Versi 1.0

KERANGKA KERJA PRIVASI NIST: SEBUAH INSTRUMEN UNTUK MENINGKATKAN PRIVASI MELALUI MANAJEMEN RISIKO BISNIS, VERSI 1.0

16 Januari 2020

Publikasi ini tersedia secara gratis di:
https://doi.org/10.6028/NIST.CSWP.01162020id

National Institute of Standards and Technology
U.S. Department of Commerce

Ringkasan Kerangka Kerja EKSEKUTIF

Selama lebih dari dua dekade, internet dan teknologi informasi yang terkait telah mendorong inovasi, kemajuan ekonomi, dan peningkatan pelayanan sosial yang belum pernah terjadi sebelumnya. Banyak dari manfaat-manfaat tersebut didorong oleh data tentang individu yang mengalir melalui suatu ekosistem yang kompleks. Akibatnya, individu-individu mungkin tidak dapat memahami konsekuensi potensial untuk privasi mereka saat mereka berinteraksi dengan sistem, produk, dan layanan jasa. Pada saat yang sama, organisasi-organisasi mungkin tidak menyadari sepenuhnya konsekuensi ini bagi individu-individu, bagi masyarakat, maupun bagi organisasi-organisasi, yang dapat mempengaruhi merek-merek dagang mereka, keuntungan dasar, dan prospek-prospek pertumbuhan mereka di masa yang akan datang.

Melalui proses yang transparan, berbasis kesepakatan bersama termasuk baik pemangku kepentingan privat maupun publik untuk menghasilkan perangkat sukarela ini, *National Institute of Standards and Technology* (NIST) menerbitkan Kerangka Kerja Privasi: Sebuah Instrumen untuk Meningkatkan Privasi melalui Manajemen Risiko Bisnis, untuk memungkinkan praktek rekayasa privasi yang lebih baik yang mendukung privasi berdasarkan konsep desain dan membantu organisasi-organisasi dalam melindungi privasi individu. Kerangka Kerja Privasi dapat mendukung organisasi-organisasi dalam hal :

- Membangun kepercayaan pemakai konsumen dengan cara mendukung pengambilan keputusan secara etis dalam produk dan layanan jasa desain atau penerapan yang mengoptimalkan penggunaan data yang bermanfaat yang juga meminimalkan konsekuensi yang merugikan bagi privasi individu dan masyarakat secara keseluruhan;[1]
- Memenuhi kewajiban-kewajiban yang harus dipatuhi saat ini, serta produk-produk yang sesuai dengan masa depan dan layanan-layanan yang bisa memenuhi kewajiban-kewajiban dalam teknologi dan kebijakan lingkungan yang selalu berubah ; dan
- Memfasilitasi komunikasi tentang praktek privasi dengan para individu, mitra bisnis, penilai, dan regulator.

Memperoleh manfaat dari data sekaligus mengelola risiko secara simultan terhadap privasi individu tidak sesuai untuk bisa dipakai menjadi solusi atas semua permasalahan. Seperti membangun rumah, di mana pemilik rumah membuat pilihan tata letak dan desain sambil mengandalkan fondasi yang dibuat dengan baik, perlindungan privasi sebaiknya memungkinkan pilihan individu, selama mitigasi risiko privasi yang efektif sudah direncanakan ke dalam produk-produk dan layanan-layanan. Kerangka Kerja Privasi — melalui pendekatan berbasis risiko dan hasil — cukup fleksibel untuk menangani beragam kebutuhan privasi, memungkinkan solusi yang lebih inovatif dan efektif yang dapat memberikan hasil yang lebih baik bagi individu-individu dan organisasi-organisasi, dan tetap mengikuti tren-tren teknologi, seperti kecerdasan buatan (AI) dan *Internet of Things* (IoT).

Kerangka Kerja Privasi mengikuti struktur Kerangka Kerja untuk Meningkatkan Keamanan Infrastruktur Kritis Siber (Kerangka Kerja Keamanan Siber) [1] untuk memfasilitasi pemakaian kedua kerangka kerja secara bersamaan. Seperti juga Kerangka Kerja Keamanan Siber, Kerangka Kerja Privasi terdiri dari tiga bagian: Inti, Profil-Profil, dan Tingkat-Tingkat Implementasi. Setiap komponen memperkuat manajemen risiko atas privasi

[1] Tidak ada standar objektif untuk pengambilan keputusan secara etis; semua itu didasarkan pada norma, nilai, dan harapan hukum dalam masyarakat tertentu.

melalui hubungan antara penggerak bisnis dan misi organisasi, pemegang peran dan penanggung jawab organisasi, dan aktivitas-aktivitas perlindungan privasi.

