadi yang akan melibatkan pemroses eksternal dalam hal ini penyedia layanan analisis data. Kebijakan privasi yang memerlukan persetujuan (*consent*) terkait pengumpulan data pribadi. **Mengambil persetujuan (*consent*) khusus terkait pengungkapan (*disclosure*) untuk program dan**	Berdasarkan prinsip penggunaan data pribadi yang adil (FIPP) terkait pengakuan hak individu. **Persetujuan khusus diperlukan karena ada proses pengungkapan (*disclosure*) data ke pihak ketiga.**

pengkayaan data pribadi yang dikelola media.	
Kebijakan Privasi dan Standar Prosedur Pengelolaan Data Pribadi	
Menetapkan bagian organisasi yang bertanggungjawab mengelola data pendaftaran, misalnya Tim Layanan Pelanggan, dan menciptakan alur kerja dan otoritasnya dalam rangka pembatasan akses tim pengelola. Aplikasi dan sistem pengelolaan menyiapkan *layanan logging* untuk mencatat setiap pemrosesan yang terjadi pada setiap titik pribadi. Menciptakan alur kerja dan batasan akses untuk tim lain yang mungkin mengakses data pribadi yang dikelola dan hasil turunannya. Menciptakan alur kerja pengelolaan infrastruktur layanan dan penyimpanan, misalnya proses backup data dan retensinya, rotasi *file log* akses, dan proses lain yang diperlukan oleh tim teknologi. **Menetapkan mekanisme dan prosedur pengungkapan data ke pihak ketiga dalam proses pelaksanaan kegiatan, termasuk pembatasan akses dan jangka waktu retensi data pribadi pengguna.** **Menetapkan prosedur dan mekanisme pemantauan dan**	Berdasarkan prinsip penggunaan data pribadi yang adil (FIPP) terkait pengakuan hak individu. Analisis risiko data subjek berdasarkan model *Calo's Harm Dimensions* dan *Nissenbaum's Contextual Integrity*.

pemeriksaan kepatuhan terhadap persyaratan teknis pemrosesan data pribadi oleh pihak ketiga secara berkala selama masa retensi pemrosesan.	

Praktikum

Lakukan analisis yang sama untuk semua proses pemanfaatan data pribadi di media yang Anda kelola.

Modul 2.4: Analisis Dampak Pengiriman Data Pribadi ke Pihak Ketiga (*Data Transfers Impact Assessment*)

Deskripsi: Modul ini memberikan gambaran bagaimana proses melakukan penilaian dampak transfer data pribadi dalam rangka pemrosesan data pribadi untuk memenuhi landasan hukum pemrosesannya.

Tujuan: Pada sesi ini, peserta akan dibawa untuk melihat proses transfer data pribadi dan melihat secara detail tujuan hal ini dilakukan, persyaratan regulasi dan teknis, jenis data dan mekanisme atau tahapan proses transfer. Dengan mengetahui informasi tersebut, peserta bisa diminta untuk melakukan analisis potensi dampak risiko pada pelindungan data pribadi dan manfaat proses transfer data tersebut untuk mencapai tujuan pemrosesan data pribadi.

Durasi: 45 menit

Metodologi: Presentasi, diskusi dan praktikum untuk memaparkan prinsip dasar tentang pemrosesan dan pelindungan data pribadi dalam proses transfer data.

Pokok Bahasan

2.4.1 Analisis Dampak Transfer Data Pribadi

Tujuan dari penilaian dampak transfer data ke pihak ketiga adalah mengidentifikasi potensi risiko dan manfaat dari inisiatif transfer data pribadi, termasuk bagaimana hal ini dapat mempengaruhi pemangku kepentingan yang berbeda dan sistem manajemen data yang lebih luas dan bagaimana data pribadi akan dilindungi berdasarkan undang-undang pelindungan data di negara penerima.

Berdasarkan GDPR persyaratan atau restriksi transfer data pribadi bertujuan untuk memastikan tingkat pelindungan data pribadi yang setara dengan yang disyaratkan oleh GDPR. Oleh karena penilaian dampak transfer data pribadi menjadi sebuah kewajiban (*mandatory*). Dan prinsip-prinsip ini diadopsi dalam UU PDP untuk memastikan hal yang sama. Ini mensyaratkan bahwa penerima transfer data, baik pengendali atau pemroses data pribadi wajib menerapkan tingkat pelindungan yang setara.

UU PDP Pasal 55 & 56 mengatur hak dan kewajiban pengendali data pribadi dalam proses transfer data. Aturan itu memungkinkan pengendali data pribadi untuk melakukan transfer data ke pengendali atau prosesor data pribadi lain dalam atau di luar yurisdiksi hukum Republik Indonesia. Salah satu syarat melakukan transfer data, pengendali data pribadi wajib melakukan penilaian dampak transfer data pribadi.

Meskipun UU PDP belum mengatur kriteria *Data Transfer Impact Assessment*, tetapi RPP UU PDP saat ini telah mengatur kriteria efektivitas instrumen hukum yang mensyaratkan pengendali data pribadi untuk mempertimbangkan:

- Dasar regulasi yang digunakan;
- Tujuan transfer dan pemrosesan Data Pribadi;
- Pihak yang terlibat dalam pemrosesan Data Pribadi;
- Lingkup sektor transfer Data Pribadi;
- Kategori Data Pribadi yang ditransfer;
- Pilihan mekanisme transfer Data Pribadi yang digunakan;
- Tempat penyimpanan dan akses terhadap Data Pribadi;
- Format Data Pribadi yang akan ditransfer, misalnya dalam teks biasa/disamarkan atau dienkripsi;
- Kemungkinan Data Pribadi dapat ditransfer lebih lanjut dari negara penerima ke negara lainnya;
- Tindakan penilaian terhadap risiko atau dampak terhadap hak-hak Subjek Data Pribadi akibat transfer Data Pribadi;
- Data Pribadi yang ditransfer cukup, relevan, dan terbatas pada yang diperlukan untuk tujuan transfer Data Pribadi; dan
- Langkah prosedural dan evaluasi terhadap pelaksanaan transfer Data Pribadi

Praktikum

Terdapat dua studi kasus yang dapat digunakan untuk melakukan latihan penilaian dampak transfer data pribadi dalam modul-modul sebelumnya, yaitu (1) Pemrosesan data pribadi terkait analisis penggunaan layanan platform publikasi media dengan menggunakan layanan pihak ketiga, dalam hal ini umumnya menggunakan layanan Google Analytics, dan (2) Dalam rangka kerjasama unit usaha lain, pelaksanaan kegiatan dalam rangka pemrosesan data pribadi mengharuskan data pribadi ditransfer ke mitra untuk melaksanakan pemenuhan kewajiban, mitra biro perjalanan (dalam modul 2.2) dan mitra pelaksana uji kendarai atau *test drive* (dalam modul 2.3). Lakukan proses penilaian pada dua kasus ini akan memberikan gambaran bagaimana penilaian dampak transfer data pribadi terhadap risiko pelindungan privasi. Untuk kasus kedua yang

memberikan gambaran transfer data pribadi dalam yurisdiksi hukum Republik Indonesia, pilih salah satu kasus saja.

Modul 2.5: Mitigasi & Manajemen Insiden Keamanan Data Pribadi dan Peran *Data Protection Officer* (DPO)

Deskripsi: Seluruh panduan pendekatan pelindungan data pribadi telah diimplementasikan. Selanjutnya bagaimana melakukan mitigasi dan pengelolaan insiden kebocoran data pribadi pada saat hal itu terjadi. Bagaimana DPO berperan dalam setiap proses operasional pelindungan data pribadi

Tujuan: Peserta pelatihan memahami apa dan bagaimana menyiapkan langkah-langkah ketika terjadi insiden kegagalan pelindungan data pribadi dan memahami fungsi dan tugas DPO

Durasi: 90 menit

Metodologi: Presentasi, diskusi dan praktikum pembuatan rencana pengelolaan insiden.

Pokok Bahasan

Tujuannya implementasi pelindungan data pribadi dalam platform publikasi media digital adalah meminimalkan maksimum resiko yang dihadapi oleh subjek data, dalam hal ini data pribadi pemangku kepentingan perusahaan media dan yang lebih khusus adalah pengguna atau audiens. Meskipun semua tindakan dan upaya maksimal telah diambil berdasarkan kerangka kerja keamanan siber (*cybersecurity framework*), tetapi tidak ada yang bisa menjamin tidak akan terjadi insiden, salah satunya yang paling sering terjadi adalah kebocoran data pribadi (*data breach*).

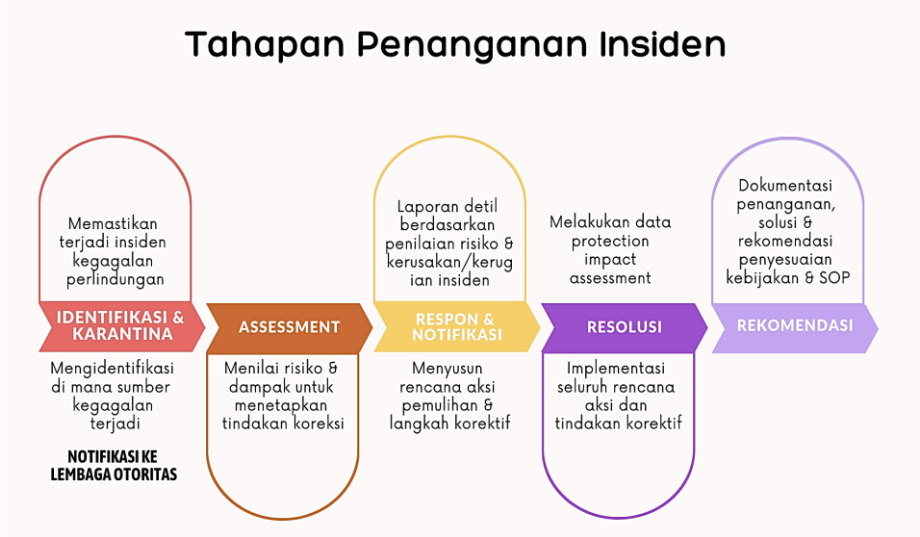
Pasal 46 UU PDP (UU No. 27 Th. 2022 tentang Pelindungan Data Pribadi) menggunakan terminologi kegagalan pelindungan data pribadi, yang didefinisikan sebagai "*kegagalan melindungi Data Pribadi seseorang dalam hal kerahasiaan, integritas, dan ketersediaan Data Pribadi, termasuk pelanggaran keamanan, baik yang disengaja maupun tidak disengaja, yang mengarah pada pengrusakan, kehilangan, perubahan, pengungkapan, atau akses yang tidak sah terhadap Data Pribadi yang dikirim, disimpan, atau diproses*." Dengan demikian kegagalan pelindungan data pribadi dilihat dalam tiga aspek, yaitu kerahasiaan data, yang menyangkut membuat dapat diaksesnya data pribadi secara tidak sah (*unlawful access*); integritas data, yang menyangkut pengubahan dan penghapusan sebagian atau seluruh elemen data pribadi; dan aspek ketersediaan data untuk pemenuhan kontrak layanan subjek data.

Selanjutnya pada ayat berikutnya, Undang-undang mewajibkan pengendali data untuk melaporkan insiden yang terjadi paling lama 3X24 jam sejak insiden kegagalan pelindungan data pribadi terjadi. Pelaporan secara tertulis insiden tersebut ditujukan kepada subjek data dan lembaga sebagai pemegang otoritas pelindungan data pribadi yang ditunjuk. Materi yang harus dilaporkan menyangkut data yang terungkap atau terkait insiden, kapan dan bagaimana insiden terjadi, dan yang ketiga adalah upaya yang telah dan akan dilakukan oleh pengendali data pribadi untuk mengatasi dan memulihkan dampak insiden tersebut. Selain melaporkan kepada pihak terkait insiden, UU PDP juga memerintahkan pengendali data untuk membuat pengumuman terkait insiden kegagalan pelindungan data pribadi, apabila insiden tersebut berdampak pada terganggunya pelayanan publik dan/atau berdampak serius terhadap kepentingan publik.

Langkah-langkah penangan insiden kegagalan pelindungan data pribadi, Menimbang faktor risiko dan konsekuensi insiden yang

terjadi, pengendali data harus bertindak cepat dan menanganinya dengan serius dan menempatkannya pada prioritas tertinggi untuk segera mendapatkan resolusi. Langkah-langkah yang dapat ditempuh untuk merespon insiden kegagalan pelindungan adalah:

1. **Identifikasi & karantina**, Pengendali data pribadi harus memastikan bahwa insiden kegagalan pelindungan data pribadi telah terjadi, dan menemukan titik terjadinya insiden dan data pribadi apa yang terlibat dalam insiden. Masuk pada dalam tahap ini, tindakan yang segera harus diambil oleh pengendali data untuk membatasi & menahan (*contain*) dampak meluasnya insiden. Tindakan ini akan menghentikan dan mengkarantina layanan untuk menahan menjalarnya dampak insiden lebih luas. Pada titik ini pengendali data dapat membuat laporan awal kepada otoritas yang ditunjuk tentang kejadian dan data pribadi yang terdampak insiden.



2. ***Assessment* risiko dan bahaya insiden**, Penilaian risiko dan bahaya ini untuk mendapatkan gambaran tingkat risiko yang dihadapi subjek data, besarnya data yang terlibat dan dampaknya (*magnitude*, *sensitivity* & *volume*). Hasil penilaian risiko dan dampak ini akan menentukan bagaimana proses pemulihan dan perbaikan agar insiden serupa tidak terjadi ke depan.

3. **Respon dan Notifikasi insiden**, Berdasarkan penilaian risiko dan kerusakan (*harm*) yang terjadi dan rencana tindakan (*action plans*) untuk proses pemulihan dan perbaikan, pengendali data sebagaimana diamanatkan oleh UU PDP harus membuat laporan detail insiden, upaya penanganan dan langkah-langkah korektif agar insiden serupa tidak terjadi ke depan.

   Pemberitahuan yang sama seyogyanya dikirimkan kepada subjek data, yang menjelaskan insiden dan kerusakan/kerugian (*harm*) yang terjadi dan risiko yang mungkin akan dihadapi oleh subjek data. Akan tetapi, keputusan untuk mengirimkan notifikasi ke subjek data terdampak bergantung pada besarnya risiko yang muncul. Apabila ada risiko kerugian yang dapat diperkirakan akibat insiden, maka subjek data terdampak harus diberitahu. Notifikasi itu mungkin tidak tepat jika hal itu kemungkinan besar malah menyebabkan lebih banyak kerugian daripada manfaatnya.

4. **Penyelesaian insiden**, Menyelesaikan semua kegiatan & implementasi tindakan korektif, dan memastikan telah dilakukan *data protection impact assessment* (DPIA) oleh pejabat pelindungan data (*data protection officer* atau DPO). Termasuk dalam aktivitas ini mendokumentasikan setiap perubahan yang dilakukan.

5. **Rekomendasi**, Pengalaman kejadian insiden kegagalan pelindungan data pribadi, sekecil apapun insidennya, pasti

memberikan pemahaman baru yang dapat digunakan untuk melakukan perbaikan, baik sistem, prosedur standar dan kebijakan-kebijakan dalam operasi pengelolaan dan pelindungan dalam konteks operasional bisnis perusahaan media. Untuk itu catatan-catatan dan dokumentasi manajemen penanganan insiden harus dijadikan masukan kebijakan operasional dan perlu dilakukan sinkronisasi terhadap semua perkembangan implementasi teknologi, pengelolaan produk dan layanan usaha dan operasional pelindungan data pribadi.

Komponen-komponen dalam penanganan dan manajemen insiden kegagalan pelindungan data pribadi:

(1) Mengetahui dan memahami subjek dan objek yang dilindungi dalam konteks pelindungan data pribadi. Seluruh aktor yang terlibat dalam proses bisnis harus memiliki pengetahuan dasar tentang PDP, data pribadi, subjek data, pemroses data, pengendali data, dan otoritas pelindungan data pribadi. Pengetahuan klasifikasi data pribadi akan memberikan pemahaman tingkat sensitivitas insiden yang terjadi oleh semua pemangku kepentingan.

(2) Pembentukan Tim Pemenangan Insiden. Ini adalah tim *ad hoc* yang bekerja untuk menangani insiden. Di sini peran pejabat pelindungan data pribadi atau DPO sangat penting dalam mengorkestrasi rencana respon insiden, meminimalkan dampak, dan memastikan kepatuhan terhadap regulasi di seluruh proses. DPO akan menjadi ketua tim dalam penanganan insiden.

Anggota tim yang lain akan bergantung pada bagian di mana insiden terjadi. Bila insiden terjadi pada sisi pelayanan pelanggan, maka tim pelayanan pelanggan (*customer care*) akan terlibat. Begitu juga bila insiden terjadi pada bagian penjualan, maka

anggota tim dari sini akan dilibatkan untuk memberikan konteks insiden. Anggota yang lain relatif tetap adalah staf teknologi informasi terutama bidang keamanan informasi (*information/cyber security*) dan pengembang aplikasi, staf bagian komunikasi publik, dan staf bagian legal.

Keseluruhan tim akan melakukan tahapan-tahapan penanganan insiden dan memastikan implementasinya, termasuk menyiapkan bahan-bahan untuk proses komunikasi dan pelaporan, baik secara internal maupun eksternal, ke otoritas pelindungan data pribadi, subjek data, dan publik jika diperlukan.

(3) Penyiapan rencana komunikasi. Ini adalah hal penting, karena insiden membawa dampak risiko dan kerugian bagi subjek data dan tentu saja pada organisasi pengendali data, paling tidak kerusakan terkait nama baik dan reputasi. Seluruh proses komunikasi yang diamanatkan oleh UU PDP harus disiapkan dengan baik, agar meminimalkan risiko dan kerugian, termasuk kerugian reputasi apabila salah dalam menangani komunikasi ke publik.

Pejabat Pelindungan Data (*Data Protection Officer - DPO*), Meskipun telah disinggung sedikit sebelumnya, peran pejabat pelindungan data atau DPO di dalam pengelolaan insiden dan dalam operasional pelindungan data pribadi secara ringkas akan dijelaskan pada bagian ini. Secara deskriptif berikut ini peran dan tanggung jawab DPO dalam operasional pelindungan data pribadi.

(1) **Manajemen insiden kegagalan pelindungan data pribadi**, DPO berperan penting dalam orkestrasi rencana respon insiden. Jika terjadi insiden, DPO memastikan pelanggaran tersebut dikelola secara efektif dan efisien. Hal ini termasuk menjalin hubungan dengan otoritas regulasi terkait, mengelola komunikasi dengan

pihak-pihak yang terkena dampak, dan menerapkan langkah-langkah untuk mencegah pelanggaran di masa depan.

(2) **Memonitor kepatuhan terhadap Undang-undang PDP**, Salah satu tugas utama DPO adalah memantau kepatuhan organisasi terhadap undang-undang dan peraturan pelindungan data pribadi yang berlaku. Hal ini mencakup pengawasan ketat terhadap aktivitas pemrosesan data organisasi, mengidentifikasi potensi ancaman terhadap privasi data, dan mengambil tindakan yang tepat untuk memitigasi risiko.

(3) **Pelatihan dan Pendidikan**, DPO bertanggung jawab untuk mendidik karyawan tentang persyaratan kepatuhan dan prinsip pelindungan data pribadi. Mereka juga harus mengadakan sesi pelatihan untuk meningkatkan pemahaman dan praktik karyawan mengenai pelindungan data pribadi.

(4) **Menangani Permintaan Subjek Data**, Berdasarkan undang-undang PDP, individu mempunyai hak untuk mengakses, memperbaiki, atau menghapus data pribadi mereka. DPO bertanggung jawab untuk menangani permintaan ini secara tepat waktu dan patuh.

(5) **Mempromosikan Budaya Pelindungan Data Pribadi**, DPO harus berusaha untuk menanamkan budaya pelindungan data dalam perusahaan, memastikan semua orang memahami pentingnya melindungi data pribadi.

(6) **Dokumentasi**, DPO pun bertanggung jawab untuk menyimpan catatan komprehensif dari semua aktivitas pemrosesan data yang dilakukan oleh perusahaan, termasuk tujuan pemrosesan dan berbagi-pakai data pribadi dengan pihak ketiga.

(7) **Tetap Mengikuti Perubahan**, Adalah tanggung jawab DPO untuk selalu mengikuti perkembangan perubahan undang-undang dan praktik terbaik terkait pelindungan data.

Peran DPO dapat diisi secara internal dari organisasi atau perusahaan media. Dengan peran sepenting itu dan tanggungjawab besar dalam memastikan pelindungan data pribadi, setidaknya DPO untuk perusahaan digital perlu mempunyai pengetahuan dasar teknologi informasi dan keamanan digital (*cybersecurity*)

Praktikum

Anggaplah Anda mengelola media digital yang salah satu layanannya adalah mengirimkan *newsletter* secara berkala terkait ringkasan isu-isu penting selama hari ini. Karena ada kesalahan atau kecerobohan, alamat pengiriman *newsletter* pelanggan terbagi ke seluruh pelanggan. Hal ini terjadi karena kumpulan alamat *email* tersebut terpasang pada *field* alamat *email* penerima *newsletter*. Akibatnya selain terkirim email berganda, alamat email sebagai bagian data pribadi tersebar ke seluruh pelanggan *newsletter*. Lakukan analisa penanganan insiden ini.

2.6 Daftar Periksa (*checklist*) Dokumentasi Kepatuhan terhadap UU PDP bagi Perusahaan Media Digital

Kualifikasi:

1. Dokumen ini merupakan dokumen yang bersifat panduan, tidak mengikat secara hukum, dan hanya memberikan penjelasan langkah – langkah praktis tata kelola pelindungan data pribadi. Dokumen ini bukan merupakan suatu nasihat hukum sehingga pemanfaatan dan penggunaannya tidak menjadi tanggung jawab penyusun.

2. Dokumen ini disusun berdasarkan analisis terhadap kebutuhan pemenuhan kewajiban pelindungan data pribadi yang dikumpulkan dari lima perusahaan pers anggota AMSI. Pemakaian oleh pihak selain lima perusahaan pers anggota AMSI membutuhkan penyesuaian yang mungkin saja belum terakomodasi dalam dokumen ini.
3. Dokumen ini disusun dengan merujuk peraturan perundang – undangan terkait, praktik industri serta rancangan peraturan perundang – undangan. Mengingat sifat rujukan rancangan peraturan perundang – undangan dapat berubah, maka pengguna dokumen ini perlu untuk memastikan kesesuaian dan keterbaruan informasi yang berlaku dalam dokumen ini.

Petunjuk Penggunaan:

Checklist ini memberikan informasi teknis dan praktis yang dapat diikuti oleh pembacanya dalam menghadirkan tata kelola data pribadi pada organisasinya. *Point of view* checklist ini diambil dari sudut pandang pengendali data pribadi. Meskipun beberapa informasi dalam dokumen ini cukup detil, beberapa informasi teknis dari peraturan perundang - undangan tidak disertakan untuk efisiensi dokumen. Pengguna dokumen ini diminta untuk tetap memastikan kesesuaian informasi dari checklist ini dengan ketentuan peraturan perundang – undangan yang berlaku.

Keluaran dari checklist ini adalah daftar aksi yang perlu dilakukan, dalam bentuk implementasi teknis dan penyediaan aturan internal, kebijakan (policy), atau prosedur standar operasi (SOP), untuk melengkapi persyaratan kepatuhan terhadi UU PDP.

Kolom Status dapat diisi dengan tingkat kepatuhan terhadap UU PDP atas subjek bahasan. Pada subjek-subjek bahasan yang belum memenuhi aturan kepatuhan perlu dibuat rencana aksi pemenuhannya yang akan menjadi keluaran checklist ini.

Checklist:

No.	Kewajiban Pelindungan Data Pribadi	Status
1.	**Memeriksa Keberlakuan UU PDP terhadap Perusahaan Pers**	
2.	**Mengetahui jenis data pribadi yang dikumpulkan oleh Perusahaan Pers** 2.1. Sesuai UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, data pribadi terdiri atas ● Data pribadi bersifat spesifik meliputi, data dan informasi kesehatan, data biometrik, data genetika, catatan kejahatan, data anak, data keuangan pribadi dan/atau data lain sesuai ketentuan peraturan perundang-undangan. ● Data pribadi bersifat umum meliputi, nama lengkap, jenis kelamin, kewarganegaraan, agama, status perkawinan, dan/atau data pribadi yang dikombinasikan untuk mengidentifikasikan seseorang. Selain data pribadi spesifik, maka data pribadi lain dianggap bersifat umum. 2.2. Perbedaan jenis data pribadi yang diproses dapat mengakibatkan timbulnya kewajiban hukum kepada Perusahaan Pers sebagai pengendali data pribadi pada saat melakukan pemrosesan data pribadi, serta penerapan kebijakan manajemen informasi dan langkah pelindungan yang sesuai dengan data pribadi/aset Perusahaan Pers yang ingin dilindungi.	
3.	**Memeriksa asal data pribadi yang dikumpulkan** Data Pribadi dapat dikumpulkan langsung oleh	

	Perusahaan Pers dari individu sebagai subjek data pribadi di berbagai kesempatan, atau Perusahaan Pers menerima data pribadi. Perbedaan asal data pribadi dapat menimbulkan perbedaan posisi dan kewajiban hukum Perusahaan Pers.	
4.	**Memeriksa kategori subjek data pribadi yang dikumpulkan data pribadinya** 4.1. Kategori subjek data pribadi yang diproses data pribadinya oleh Perusahaan Pers meliputi konsumen yang mendaftarkan diri menjadi pelanggan layanan Perusahaan Pers, karyawan yang menandatangani perjanjian kerja, penyedia jasa/barang bagi Perusahaan Pers yang menandatangani perjanjian kerja sama. 4.2. Secara normatif tidak terdapat perbedaan kewajiban, namun secara teknis Perusahaan Pers dapat memilki jalur komunikasi, penanggungjawab pemrosesan data pribadi, serta ketentuan teknis lain yang berbeda tergantung kategori subjek data pribadi.	
5.	**Melakukan Pemetaan Ragam Kegiatan Pemrosesan Data Pribadi yang dilakukan Perusahaan Pers** 5.1. Pemetaan kegiatan pemrosesan data pribadi dilakukan dengan membuat diagram pemrosesan data pribadi sejak pengumpulan data pribadi dilaksanakan serta bentuk kegiatan pemrosesan data pribadi yang dilakukan oleh Perusahaan Pers. 5.2. Pemetaan juga dilakukan dengan memetakan pihak dalam maupun luar perusahaan yang memiliki akses dan terlibat pada kegiatan	

	pemrosesan data pribadi Perusahaan Pers sehingga peran dan tanggung jawab setiap pihak dalam kegiatan pemrosesan data pribadi Perusahaan Pers dapat diketahui. 5.3. Kegiatan ini juga dapat dilengkapi dengan alat, instrumen, perangkat, software dan/atau fitur yang digunakan untuk memproses data pribadi oleh perusahaan. Melalui pemetaan ini, Perusahaan Pers dapat memahami data pribadi yang diproses oleh instrumen pemroses data pribadi, kebijakan penggunaan yang menjadi dasar pemanfaatan instrumen pemroses data pribadi, serta dapat memperkirakan risiko yang dapat terjadi pada saat pemrosesan data pribadi dilakukan.	
6.	**Memeriksa posisi perusahaan dalam kegiatan pemrosesan data pribadi** 6.1. Pemeriksaan posisi dapat dilakukan dengan memahami tugas, peran, dan tanggung jawab perusahaan pers dalam pemrosesan data pribadi. UU PDP mengatur bahwa pengendali data pribadi merupakan pihak yang menentukan tujuan dan melakukan kendali pemrosesan Data Pribadi, sedangkan prosesor data pribadi adalah pihak yang bertindak sendiri-sendiri atau bersama-sama dalam melakukan 6.2. Pemrosesan Data Pribadi atas nama Pengendali Data Pribadi. Perbedaan posisi ini dapat mempengaruhi tanggungjawab hukum Perusahaan Pers dalam pemrosesan data pribadi, 6.3. Pada praktiknya pemeriksaan dapat dilakukan dengan memeriksa perjanjian kerja sama yang menjadi dasar terjadinya kegiatan pemrosesan data pribadi yang dilakukan dengan pihak lain.	

	Dalam hal tidak ada pihak lain yang memiliki kewenangan menentukan tujuan pemrosesan data pribadi, maka perusahaan pers adalah pengendali data pribadi.	
7.	**Menentukan dasar pemrosesan data pribadi yang sesuai untuk digunakan perusahaan** 7.1. UU PDP secara garis besar memberikan pengendali data pribadi pilihan dasar pemrosesan data pribadi baik atas dasar persetujuan, perjanjian, pemenuhan kewajiban hukum, pelindungan kepentingan vital, pelaksanaan tugas kepentingan umum, maupun pelaksanaan kepentingan yang sah, tergantung konteks, kebutuhan, dan kondisi pengendali data pribadi. Setiap penggunaan dasar pemrosesan memiliki persyaratan dan kewajiban yang harus dipenuhi, 7.2. Perusahaan pers, sebagai suatu entitas privat, pada umumnya dapat menggunakan dasar pemrosesan berupa persetujuan, perjanjian, maupun pelaksanaan kepentingan yang sah sebagai dasar pemrosesan data pribadi. Konsekuensi pemilihan dasar hukum tersebut akan terlihat pada dokumen terkait pemrosesan data pribadi yang disiapkan oleh Perusahaan Pers. 7.3. Dalam hal Perusahaan Pers bertindak sebagai prosesor maka dasar pemrosesan data pribadi akan ditentukan oleh pihak yang menjadi Pengendali Data Pribadi.	

8.	**Melakukan *review* dokumen, produk, atau keluaran yang berpotensi mengandung data pribadi** *Review* terhadap dokumen atau produk yang telah dipublikasikan oleh perusahaan pers perlu dilakukan untuk memahami potensi publikasi data pribadi, sebagai bagian pemrosesan data pribadi. Pada umumnya, dokumen atau produk yang mengandung data pribadi meliputi pengumuman kegiatan dengan data pribadi subjek data sebagai narahubung, informasi narahubung suatu pengumuman resmi, dan bentuk keluaran lain.	
9.	**Menunjuk Pejabat Pelindungan Data Pribadi** 9.1. UU PDP mewajibkan pengendali dan prosesor menunjuk pejabat pelindungan data pribadi, dalam hal melakukan pemrosesan data pribadi untuk pelayanan publik, kegiatan inti Pengendali Data Pribadi memiliki sifat, ruang lingkup, dan/ atau tujuan yang memerlukan pemantauan secara teratur dan sistematis atas Data Pribadi dengan skala besar; dan kegiatan inti Pengendali Data Pribadi terdiri dari pemrosesan Data Pribadi dalam skala besar untuk Data Pribadi yang bersifat spesifik dan/ atau Data Pribadi yang berkaitan dengan tindak pidana. 9.2. Mengingat saat ini Perusahaan Pers memproses data konsumen dan karyawan secara sistematis, dan dapat dikualifikasikan sebagai pemrosesan data pribadi dengan skala besar (mengingat hingga kini belum ada kriteria spesifik tentang skala besar), maka Perusahaan Pers wajib untuk menunjuk Pejabat Pelindungan Data Pribadi. 9.3. Pejabat Pelindungan Data Pribadi secara umum bertugas memantau dan memastikan kepatuhan	

	Pengendali dan Prosesor dalam kegiatan pemrosesan data pribadi. Perlu diingat Pejabat Pelindungan Data Pribadi tidak secara langsung melakukan kegiatan pemrosesan data pribadi, namun hanya memastikan kepatuhan pihak, unit atau individu yang terlibat dalam pemrosesan data pribadi pengendali atau prosesor melaksanakan kewajiban sesuai peraturan perundang – undangan. 9.4. UU PDP mensyaratkan Pejabat Pelindungan Data Pribadi untuk ditunjuk berdasarkan profesionalitas, pengetahuan mengenai hukum, praktik Pelindungan Data Pribadi, dan kemampuan untuk memenuhi tugas-tugasnya. Hingga saat dokumen ini selesai disusun, belum terdapat sertifikasi resmi dari lembaga manapun untuk pelatihan pejabat pelindungan data pribadi yang diakui oleh Pemerintah.	
10.	**Menyiapkan Kebijakan Privasi (Privacy Notice) Bagi Subjek Data** 10.1. Secara spesifik, UU PDP memang belum mensyaratkan kewajiban penyiapan kebijakan privasi. Namun kewajiban pemberitahuan pemrosesan data pribadi turut diatur pada PP PSTE yang berlaku kepada seluruh sistem elektronik, termasuk di antaranya para pengendali dan proses data pribadi. Pada praktiknya, pengendali dan prosesor data pribadi juga menginformasikan kegiatan pemrosesan data pribadi yang dilakukannya kepada subjek data pribadi sebagai bentuk transparansi dan akuntabilitas. 10.2. Dokumen Kebijakan Privasi, diwajibkan menggunakan bahasa Indonesia, dan paling	

	sedikit berisi informasi: • Jenis data pribadi, informasi dan relevansi pengumpulan informasi dan data pribadi tersebut, • Tujuan pemrosesan data pribadi, • Dasar hukum pemrosesan data pribadi, • Jangka waktu penyimpanan data pribadi, • Hak subyek data pribadi, • Narahubung yang dapat dihubungi, • Pihak yang terlibat dalam kegiatan pemrosesan data pribadi. • Ketentuan pembaruan Kebijakan Privasi, • Kegiatan pemrosesan data pribadi yang dilakukan, dan • Ketentuan dalam hal terjadi kegagalan pelindungan data pribadi. 10.3. Dokumen ini dapat digunakan untuk memenuhi persyaratan pemrosesan data pribadi konsumen, karyawan, maupun vendor, selama dijelaskan dalam dokumen ini. Selain itu, dokumen ini akan menjadi dasar bagi subjek data pribadi ketika mengajukan upaya hukum atau ganti rugi terkait pemrosesan data pribadi (apabila ada).	
11.	**Menyiapkan Mekanisme Pengumpulan Persetujuan Subjek Data Sebelum Pemrosesan Data Pribadi Dilakukan** 11.1. Sebagai salah satu dasar pemrosesan, persetujuan perlu untuk dikumpulkan oleh Pengendali data pribadi. UU PDP mensyaratkan permintaan persetujuan	

	dilakukan secara opt-in dan eksplisit. Hal ini berarti pengendali data harus mendapatkan persetujuan dari subjek data pribadi secara afirmatif, berdasarkan tindakan atau pernyataan yang secara terang menjelaskan persetujuan subjek data pribadi terhadap pemrosesan data pribadi. 11.2. Pada praktiknya, akan terdapat metode pengumpulan persetujuan data pribadi yang berbeda, tergantung subjek data pribadi yang memberikan persetujuan. Dalam kegiatan pemrosesan data pribadi oleh perusahaan pers, bentuk pengumpulan persetujuan dilakukan sebagai berikut: ● Apabila pengumpulan data pribadi dilakukan terhadap karyawan, maka pengumpulan persetujuan karyawan dapat dilaksanakan pada saat penandatanganan perjanjian kerja, selama perjanjian tersebut menyertakan klausa permintaan persetujuan data pribadi. ● Apabila pengumpulan data pribadi dilakukan terhadap konsumen, maka pengumpulan persetujuan konsumen dapat dilaksanakan dengan menyediakan *check-box* yang menyatakan konsumen menyetujui dilakukan pemrosesan data pribadi. Check-box dapat disediakan pada kesempatan pertama sebelum terjadi pemrosesan data pribadi. Biasanya dilakukan sebelum pengumpulan cookies melalui penyediaan cookies wall, atau sebelum konsumen mendaftar sebagai	

	pengguna/pelanggan suatu layanan. ● Apabila pengumpulan data pribadi dilakukan terhadap vendor, maka pengumpulan persetujuan vendor dapat dilaksanakan pada saat penandatanganan perjanjian kerja, sama, sepanjang perjanjian tersebut menyertakan klausa permintaan persetujuan data pribadi. 11.3. Sebagai bentuk pelaksanaan kewajiban ini secara teknis, pengendali dapat mengalokasikan salah satu database yang dimiliki, dikhususkan untuk menyimpan metadata persetujuan yang direkam secara digital. Paling sedikit, dalam praktiknya, metadata tersebut terdiri dari: *timestamp*, jenis data pribadi yang dikumpulkan/proses, tujuan, *user identifier* (seperti user ID), status *consent*, dan kalimat persetujuan/*consent statement*.	
12.	**Menyusun Kebijakan Internal Pemrosesan Data Pribadi** 12.1. Secara spesifik, UU PDP memang belum mensyaratkan kewajiban penyiapan kebijakan internal pemrosesan data pribadi. Namun kewajiban untuk memiliki kebijakan tata kelola turut diatur pada PP PSTE yang berlaku kepada seluruh sistem elektronik, termasuk di antaranya para pengendali dan proses data pribadi. UU PDP sendiri mensyaratkan pengendali menyusun dan menerapkan langkah teknis operasional untuk melindungi data pribadi dari gangguan pemrosesan. 12.2. Pada praktiknya, pengendali dan prosesor	

	data pribadi menyusun kebijakan internal pemrosesan data pribadi sebagai bagian dari kebijakan pengelolaan informasi dan/atau sistem elektronik dalam perusahaannya. 12.3. Kebijakan Internal Dokumen tersebut meliputi, antara lain, sebagai berikut: ● aspek-aspek privasi dalam kegiatan pemrosesan data pribadi oleh perusahaan pers, baik privacy by design dan privacy by default dalam pengembangan perangkat lunak atau *software development lifecycle;* ● jenis dan ragam data pribadi yang diproses oleh perusahaan pers; ● pembagian tanggung jawab pihak internal dalam pemrosesan data pribadi; ● kewajiban perusahaan pers kepada subjek data pribadi; ● mekanisme penanganan pelaksanaan hak subjek data pribadi; ● ketentuan respon dalam hal terjadi kegagalan pelindungan data pribadi; ● ketentuan pelibatan pihak ketiga dalam pemrosesan data pribadi; ● bentuk kegiatan pemrosesan data pribadi yang dilakukan oleh organisasi; ● jangka waktu penyimpanan data pribadi; ● larangan serta kewajiban individual yang terlibat dalam pemrosesan data pribadi; ● pemrosesan data pribadi yang diterima	

	dari selain subjek data; ● mekanisme pengiriman data pribadi ke pihak lain di dalam dan luar negeri; ● mekanisme ketika organisasi melakukan pemisahan, pengambilalihan, peleburan, penggabungan, dan pembubaran badan hukum; ● mekanisme audit, prosedur pengoperasian, tugas, wewenang, dan kontak pejabat pelindungan data pribadi; ● ketentuan klasifikasi informasi (*information classification policy*) yang mengatur segregasi dan klasifikasi data pribadi yang diproses oleh perusahaan pers yang dapat dicantumkan dalam kebijakan pelindungan data pribadi serta mendefinisikan bagaimana penanganan dan langkah keamanan yang harus diimplementasikan atas bentuk informasi tertentu; ● Ketentuan terkait kriptografi dan enkripsi untuk memastikan keamanan, integritas, dan ketersediaan data pribadi; ● kebijakan terkait keamanan operasional yang mencakup namun tidak terbatas kepada *backup*, *logging and monitoring*, *penetration testing,* keamanan terhadap *malware*, dan *vulnerability management*; ● manajemen keamanan informasi dan insiden keamanan informasi yang mencakup proses dan peran dan tanggung jawab karyawan dalam hal terjadi insiden keamanan; dan	