- Inti memungkinkan sebuah dialog — dari level eksekutif hingga level penerapan/operasional — tentang pentingnya aktivitas perlindungan privasi dan hasil yang diinginkan.
- Profil-profil memungkinkan pengutamaan hasil dan aktivitas yang paling sesuai dengan nilai privasi organisasi, misi atau kebutuhan bisnis, dan risiko.
- Tingkat-tingkat Implementasi yang mendukung pengambilan keputusan dan komunikasi tentang kecukupan proses dan sumber daya organisasiorganisasi untuk mengelola risiko privasi.

Singkatnya, Kerangka Kerja Privasi dimaksudkan untuk membantu organisasi-organisasi membangun pondasi privasi yang lebih baik dengan membawa risiko privasi sejajar dengan portofolio dari risiko organisasi mereka yang lebih luas.

Ucapan Terima Kasih

Publikasi ini adalah hasil upaya kolaboratif antara NIST dan organisasi dan pemangku kepentingan baik organisasi di sektor publik dan privat. Dalam mengembangkan Kerangka Kerja Privasi, NIST mengandalkan tiga lokakarya publik, permintaan informasi atau *request for information* (RFI), permintaan komentar atau *request for comment* (RFC), lima webinar, dan ratusan interaksi langsung dengan pemangku kepentingan.[2] NIST mengucapkan terima kasih kepada semuanya yang telah berkontribusi dalam publikasi ini.

[2] Arsip pengembangan secara lengkap dapat ditemukan di https://www.nist.gov/privacy-framework .

Daftar Isi

Daftar Gambar

Daftar Tabel

1.0 Pengenalan Kerangka kerja Kerja Privasi

Selama lebih dari dua dasawarsa ini, internet dan teknologi informasi yang terkait telah mendorong inovasi, nilai ekonomi, dan akses ke layanan sosial yang belum pernah terjadi sebelumnya. Banyaknya manfaat ini didorong oleh *data tentang individu* yang mengalir melalui suatu ekosistem yang kompleks. Akibatnya, individu mungkin tidak dapat memahami konsekuensi potensial untuk privasi mereka saat mereka sedang berinteraksi dengan sistem, produk, dan layanan. Organisasi-organisasi mungkin juga tidak sepenuhnya menyadari akan konsekuensinya. Kegagalan untuk mengelola risiko privasi dapat menimbulkan konsekuensi merugikan langsung baik pada tingkat individu maupun masyarakat, dengan efek lanjutan pada merek-merek dagang organisasi, dasar organisasi, dan prospek-prospek pertumbuhan di masa yang akan datang. Menemukan cara untuk terus memperoleh manfaat dari *pemrosesan data* sekaligus melindungi privasi individu sangat menantang, dan tidak sesuai untuk menjadi solusi atas semua permasalahan.

Privasi itu menantang karena tidak hanya merupakan sebuah kesatuan konsep yang membantu melindungi nilai-nilai penting seperti otonomi dan martabat manusia, tetapi juga cara-cara untuk mencapai tujuannya yang bervariasi.[3] Misalnya, privasi dapat dicapai melalui dengan melakukan pengasingan, pengamatan terbatas, atau kontrol individu atas aspek identitas mereka (misalnya tubuh, data, dan reputasi).[4] Selain itu, otonomi dan martabat manusia juga bukan, konstruksi terukur yang tetap; mereka dapat disaring melalui keragaman budaya dan perbedaan individu. Sifat privasi yang luas dan berubah-ubah ini mempersulit komunikasi yang jelas mengenai risiko privasi, baik itu di dalam dan di antara organisasiorganisasi dengan individu. Hal yang hilang adalah keberadaan bahasa umum dan perangkat praktis yang cukup fleksibel untuk mengatasi beragamnya kebutuhan privasi.

Kerangka Kerja Privasi NIST sukarela (Voluntary NIST Privacy Framework) ini: Sebuah Perangkat untuk Meningkatkan Privasi melalui Manajemen Risiko (Kerangka Kerja Privasi) dimaksudkan agar dapat digunakan secara luas oleh organisasi-organisasi dari semua bidang dan ukuran teknologi, sektor, hukum, maupun yurisdiksi tertentu. Menggunakan sebuah pendekatan umum — yang dapat disesuaikan dengan setiap penggerak organisasi-organisasi manapun di dalam *ekosistem pemrosesan data* — yang mana tujuan Kerangka Kerja Privasi adalah untuk membantu organisasi-organisasi dalam mengelola risiko privasi dengan:

- Mempertimbangkan privasi saat mereka merancang dan menerapkan sistem-sistem, produk-produk, dan layanan-layanan yang berdampak pada [data pribadi] individu;
- Tata cara komunikasi tentang praktek privasi mereka; dan
- Mendorong kolaborasi tenaga kerja lintas organisasi-organisasi — misalnya, diantara para