	• Ketentuan terkait *Business Continuity* dan *Disaster Recovery* yang mencakup keberlangsungan bisnis dalam hal terjadi bencana alam dan/atau kondisi lain serupa.	
13.	**Menyiapkan Data Protection Impact Assessment** 13.1. UU PDP mensyaratkan pengendali untuk melakukan Data Protection Impact Assessment (DPIA) atau penilaian dampak pemrosesan data pribadi yang memiliki risiko tinggi, meliputi pengambilan keputusan secara otomatis yang memiliki akibat hukum atau dampak yang signifikan terhadap Subjek Data Pribadi, pemrosesan atas Data Pribadi yang bersifat spesifik, pemrosesan Data Pribadi dalam skala besar, pemrosesan Data Pribadi untuk kegiatan evaluasi, penskoran, atau pemantauan yang sistematis terhadap Subjek Data Pribadi, pemrosesan Data Pribadi untuk kegiatan pencocokan atau penggabungan sekelompok data, penggunaan teknologi baru dalam pemrosesan Data Pribadi, dan/ atau, pemrosesan Data Pribadi yang membatasi pelaksanaan hak Subjek Data Pribadi. 13.2. UU PDP sendiri belum secara spesifik mengatur kriteria tentang DPIA, namun merujuk pada praktik industri, serta RPP UU PDP, kriteria DPIA sebagai berikut: • deskripsi secara sistematis mengenai kegiatan pemrosesan Data Pribadi dan tujuan pemrosesan Data Pribadi, termasuk kepentingan dari Pengendali Data Pribadi dari pemrosesan ini;	

	• penilaian kebutuhan dan proporsionalitas antara tujuan dan kegiatan pemrosesan Data Pribadi; • penilaian risiko terhadap pelindungan hak Subjek Data Pribadi; dan • langkah yang digunakan Pengendali Data Pribadi untuk melindungi Subjek Data Pribadi dari risiko pemrosesan Data Pribadi.	
14.	**Menyiapkan Data *Transfer Impact Assessment*** 14.1. UU PDP mensyaratkan pengendali data melakukan *data transfer impact assessment* atau penilaian atas setiap kegiatan pengiriman data pribadi ke pihak ketiga (baik di dalam negeri maupun di luar negeri) dalam bentuk penilaian efektifitas instrumen hukum yang digunakan sebagai dasar pengiriman data pribadi. 14.2. UU PDP belum mengatur kriteria Data Transfer Impact Assessment, namun RPP UU PDP saat ini telah mengatur kriteria efektifitas instrumen hukum yang mensyaratkan pengendali data pribadi untuk mempertimbangkan: • Dasar regulasi yang digunakan; • Tujuan transfer dan pemrosesan Data Pribadi; • Pihak yang terlibat dalam pemrosesan Data Pribadi; • Lingkup sektor transfer Data Pribadi; • Kategori Data Pribadi yang ditransfer;	

	• Pilihan mekanisme transfer Data Pribadi yang digunakan; • Tempat penyimpanan dan akses terhadap Data Pribadi; • Format Data Pribadi yang akan ditransfer, misalnya dalam teks biasa/disamarkan atau dienkripsi; • Kemungkinan Data Pribadi dapat ditransfer lebih lanjut dari negara penerima ke negara lainnya; • Tindakan penilaian terhadap risiko atau dampak terhadap hak-hak Subjek Data Pribadi akibat transfer Data Pribadi; • Data Pribadi yang ditransfer cukup, relevan, dan terbatas pada yang diperlukan untuk tujuan transfer Data Pribadi; dan • Langkah prosedural dan evaluasi terhadap pelaksanaan transfer Data Pribadi	
15.	**Menyiapkan *Legitimate Interest Assesment* (jika diperlukan)** 15.1. UU PDP mensyaratkan pengendali data pribadi untuk melakukan analisis kepentingan yang sah dalam hal pengendali data pribadi menggunakan kepentingan yang sah atau legitimate interest sebagai dasar pemrosesan data pribadi. 15.2. UU PDP belum mengatur kriteria *Legitimate Interest Assessment*, namun RPP UU PDP mengatur bahwa pengendali data pribadi dapat menggunakan kepentingan yang sah sebagai	

	dasar pemrosesan data pribadi apabila: ● telah melakukan analisis terhadap keperluan, tujuan, dan keseimbangan antara hak Subjek Data Pribadi dan kepentingan Pengendali Data Pribadi dengan hasil analisis menunjukkan bahwa Pengendali Data Pribadi memiliki kepentingan yang sah untuk melakukan pemrosesan Data Pribadi; dan ● telah melakukan penilaian bahwa pemrosesan yang menggunakan dasar pemrosesan Data Pribadi pemenuhan kepentingan yang sah lainnya tidak merugikan Subjek Data pribadi dengan hasil Pengendali Data Pribadi memiliki dan telah melakukan langkah untuk mengurangi dampak dari pemrosesan Data Pribadi.	
16.	**Menyiapkan Perekaman Kegiatan Pemrosesan Data Pribadi / *Record of Processing Activities* (RoPA)** 16.1. UU PDP mewajibkan pengendali data pribadi untuk melakukan perekaman kegiatan pemrosesan data pribadi/ Record of Processing Activities (RoPA). Perekaman ini memiliki fungsi sebagai bentuk inventarisasi kegiatan pemrosesan data pribadi yang dilakukan oleh Pengendali Data Pribadi. 16.2. Namun UU PDP belum menjelaskan kriteria RoPA. RPP UU PDP saat ini telah mengatur ketentuan RoPA, untuk disimpan dalam bentuk tertulis secara elektronik/non-elektronik dan mengandung informasi sebagai berikut:	

	• nama dan detail kontak Pengendali Data Pribadi, Pengendali Data Pribadi Bersama, dan/atau Prosesor Data Pribadi; • kontak Pejabat Pelindungan Data Pribadi; • sumber pengumpulan dan tujuan pengiriman Data Pribadi; • dasar pemrosesan Data Pribadi; • tujuan pemrosesan Data Pribadi; • jenis Data Pribadi; • kategori Subjek Data Pribadi; • pihak selain Pengendali Data Pribadi yang dapat mengakses Data Pribadi; • pemenuhan hak Subjek Data Pribadi; • pemetaan aliran Data Pribadi; • masa retensi; dan • langkah teknis dan organisasi dalam rangka pengamanan Data Pribadi.	
17.	**Menerapkan Fitur – fitur Keamanan Informasi Pada Perangkat dan/atau Instrumen Teknis yang Memproses Data Pribadi** UU PDP mensyaratkan pengendali data pribadi menyusun dan menerapkan langkah teknis operasional untuk melindungi data pribadi dari gangguan pemrosesan. Pada praktiknya langkah tersebut dapat dilakukan dalam bentuk sebagai berikut: • Melakukan enkripsi dan/atau *data masking* atas data pribadi yang diproses dan dikelola oleh	

	Perusahaan pers ● Mengimplementasikan *multifactor authentication* untuk memastikan bahwa karyawan atau personel bersangkutan yang akan mengakses data pribadi ● Memiliki audit log atau *trail log* atas aktifitas yang dilakukan oleh karyawan atau personel atas data pribadi (seperti: melihat, menghapus, mereplikasi, dan lainnya), yang direviu setidaknya sekali setahun untuk memastikan bahwa akses terhadap data pribadi diberikan kepada karyawan yang relevan ● Mengimplementasikan *user access matrix* untuk memastikan bahwa hanya karyawan-karyawan tertentu dan berkepentingan saja yang dapat mengakses data pribadi, baik akses secara fisik maupun secara digital. ● Melakukan kontrol atas akses terhadap informasi melalui *user management.* ● Memastikan bahwa metode pengiriman data pribadi yang dipilih merupakan metode pengiriman yang aman, seperti API dengan mengimplementasikan langkah-langkah keamanan yang sesuai (contoh: enkripsi saat data *at-rest* dan *in-transit*). ● Menerapkan keamanan informasi pada setiap fase kepegawaian. Hal ini mencakup verifikasi latar belakang calon karyawan, melakukan pelatihan keamanan informasi, adanya proses disiplin dalam hal terjadi kebocoran data, dan ketentuan keamanan informasi setelah karyawan tersebut tidak lagi menjadi bagian dari perusahaan.	

18.	**Pembuatan Perjanjian Kerjasama dengan Pihak Ketiga** 18.1. Dalam hal pengendali data pribadi bekerja sama dengan pihak ketiga dalam pemrosesan data pribadi, pengendali data perlu menyiapkan perjanjian standar untuk pihak ketiga yang memproses data pribadi dengan menyertakan jaminan pelindungan data pribadi terhadap data pribadi yang disediakan oleh organisasi. Pada praktiknya hal ini dapat berupa kerja sama dengan pihak lain sebagai prosesor, kerja sama untuk pengiriman data, kerja sama pengendalian bersama (*Joint Controller*) atau bentuk kerja sama lainnya. 18.2. Jika posisi perusahaan pers sebagai pengendali data pribadi, menggunakan layanan pihak ketiga (misal: Google Cloud, Microsoft Onedrive, dsb), dapat dipahami bahwa sulit untuk melakukan pengubahan ketentuan perjanjian. Dalam hal ini, Pengendali Data Pribadi dapat mengupayakan untuk meminta penyedia layanan memberikan pernyataan yang pada intinya memberikan jaminan keamanan dan kesesuaian praktik pemrosesan data pribadi sesuai ketentuan yang berlaku. 18.3. Perusahaan pers, sebagai pengendali data pribadi, wajib memastikan bahwa pihak ketiga yang melakukan pemrosesan data pribadi atas nama perusahaan pers (jika ada) memiliki level keamanan yang mumpuni untuk menjaga kerahasiaan data pribadi. Hal ini dapat dilakukan dengan melakukan pengawasan atas pihak ketiga tersebut, melalui pelaksanaan dan pemantauan pemenuhan ketentuan perjanjian.	

	18.4. UU PDP hanya mengatur perjanjian dengan prosesor, dimana prosesor wajib mendapatkan persetujuan tertulis dari pengendali data apabila prosesor bermaksud meminta pihak lain melakukan pemrosesan data pribadi (sub-processing). Ketentuan perjanjian lebih detil diatur dalam RPP UU PDP.	
19.	**Pemberitahuan Kegagalan Pelindungan Data Pribadi** 19.1. UU PDP mensyaratkan pengendali data pribadi mengirimkan dokumen notifikasi kegagalan pelindungan data pribadi kepada subjek data pribadi dan lembaga PDP yang berisi informasi: ● Data Pribadi yang terungkap; ● Deskripsi jenis kegagalan Pelindungan Data Pribadi; ● Waktu dan cara Data Pribadi terungkap; ● Dampak kegagalan Pelindungan Data Pribadi terhadap Subjek Data Pribadi; ● Upaya penanganan dan pemulihan atas terungkapnya Data Pribadi oleh Pengendali Data Pribadi; dan ● Informasi narahubung. 19.2. Dalam hal kegagalan Pelindungan Data Pribadi mengganggu pelayanan publik dan/ atau berdampak serius terhadap kepentingan masyarakat, Pengendali Data Pribadi wajib memberitahukan kepada masyarakat mengenai kegagalan Pelindungan Data Pribadi.	

20.	**Menyediakan Kanal Komunikasi Bagi Pengguna** Perusahan Pers perlu menyediakan kanal komunikasi bagi pengguna jika terdapat keluhan atau kebutuhan pengguna melaksanakan hak sebagai subyek data dalam UU PDP. Kanal komunikasi ini perlu untuk dipublikasikan atau diinformasikan kepada pengguna pada saat data pribadi mulai dikumpulkan. Kanal komunikasi dapat berupa alamat surel khusus, kontak pesan singkat, dan/atau mekanisme sejenis yang memungkinkan pengguna memberikan informasi yang dibutuhkan untuk melaksanakan hak dan/atau keluhan.	
21.	**Melakukan Pelatihan Bagi Individual yang Memproses Data Pribadi** Perusahaan Pers perlu memberikan pelatihan tentang hal-hal yang perlu diperhatikan dalam kegiatan pemrosesan data pribadi bagi individual dan/atau pihak-pihak yang memproses data pribadi. Pelatihan perlu dilakukan untuk memberikan informasi terkait kebijakan internal perusahaan dalam pemrosesan data pribadi, dan beberapa kemampuan teknis untuk mengamankan kegiatan pemrosesan data pribadi dari ancaman keamanan siber. Selain itu, Perusahaan Pers sebagai pengendali data perlu memberikan pemahaman bagi karyawan atau personel terkait pentingnya kerahasiaan data pribadi. Pemahaman ini dapat diperkuat dengan pengenaan kewajiban penandatanganan perjanjian kerahasiaan oleh karyawan yang bertanggung jawab pada pemrosesan data pribadi untuk mencegah adanya pengungkapan data pribadi secara tanpa hak.	

22.	**Evaluasi Berkala Pelaksanaan Kebijakan** 22.1. Sebagai bentuk pemantauan efektifitas pelaksanaan kebijakan, Perusahaan Pers sebagai Pengendali Data Pribadi perlu untuk melakukan evaluasi kebijakan yang dilakukan. Hal ini diperlukan guna memastikan kebijakan yang berlaku dapat merespon kebutuhan pemrosesan data pribadi yang dilakukan oleh pengendali data pribadi. 22.2. Selain itu, Pengendali Data Pribadi juga perlu melakukan evaluasi Sistem, Solusi, Fitur, Software, Teknologi dan Instrumen terkait sejenis yang memproses data pribadi secara berkala, baik melalui pelaksanaan *penetration testing* atas sistem secara berkala, atau tes lain yang serupa.	

Didukung oleh:

BAB 3

PELINDUNGAN DATA PRIBADI DALAM JURNALISME

PELINDUNGAN DATA PRIBADI DALAM JURNALISME

3.0. Pengantar

Kebebasan pers memainkan peran penting dalam mendukung kebebasan arus komunikasi di negara demokrasi. Kegiatan jurnalistik yang sentral dalam pers menyediakan informasi yang membantu warga negara untuk berpartisipasi lebih penuh dan bermakna dalam masyarakat. Atas fungsinya melayani kepentingan umum ini, kebebasan pers harus mendapat perlindungan dalam negara demokrasi.

Sebagai *public watchdog,* pers berperan memenuhi hak publik atas informasi dan melakukan pengawasan, kritik, koreksi, dan saran terhadap hal-hal yang berkaitan dengan kepentingan umum.[4] Namun, jaminan atas hak atas kebebasan berekspresi, dan di dalamnya termasuk hak atas informasi, harus diimbangi perlindungan hak-hak lainnya, termasuk hak atas privasi. Dalam konteks jurnalisme, kegiatan jurnalistik harus dapat melindungi hak subjek peliputan dan informan/narasumber atas privasi. Secara prinsip dan dalam praktiknya, pelindungan atas privasi dalam konteks jurnalisme disesuaikan dengan ekspektasi subjek peliputan dan informan/narasumber atas privasi dengan memerhatikan *posisi mereka dalam masyarakat* dan *pengaruh atau dampak pengungkapan informasi berisi data pribadi* mereka terhadap kepentingan publik.

Tanggung jawab hukum berdasarkan UU PDP diemban oleh media tempat jurnalis bekerja, bukan masing-masing karyawan, meskipun jurnalis lepas kemungkinan besar juga memiliki kewajibannya sendiri. Jurnalis adalah

[4] Pasal 6 UU No. 40/1999 tentang Pers

pelaksana pemrosesan data pribadi yang menerima penugasan dan persetujuan dari media tempatnya bekerja, sehingga ia merupakan bagian dari pengendali data pribadi. Namun, jurnalis harus menyadari bahwa mereka dapat dinyatakan bersalah melakukan tindak pidana jika mereka memproses informasi secara "melawan hukum".

Dalam melakukan pemrosesan data pribadi, jurnalis sebagai agen dari pengendali data pribadi harus menerapkan prinsip-prinsip pelindungan data pribadi. Modul ini akan mengupas implikasi pengaturan pelindungan data pribadi dalam Undang-Undang No. 27/2022 tentang Pelindungan Data Pribadi (UU PDP) pada kegiatan jurnalistik, dan dengan demikian peran dan tugas jurnalis dalam pelindungan data pribadi.

Modul 3.1. Peran Jurnalisme dalam Memenuhi Kepentingan Umum dan Pelindungan Data Pribadi

Deskripsi:

Pelindungan data pribadi sebagai bentuk pelindungan atas privasi seringkali berbenturan dengan kebebasan berekspresi, dan dengan demikian, pemenuhan hak atas informasi dan kebebasan pers. Bagian ini membahas persinggungan antara hak dan kebebasan tersebut, serta peran jurnalisme yang bertanggung jawab di dalam menyeimbangkan pelindungan terhadap privasi dan pemenuhan hak publik atas informasi di dalam negara demokrasi.

Secara khusus, perbedaan pengaturan pelindungan data pribadi dan implikasinya pada kegiatan jurnalistik di dalam General Data Protection Regulation (GDPR) milik Uni Eropa akan dibahas, demikian pula pengaturan yang relevan dalam Undang-Undang No. 40/1999 tentang Pers (UU Pers), Undang-Undang No. 32/2002 tentang Penyiaran (UU Penyiaran), Undang-Undang No. 14/2008 tentang Keterbukaan Informasi Publik (UU KIP), serta Kode Etik Jurnalistik.

Tujuan:

- Peserta memahami tegangan kepentingan antara pelindungan data pribadi dengan kebebasan pers
- Peserta memahami titik-titik kritis dalam penerapan UU PDP yang terkait dengan kebebasan pers
- Peserta memahami perbedaan UU PDP dengan EU GDPR dalam memberikan perlindungan atas kebebasan pers, terutama terkait pengecualian kegiatan jurnalistik dari kewajiban-kewajiban pelindungan data pribadi

Metode: paparan, diskusi/tanya-jawab

Durasi: 90 menit

Pokok Bahasan

3.1.1. Hak dan Tanggung Jawab Pers terkait Hak Atas Privasi dan Kebebasan Berekspresi

Hak atas kebebasan berekspresi adalah hak yang dijamin bagi setiap orang. Hak ini mencakup kebebasan untuk mencari, menerima, dan menyampaikan segala jenis informasi dan gagasan. Hak ini merupakan elemen penting dari masyarakat demokratis dan merupakan syarat mendasar bagi masyarakat tersebut mencapai kemajuan dan untuk pemenuhan diri masing-masing individu. Selain informasi dan ide-ide yang diterima dengan baik atau dianggap tidak menyinggung, hak atas kebebasan berekspresi juga mencakup informasi yang dapat menyinggung perasaan dan bahkan mengganggu. Pluralisme media merupakan aspek penting dari hak atas kebebasan berekspresi.

Dalam melaksanakan kegiatan jurnalistik yang bertujuan menyediakan informasi bagi publik, pers menjalankan fungsi sebagai media informasi, pendidikan, hiburan, dan kontrol sosial yang penting dalam masyarakat demokratis. Pers bertugas menyebarkan informasi

mengenai segala hal yang menyangkut kepentingan umum, dan masyarakat memiliki hak untuk mendapatkan informasi tersebut.

Meski demikian, hak kebebasan berekspresi seorang jurnalis tidaklah mutlak. Jurnalis mempunyai hak dan tanggung jawab. Dalam hal ini, istilah "hak" diartikan sebagai hak prerogatif jurnalis untuk menjalankan profesinya dan melaporkan hal-hal yang bersifat publik kepentingannya, sedangkan istilah "tanggung jawab" berarti bahwa mereka harus menjalankan tugasnya dengan itikad baik dalam pengumpulan dan penyebaran informasi, serta memastikan pelaporan yang berimbang, berdasarkan kode etik jurnalistik.[5]

Jurnalis bertanggung jawab memberikan informasi yang akurat dan dapat diandalkan, memverifikasi fakta sebelum mempublikasikannya, dan memiliki landasan yang faktual dalam menulis opini sebagai bentuk kebebasan berekspresi. Dalam keadaan khusus, jurnalis dapat tidak memverifikasi pernyataan faktual. Misalnya, ketika jurnalis memberitakan isi laporan resmi atau informasi dari catatan pemerintah atau publik, mereka tidak diharuskan melakukan penelitian independen tambahan untuk memverifikasi fakta-fakta tersebut.

Dalam memastikan pelaporannya seimbang, jurnalis perlu mengupayakan untuk menghubungi subjek laporannya untuk meminta komentar sebelum publikasi. Jurnalis yang mempraktikkan jurnalisme bertanggung jawab menikmati perlindungan yang lebih kuat atas hak-hak mereka terhadap kebebasan berekspresi.

[5] UU Pers Bagian Penjelasan atas Pasal 4 ayat (1) menyebutkan bahwa "Kemerdekaan pers adalah kemerdekaan yang disertai kesadaran akan pentingnya penegakan supremasi hukum yang dilaksanakan oleh pengadilan, dan tanggung jawab profesi yang dijabarkan dalam Kode etik Jurnalistik serta sesuai dengan hati nurani insan pers."

3.1.2. Pelaksanaan Tugas Pers dalam Melindungi Hak atas Privasi dan Kebebasan Berekspresi

Pelaksanaan pelindungan hak atas kebebasan berekspresi dan hak atas privasi dapat saling bertabrakan. Di satu sisi, peliputan pers sering melibatkan pemrosesan data pribadi atas individu yang merupakan tokoh masyarakat, yaitu orang-orang yang memegang jabatan publik dan/atau menggunakan sumber daya publik. Di sisi lain, peliputan pers mengenai isu-isu yang menyangkut kepentingan publik, dapat berisiko pada privasi kelompok rentan yang menjadi subjek liputan, karena kemampuan media menyebarkan informasi dalam skala luas.

Sejalan dengan kepentingan umum yang menjadi landasan utama kerja-kerja jurnalistik dan mempertimbangkan risiko pelanggaran hak atas privasi yang ditimbulkan oleh pemrosesan data pribadi, pemrosesan data pribadi untuk peliputan media harus didasarkan pada pertimbangan bahwa manfaat untuk kepentingan umum yang dicapai dari publikasi liputan yang memuat data pribadi tersebut lebih besar daripada risiko terhadap pelanggaran privasi yang ditimbulkannya. Sejalan dengan hal ini, jurnalis dapat mempublikasikan ulang informasi pribadi yang telah dibuat publik oleh yang bersangkutan. Jurnalis juga dapat mempublikasikan ulang informasi dan foto individu yang pada awalnya diterbitkan atas persetujuan mereka, sepanjang informasi tersebut dipublikasikan untuk kepentingan umum yang sah.

Secara prinsip, data dan informasi pribadi tidak dapat dipublikasikan tanpa persetujuan dari Subjek Data Pribadi. Informasi tentang individu dapat dipublikasikan tanpa persetujuan jika terdapat kepentingan publik yang lebih penting, misalnya jika pengungkapan informasi dapat dibenarkan oleh kepentingan atau kepentingan umum. Dengan demikian, konsep kepentingan umum dapat menjadi landasan untuk pemberitaan yang mengandung data atau informasi pribadi.

Para jurnalis juga harus mengutamakan transparansi dengan menjelaskan tujuan penggunaan data kepada individu dan menghormati hak mereka untuk menarik persetujuan kapan saja. Selain itu, menjaga keamanan data yang terkumpul, melindungi identitas individu dalam pelaporan yang sensitif, dan memastikan pemahaman akan prinsip-prinsip pelindungan data pribadi adalah aspek penting dari jurnalisme yang bertanggung jawab dan etis.

Dalam konteks Indonesia, hal ini pada dasarnya telah menjadi bagian integral dari pelaksanaan UU Pers. Dewan Pers sebagai lembaga pelaksana UU Pers telah menyusun Kode Etik Jurnalistik yang disebut Kode Etik Wartawan Indonesia (KEWI). Terdapat 11 pasal dalam KEWI yang menyatakan bahwa wartawan Indonesia menempuh cara-cara profesional dalam melaksanakan tugas jurnalistik, salah satunya adalah "menghormati hak privasi" (Pasal 2 huruf b). Kemudian pada Pasal 9 tertulis bahwa "Wartawan Indonesia menghormati hak narasumber tentang kehidupan pribadinya, kecuali untuk kepentingan publik." Tersurat bahwa jurnalis dalam melakukan liputan harus memperhatikan hak privasi narasumber dan hanya membuat pemberitaan yang memuat informasi pribadi jika ada kepentingan publik atas publikasi berita tersebut.

Berbekal pada Kode Etik Jurnalistik sebagai pelaksanaan UU Pers, pada dasarnya selama ini telah dilakukan pula upaya untuk menilai proporsionalitas antara privasi dan kepentingan publik atas informasi yang diberitakan. Artinya, apabila informasi terkait privasi dinilai menyangkut kepentingan publik, maka pers dibenarkan mengungkapkannya berdasarkan UU Pers dan Kode Etik Jurnalistik. Dengan adanya UU PDP, jurnalis juga harus memahami ketentuan terkait dengan pemrosesan data pribadi, terutama berkenaan dengan prinsip-prinsip pelindungan data pribadi, hak subjek data, dan kewajiban pengendali data.

3.1.3. Kepastian Hukum untuk Kebebasan Pers dalam UU PDP

Dalam konteks persinggungan antara kebebasan pers dan pelindungan atas privasi, EU GDPR menunjukkan praktik baik dengan memberikan pengecualian bagi kerja-kerja jurnalistik dari kewajiban pemenuhan hak-hak Subjek Data Pribadi (Pasal 85 ayat 1 dan 2 EU GDPR) sebagai upaya menyeimbangan perlindungan bagi kebebasan berekspresi dan hak atas informasi dengan pelindungan data pribadi. Titik penyeimbangan ini memberi ruang yang cukup bagi jurnalis untuk melakukan kerja-kerjanya, sementara pelindungan data pribadi tetap diupayakan selama tidak bertentangan dengan kepentingan umum. Sementara itu, dalam UU PDP, tidak ada pasal pengecualian bagi pers/jurnalistik.

Selain itu, EU GDPR tidak mengatur catatan kejahatan dan data keuangan pribadi sebagai data pribadi khusus. Sementara Pasal 4 ayat (2) huruf d dan f pada UU PDP mengatur kedua jenis data tersebut sebagai data pribadi spesifik tanpa pengecualian terkait pemrosesan data untuk kepentingan publik, misalnya terkait pejabat publik atau tokoh publik lainnya. Jurnalis yang melakukan pemberitaan yang memuat kedua jenis data tersebut berpotensi dikriminalisasi.

Sementara itu, Pasal 18 ayat (2) huruf b UU KIP menyebutkan bahwa informasi yang terkait dengan "posisi seseorang dalam jabatan-jabatan publik" adalah informasi publik yang tidak dikecualikan dari pembukaan akses terhadap informasi publik. Dengan demikian, menurut UU KIP, data pribadi tokoh publik, termasuk riwayat anggota keluarga, riwayat kesehatan, Pendidikan, catatan kejahatan, hingga data keuangan pribadi, adalah informasi publik yang aksesnya dapat dibuka saat ada permohonan informasi publik.

Perbedaan lain antara UU PDP dengan EU GDPR adalah pengaturan mengenai sanksi atas pelanggaran. Pengaturan mengenai perbuatan yang dilarang (Pasal 65) serta ketentuan pidana (Pasal 67) dalam UU PDP berimplikasi pada pengenaan sanksi pidana atas kegiatan jurnalistik yang melibatkan pemrosesan data pribadi yang dianggap

"melawan hukum". Di samping sanksi pidana, pelanggaran terhadap pemenuhan tanggung jawab media sebagai pengendali data pribadi dapat dikenakan sanksi administratif (Pasal 57) dan pidana tambahan berupa "perampasan keuntungan dan/atau harta kekayaan yang diperoleh atau hasil dari tindak pidana dan pembayaran ganti kerugian" (Pasal 69). Sementara itu, EU GDPR hanya mengenakan sanksi administratif terhadap pelanggaran.

Selain UU PDP yang tidak memberi pengecualian pada kerja jurnalistik, ancaman lain berasal dari Undang-Undang tentang Informasi dan Transaksi Elektronik[6]. Pasal 26 ayat (1) dan (2) UU ITE memberi dasar bahwa penggunaan data pribadi harus dengan persetujuan subjek data. Lalu, Pasal 26 ayat (3) sampai (5) memberi dasar hukum untuk hak untuk dihapus (*right to erasure*). Seseorang lewat keputusan pengadilan dapat meminta datanya dihapus dari situs atau aplikasi. Jika sebuah berita dapat diturunkan atas permintaan seseorang yang datanya tercantum dalam berita, hal ini dapat menghambat pelaksanaan kebebasan pers.

Tanpa adanya harmonisasi antara UU PDP dengan UU Pers, UU Penyiaran, UU KIP, dan peraturan perundang-undangan lainnya yang terkait, terdapat ketidakpastian hukum terkait perlindungan atas kegiatan jurnalisme publik. Hal ini dapat menimbulkan hambatan atau ancaman bagi jurnalisme publik.

UU PDP	Topik
Pasal 4 Ayat (2) huruf d	Data Pribadi spesifik: catatan kejahatan
Pasal 4 Ayat (2) huruf f	Data Pribadi spesifik: data keuangan pribadi

[6] Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengalami perubahan pertama melalui UU No. 19 Tahun 2016 dan perubahan kedua (terakhir) melalui UU No. 1 Tahun 2024.

Pasal 15 Ayat (1)	Pengecualian pemenuhan hak-hak subjek data
Pasal 57 Ayat (2) huruf d	Denda administratif
Pasal 57 Ayat (3)	Denda administratif
Pasal 65 Ayat (2)	Larangan: pengungkapan data pribadi secara melawan hukum
Pasal 67 Ayat (2)	Sanksi pidana: pengungkapan data pribadi secara melawan hukum
Pasal 69	Sanksi pidana tambahan
Pasal 70	Sanksi pidana untuk korporasi

Tabel 1. Beberapa pasal dalam UU PDP yang berpotensi membatasi kebebasan pers

Adapun tren restriksi terhadap kebebasan pers dan kebebasan sipil secara umum melalui regulasi dan kebijakan terkait data dan tata kelola digital terjadi di berbagai belahan dunia, termasuk Asia. Pada Agustus 2023, di Filipina, jurnalis radio Jose Rizal Pajares ditahan oleh polisi kota Iriga yang menyatakan bahwa tindakan memindai tulisan polisi untuk mencari berita merupakan pelanggaran terhadap Undang-Undang Privasi Data Filipina. Di Korea Selatan, Mahkamah Agung memutuskan bahwa memberikan informasi pribadi, seperti materi dari CCTV, kepada badan investigasi dalam rangka pengajuan gugatan merupakan pelanggaran Undang-Undang Pelindungan Informasi Pribadi negara tersebut. Tren ini menunjukkan bahwa regulasi pelindungan data pribadi yang tidak dibuat dengan

memberikan keseimbangan perlindungan bagi kebebasan berekspresi dan hak atas privasi rentan digunakan untuk membungkam kebebasan sipil.

3.1.4. Potensi Sengketa Hukum

Karena pengaturan mengenai pelindungan data pribadi dalam konteks jurnalisme menyangkut beberapa peraturan perundang-undangan secara sekaligus, terdapat beberapa potensi sengketa hukum yang ditimbulkan dari persinggungan antara pelindungan data pribadi dengan kebebasan pers, dan dengan keterbukaan informasi publik.

Pertama, sengketa pers, terkait dengan apakah suatu kerja jurnalistik sudah sesuai atau melanggar Kode Etik Jurnalistik. Pada sengketa pers, Dewan Pers memiliki wewenang untuk melakukan mediasi.

Kedua, sengketa informasi publik. Hal ini terkait apakah sebuah informasi bersifat publik atau dikecualikan. Wewenang memutuskan hal ini ada pada Komisi Informasi Pusat.

Ketiga, sengketa data pribadi. Sengketa ini terkait dengan pemenuhan tanggung jawab pengendali dan pemroses data pribadi sesuai UU PDP. Sengketa ini menjadi wewenang lembaga pelindungan data pribadi yang dibentuk dalam tahun 2024.

Bahan diskusi:

1. Apa konsekuensi UU PDP bagi jurnalis lepas?
2. Identifikasi ketidakharmonisan antara UU PDP, UU KIP, dan UU Pers dan konsekuensinya bagi jurnalisme.
3. Identifikasi langkah-langkah yang diperlukan untuk menginstitusionalisasi pelindungan data pribadi di lingkungan pers.
4. Apa saja contoh kasus hukum yang mencerminkan persinggungan antara pelindungan data pribadi dan kebebasan pers di Indonesia?

5. Apa peran Dewan Pers dalam mendukung implementasi UU PDP dan di lingkungan pers dan dalam sengketa pelindungan data pribadi terkait aktivitas pers?

Bacaan lebih lanjut:

- Data protection and journalism: a guide for the media https://ico.org.uk/for-the-public/data-protection-and-journalism/
- Standar Norma dan Pengaturan Hak atas Kebebasan Berpendapat dan Berekspresi: https://www.komnasham.go.id/files/1604630519snp-kebebasan-berekspresi-dan--$SF7YZ0Z.pdf
- Personal data protection laws across the *Asia-Pacific* are now regularly misused in aid of tyranny: https://www.apc.org/en/news/personal-data-protection-laws-across-asia-pacific-are-now-regularly-misused-aid-tyranny

Modul 3.2. Pelindungan Data Pribadi dalam Pemrosesan Data untuk Kegiatan Jurnalistik

Deskripsi:

Kegiatan jurnalistik sebagai kegiatan yang mencakup pencarian, pengolahan, dan penyebarluasan informasi kepada publik melalui media massa adalah kegiatan yang hampir selalu melibatkan pemrosesan data pribadi. Meskipun tanggung jawab kegiatan jurnalistik untuk memastikan perlindungan privasi telah diatur di dalam UU Pers, UU Penyiaran, Kode Etik Jurnalistik, dan Pedoman Perilaku Penyiaran (P3), UU PDP mengatur tanggung jawab hukum tersebut secara lebih detail, secara khusus melalui pelindungan data pribadi di sepanjang pemrosesannya.

Bagian ini akan membahas aplikasi prinsip-prinsip pelindungan data pribadi dan tanggung jawab pelindungan data pribadi di sepanjang pemrosesan data pribadi. Meskipun tanggung jawab pelindungan data pribadi sebagian besar diemban oleh media tempat jurnalis bekerja, jurnalis perlu secara proaktif menerapkan prinsip-prinsip pelindungan data pribadi dalam kegiatan jurnalistik yang ia lakukan.

Tujuan:

- Peserta memahami relevansi dan aplikasi prinsip-prinsip pelindungan data pribadi dalam kegiatan jurnalistik
- Peserta memahami bentuk-bentuk pelanggaran pelindungan data pribadi
- Peserta memahami keterkaitan tanggung jawab antara jurnalis sebagai pelaksana pengendalian data pribadi dengan media tempatnya bekerja sebagai pengendali data pribadi

Metode: paparan, tanya-jawab, diskusi kelompok

Durasi: 180 menit

Pokok bahasan

3.2.1. Penerapan Prinsip-prinsip Pelindungan Data Pribadi

Sebagaimana diatur dalam Pasal 16 ayat (2), huruf a-h UU PDP, pemrosesan data pribadi dilakukan sesuai dengan prinsip-prinsip umum. Pemrosesan data pribadi harus sah secara hukum; dilakukan untuk tujuan yang spesifik; dilakukan dengan meminimisasi data yang diproses; dan harus menjamin akurasi, keutuhan, integritas, dan kerahasiaan data. Penyimpanan data pribadi harus dilakukan dalam batasan waktu tertentu. Selain itu, pemrosesan data pribadi harus dilakukan secara bertanggung jawab dan dapat dibuktikan secara

jelas. Aplikasi prinsip-prinsip di atas dalam kegiatan jurnalistik dapat dilihat pada Tabel 2.