[3] Otonomi dan martabat adalah konsep yang tercakup dalam Deklarasi Universal Hak Asasi Manusia (DUHAM), Perserikatan Bangsa-Bangsa yang dapat diakses melalui: https://www.un.org/en/universal-declaration-human-rights/

[4] Ada banyak publikasi yang memberikan gambaran mendalam tentang latar belakang privasi atau berbagai aspek konsep. Untuk dua contoh, lihat Solove D (2010) *Memahami Privasi* (Harvard University Press, Cambridge, MA), https://ssrn.com/abstract=1127888; dan Selinger E, Hartzog W (2017) Ketidakjelasan dan Privasi, *Ruang untuk Masa Depan: Pendamping Filsafat Teknologi,* eds Pitt J, Shew A (Taylor & Francis, New York, NY), Bab 12, 1st Ed., https://doi.org/10.4324/9780203735657.

eksekutif, hukum, dan teknologi informasi (TI) — melalui pengembangan profil-profil, pemilihan tingkatan-tingkatan, dan pencapaian berbagai macam hasil.

1.1 Gambaran Umum Kerangka Kerja Privasi

Seperti yang ditunjukkan pada **Gambar 1**, Kerangka Kerja Privasi terdiri dari tiga bagian, yaitu Inti, Profil-Profil, dan Tingkat-Tingkat Implementasi. Setiap komponen memperkuat bagaimana organisasi mengelola risiko privasi organisasimelalui hubungan antara penggerak bisnis atau misi organisasi, pemegang peran dan penanggung jawab organisasi, dan aktivitas-aktivitas perlindungan privasi. Sebagaimana dijelaskan lebih lanjut di bagian 2:

Gambar 1: Inti, Profil, dan Tingkat Implementasi

- *Inti* adalah sekumpulan aktivitas perlindungan privasi dan hasil yang memungkinkan untuk mengkomunikasikan prioritas kegiatan perlindungan privasi dan hasil pada seluruh elemen organisasi dari tingkat eksekutif ke tingkat implementasi / operasional. Inti selanjutnya dibagi menjadi Kategori dan Sub-kategori kunci— yang mempunyai hasil yang berlainan— untuk setiap masing-masing Fungsi.
- Sebuah *Profil* mewakili aktivitas-aktivitas privasi organisasi saat ini atau hasil-hasil yang diinginkan. Untuk mengembangkan Profil, sebuah organisasi dapat meninjau semua hasil dan aktivitas pada wilayah Inti untuk menentukan mana yang paling penting untuk difokuskan berdasarkan penggerak bisnis atau misi organisasi, peran ekosistem pemrosesan data, jenis pemrosesan data, dan kebutuhan privasi individu. Sebuah organisasi dapat membuat atau menambahkan Fungsi, Kategori, dan Sub-kategori sesuai kebutuhan. Profil dapat digunakan untuk mengidentifikasi peluang untuk meningkatkan sikap privasi dengan membandingkan Profil 'Saat Ini' (dengan status 'apa adanya') dengan Profil 'Target' (dengan status "menjadi"). Profil-profil dapat digunakan untuk melakukan penilaian diri pribadi dan untuk berkomunikasi dalam suatu organisasi atau antar organisasi tentang bagaimana risiko privasi dikelola.
- *Tingkat-tingkat Implementasi* menyediakan sebuah titik referensi tentang bagaimana sebuah organisasi memandang risiko privasi dan apakah hal ini sudah mempunyai proses dan sumber-sumber yang cukup ditempatkan pada manajemen risiko tersebut. Tingkatan-tingkatan ini mencerminkan kemajuan dari tanggapan yang informal, reaktif ke pendekatan yang cerdas dan risikonya terinformasi penuh. Saat memilih Tingkatan, organisasi harus mempertimbangkan Profil Targetnya dan bagaimana pencapaian dapat didukung atau dihambat oleh praktek manajemen risikonya saat ini, tingkat integrasi risiko privasi yang dimasukkan ke dalam portfolio manajemen risiko, hubungan ekosistem pemrosesan datanya, dan komposisi tenaga kerja dan program pelatihannya.

1.2 Manajemen Risiko Privasi

Meskipun beberapa organisasi memiliki pemahaman yang kuat tentang *manajemen risiko privasi, tapi* sebuah pemahaman umum dari banyak aspek dari topik ini masih belum tersebar luas.[5] Untuk mempromosikan pemahaman yang lebih luas, bagian ini mencakup konsep dan pertimbangan yang organisasi-organisasi mungkin bisa menggunakannya untuk mengembangkan, meningkatkan, atau mengkomunikasikan perihal manajemen risiko privasi. Lampiran D menyediakan informasi tambahan mengenai praktik kunci manajemen risiko privasi.