Prinsip pelindungan data pribadi	Aplikasi dalam kegiatan jurnalistik
Keabsahan, keadilan dan transparansi	Jurnalis perlu memahami landasan hukum pemerolehan dan pengumpulan data pribadi yang dilakukannya[7]. Meskipun UU PDP tidak mengatur secara jelas mengenai landasan hukum pemrosesan data pribadi untuk kegiatan jurnalisme, landasan hukum berikut relevan digunakan: 1. persetujuan dari Subjek Data Pribadi 2. pelaksanaan tugas dalam rangka kepentingan umum 3. pemenuhan kepentingan yang sah lainnya dengan memperhatikan hak-hak Subjek Data Pribadi Dalam hal pemrosesan data pribadi spesifik, jurnalis perlu memastikan bahwa intrusi terhadap privasi Subjek Data Pribadi dapat dijustifikasi atas dasar melayani kepentingan umum.
Pembatasan tujuan	Jurnalis harus memastikan bahwa data pribadi yang dikumpulkan dan diprosesnya untuk suatu kegiatan jurnalistik tidak digunakan untuk kegiatan lainnya.
Minimalisasi data	Jurnalis harus memastikan bahwa ia tidak mengumpulkan dan memproses data

[7] Pasal 20 ayat (1) UU PDP mengatur bahwa "Pengendali Data Pribadi wajib memiliki dasar pemrosesan Data Pribadi" di mana ayat (2) menjabarkan 6 (enam) dasar hal tersebut.

	pribadi yang tidak diperlukan dan tidak relevan untuk kepentingan kegiatan jurnalistik yang dilakukannya.
Akurasi dan kelengkapan data	Jurnalis harus memastikan bahwa data pribadi yang dikumpulkan dan diprosesnya menjadi liputan jurnalistik akurat. Dengan demikian, jurnalis harus mengambil langkah-langkah wajar dalam memverifikasi data yang diperoleh atau dikumpulkannya. Dalam konteks data pribadi yang diperoleh tidak utuh dan hal ini memengaruhi publikasi, jurnalis harus mengartikulasikan hal ini.
Batasan penyimpanan	Jurnalis harus memastikan bahwa data pribadi yang diperoleh atau dikumpulkannya hanya disimpan selama jangka waktu yang dibutuhkan untuk mencapai tujuan pemrosesan data pribadi tersebut untuk kepentingan kegiatan jurnalistik. Dalam hal jurnalis dapat menjustifikasi penyimpanan data pribadi untuk durasi yang lebih lama dari suatu peliputan yang spesifik, jurnalis perlu mempertimbangkan langkah-langkah untuk meningkatkan kerahasiaan dan keamanan data pribadi yang disimpan, termasuk dengan menerapkan pseudonimisasi.
Integritas dan kerahasiaan	Jurnalis harus memastikan bahwa data pribadi yang diproses dan disimpannya terlindungi dari pengaksesan, pengubahan, penggunaan, pengungkapan, perusakan,

	dan/atau penghilangan oleh pihak-pihak yang tidak memiliki otorisasi maupun secara tidak sengaja. Dengan demikian, jurnalis perlu mengambil langkah-langkah wajar dalam mengamankan data pribadi yang diprosesnya, terutama yang disimpan di dalam gawai yang dikelolanya dan dalam keadaan dengan risiko keamanan yang tinggi.
Transparansi dan akuntabilitas	Jurnalis harus dapat menunjukkan bahwa ia telah mengambil langkah-langkah wajar untuk memastikan pelindungan data pribadi, sesuai dengan kebijakan dan prosedur media tempatnya bekerja. Saat pengumpulan data untuk kegiatan jurnalistik didasarkan pada persetujuan Subjek Data Pribadi, jurnalis memberitahukan tujuan dan aktivitas pemrosesan data kepada Subjek Data Pribadi. Dalam hal terjadi kegagalan pelindungan data pribadi dalam konteks jurnalistik, media tempat jurnalis bekerja harus memberikan notifikasi kepada Subjek Data Pribadi.

Tabel 2. Aplikasi prinsip-prinsip pelindungan data pribadi dalam kegiatan jurnalistik

3.2.2. Landasan Hukum untuk Pemerolehan dan Pengumpulan Data Pribadi

Dalam sebuah rapat redaksi, jurnalis kerap kali memiliki informasi awal untuk diusulkan dalam liputan yang belum disepakati oleh redaksi. Dalam hal jurnalis bekerja pada sebuah media, jurnalis perlu mengajukan usulan liputan tanpa mencantumkan data pribadi narasumber dan informan. Dalam hal jurnalis adalah jurnalis lepas yang bekerja pada suatu media berdasarkan proyek, jurnalis lepas perlu membuat kesepakatan atau kontrak di mana tanggung jawab masing-masing pihak terkait pelindungan data pribadi dijelaskan secara rinci.

Sebagaimana dijelaskan di atas, jurnalis harus memahami landasan hukum pemrosesan data yang dilakukannya untuk kegiatan jurnalistik. Jurnalis, sebagai bagian media (dalam hal ini berperan sebagai pengendali data pribadi), harus menggunakan landasan hukum pemrosesan data pribadi yang paling relevan dan mempertimbangkan jika ada lebih dari satu landasan yang berlaku. Meskipun UU PDP tidak mengatur secara jelas mengenai landasan hukum pemrosesan data pribadi yang relevan untuk kegiatan jurnalistik, secara umum, "pemenuhan kepentingan yang sah lainnya dengan memperhatikan tujuan, kebutuhan, dan keseimbangan kepentingan Pengendali Data Pribadi dan hak Subjek Data Pribadi" (Pasal 20 ayat (2) huruf f UU PDP) dan "persetujuan yang sah secara eksplisit dari Subjek Data Pribadi" (Pasal 20 ayat (2) huruf a UU PDP) dapat digunakan sebagai landasan hukum untuk kegiatan jurnalistik.[8] Interpretasi ini sejalan dengan praktik di Inggris dan Uni Eropa.

[8] Di samping kedua landasan tersebut, terdapat pula dorongan agar kegiatan jurnalistik oleh pers dapat masuk ke dalam cakupan "pemenuhan kewajiban hukum dari Pengendali Data Pribadi sesuai dengan ketentuan peraturan perundang-undangan" di mana UU No. 40/1999 tentang Pers mengatur kewajiban hukum pers dan/atau "pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan Pengendali Data Pribadi berdasarkan peraturan perundang-undangan" di mana Pasal 6 UU No. 40/1999 tentang Pers mengatur tugas dan fungsi pers diselenggarakan dalam rangka melayani kepentingan umum.

Landasan kepentingan yang sah dapat digunakan untuk kegiatan jurnalistik karena adanya kepentingan publik mendapatkan informasi yang relevan dan akurat. Pemrosesan data pribadi yang menggunakan landasan ini harus dilakukan dengan memperhatikan tujuan, kebutuhan, dan keseimbangan kepentingan Pengendali Data Pribadi dan hak Subjek Data Pribadi. Pemrosesan data menggunakan landasan kepentingan yang sah harus mempertimbangkan ekspektasi wajar Subjek Data atas privasi mereka dan segala kerugian yang mungkin muncul.

Artikel 6(1)(f) UK GDPR misalnya mengatur mengenai asesmen kepentingan yang sah *(legitimate interest assessment)*, yang terdiri atas uji tujuan *(purpose test)*, uji kebutuhan *(necessity test)*, dan c *(balancing test)*. Penerapan asesmen ini dapat dilihat pada Tabel 3 berikut ini.

Uji	Pertanyaan kunci	Penerapan
Uji tujuan	- Apakah ada kepentingan sah di balik pemrosesan? - Apakah pemrosesan data sah secara hukum? - Apakah pemrosesan data etis?	Jurnalis harus menilai apakah ada pemrosesan data pribadi dilakukan untuk suatu kepentingan yang sah.
Uji kebutuhan	- Apakah pemrosesan tersebut diperlukan untuk tujuan tersebut? - Apakah pemrosesan data proporsional dan tepat sasaran untuk mencapai	Jurnalis harus memastikan bahwa pemrosesan data pribadi yang dilakukan benar-benar diperlukan untuk mencapai tujuan jurnalistik

	tujuannya? - Apakah ada alternatif yang tidak terlalu mengganggu selain memproses data ini atau selain memproses data dengan cara ini?	tertentu. Misalnya, apakah data tersebut penting untuk mengungkap fakta atau konteks yang relevan dalam suatu pemberitaan.
Uji keseimbangan	- Apakah kepentingan sah untuk memproses data melampaui pemenuhan kepentingan, hak, atau kebebasan Subjek Data? - Apakah pemrosesan data berisiko tinggi bagi Subjek Data? - Apa kemungkinan dampak pemrosesan data terhadap Subjek Data?	Jurnalis harus selalu mempertimbangkan apakah kepentingan sah yang ingin dicapai melalui pemrosesan data seimbang dengan dampak pemrosesan data bagi kepentingan, hak dasar, dan kebebasan Subjek Data. Dengan kata lain, risiko gangguan atas privasi dan kepentingan Subjek Data harus dapat dijustifikasi dengan besarnya kepentingan yang sah yang akan dicapai dari pemrosesan data. Pemrosesan data

		anak-anak dan kelompok rentan lainnya harus dilakukan dengan lebih berhati-hati untuk memastikan kepentingan dan hak-hak mereka terlindungi.

Tabel 3. Asesmen kepentingan yang sah *(legitimate interest assessment)*

Persetujuan yang sah terkadang dapat digunakan sebagai landasan kegiatan jurnalistik, misalnya dalam menggunakan data pribadi spesifik. Meskipun persetujuan yang sah adalah landasan hukum yang paling kuat, data pribadi dapat diproses tanpa persetujuan selama ada kepentingan sah lainnya yang lebih penting, yang dalam konteks jurnalistik adalah kepentingan umum.

Yang perlu diingat adalah dalam publikasi data atau informasi pribadi apapun yang dilakukan tanpa persetujuan, semakin privat sifat suatu data atau informasi, dan dengan demikian semakin sedikit signifikansinya bagi kepentingan umum, maka semakin tinggi kebutuhan untuk berhati-hati dalam memproses data pribadi dan mempublikasikannya. Pada prinsipnya, Subjek Data Pribadi yang bukan merupakan figur publik memiliki ekspektasi yang lebih besar atas hak privasi mereka. Namun, dalam hal tindakan mereka mungkin membawa mereka ke ruang publik, tidak ada larangan mutlak bagi jurnalis untuk membuat liputan tentang mereka, bahkan tanpa persetujuan mereka.

Pasal 25 ayat (1) dan Pasal 26 ayat (1) UU PDP secara spesifik mengatur bahwa pemrosesan data pribadi anak dan penyandang disabilitas diselenggarakan secara khusus. Data anak hanya dapat

diproses dengan persetujuan dari orang tua dan/atau walinya (Pasal 25 ayat (2)), sedangkan data penyandang disabilitas hanya dapat diproses dengan persetujuan penyandang disabilitas dan/atau walinya (Pasal 26 ayat (3)). Pada prinsipnya, pemrosesan data pribadi kelompok rentan harus dilakukan dengan lebih berhati-hati dan mempertimbangkan risiko pemrosesan data terhadap kerentanan mereka. Penjelasan mengenai cakupan dan dampak pemrosesan data untuk memperoleh persetujuan dari kelompok rentan juga harus dibuat ringkas dan mudah dimengerti, termasuk dengan menggunakan gambar atau materi audiovisual.

Jika jurnalis menggunakan persetujuan sebagai landasan pemrosesan data pribadi, jurnalis perlu merekam siapa Subjek Data yang memberikan persetujuan, kapan dan bagaimana persetujuan diberikan, dan informasi apa yang *disembarked* kepada Subjek Data dalam memperoleh persetujuan. Penggunaan formulir persetujuan untuk kegiatan jurnalistik yang telah disediakan oleh media dapat berguna dalam hal ini.

Konsekuensi dari pemrosesan data yang didasarkan pada persetujuan adalah bahwa persetujuan tersebut dapat ditarik kapan saja oleh Subjek Data Pribadi. Oleh karena itu, jurnalis perlu mempertimbangkan dengan matang penggunaan landasan ini.

3.2.3. Pemerolehan Data Pribadi dalam Jurnalisme Investigasi

Pada praktiknya, jurnalis tidak selalu dapat menginformasikan kegiatan pemerolehan data yang dilakukan kepada Subjek Data Pribadi yang menjadi subjek reportasenya, terutama dalam konteks jurnalisme investigasi. Jika jurnalis memang perlu menggunakan metode penyamaran atau metode rahasia untuk melakukan liputan, jurnalis hanya dapat melakukannya jika pemerolehan data ini dapat dibenarkan demi kepentingan publik, dan bahwa dampak merugikan yang ditimbulkan dari pemberitahuan kepada subjek data mengenai pemerolehan data terhadap kerja jurnalistik yang dimaksud dapat dibuktikan. Pentingnya liputan, sejauh mana informasi dapat berfungsi, tingkat intrusi terhadap privasi, dan potensi dampak

terhadap subjek data dan pihak ketiga merupakan faktor-faktor yang relevan untuk dipertimbangkan jurnalis.

Jurnalis juga perlu memperhatikan risiko pemidanaan terkait dengan pemerolehan atau pengumpulan, dan penggunaan data pribadi secara melawan hukum sebagaimana diatur dalam Pasal 65 UU PDP. Risiko ini semakin tinggi bagi pers di Indonesia mengingat ketiadaan memuat kegiatan jurnalistik dalam UU PDP.

3.2.4. Akurasi dan Minimalisasi dalam Penyimpanan (Retensi) Data Pribadi

Kontak narasumber/*informan* dan latar belakang penelitian adalah sumber daya yang penting untuk kegiatan jurnalistik. Jurnalis umumnya menyimpan informasi berisi data pribadi tersebut untuk jangka waktu lama atau bahkan tanpa batas waktu tertentu, meskipun tidak ada peliputan spesifik yang sedang dikerjakannya. Dalam hal ini, jurnalis tetap harus memastikan penerapan prinsip-prinsip pelindungan data pribadi dalam penyimpanan informasi tersebut.

Jurnalis harus meninjau akurasi dari data dan informasi pribadi yang disimpannya dari waktu ke waktu untuk kekinian dan relevansinya dalam mendukung kerja jurnalistik. Mempertahankan kepercayaan masyarakat dengan memastikan akurasi data dalam pemberitaan dapat melindungi kepentingan umum yang dilayani oleh jurnalisme, meningkatkan reputasi sebagai sumber informasi bagi jurnalis serta media tempatnya bekerja. Sepanjang memungkinkan, jurnalis perlu menyimpan catatan tentang narasumbernya dan sumber informasi lain yang digunakan dalam melakukan pemberitaan agar jika diperlukan, pihak lain dapat menverifikasi akurasi informasi tersebut. Pencatatan juga memperjelas tentang jenis data pribadi yang disimpan, alasannya, dan Subjek Data terkait.

Jurnalis perlu secara berkala menghapus informasi pribadi yang tidak lagi relevan dan akurat. Hal ini sejalan dengan prinsip minimalisasi. Jika data pribadi yang disimpan oleh jurnalis tidak relevan dengan suatu peliputan tertentu, data tersebut mungkin masih relevan dengan

tujuan jurnalistik secara umum. Kuncinya adalah jurnalis dapat memiliki justifikasi mengapa data tersebut relevan untuk disimpan. Cara peninjauan informasi yang disimpan dan penyimpanan masa depan perlu ditetapkan dalam kebijakan redaksi media tempat jurnalis bekerja.

3.2.5. Integritas dan Keamanan dalam Penyimpanan Data Pribadi

Jurnalis harus menjaga keamanan data pribadi yang disimpan dan dikelolanya. Hal ini termasuk menjaganya dari akses dan penggunaan yang tidak sah atau melanggar hukum serta kehilangan, kehancuran, atau kerusakan yang tidak disengaja. Untuk itu, selain mengandalkan langkah-langkah keamanan teknis (elektronik) dan fisik, kebijakan dan prosedur, serta pelatihan dan pengawasan yang diberlakukan oleh media tempatnya bekerja, jurnalis juga perlu menerapkan langkah-langkah pengamanan yang tepat dan proporsional.

Baik media maupun jurnalis perlu mempertimbangkan peningkatan risiko keamanan yang mungkin timbul akibat pekerjaan yang dilakukan jurnalis, misalnya, terkait kerja jarak jauh, penggunaan perangkat portabel, seperti laptop dan ponsel pintar, serta media portabel, seperti *memory stick USB*.

Jurnalis perlu memiliki kapasitas untuk menerapkan kebiasaan dan teknologi yang mendukung pelindungan keamanan data. Kebiasaan yang dimaksud termasuk mengakses data sesuai dengan level otorisasinya, menggunakan perangkat keras dan lunak yang aman, menyimpan data cadangan *(back-up data)* secara aman, serta menggunakan jaringan internet dan komunikasi yang aman. Teknologi yang dimaksud termasuk enkripsi, *firewalls,* dan autentikasi.

3.2.6. Asesmen Kepentingan Umum dalam Pengungkapan Berita

Meskipun informasi pribadi diperoleh dan disimpan secara adil, jurnalis perlu mempertimbangkan informasi apa saja yang dapat dipublikasikan. Pertimbangan yang harus dilakukan mencakup berapa banyak data pribadi yang perlu dipublikasikan untuk melaporkan

berita dengan benar, seimbang dengan tingkat gangguan terhadap kehidupan subjek data, dan potensi kerugian yang mungkin ditimbulkannya.

Misalnya, jika sebuah berita bersifat sangat mengganggu atau berbahaya bagi Subjek Data Pribadi (narasumber/*informan*), maka publikasi data pribadi akan menjadi tidak adil bagi subjek data. Hal ini terutama ditemukan pada pemberitaan yang unsur kepentingan publiknya terbatas, tidak terlalu jelas, atau nihil. Hal ini juga terjadi pada pemberitaan yang publikasinya perlu ditunda setelah ada hasil verifikasi data. Kepentingan umum harus dipertimbangkan dalam melakukan publikasi laporan. Dalam melakukan publikasi produk jurnalistik yang memuat data pribadi, harus dipastikan bahwa tingkat kepentingan publik yang dicapai melalui publikasi melebihi intrusi atas privasi Subjek Data Pribadi yang menjadi subjek peliputan (narasumber/*informan*).

Untuk melakukan pertimbangan yang objektif atas unsur "kepentingan umum" dalam publikasi, redaksi dan jurnalis perlu mempertimbangkan situasi sosial-politik-budaya di tengah masyarakat, menyeimbangkan argumen-argumen yang mendukung dan menentang publikasi, serta memutuskan apakah kepentingan umum paling baik dilayani melalui publikasi.

Secara umum, kepentingan umum berkaitan dengan hal-hal yang mempengaruhi masyarakat dan menjadi perhatian masyarakat. Hal ini mencakup, tapi tidak terbatas pada kepentingan untuk:

- menjunjung tinggi standar integritas dalam penyelenggaraan negara dan hal lainnya yang memengaruhi publik;
- memastikan keadilan dan perlakuan yang adil bagi semua;
- mendorong transparansi dan akuntabilitas;
- mendorong pemahaman dan keterlibatan masyarakat dalam proses demokrasi; dan
- memastikan pengelolaan dan penggunaan sumber daya publik secara baik.

Terdapat pula kepentingan umum atas topik yang lebih spesifik. Misalnya, topik terkait dengan kesehatan dan keselamatan masyarakat, kejahatan dan perilaku anti-sosial, keamanan nasional, penyalahgunaan jabatan publik, serta penyalahgunaan aset publik.

Secara umum, terdapat kepentingan publik lebih tinggi yang melandasi publikasi informasi ketika Subjek Data Pribadi:

- merupakan figur publik (individu yang mendapat paparan media karena fungsi atau komitmennya); atau
- mempunyai peran dalam kehidupan masyarakat lebih luas, di mana masyarakat berkepentingan untuk mempunyai akses terhadap sejumlah informasi tentang dirinya. Politisi, pejabat publik, pelaku bisnis, dan anggota profesi yang diatur adalah contoh individu dengan peran seperti ini.

Pedoman mengenai Perlindungan Privasi di Media *(Guidelines on Safeguarding Privacy in the Media)* yang dikeluarkan oleh Konsil Eropa *(Council of Europe)* menawarkan kerangka untuk menyeimbangkan hak privasi dan kebebasan berekspresi. Faktor pertama yang perlu dipertimbangkan adalah *kontribusi dari pemberitaan bermuatan informasi pribadi bagi wacana/diskursus publik demi kepentingan umum*. Pemberitaan mengenai kelahiran bayi dalam suatu negara berbentuk monarki berdasarkan keturunan, terpidana yang dikaitkan dengan kasus pembunuhan yang belum tuntas, atau perilaku konsumtif keluarga pejabat publik, misalnya adalah beberapa contoh berita bermuatan informasi pribadi yang memiliki nilai kepentingan umum untuk alasan yang berbeda-beda.

Faktor kedua adalah *peran atau kedudukan subjek liputan di tengah masyarakat*. Warga privat memiliki ekspektasi atas privasi yang lebih tinggi dibandingkan dengan figur publik. Dalam menentukan apakah seseorang termasuk figur publik/tokoh masyarakat, jurnalis perlu memperhatikan apakah orang tersebut telah masuk ke dalam domain publik dengan berpartisipasi dalam diskusi/wacana publik atau secara aktif menarik perhatian publik atas apa yang dilakukannya.

Semakin besar peran dan pengaruh seorang tokoh masyarakat, sewajarnya semakin tinggi pula risiko bahwa kehidupan pribadinya mendapatkan pengawasan lebih ketat dibanding individu privat. Figur publik yang ekspektasi privasinya paling rendah adalah politisi. Aktivitas atau tindakan pribadi tertentu yang dilakukan figur publik tidak dapat dianggap sebagai aktivitas atau tindakan non-publik jika memiliki dampak sosial, ekonomi, politik, maupun budaya. Di sisi lain, jurnalis harus menghormati ekspektasi figur publik terhadap privasinya ketika mereka terlibat dalam kegiatan yang murni pribadi, seperti berolahraga, berjalan, atau berlibur, jika pemberitaan yang dimuat tidak berdampak bagi kepentingan umum.

Selain itu, jurnalis juga harus sangat berhati-hati saat memberitakan mengenai kelompok rentan atau kelompok berkebutuhan khusus. Anak-anak dan remaja, misalnya, dilindungi karena kerentanan yang melekat pada usia mereka. Pertimbangan khusus harus diberikan pada kedewasaan seorang anak ketika mengutip komentarnya. Anak tersebut mungkin tidak cukup menyadari dampak dari komentarnya dan media mempunyai tanggung jawab etis untuk tidak menyebabkan kerugian padanya.

Faktor ketiga adalah *perilaku subjek pemberitaan.* Jika figur publik telah terlebih dahulu secara sukarela mengungkapkan informasi pribadinya kepada publik, maka sewajarnya informasi yang telah tersedia tersebut dapat dijadikan bahan pemberitaan.

Faktor keempat adalah *cara memperoleh informasi dan kebenarannya*. Jurnalis terikat untuk bertindak dengan itikad baik dan bertanggung jawab termasuk dalam menyediakan fakta yang akurat, informasi yang dapat diandalkan dan tepat sesuai dengan etika jurnalistik. Jurnalis harus menggunakan cara yang adil untuk memperoleh informasi dan menunjukkan rasa hormat terhadap terhadap subjek pemberitaan.

Faktor kelima adalah *konten, bentuk, dan konsekuensi publikasi.* Penting bagi jurnalis untuk mempertimbangkan media publikasi di mana subjek pemberitaan merepresentasikan dirinya. Terkait konten, perhatian khusus harus diberikan ketika subjek pemberitaan

dipresentasikan secara negatif dalam berita, karena pemberitaan demikian berpotensi memberikan dampak negatif padanya. Dalam meninjau konsekuensi publikasi, jurnalis juga perlu mempertimbangkan dampak negatif publikasi terhadap kerabat subjek pemberitaan yang mungkin akan menghadapi ancaman. Pertimbangan ini berguna untuk menentukan perlu atau tidaknya mengungkap identitas subjek pemberitaan atau narasumber. Memisahkan antara fakta dan opini narasumber ketika melaporkan pemberitaan tentangnya juga dapat mereduksi ketidakakuratan dalam pemberitaan, dan dengan demikian, risiko negatif bagi narasumber.

3.2.7. Publikasi Data Pribadi yang Diperoleh dari Sumber Anonim

Kerahasiaan dan keamanan data pribadi Subjek Data adalah tanggung jawab Pengendali Data Pribadi menurut UU PDP. Pengungkapan atas data pribadi tersebut harus berdasarkan alasan yang sah dan dilakukan secara adil bagi Subjek Data Pribadi. Dengan demikian, data pribadi yang didapat dari sumber anonim atau proses *off-the-record* tidak bisa serta merta masuk dalam berita. Pengungkapan informasi tentang individu yang menjadi narasumber/informan (atau siapapun yang diidentifikasi dalam informasi tersebut) hanya perlu dilakukan jika individu tersebut mengizinkan, atau jika ada alasan kuat yang wajar untuk melakukannya. Dengan demikian, dalam hal terdapat permintaan hak akses atas data pribadi yang rahasia, jurnalis dan media tempatnya bekerja perlu menanyakan persetujuan Subjek Data Pribadi.

3.2.8. Publikasi Data Pribadi yang Sudah Menjadi Data Publik

Dalam liputan mendalam atau investigasi, jurnalis sering mengakses data pribadi yang spesifik, seperti harta kekayaan, kondisi kesehatan, dan catatan kejahatan. Dalam konteks UU PDP saat ini, di mana pada satu sisi jenis data pribadi tersebut wajar diproses untuk kegiatan jurnalistik, dikategorikan sebagai data pribadi spesifik yang perlu mendapatkan perlindungan lebih, akan tetapi pada sisi kegiatan

jurnalistik tidak mendapatkan pengecualian dan perlindungan lebih. Jurnalis perlu lebih berhati-hati dalam melakukan akses dan pengungkapan jenis-jenis data tersebut dalam liputannya.

Sedapat mungkin, jurnalis perlu memprioritaskan data yang sudah berada di domain publik, misalnya Laporan Harta Kekayaan Penyelenggara Negara (LHKPN), Sistem Informasi Penelusuran Perkara (SIPP) Pengadilan, *Organized Crime and Corruption Reporting Project (OCCRP) Aleph, Open Corporates, Open Ownership,* dan *International Consortium of Investigative Journalists (ICIJ) Offshore Leaks Database.*

Kepentingan untuk melindungi hak privasi tidak secara otomatis menurun hanya karena beberapa informasi pribadi atau informasi serupa sudah ada di domain publik. Yang membedakan pengaksesan dan pengungkapan data pribadi yang berasal dari sumber privat dengan dari domain publik adalah tingkat intrusi terhadap privasi. Jika informasi tentang individu tersebut sudah ada domain publik, ekspektasi individu terhadap privasi tidak sama dengan jika informasi tersebut belum tersedia di domain publik. Oleh karena itu, penting bagi jurnalis untuk membandingkan informasi yang dimilikinya dengan yang sudah tersedia di domain publik.

3.2.9. Pembagian Data

Dalam berbagi data dengan sesama jurnalis untuk keperluan kegiatan jurnalistik, jurnalis perlu memerhatikan prosedur redaksi media tempatnya bekerja dan memastikan penerapan prinsip-prinsip pelindungan data pribadi. Sedangkan mekanisme pembagian data antar jurnalis dan media yang masih berada dalam satu grup perusahaan/sindikasi media perlu diatur melalui mekanisme pengendalian data gabungan (*joint controllership*) yang ditetapkan oleh menajemen perusahaan media atau di tingkatan grup perusahaan/sindikasi media.

3.2.10. Hak Narasumber untuk Mengakses, Mengoreksi, dan Menarik Persetujuan Pemrosesan Data Pribadi

UU PDP mengatur hak Subjek Data Pribadi untuk mengakses, mengoreksi, dan menarik persetujuan pemrosesan data pribadi. Dalam hal ini, media perlu menyediakan sarana komunikasi bagi narasumber/informan untuk dapat mengomunikasikan permintaan-permintaan terkait dengan pemenuhan haknya sebagai Subjek Data Pribadi.

Jurnalis dan media tempatnya bekerja dapat memberikan akses kepada narasumber/informan mengenai data pribadi apa saja yang dikelolanya atas Subjek Data tersebut selama hal tersebut tidak berisiko pada kegiatan jurnalistik.

Secara umum, Subjek Data Pribadi dapat meminta data pribadinya dihapus, termasuk jika jurnalis atau redaksi media memproses data pribadi secara tidak sah atau mengandalkan persetujuan secara sah dan persetujuan tersebut ditarik kembali. Jika sebuah berita yang memuat data pribadi sudah diterbitkan dan narasumber sebagai Subjek Data meminta koreksi, hal ini telah diatur dalam mekanisme Hak Jawab[9] dan Hak Koreksi[10] dalam UU Pers.

Dalam hal Subjek Data menarik persetujuan atas pemrosesan data pribadinya dan meminta data pribadinya dihapus berikut dengan pemberitaan yang menggunakan data pribadi tersebut, hak tersebut tak secara absolut berlaku mengingat pemrosesan data pribadi dalam kegiatan jurnalistik dilakukan untuk kepentingan umum. UU Pers juga mengatur bahwa berita sudah ditayangkan telah informasi publik,

[9] Hak Jawab adalah hak seseorang atau sekelompok orang untuk memberikan tanggapan atau sanggahan terhadap pemberitaan berupa fakta yang merugikan nama baiknya (UU Pers Pasal 1 ayat 11).
[10] Hak Koreksi adalah hak setiap orang untuk mengoreksi atau memberitahukan kekeliruan informasi yang diberitakan oleh pers, baik tentang dirinya maupun tentang orang lain (UU Pers Pasal 1 ayat 12).

sehingga data pribadi yang muncul dalam sebuah berita tidak dapat ditarik kembali.

Pemenuhan hak-hak Subjek Data Pribadi atas informasi mereka yang diproses untuk keperluan jurnalistik dilakukan sesuai dengan prosedur media tempat jurnalis bekerja.

Bahan diskusi

1. Sejauh apa jurnalis atau media tempatnya bekerja telah mengimplementasikan prinsip-prinsip pelindungan data pribadi untuk kegiatan jurnalistik?
2. Mekanisme apa yang tersedia untuk jurnalis dan media tempatnya bekerja untuk memperjelas tanggung jawab dan beban pertanggungjawaban dalam hal pelanggaran pelindungan data pribadi terjadi karena kelalaian jurnalis?
3. Keadaan/situasi apa yang membuat jurnalis perlu mengambil keputusan-keputusan mandiri mengenai pemrosesan data pribadi di luar keputusan redaksi?
4. Konsekuensi baru apa yang ditimbulkan UU PDP bagi pemrosesan data pribadi untuk kegiatan jurnalistik?
5. Bagaimana media tempat jurnalis bekerja mengatur mengenai pembagian data pribadi antarjurnalis dalam satu perusahaan dan lintas perusahaan dalam satu grup?

Bacaan lebih lanjut:

- Pentingnya Mengakomodasi Pengecualian Tujuan Jurnalistik dalam Kebijakan Pelindungan Data Pribadi: https://aji.or.id/data/pentingnya-mengakomodasi-pengecualian-tujuan-jurnalistik-dalam-kebijakan-pelindungan-data
- Guidelines on safeguarding privacy in the media
- Modul Pelindungan Data Pribadi Bagi Masyarakat Sipil: https://www.tifafoundation.id/buku/modul-perlindungan-data-pribadi-bagi-masyarakat-sipil/

Modul 3.3. Pelanggaran Pelindungan Data Pribadi dalam Kegiatan Jurnalistik

Deskripsi:

Meskipun jurnalis telah menerapkan langkah-langkah pelindungan data pribadi sebagaimana diatur dalam prosedur media tempatnya bekerja, tidak jarang jurnalis perlu mengambil langkah mandiri di luar ruang redaksi untuk memastikan pelindungan atas data pribadinya dan data yang dikelolanya. Bagian ini mengupas bentuk-bentuk pelanggaran pelindungan data pribadi, manajemen insiden keamanan data, dan pihak-pihak yang dapat dihubungi jurnalis dalam merespons insiden keamanan.

Tujuan:

- Peserta memahami bentuk-bentuk pelanggaran pelindungan data pribadi
- Peserta mengerti hal-hal yang perlu dilakukan ketika terjadi insiden keamanan
- Peserta mengerti peran yang dilakukan perusahaan media, organisasi jurnalis dan organisasi masyarakat sipil lainnya dalam pelindungan data pribadi

Metode: paparan, diskusi/tanya-jawab

Durasi: 90 menit

Pokok bahasan

3.3.1. Bentuk-bentuk Pelanggaran Pelindungan Data Pribadi

Pasal 46 ayat (1) UU PDP mengatur bahwa “kegagalan Pelindungan Data Pribadi" adalah “kegagalan pelindungan data pribadi seseorang dalam hal kerahasiaan, integritas, dan ketersediaan data pribadi, termasuk pelanggaran keamanan, baik yang disengaja maupun tidak disengaja, yang mengarah pada perusakan, kehilangan, perubahan, pengungkapan, atau akses yang tidak sah terhadap data pribadi yang dikirim, disimpan, atau diproses.” Dalam hal terjadi kegagalan Pelindungan Data Pribadi, pemberitahuan secara tertulis kepada Subjek Data Pribadi dan Lembaga PDP perlu dilakukan dalam waktu 3 x 24 jam (Pasal 46 ayat 1 UU PDP). Dalam hal tertentu, Pengendali Data Pribadi wajib memberitahukan kepada masyarakat mengenai kegagalan Pelindungan Data Pribadi (Pasal 46 ayat 3 UU PDP). Dalam konteks jurnalistik, media tempat jurnalis bekerja adalah pihak yang bertanggung jawab melakukan pemberitahuan ini.

Di samping kegagalan pelindungan data pribadi yang lebih mengacu pada aspek keamanan di atas, yaitu kerahasiaan *(confidentiality),* integritas *(integrity),* dan ketesediaan *(availability),* pelanggaran terhadap tanggung jawab pelindungan data pribadi dapat terjadi dalam berbagai tahapan pemrosesan data pribadi. Tabel 4 di bawah ini memberikan beberapa contoh potensi pelanggaran yang perlu diantisipasi dalam kegiatan jurnalistik. Dalam hal ini, media tempat jurnalis bekerja perlu mengantisipasi berbagai potensi pelanggaran ini dalam prosedur tata kelola data dan kebijakan privasinya.

Tahap pemrosesan	Contoh pelanggaran
Pemerolehan dan pengumpulan	Pemerolehan data tanpa landasan hukum yang sah
Pengolahan dan penganalisisan	Hasil pengolahan data secara otomatis berdampak pada diskriminasi atau bentuk ketidakadilan lainnya bagi

	subjek data; pengolahan data pribadi yang diperoleh untuk tujuan jurnalistik untuk tujuan lainnya
Penyimpanan	Kebocoran data; akses data oleh pihak tanpa otorisasi
Perbaikan dan pembaruan	Data tidak akurat dan aktual yang dijadikan bahan liputan
Penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan	Transfer data kepada pihak ketiga tanpa landasan hukum yang sah
Penghapusan atau pemusnahan	Penyimpanan data yang diperoleh berdasarkan persetujuan yang sah di luar batas retensi

Tabel 4. Contoh pelanggaran terhadap tanggung jawab pelindungan data pribadi

3.3.2. Manajemen Insiden Keamanan Data

Jurnalis di era digital ini harus mampu mengamankan data pribadinya dan data pribadi yang dikelolanya, termasuk narasumber/informan maupun subjek peliputan. Terdapat berbagai faktor yang membentuk profil risiko keamanan jurnalis. Jurnalis liputan investigasi dan jurnalis yang bekerja di daerah dengan situasi politik yang tidak stabil, misalnya, menghadapi lebih banyak risiko keamanan dibandingkan jurnalis lainnya. Hal ini membuat kebutuhan akses terhadap sarana teknologi informasi dan komunikasi yang aman lebih tinggi. Ketersediaan akses internet juga menjadi salah satu faktor yang memengaruhi kemudahan memproses data dengan aman. Jurnalis yang bekerja di daerah di mana pemutusan internet *(internet shutdown)* sering dilakukan, misalnya, perlu secara adaptif memanfaatkan teknologi informasi dan komunikasi yang dapat

bekerja dengan akses internet minim, membiasakan penggunaan teknologi enkripsi, dan melakukan penyalinan data (*back-up*).

Dalam hal jurnalis menghadapi situasi di mana terjadi insiden keamanan yang memengaruhi keamanan data pribadi yang dikelolanya, jurnalis perlu menerapkan langkah-langkah yang diatur dalam prosedur media tempatnya bekerja. Pada umumnya, hal ini mencakup:

- pengidentifikasian bentuk insiden keamanan, sumber, kronologi, dan dampaknya;
- pelaporan insiden ke media, organisasi pers terkait, dan organisasi penanganan insiden keamanan yang relevan;
- asesmen, investigasi, dan analisis oleh pihak-pihak yang telah dihubungi oleh jurnalis;
- penanganan insiden, termasuk karantina/isolasi terhadap insiden untuk menghindari dampak lebih luas;
- pemberitahuan kepada pihak-pihak terdampak;
- pemulihan atas teknologi dan pihak terdampak; dan
- penyesuaian untuk meningkatan mekanisme dan postur keamanan.