1.2.1 Manajemen Risiko Keamanan Siber dan Privasi

Sejak dirilis pada 2014, Kerangka Kerja Keamanan Siber telah membantu organisasi-organisasi untuk mengkomunikasikan dan mengelola risiko keamanan siber. [1] Meskipun pengelolaan risiko keamanan siber berkontribusi dalam mengelola risiko privasi, namun hal ini belum cukup karena risiko privasi juga dapat muncul dengan cara yang tidak terkait dengan *insiden keamanan siber,* seperti yang diilustrasikan pada **Gambar 2.** Memiliki pemahaman umum tentang asal usul keamanan siber yang berbeda-beda dan risiko privasi adalah hal yang penting untuk menentukan solusi paling efektif untuk mengatasi risiko.

Gambar 2: Hubungan Risiko Keamanan Siber dan Privasi

Tindakan Data

Siklus hidup data operasi, termasuk, tetapi tidak terbatas pada pengumpulan, penyimpanan, pencatatan, pembuatan , transformasi, pemakaian, pengungkapan rahasia, berbagi, transmisi, dan pembuangan.

Pengolahan data

Kumpulan kolektif tindakan data.

Pendekatan Kerangka Kerja Privasi ke risiko privasi adalah untuk pertimbangan *aktivitas privasi* sebagai potensi masalah yang dapat dialami individu yang timbul dari operasi sistem, produk, atau layanan dengan data, baik dalam bentuk digital maupun non digital, melalui siklus hidup lengkap dari pengumpulan data hingga penghapusannya.

Kerangka Kerja Privasi menjelaskan operasi-operasi data ini dalam bentuk tunggal sebagai *tindakan data* dan secara kolektif sebagai pemrosesan data. Masalah-masalah yang dapat dialami individu sebagai hasil dari pemrosesan data dapat diungkapkan dengan berbagai cara, tetapi NIST menggambarkannya mulai dari dampak tipe alamiah seperti rasa malu atau stigma hingga bahaya yang lebih nyata seperti diskriminasi, kerugian ekonomi, atau cedera fisik.[6]

Dasar dari masalah yang mungkin dialami individu dapat bervariasi. Seperti yang digambarkan dalam **Gambar 2,** masalah muncul sebagai efek merugikan dari pemrosesan data yang dilakukan organisasi-organisasi untuk memenuhi misi atau tujuan bisnis mereka. Contohnya adalah kekhawatiran yang dimiliki komunitas tertentu tentang pemasangan “pengukur

[5] Lihat *Ringkasan Analisis Tanggapan atas Permintaan Kerangka Kerja Privasi NIST untuk Informasi* [2] di hal. 7.

[6] NIST telah membuat katalog ilustrasi masalah untuk digunakan dalam penilaian risiko privasi. Lihat *Metodologi Penilaian Risiko Privasi NIST* [3]. Organisasi Organisasi lain mungkin telah menciptakan kategori masalah lain, atau mungkin menyebutnya sebagai konsekuensi atau bahaya yang merugikan.

pintar" sebagai bagian dari Jaringan Listrik Pintar (*Smart Grid*), sebuah upaya nasional pengembangan teknologi untuk meningkatkan efisiensi energi.[7] Kemampuan pengukur ini untuk mengumpulkan, mencatat, dan mendistribusikan informasi yang sangat terperinci tentang pemakaian listrik rumah tangga yang dapat memberikan wawasan tentang perilaku orang di dalam rumahnya.[8] Meteran tersebut beroperasi sebagaimana dimaksud, tetapi pemrosesan datanya dapat menyebabkan seseorang merasa diawasi.

Dalam dunia yang semakin terhubung, beberapa masalah dapat muncul hanya dari interaksi individu dengan berbagai sistem, produk, dan layanan, bahkan ketika data yang sedang diproses tidak secara langsung terkait dengan identifikasi individu. Misalnya, teknologi kota-kota pintar atau "*smart cities*" dapat digunakan untuk mengubah atau mempengaruhi perilaku orang seperti di mana atau bagaimana mereka bergerak di kota tersebut.[9] Berbagai masalah juga bisa muncul, dimana terdapat *hilangnya kerahasiaan, integritas,* atau *ketersediaan* di beberapa titik dalam pemrosesan data, seperti pencurian data oleh peretas eksternal atau akses ilegal atau pemakaian data yang tidak sah oleh karyawan. **Gambar 2** menunjukkan berbagai jenis peristiwa privasi yang berhubungan dengan keamanan siber mengalami tumpang tindih antara privasi dan risiko keamanan siber.