Di samping langkah-langkah umum di atas, umumnya jurnalis melakukan langkah-langkah mandiri untuk mengisolasi insiden, termasuk dengan mengganti *password*, memindahkan data, dan melaporkan langsung kepada pihak terkait (misalnya, perusahaan teknologi digital dalam konteks insiden keamanan terjadi melalui mediasi teknologi/*platform* digital).

Sebagai pelaksana tugas dari media tempatnya bekerja, jurnalis harus dapat menunjukkan kepatuhannya terhadap UU PDP dalam pemrosesan data pribadi yang dilakukannya. Dalam hal kegagalan pelindungan data pribadi terjadi karena kelalaian atau kurangnya kapasitas jurnalis, jurnalis perlu mendiskusikan konsekuensi dari hal ini dengan media tempatnya bekerja.

3.3.3. Menghubungi Jaringan Pendukung

Dalam menghadapi berbagai insiden yang mengancam keamanannya maupun data yang dikelolanya, selain menghubungi media tempatnya bekerja, jurnalis dapat menghubungi organisasi yang relevan dengan profesinya, seperti Aliansi Jurnalis Independen (AJI), Ikatan Jurnalis Televisi Indonesia (IJTI), Persatuan Wartawan Indonesia (PWI), dan Pewarta Foto Indonesia (PFI). Untuk pendampingan hukum, Lembaga Bantuan Hukum Pers (LBH Pers) dapat dihubungi. Untuk Panduan Keamanan Digital untuk Jurnalis, Digital Defenders Partnership (DDP), dan Digital Security Helpline AccessNow adalah beberapa pihak yang dapat dihubungi.

Bahan diskusi:

1. Identifikasi berbagai bentuk potensi pelanggaran pelindungan data pribadi lainnya dalam kegiatan jurnalistik.

2. Dalam konteks kegagalan pelindungan data pribadi terjadi karena kelalaian jurnalis, bagaimana mekanisme pertanggungjawabannya antara jurnalis dengan media tempatnya bekerja?

Bacaan lebih lanjut:

1. Penilaian mandiri risiko keamanan digital: https://advokasi.aji.or.id/perangkat-penilaian-risiko/id/quest/keamanan-digital/
2. Panduan Keamanan Digital untuk Jurnalis: https://advokasi.aji.or.id/safety?artikel=43&kategori=4

Didukung oleh:

BAB 4

PELINDUNGAN DATA PRIBADI UNTUK STAF MEDIA NON-REDAKSIONAL

PELINDUNGAN DATA PRIBADI UNTUK STAF MEDIA NON-REDAKSIONAL

Modul 4.1. Pentingnya Pelindungan Data Pribadi untuk Staf Non-Redaksional

Deskripsi: Di tahap awal, peserta diminta berbagi cerita/pengalaman tentang bagaimana cara mereka memanfaatkan PDP dalam melakukan tugas sebagai staf non-redaksi. Hal ini mencakup bagaimana para pekerja non-redaksi mengelola data pribadi dan ketika menjadi subjek data. Ini mencakup bagaimana mereka meminimalisasi risiko kebocoran atau pelanggaran data pribadi atau menghadapi tantangan tersebut.

Kemudian pembicara menjelaskan dalam bentuk presentasi tentang manfaat, cara pemanfaatan, tantangan dan bagaimana manajemen risiko yang dapat dilakukan staf non redaksional media terkait data pribadi. Sesi ini dimaksudkan untuk mengidentifikasi dan mengukur tingkat pemahaman, pengetahuan, serta pengalaman peserta dalam konteks PDP untuk staf non redaksional.

Tujuan: Peserta Memahami Pentingnya Pelindungan Data Pribadi untuk pekerja non-redaksional di media

Metode: Pemaparan dan Tanya jawab

Durasi: 60 menit

Pokok Bahasan

4.1.1. Beberapa Kasus Peretasan di Perusahaan Media

Pada 2011, sebanyak 1,27 juta akun pengguna Washington Post diretas. Insiden besar ini cukup mengguncang kepercayaan masyarakat karena merupakan salah satu serangan pertama terhadap perusahaan media bergengsi. Peretas dapat masuk melalui situs Pekerjaan *Washington Post*. Mereka mencuri nama pengguna dan alamat email — kemungkinan besar untuk melakukan penipuan *phishing*, menurut *PCMag*.

Data para pelanggan Dow Jones, bagian dari *The Wall Street Journal*, antara Juli 2012 dan Agustus 2015 pernah diretas. Laporan mengungkapkan bahwa para peretas mendapatkan informasi kartu kredit dari hampir 3.500 orang — bersama dengan nama, alamat, alamat email, dan nomor telepon. Tujuan para peretas adalah mengirimkan permintaan palsu, menurut *Wall Street Journal*. Perusahaan menduga insiden tersebut adalah bagian dari pelanggaran data multi-perusahaan yang jauh lebih besar[11].

Pada 2015 juga, induk perusahaan Ashley Madison, Avid Life Media, menyebutkan para peretas yang mengaku bernama *The Impact Team* telah memperoleh akses pada jejaring komputer dan mempublikasikan data pribadi sensitif 10 giga yang berisi nama, alamat, alamat surel, dan rincian kartu kredit pelanggan.

Di Indonesia, serangan digital juga terjadi pada media. Pada 2020, laman tempo.co diretas dan pada 2022 belasan akun awak redaksi

[11] *Dow Jones Becomes Latest Company to Disclose Data Breach*. (2015, October 9). NBC News. https://www.nbcnews.com/tech/security/dow-jones-says-hack-may-have-exposed-card-info-3-n441886

Narasi diretas. Kasus-kasus di atas merupakan peringatan betapa rentannya penyerangan terhadap media dan bagaimana data pribadi, bukan hanya para pekerja media, tapi juga publik, bocor. Seringkali, serangan-serangan masuk melalui berbagai cara, termasuk terhadap pekerja media di luar awak redaksi, seperti halnya yang terjadi pada akun media sosial *Associated Press*.

4.1.2. Tantangan Pelindungan Data Pribadi Pekerja Media

Kebutuhan untuk memperkuat pelindungan data pribadi bagi pekerja non-redaksi menjadi penting karena beberapa hal. Pertama, sejumlah pekerjaan non-redaksional di media belakangan memerlukan sejumlah pengumpulan data pribadi pada pihak di luar perusahaan. Kedua, pemahaman soal Pelindungan Data Pribadi bagi kalangan pekerja non-redaksi masih lemah. Terakhir, kebocoran data pribadi bagi beberapa jenis pekerjaan tertentu yang bersifat non-redaksional dapat mempengaruhi kerja-kerja jurnalisme dan reputasi perusahaan.

Sejumlah jenis pekerja media melibatkan pengumpulan data pribadi pada pihak luar untuk dapat melakukan kerja-kerjanya. Salah seorang staf keuangan mengaku ia kerap dimintai data pribadi oleh klien-klien perusahaan media. Data yang sering diminta adalah Kartu Tanda Penduduk dan nomor telepon pribadi. KTP umum diminta sebagai bagian dari transaksi keuangan.

Padahal, kesadaran tentang pelindungan data pribadi mulai muncul bagi para pekerja media. Kesadaran ini muncul karena mengalami kerugian akibat pencurian data pribadi atau melihat hal serupa terjadi pada rekan atau keluarganya. Sebagai contoh, salah seorang pekerja media melihat bagaimana kerabatnya tidak dapat menggunakan subsidi listrik karena data pribadinya telah digunakan orang lain. Ada

juga yang pernah mengalami peretasan pada akun percakapan WhatsApp[12].

Meskipun terjadi pengumpulan data pribadi, para pekerja media non-redaksi mendapati bahwa tidak ada transparansi dan akuntabilitas pada proses-proses selanjutnya. Ketika bekerjasama dengan pihak lain, para pegawai bagian kerja sama atau staf keuangan mengaku tidak memiliki pengetahuan soal bagaimana data pribadi mereka diolah (atau mungkin ditelaah), disimpan, ditransfer, ditampilkan, dan apakah ada siklus data yang berakhir dengan penghapusan.

Kebocoran data pribadi yang umum dialami para pekerja media adalah kebocoran nomor telepon. Ini mengakibatkan sejumlah ketidaknyamanan. Di antaranya adalah masuknya nomor telepon asing yang tiba-tiba menghubungi mereka untuk menawarkan jasa.

4.1.3. Memanfaatkan Pelindungan Data Pribadi Pekerja Media

Undang-undang Pelindungan Data Pribadi memberikan pengakuan pada hak-hak subjek data. Dalam hal ini, para pekerja media dapat memanfaatkan Undang-undang Pelindungan Data Pribadi dengan sejumlah cara.

Pertama, para pekerja media dapat meminta penjelasan sebelum menyerahkan data-data pribadi pada mitra media. Para pekerja media ketika bertemu dengan mitra media, baik itu swasta maupun pemerintah, dapat menerapkan Pasal 21 (1) dalam UU Pelindungan Data Pribadi. Pasal tersebut menjelaskan bahwa pengumpulan data pribadi berdasarkan persetujuan subjek data dan wajib menyampaikan informasi mengenai:

[12] Focus Group Discussion, 25 Februari 2024.

1. Legalitas dari pemrosesan Data Pribadi;
2. Tujuan pemrosesan Data Pribadi;
3. Jenis dan relevansi Data Pribadi yang akan diproses;
4. Jangka waktu retensi dokumen yang memuat Data Pribadi;
5. Rincian mengenai Informasi yang yang digunakan dan jangka waktu pemrosesan Data Pribadi;

Dalam hal ini, para pekerja media mulai memiliki kesadaran untuk menanyakan formulir atau deklarasi yang berisikan keterangan atau informasi-informasi di atas. Meskipun belum merupakan hal yang lumrah, setidaknya formulir-formulir atau *statement* sederhana dapat menjadi awalan untuk mengembangkan mekanisme di atas.

Kedua, para pekerja media dapat meminta akses mengenai data pribadi yang pernah ia kumpulkan pada mitra dari media tersebut. Hal ini sesuai dengan Pasal 32 dalam UU Pelindungan Data Pribadi. Pasal tersebut mewajibkan Pengendali Data memberi akses selama maksimal 3x24 jam.

Ketiga, para pekerja media dapat meminta penghapusan atau pemusnahan data-data pribadinya dari mitra perusahaan media, yang dalam hal ini bertugas sebagai pengendali data. Permintaan ini dapat dilakukan karena hal tersebut merupakan hak sebagai subjek data dan diatur lebih rinci dalam Pasal 43 dan Pasal 44. Terlebih, jika masa retensi dan tujuan pengolahan data sudah tercapai, pengendali data pribadi juga wajib melakukan penghapusan.

Pada lain sisi, ketika pekerja media perlu mengumpulkan data pribadi dari publik, mereka mendapatkan kepastian soal langkah apa yang perlu diambil. Salah satu peserta FGD menyebut, media tempat ia bekerja membuat pernyataan dalam survey tersebut yang berisikan komitmen bahwa data pribadi yang dikumpulkan akan diolah berdasarkan tujuan spesifik.

4.1.4. Manajemen Risiko dan Penanganan PDP Jika Bocor

Di luar dari hal-hal di atas, para pekerja media non-redaksi juga melakukan sejumlah langkah-langkah untuk mengelola risiko dan penanganan ketika terjadi kebocoran data. Sejumlah langkah tersebut pada prinsipnya meminimalisasi pengumpulan data pribadi atau mengecoh data (seperti pada penggunaan VPN), terutama ketika data tersebut dianggap tidak relevan. Di antaranya adalah penggunaan alat seperti ekstensi dan VPN, penggunaan lebih dari satu nomor telepon, mematikan lokasi perangkat, dan manajemen sandi.

Penggunaan VPN berfungsi untuk melindungi data pribadi ketika berselancar. Ini karena VPN mengubah alamat IP dari tempat asal. Akan tetapi, penggunaan VPN ini memiliki kelemahan bagi pekerja media yang bersifat lepas. Pekerja lepas di media tidak memiliki kantor dan bekerja dengan mengandalkan data dari telepon seluler atau *wi-fi* publik. Kecepatan internet dari kedua sumber tersebut sering tidak cukup untuk menggunakan VPN. Akibatnya, pekerjaan menjadi tidak nyaman.

Selain VPN, penggunaan ekstensi juga dilakukan untuk mengamankan data pribadi. Ekstensi peramban yang digunakan berfungsi untuk melacak jika ada kebocoran data pribadi. Jika terjadi, maka ekstensi tersebut akan memberitahukan pada pengguna. Setelahnya, pengguna dapat mengambil langkah-langkah yang dianggap perlu. Di antaranya adalah penggantian kata sandi atau bahkan penghapusan akun secara permanen.

Penggunaan lebih dari satu nomor telepon juga umum dilakukan, terutama untuk pekerja media yang banyak berurusan dengan mitra media. Ini karena ada kebutuhan untuk berkomunikasi secara profesional dan kebutuhan untuk menjaga privasi ketika tidak bekerja.

Akan tetapi, cara ini dianggap kurang praktis juga bagi pekerja media yang tidak mendapatkan fasilitas dari kantor. Oleh karena itu, perusahaan media didorong untuk menjadikan telepon genggam dan nomor telepon sebagai bagian dari fasilitas penunjang pekerjaan.

Pelindungan data pribadi yang umum dilakukan juga adalah mematikan lokasi pada perangkat telepon genggam. Cara ini cukup sederhana untuk meminimalisasi risiko pelacakan lokasi. Cara-cara ini ditempuh terutama ketika tengah melakukan pekerjaan yang dianggap berisiko.

Mitigasi lain terhadap pelindungan data pribadi adalah manajemen sandi. Kata sandi diubah secara berkala. Kata sandi terbaru dicatat secara tertulis atau menggunakan pengelolaan sandi, seperti *bitwarden*. Ada juga pekerja media lepas yang menggunakan *dongle* khusus. *Dongle* ini digunakan terutama untuk akun-akun yang berkaitan dengan tugas-tugas di perusahaan.

Modul 4.2. Pelindungan Data Pribadi dalam Pengelolaan Sumber Daya Manusia Pekerja Media

Deskripsi: Bagian ini akan memberikan penjelasan tentang Pelindungan Data Pribadi dalam lingkup Pengelolaan Sumber Daya Manusia. Bagian ini dijelaskan dalam konteks karena esensi sumber daya manusia berurusan dengan berbagai jenis informasi tentang individu yang bekerja di dalam sebuah organisasi, maka sangat penting untuk memiliki garis besar yang jelas tentang bagaimana data akan diproses.

Tujuan: Peserta Memahami Pelindungan Data Pribadi untuk pekerja non-redaksional di media khususnya dalam konteks Pengelolaan Sumber Daya Manusia

Metode: Pemaparan dan Tanya jawab

Durasi: 60 menit

Pokok Bahasan

4.2.1. Pemrosesan Data Pribadi dalam Pengelolaan Sumber Daya Manusia

Dalam hubungan ketenagakerjaan dan juga dalam aktivitas SDM, pihak yang terlibat adalah pemberi kerja dan orang perorangan yang memiliki kualitas calon, karyawan, atau mantan karyawan.

Jenis data, tujuan pemrosesan, dan dasar hukumnya harus dianalisis sesuai dengan tiga tahap yang ada dalam kegiatan SDM: a) perekrutan; b) perekrutan dan pelaksanaan kontrak; dan c) setelah pemutusan hubungan kerja

a. Perekrutan

Menurut Edwin B. Flippo, rekrutmen adalah "proses pencarian calon karyawan prospektif dan mendorong mereka untuk melamar pekerjaan di sebuah organisasi". Pada dasarnya, ini adalah proses mencari kandidat yang paling berkualifikasi untuk suatu pekerjaan yang terbuka, secara tepat waktu dan efektif secara biaya. Perusahaan kemudian dapat memilih pelamar dengan kualifikasi yang terkait dengan deskripsi pekerjaan. Rekrutmen sering dimulai ketika seorang manajer memulai permintaan karyawan (dokumen yang menentukan posisi/jabatan pekerjaan, departemen, tanggal karyawan dibutuhkan untuk bekerja, dan detail lainnya). Dengan informasi ini, manajer dapat merujuk ke deskripsi pekerjaan yang tepat

untuk menentukan kualifikasi yang diperlukan oleh orang yang direkrut. Langkah selanjutnya dalam proses rekrutmen adalah menentukan apakah karyawan yang berkualifikasi tersedia di dalam organisasi (sumber internal) atau apakah perlu mencari sumber eksternal, seperti perguruan tinggi, universitas, dan platform lainnya. Saat dilakukan secara internal, akses ke data pribadi sangat berguna. Basis data sumber daya manusia adalah perangkat rekrutmen berharga yang memungkinkan organisasi untuk menentukan apakah karyawan saat ini memiliki kualifikasi untuk mengisi posisi terbuka. Kandidat adalah subjek data karena mereka dapat diidentifikasi melalui data pribadi yang mereka berikan kepada perusahaan saat melamar pekerjaan. Seperti yang disebutkan sebelumnya, resume mereka mungkin mencakup nama, alamat, atau nomor telepon mereka.

Pertanyaan yang muncul secara alami adalah elemen wajib apa yang harus ada dalam resume atau data pribadi apa yang harus disediakan saat melamar pekerjaan. Hal ini bervariasi antar negara, tetapi umumnya elemen utama tetap sama: informasi pribadi (nama, alamat, dan informasi kontak), riwayat pekerjaan, dan pendidikan. Di beberapa negara, selama proses aplikasi, ada persyaratan untuk mengungkapkan layanan militer. Beberapa perusahaan lebih suka menggunakan formulir aplikasi standar daripada menerima resume dari pelamar. Alasannya bisa untuk menghindari menerima informasi yang tidak perlu atau penghilangan informasi yang merugikan bagi pelamar. **Meskipun begitu, dalam formulir aplikasi pekerjaan standar, pertanyaan yang berpotensi diskriminatif tentang faktor-faktor seperti jenis kelamin, ras, usia, catatan pidana, asal usul nasional, kewarganegaraan, tempat lahir, tanggungan, cacat, agama, warna kulit, dan status pernikahan harus dihindari.** Sebagai contoh, pemerintah Inggris melarang perekrut untuk menanyakan kepada pelamar tentang status pernikahan

mereka atau apakah mereka memiliki anak atau berencana untuk memiliki anak.