Saat sebuah organisasi dapat mengidentifikasi kemungkinan masalah tertentu yang timbul dari pemrosesan data, dimana Kerangka Kerja Privasi merujuk kepada *tindakan data bermasalah,* hal itu dapat meninjau dampak yang seharusnya terjadi dari tindakan data yang bermasalah tersebut. Peninjauan dampak dimana risiko privasi dan risiko organisasi saling berhubungan. Individu-individu, baik sendiri atau berkelompok – (termasuk di tingkat masyarakat) - mengalami dampak langsung dari masalah-masalah. Sebagai akibat dari masalah yang dialami individu, sebuah organisasi mungkin mengalami dampak seperti biaya ketidakpatuhan, kerugian pendapatan yang timbul dari pengabaian produk dan layanan oleh pemakai , atau keterpurukan reputasi merek dagang eksternal atau budaya internal. Organisasi-organisasi biasanya mengelola jenis dampak ini di tingkat manajemen risiko bisnis; dengan menghubungkan masalah yang dialami individu ke dampak yang dipahami secara lebih baik pada organisasi, organisasi-organisasi dapat membawa risiko privasi menjadi seimbang dengan risiko lain yang mereka kelola dalam portofolio mereka yang lebih luas dan mendorong pengambilan keputusan yang lebih tepat tentang alokasi sumber daya untuk memperkuat program privasi. **Gambar 3** menggambarkan hubungan antara risiko privasi dan risiko organisasi.

[7] Lihat, misalnya, NIST Interagency atau Laporan Internal (IR) 7628 Revisi 1 Volume 1, *Panduan untuk Keamanan Siber Jaringan Cerdas: Volume 1 - Strategi Keamanan Siber Jaringan Cerdas, Arsitektur, dan Persyaratan Tingkat Tinggi* di [4] halaman. 26.

[8] Lihat NIST IR 8062, *Pengantar Rekayasa Privasi dan Manajemen Risiko dalam Sistem Federal* di [5] hal. 2. Untuk jenis risiko privasi tambahan yang terkait dengan efek merugikan pada pemrosesan data individu, lihat Lampiran E dari NIST IR 8062.

[9] Lihat Newcombe T (2016) Masalah Keamanan, Privasi, Tata Kelola Tentang Teknologi Kota Cerdas Berkembang. *Teknologi Pemerintah.* Tersedia di http://www.govtech.com/Security-Privacy-Governance-Concerns-About-Smart-City-Technologies-Grow.html .

Gambar 3: Hubungan Antara Risiko Privasi dan Risiko Organisasi

1.2.2 Penilaian Risiko Privasi

Manajemen risiko privasi adalah rangkaian proses lintas organisasi yang membantu organisasi-organisasi untuk memahami bagaimana sistem, produk, dan layanan mereka mungkin menimbulkan masalah bagi individu dan bagaimana mengembangkan solusi efektif untuk mengelola risiko. *Peninjauan risiko privasi* adalah sub-proses untuk mengidentifikasi dan mengevaluasi risiko privasi tertentu. Secara umum, peninjauan risiko privasi menghasilkan informasi yang dapat membantu organisasi-organisasi untuk menimbang manfaat dari pemrosesan data terhadap risiko dan untuk menentukan respons yang tepat — terkadang disebut sebagai proporsionalitas.[10] Organisasi-organisasi dapat memilih untuk memprioritaskan dan menanggapi risiko privasi dengan cara yang berbeda, tergantung pada potensi dampaknya bagi individu-individu dan dampak akhir bagi organisasi-organisasi. Beberapa pendekatan respon meliputi:[11]

- Meringankan risiko (misalnya, organisasi-organisasi mungkin dapat menerapkan langkah-langkah teknis dan/atau kebijakan pada berbagai sistem, produk, atau layanan yang meminimalkan risiko ke tingkat yang dapat diterima);
- Mentransfer atau membagi risiko (misalnya, kontrak-kontrak adalah cara untuk membagi atau mentransfer risiko ke organisasi-organisasi lain, pemberitahuan privasi dan mekanisme persetujuan adalah cara membagi risiko dengan berbagai individu);
- Menghindari risiko (misalnya, organisasi-organisasi dapat menentukan bahwa risiko lebih besar daripada keuntungan-keuntungan yang akan didapat, dan membatalkan atau menghentikan pemrosesan data); atau
- Menerima risiko (misalnya, organisasi-organisasi dapat mempertahankan masalah bagi individu seminimal mungkin atau seperti tidak mungkin terjadi, oleh karena itu manfaatnya lebih besar daripada risikonya, dan tidak perlu menginvestasikan sumber daya dalam mitigasi).

[10] Lihat Pengawas Perlindungan Data Eropa (2019) *Kebutuhan & Proporsionalitas.* Tersedia di https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en.

[11] Lihat Publikasi Khusus NIST (SP) 800-39, *Mengelola Risiko Keamanan Informasi: Tampilan Organisasi-Organisasi, Misi, dan Sistem Informasi* [6].