Selain itu, pertanyaan tentang kesehatan atau cacat hanya diperbolehkan jika:

a) ada persyaratan yang diperlukan dari pekerjaan yang tidak dapat dipenuhi dengan penyesuaian yang wajar,
b) untuk mengetahui apakah seseorang memerlukan bantuan untuk mengikuti tes seleksi atau wawancara, atau
c) dalam kasus 'tindakan positif' yang diambil untuk merekrut orang cacat.

Ada perdebatan besar tentang apakah harus menambahkan foto ke resume atau tidak. Di negara-negara seperti Irlandia, Inggris, dan Amerika Serikat, hukum anti-diskriminasi dan ketenagakerjaan yang ketat tidak mengizinkan penggunaan foto dalam resume. Oleh karena itu, perusahaan, sebagai langkah pencegahan, lebih suka tidak melihat foto kandidat yang menyertai aplikasi pekerjaan. Mereka menganggap bahwa fotografi bukanlah elemen wajib dalam tahap rekrutmen, kecuali untuk pekerjaan-pekerjaan di mana penampilan dan kondisi fisik karyawan sangat relevan (misalnya, presenter berita, pembawa acara TV, model, dan sebagainya). Dalam kasus lain, pemrosesan gambar kandidat tidak dapat dibenarkan dan dapat dianggap, sesuai keadaannya, sebagai penyalahgunaan atau diskriminatif. Selain itu, menentukan usia Anda adalah pisau bermata dua. Hal ini bisa menjadi masalah bagi pelamar pekerjaan yang dapat menjadi korban *ageism* (diskriminasi karena terlalu tua atau terlalu muda untuk pekerjaan tertentu) atau, di sisi lain, bisa bermanfaat dalam konteks praktik keberagaman dan inklusi organisasi. Menurut Pasal 10 dari GDPR, pengusaha tidak boleh memproses data pribadi yang berkaitan dengan pelanggaran atau

vonis pidana dari kandidat, kecuali ini merupakan syarat pekerjaan yang diberikan oleh hukum nasional atau Eropa.

Keanekaragaman di tempat kerja menjadi penting karena itu belum pernah terjadi sebelumnya secara historis. Keanekaragaman melampaui karakteristik demografis seperti usia, ras, atau jenis kelamin dan dapat didefinisikan sebagai pemahaman, penerimaan, dan penilaian perbedaan antara orang-orang dari ras, etnisitas, jenis kelamin, usia, agama, cacat, dan orientasi seksual yang berbeda, serta perbedaan dalam kepribadian, keterampilan, dan pendidikan. Selain itu, pengusaha dapat memproses data sensitif seperti etnis, usia, orientasi seksual, keyakinan spiritual, atau cacat sebagai bagian dari program pemantauan kesempatan yang sama. Selama fase rekrutmen, pengusaha memproses berbagai jenis data pribadi, seperti: data identitas (nama, nama belakang), rincian kontak (alamat rumah, alamat email, nomor telepon), data tentang karakteristik fisik dan/atau fisiologis (jenis kelamin, usia, gambar, suara), data tentang pendidikan (latar belakang pendidikan, studi, spesialisasi, sertifikasi), data tentang pengalaman profesional (pekerjaan sebelumnya, masa kerja), data lain yang disertakan oleh kandidat dalam resume dan/atau dokumen yang dikirim untuk melamar pekerjaan (surat rekomendasi/surat niat). Pemrosesan data yang disebutkan di atas bertujuan untuk proses rekrutmen sumber daya manusia di dalam organisasi pengontrol.

Yang terakhir namun tidak kalah pentingnya, pada tahap wawancara, kandidat dapat mengungkapkan data pribadi baru yang belum disebutkan sebelumnya dalam dokumen yang dikirimkan untuk seleksi. Pengontrol harus menyediakan pelindungan untuk informasi baru ini, meskipun disampaikan secara lisan dan tidak disimpan. Jika pengusaha telah melakukan *outsourcing* rekrutmen dan seleksi staf, ia harus memastikan

bahwa orang yang diotorisasi (perusahaan yang menyediakan layanan rekrutmen) memiliki jaminan tentang kepatuhan terhadap peraturan Pelindungan Data Pribadi. Dalam situasi khusus untuk tahap rekrutmen, direpresentasikan oleh pemrosesan data pribadi kandidat yang tidak terpilih oleh pengontrol data. Pengontrol data memiliki kewajiban untuk menghapus data kandidat yang tidak terpilih atau mendapatkan persetujuan jika ingin melakukan penyimpanan data mereka. Pengontrol dapat menghubungi orang yang bersangkutan jika dibutuhkan/ dibuka kembali proses perekrutan.

b. Pekerjaan dan Pelaksanaan Kontrak Kerja

Dalam menjalankan hubungan kerja, sebagai pengendali data, memproses data pribadi pekerja dengan volume yang besar dan bervariasi. Selain data yang dikumpulkan pada tahap sebelumnya, yaitu rekrutmen dan penyerahan kontrak kerja individu, selama pelaksanaan kontrak kerja individu, pengusaha dapat memproses informasi berikut: pengenal unik, seperti nomor induk kependudukan (NIK), nomor jaminan BPJS, seri kartu kerja, sampai nomor rekening perbankan, jumlah gaji, posisi dan pekerjaan, periode cuti, data kesehatan (informasi yang diperoleh dari pemeriksaan medis wajib, informasi yang dihasilkan dari izin sakit), gambar (diproses melalui sistem pengawasan internal), keanggotaan serikat pekerja, keyakinan agama (tergantung pada hal tersebut pengusaha memberikan karyawan beberapa hari libur) dan data lainnya. Bergantung pada objek kegiatan organisasi dan posisi yang dipegang oleh karyawan, berbagai kategori data pribadi akan diproses.

Dalam menjalankan hubungan kerja, pengusaha memproses data pribadi untuk tujuan-tujuan beragam, seperti: a) tujuan pemenuhan kewajiban dan penggunaan hak-hak tertentu di

bidang ketenagakerjaan, keamanan sosial, dan perlindungan sosial dalam konteks penyelesaian, pelaksanaan, dan penghentian kontrak kerja; b) tujuan pemenuhan kewajiban fiskal (pajak, bea, dan kontribusi) dari pengusaha atau, jika ada, karyawan; c) tujuan terkait pencegahan medis atau kerja kedokteran, penilaian kapasitas kerja karyawan atau kepatuhan dengan peraturan keselamatan dan kesehatan kerja; d) tujuan pembayaran gaji dan manfaat lain yang ditawarkan oleh pengusaha.

c. Setelah Pemutusan Hubungan Kerja

Setelah berakhirnya hubungan kerja, keperluan pemrosesan data pribadi mantan karyawan menjadi minimum, yang mana umumnya terbatas pada penyimpanan data yang ada dalam file personalia. Pengusaha dapat menghapus data pribadi dari file personalia atas inisiatifnya sendiri atau atas permintaan mantan karyawan, kecuali untuk data yang pengusaha memiliki kewajiban hukum untuk menyimpannya (misalnya, di Rumania, daftar gaji harus disimpan selama 50 tahun untuk menjamin kemungkinan perhitungan yang tepat dan perhitungan ulang pensiun). Satu aspek yang patut disebutkan adalah bahwa pengusaha harus memberi petunjuk kepada karyawan tentang cara memproses data pribadi dalam menjalankan aktivitas kerja, tetapi juga tentang kewajiban kerahasiaan yang dimiliki karyawan terkait data dan informasi yang pernah mereka akses dalam pelaksanaan kontrak kerja. Dengan demikian, kewajiban kerahasiaan dipenuhi karyawan baik selama periode kerja dan untuk jangka waktu yang sudah ditentukan setelah pengakhiran/ setelah ia tidak lagi memiliki status karyawan.

Referensi : Tataru, G. F., & Tataru, S. R. (Year). *Human Resources and Personal Data Protection: An Indissoluble Relationship. Journal*

of Public Administration, Finance and Law, diakses melalui: *https://www.researchgate.net/publication/348391095_HUMAN_RESOURCES_AND_PERSONAL_DATA_PROTECTION_AN_INDISSOLUBLE_RELATIONSHIP*

Modul 4.3. Pelindungan Data Pribadi dalam Kerja-kerja Pemasaran Media

Deskripsi

Kerja-kerja pemasaran merupakan bagian yang banyak terlibat dalam proses pengumpulan data pribadi, penyimpanan data pribadi, pengolahan data pribadi, penyajian data pribadi, dan penghancuran data tersebut. Ini karena pemasaran merupakan ujung tombak perusahaan media dalam berhubungan dengan konsumen media maupun dengan mitra media yang hendak beriklan atau bekerjasama. Untuk itu, pekerja pemasaran membutuhkan pengetahuan mengenai pelindungan data pribadi agar dapat bekerja sesuai dengan kaidah pelindungan data pribadi.

Tujuan

Pekerja pemasaran dapat menjalankan tugasnya berdasarkan prinsip-prinsip pelindungan data pribadi.

Metode: Presentasi dan tanya jawab

Durasi: 60 Menit

Pokok Bahasan

4.3.1. Kerja-kerja Pemasaran dan Kerja Sama dalam Kerangka Pelindungan Data Pribadi

Kerja-kerja pemasaran memainkan peran penting dalam pengelolaan data pribadi di sebuah media. *Marketing* banyak berurusan dengan departemen informasi dan teknologi. *Marketing* juga merupakan perwakilan media ketika berurusan dengan konsumen pembaca, terutama ketika sebuah media menggunakan model berlangganan atau mengumpulkan donasi dari konsumennya. Terlebih, laporan *Journalism, Media, and Technology Trends and Predictions* (*Reuters Institute dan University of Oxford,* 2024) menemukan bahwa penerbit menganggap sumber utama pendapatan adalah keanggotaan dan langganan digital (80 persen). Angka ini melebihi sumber dari penayangan iklan sebanyak 72 persen.

Untuk itu, ada sejumlah langkah teknis yang dibutuhkan dalam pengumpulan data pelanggan atau publik. Secara prinsip, proses pengumpulan membutuhkan persetujuan secara eksplisit dan implisit dan menunjukkan pemberitahuan pengumpulan data. Ketika pengumpulan data aktif, bagian pemasaran cukup membuat *profiling* data pribadi konsumen seperlunya. Artinya, bagian pemasaran perlu memastikan bahwa terdapat unsur persetujuan dan menunjukkan pemberitahuan pengumpulan data. Ini mencakup tujuan penggunaan data dan lama penyimpanan data yang akan dilakukan perusahaan media. Hal yang sama berlaku jika perusahaan media tidak menerapkan sistem berlangganan atau *paywall*. *Marketing* sebaiknya mengomunikasikan agar ada persetujuan di awal ketika konsumen mengunjungi laman media.

Dalam hal pemrosesan data pribadi, ada kalanya diperlukan keterlibatan pihak ketiga. Pihak ketiga ini bertugas melakukan

pengolahan data lebih rinci. Pihak ketiga ini bisa saja berasal dari luar yuridiksi Indonesia atau berada dalam yuridiksi Indonesia. Jika pihak ketiga ini berada dalam yuridiksi Indonesia, pekerja pemasaran perlu memastikan bahwa pihak ketiga tersebut akan bertindak untuk menjaga data pribadi dari kebocoran dan penggunaan yang di luar perjanjian dengan subjek data.

Jika pihak ketiga berada di luar yuridiksi Indonesia, pemasaran perlu memastikan bahwa, sebagaimana diatur dalam Pasal 56 ayat 2 UU PDP, "(2) Dalam melakukan transfer Data Pribadi sebagaimana dimaksud pada ayat (l), Pengendali Data Pribadi wajib memastikan negara tempat kedudukan Pengendali Data Pribadi dan/ atau Prosesor Data Pribadi yang menerima transfer Data Pribadi memiliki tingkat Pelindungan Data Pribadi yang setara atau lebih tinggi dari yang diatur dalam Undang-Undang ini." Selain itu, proses transfer data perlu memerhatikan Peraturan Pemerintah, yang hingga modul ini disusun belum diterbitkan.

Ketika bertemu dengan calon klien yang hendak memasang iklan atau mitra yang akan bekerjasama, pemasaran juga kerap harus meyakinkan pihak-pihak tersebut akan profil konsumen media. Untuk itu, data pribadi pengguna, termasuk profil sosiodemografi, mungkin perlu ditampilkan. Dalam hal ini, pekerja pemasaran perlu menyusun penampilan data secukupnya sesuai dengan kebutuhan.

Hal serupa juga berlaku jika di dalam proses pengungkapan data pribadi, sedapat mungkin menggunakan prinsip minimalisasi data, artinya data yang diungkapkan (*disclosed*) seminimum mungkin sejauh mencukupi proses pengungkapan yang dimandatkan. Pengungkapan data juga harus bersifat anonim.

Modul 4.4 Pelindungan Data Pribadi dalam Pengelolaan Media Sosial

Deskripsi

Akun media sosial sebuah perusahaan media merupakan bagian penting yang bertugas menyebarkan karya-karya jurnalistik. Data dari akun-akun media sosial media wajib mendapat pelindungan agar tidak disalahgunakan dan jatuh ke pihak lain.

Tujuan

Memberikan pemahaman pelindungan data pribadi bagi petugas media sosial.

Metode: Presentasi dan tanya jawab

Durasi: 60 menit

Pokok Bahasan

Selain bagian keuangan dan kerja sama, para pekerja media juga kerap melibatkan data pribadi ketika menggunakan gawai milik pribadi. Di media-media besar, kerja media mungkin dilakukan secara lebih profesional, semisal dari komputer kantor yang lebih aman. Akan tetapi, di media-media rintisan, kerja media kerap dilakukan dari telepon genggam atau komputer pribadi. Bahkan, beberapa menggunakan nomor telepon pribadi untuk verifikasi akun yang berkaitan dengan kantor, seperti akun media sosial.

April 2013, akun *Twitter Associated Press* mencuit adanya ledakan di Gedung Putih yang menyebabkan Presiden Barack Obama terluka. Dalam enam menit, indeks pasar saham *Dow Jones Industrial Average*

menunjukan adanya penurunan hingga 150 poin. Peretasan itu mengakibatkan pasar saham turun hingga USD 136 miliar atau Rp 2,135 triliun. Sebuah kelompok bernama *Syrian Electronic Army* mengklaim bertanggung jawab atas serangan tersebut[13].

4.4.1. Langkah Pengamanan Akun Media Sosial Perusahaan Media

Untuk itu, ada sejumlah prosedur yang sebaiknya dijalankan untuk mengamankan data dari akun-akun media sosial perusahaan. Pertama, sebaiknya petugas media sosial menggunakan gawai tersendiri untuk mengakses akun media sosial perusahaan. Gawai ini juga sebisa mungkin tidak digunakan untuk kegiatan-kegiatan lain guna mengurangi risiko. Jika langkah ini tidak memungkinkan, sebaiknya jumlah gawai yang dapat mengakses akun dibatasi. Perlu ada peraturan yang diberlakukan untuk petugas media sosial dalam menggunakan gawai tersebut. Di antaranya adalah larangan untuk menekan atau mengikuti tautan-tautan yang tidak diperlukaan dalam kerja-kerja pengelolaan media sosial sebuah perusahaan media. Selain itu, tidak diperbolehkan menginstal aplikasi tambahan yang dianggap tidak perlu dalam perangkat yang digunakan untuk mengakses akun media sosial.

Kedua, akses akun media sosial tidak menggunakan jaringan publik atau tempat-tempat umum seperti kafe. Ini karena jaringan publik rentan untuk memberikan akses pada peretas mencuri informasi pribadi dan menginstal perangkat lunak berbahaya (*mallicious software*) tanpa sepengetahuan pemilik akun.

Ketiga, seringkali penggunaaan kata sandi yang kuat tidaklah cukup. Untuk itu, akun media sosial perusahaan perlu menggunakan

[13] *AP Twitter account hacked in fake "White House blasts" post*. (2013, April 24). BBC News. https://www.bbc.com/news/world-us-canada-21508660

pengamanan autentikasi dua faktor. Autentikasi dua faktor akan menambah lapisan pengaman selain sandi. Verifikasi tambahan ini dapat berasal dari aplikasi lain, seperti *Google Authenticator*. Pilihan lain adalah penggunaan USB password manager. *Dongle* ini akan memastikan bahwa hanya mereka yang memegang *hardware* tersebut yang dapat mengakses akun media sosial perusahaan.

Keempat, aktifkan notifikasi masuk di semua akun. Ini akan membuat aktivitas *login* terpantau. Jika terdapat *login* yang mencurigakan, admin media sosial dapat segera melakukan pengamanan akun dengan mengganti sandi dan memastikan akses *login* yang mencurigakan sudah tidak dapat mengakses akun kembali.

Kelima, penggunaan VPN untuk mengakses media sosial. VPN dapat menyembunyikan jejak pemakai. Akan tetapi, kelemahan dari VPN ini adalah dibutuhkannya koneksi yang kuat. Untuk itu, sistem ini tidak efektif digunakan untuk lokasi-lokasi dengan jaringan yang buruk.

Keenam, tidak ada salahnya berinvestasi dengan membayar antivirus. Setelah menginstal antivirus, ada baiknya dilakukan pemindaian secara berkala untuk memastikan tidak ada virus.

4.4.2. Mitigasi Peretasan

Meskipun langkah-langkah tersebut sudah dilakukan, ada kalanya peretasan tetap terjadi. Berikut merupakan langkah-langkah yang disarankan jika terjadi peretasan atau pengambilalihan akun media sosial.

Pertama, jika terlacak adanya akses yang mencurigakan atau tidak diizinkan, sebaiknya petugas media sosial harus segera mengganti kata sandi. Penggantian kata sandi ini juga harus diikuti dengan aktivitas keluar dari gawai-gawai yang mencurigakan untuk

mengamankan akun. Jika akun sudah keluar dan diambil alih, usahakan untuk masuk ulang dengan klik tombol/ menu lupa kata sandi.

Kedua, umumkan jika terjadi peretasan sebelum akun media sosial dapat kembali diambil alih. Pengumuman dapat menggunakan *website* atau saluran lainnya. Pengumuman ini berfungsi untuk memastikan bahwa mencegah/ mengurangi risiko penipuan yang mengatasnamakan korban atau pihak yang diretas.

Ketiga, hubungi layanan yang digunakan. Penyedia media sosial memiliki dukungan layanan. Cara ini bisa ditempuh jika terjadi peretasan untuk memulihkan kembali akun.

Terakhir, tim pengelola media sosial perlu melakukan evaluasi jika terjadi kebocoran. Evaluasi ini bertujuan untuk mencegah persoalan serupa. Selain itu, evaluasi juga berguna untuk mencari titik yang dapat meningkatkan pelindungan data.

Didukung oleh:

PELINDUNGAN DATA PRIBADI DALAM JURNALISME DAN MEDIA

Jl. Palmerah Barat, Grogol Utara, Kec. Kby. Lama, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12210
E-mail : admin@amsi.or.id
Web : www.amsi.or.id