Penilaian-penilaian risiko privasi sangat penting karena, seperti disebutkan di atas, privasi adalah kondisi yang melindungi berbagai nilai. Metode untuk melindungi nilai-nilai ini mungkin berbeda, terlebih lagi, mungkin saling berlawanan satu sama lain. Berdasarkan pada tujuannya, jika suatu organisasi mencoba mendapatkan privasi dengan membatasi observasi, hal ini dapat mengarah pada penerapan langkah-langkah seperti arsitektur data yang terdistribusi atau teknik kriptografi yang meningkatkan privasi dengan menyembunyikan data bahkan dari organisasi tersebut. Jika sebuah organisasi juga mencoba mengaktifkan kontrol individu, tindakan tersebut dapat menimbulkan konflik. Misalnya, jika seorang individu meminta akses ke data, organisasi mungkin tidak dapat menyediakan data, jika data tersebut telah didistribusikan atau dienkripsi dengan cara yang tidak dapat diakses oleh organisasi. Penilaian risiko privasi bisa membantu organisasi mengerti nilai keadaan seperti apa yang harus dilindungi, metode apa yang harus digunakan, dan bagaimana menyeimbangkan implementasi dari berbagai tipe ukuran.

Terakhir, penilaian risiko privasi membantu organisasi-organisasi membedakan antara risiko privasi dan risiko kepatuhan. Mengidentifikasi apakah pemrosesan data dapat menimbulkan masalah bagi individu, bahkan ketika organisasimungkin sudah sepenuhnya mematuhi undang-undang atau peraturan yang berlaku, dapat membantu pengambilan keputusan secara etis dalam sistem, produk, dan layanan desain atau penyebaran data. Meskipun tidak ada standar objektif untuk pengambilan keputusan secara etis, hal itu didasarkan pada norma, nilai, dan harapan hukum dalam masyarakat secara alamiah. Hal ini memfasilitasi pengoptimalan pemakaian data yang bermanfaat sekaligus meminimalkan konsekuensi yang merugikan bagi privasi individu dan masyarakat secara keseluruhan, serta menghindari hilangnya kepercayaan yang merusak reputasi organisasi, lambatnyapenyesuaian, atau menyebabkan ditinggalkannya produk dan layanan.

Lihat Lampiran D untuk informasi lebih lanjut mengenai aspek operasional penilaian risiko privasi.

1.3 Ringkasan Dokumen

Sisa dari dokumen ini berisi bagian dan lampiran berikut:

- **Bagian 2** menjelaskan komponen-komponen Kerangka Kerja Privasi: Inti, Profil-profil, dan Tingkat-tingkat Implementasi.
- **Bagian 3** menyajikan contoh-contoh bagaimana Kerangka Kerja Privasi dapat digunakan.
- **Bagian Referensi** mencantumkan daftar referensi untuk dokumen tersebut.
- **Lampiran A** menyajikan Inti Kerangka Kerja Privasi Inti dalam format tabel: Fungsi, Kategori, dan Subkategori.
- **Lampiran B** berisi daftar istilah-istilah yang terpilih.
- **Lampiran C** mencantumkan akronim-akronim yang digunakan dalam dokumen ini.
- **Lampiran D** mempertimbangkan praktik utama yang berkontribusi pada manajemen risiko privasi yang sukses.
- **Lampiran E** mendefinisikan tingkat-tingkat Implementasi.

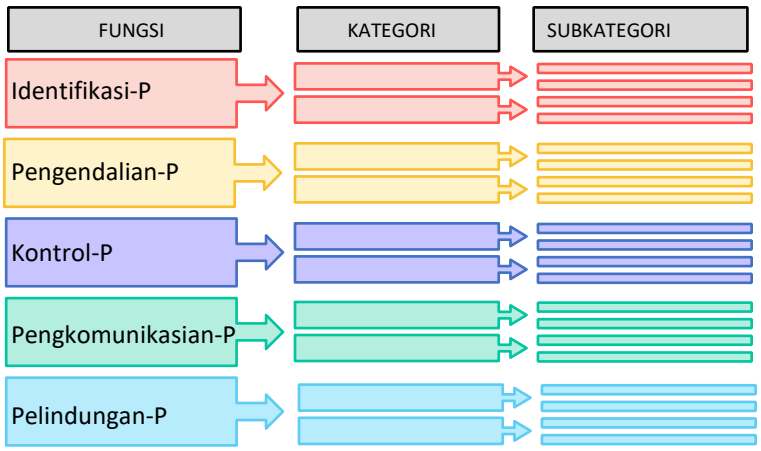
2.0 Dasar-dasar Kerangka Kerja Privasi

Kerangka Kerja Privasi menyediakan bahasa umum untuk memahami, mengelola, dan mengkomunikasikan risiko privasi dengan pemangku kepentingan internal dan eksternal. Ini dapat disesuaikan dengan pemegang peran organisasi manapun dalam ekosistem pemrosesan data. Hal ini dapat digunakan untuk membantu mengidentifikasi dan memprioritaskan tindakan untuk mengurangi risiko privasi, dan hal ini juga adalah perangkat untuk menyelaraskan pendekatan kebijakan, bisnis, dan

teknologi untuk mengelola risiko.

2.1 Inti

Berangkat dari Lampiran A, Inti menyediakan meningkatnya serangkaian aktivitas dan hasil yang semakin terperinci yang memungkinkan dialog tentang pengelolaan risiko privasi. Seperti yang digambarkan dalam **Gambar 4,** Inti terdiri dari Fungsi-Fungsi, Kategori-Kategori, dan Subkategori-Subkategori.



Gambar 4: Struktur Inti Kerangka Kerja Privasi

Elemen-elemen Inti bekerja bersama:

- *Fungsi-fungsi* mengatur pondasi aktivitas privasi di level tertingginya. Mereka membantu organisasi dalam mengekspresikan manajemen risiko privasinya dengan pemahaman dan pengelolaan pemrosesan data, memungkinkan pengambilan keputusan *manajemen risiko*, menentukan bagaimana interaksi dengan individu, dan meningkatkan kapasitas dengan belajar dari aktivitas sebelumnya. Mereka tidak dimaksudkan untuk membentuk jalur yang bertahap atau mengarah ke keadaan akhir yang diinginkan tapi statis. Sebaliknya, Fungsi harus dilakukan secara bersamaan dan terus menerus untuk membentuk atau meningkatkan budaya operasional yang bisa mengatasi sifat dinamis dari risiko privasi.

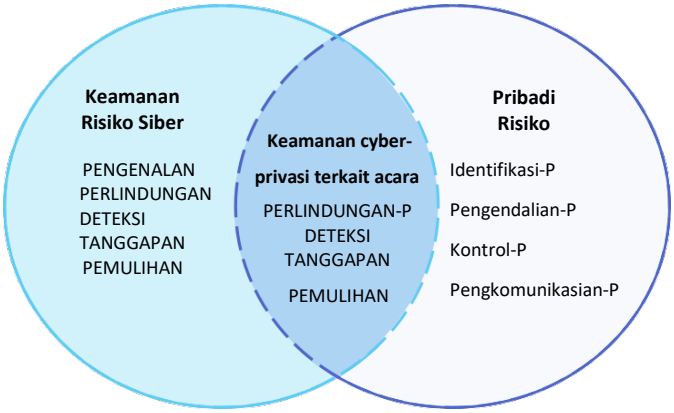
- *Kategori* adalah subdivisi dari suatu Fungsi ke dalam grup hasil dari privasi yang terkait erat dengan kebutuhan terprogram dan aktivitas tertentu.

- *Subkategori* membagi lebih lanjut suatu Kategori menjadi hasil khusus dari aktivitas-aktivitas teknis dan/atau manajemen. Mereka memberikan serangkaian hasil, yang meski tidak lengkap, membantu mendukung pencapaian hasil di setiap Kategori.

Lima Fungsi, Pengidentifikasian-P, Pengendalian-P, Pengontrolan-P, Pengkomunikasian-P, dan Perlindungan-P, yang didefinisikan di bawah ini, dapat digunakan untuk mengelola risiko privasi yang timbul dari pemrosesan data.[12] Perlindungan-P secara khusus berfokus pada pengelolaan risiko yang terasosiasi dengan peristiwa keamanan siber yang terkait dengan peristiwa privasi (misalnya, *pelanggaran privasi).* Kerangka Kerja Keamanan Siber, meski dimaksudkan untuk mencakup semua jenis insiden keamanan siber, bisa dimanfaatkan untuk lebih mendukung manajemen risiko yang berhubungan dengan peristiwa keamanan siber yang terkait privasi dengan menggunakan Fungsi Deteksi, Respon, dan Pemulihan.

[12] "-P" di akhir setiap nama Fungsi menunjukkan bahwa itu berasal dari Kerangka Kerja Privasi untuk menghindari kebingungan dengan Fungsi Kerangka Kerja Keamanan Siber.

Alternatifnya organisasi-organisasi dapat menggunakan, kelima dari Fungsi Kerangka Kerja Keamanan Siber dalam hubungannya dengan Pengidentifikasian-P, Pengendalian-P, Pengontrolan-P, Pengkomunikasian-P, dan Perlindungan-P, untuk secara kolektif menangani risiko privasi dan keamanan siber. **Gambar 5** menggunakan diagram Venn dari bagian 1.2.1 untuk mendemonstrasikan bagaimana Fungsi-Fungsi dari kedua kerangka kerja dapat digunakan dalam berbagai kombinasi untuk mengelola berbagai aspek privasi dan risiko keamanan siber. Kelima Fungsi Kerangka Kerja Privasi tersebut didefinisikan sebagai berikut:



Gambar 5: Menggunakan Fungsi untuk Mengelola Keamanan Siber dan Risiko-risiko Privacy

- *Pengidentifikasian-P* - Mengembangkan pemahaman organisasi untuk mengelola risiko privasi bagi individu yang timbul dari pemrosesan data.

  Aktivitas di Fungsi Pengidentifikasian-P adalah dasar untuk pemakaian Kerangka kerja Privasi yang efektif. Menginventarisir keadaan data yang mana yang diproses, memahami kepentingan privasi individu yang secara langsung atau tidak langsung dilayani atau dipengaruhi oleh organisasi, dan melakukan penilaian risiko yang memungkinkan organisasi untuk memahami lingkungan bisnis di mana mereka beroperasi dan mengidentifikasi serta memprioritaskan risiko privasi.

- *Pengendalian-P* - Mengembangkan dan menerapkan struktur tata kelola organisasi untuk memungkinkan pemahaman berkelanjutan tentang prioritas manajemen risiko organisasi yang diinformasikan oleh risiko privasi.

  Fungsi Pengendalian-P memiliki dasar yang sama, tetapi berfokus pada aktivitas-aktivitas tingkat organisasi seperti menetapkan nilai dan kebijakan privasi organisasi, mengidentifikasi persyaratan hukum/ peraturan, dan memahami *risiko toleransi* yang memungkinkan organisasi untuk bisa fokus dan memprioritaskan upayanya, sesuai dengan strategi manajemen risiko dan kebutuhan bisnisnya.

- *Pengontrolan-P* - Mengembangkan dan menerapkan aktivitas-aktivitas yang sesuai yang memungkinkan organisasi atau individu mengelola data dengan perincian yang memadai untuk mengelola risiko privasi.

  Fungsi Pengontrolan-P mempertimbangkan manajemen pemrosesan data dari sudut pandang organisasi-organisasi dan individu-individu.

- *Pengkomunikasian-P* - Mengembangkan dan menerapkan aktivitas yang sesuai untuk memungkinkan organisasi dan individu memiliki pemahaman yang dapat diandalkan dan terlibat dalam dialog tentang bagaimana data diproses dan risiko privasi yang terkait..

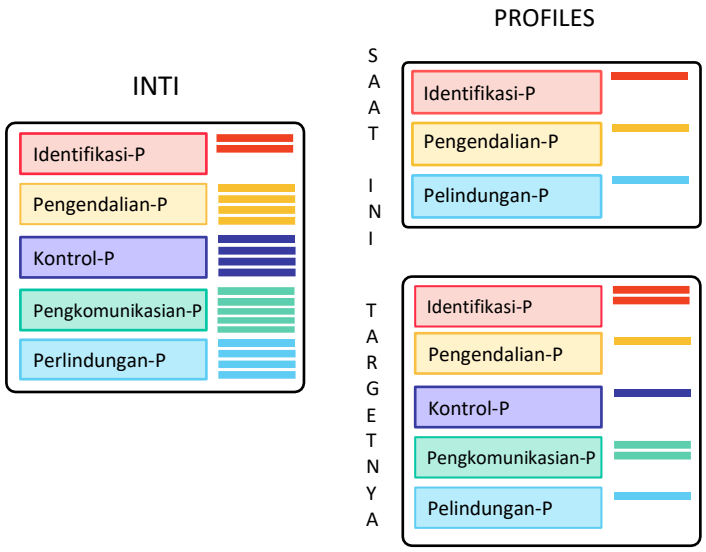
  Fungsi Pengkomunikasian-P mengakui bahwa organisasi dan individu mungkin perlu mengetahui bagaimana data diproses untuk bisa mengelola risiko privasi secara efektif.

- *Perlindungan-P* - Mengembangkan dan menerapkan pengamanan pemrosesan data yang sesuai.

  Fungsi Perlindungan-P mencakup perlindungan data untuk mencegah peristiwa privasi terkait keamanan siber, tumpang tindih antara privasi dan manajemen risiko keamanan siber

2.2 Profil-Profil

Profil-Profil adalah pilihan dari Fungsi, Kategori, dan Subkategori tertentu dari Inti yang telah diprioritaskan oleh organisasi untuk membantu mengelola risiko privasi. Profil-Profil dapat digunakan untuk mendeskripsikan status saat ini dan status target yang diinginkan dari aktivitas privasi tertentu. Profil Saat Ini menunjukkan hasil-hasil privasi yang sedang dicapai organisasi, sedangkan Profil Target menunjukkan hasil yang diperlukan untuk mencapai tujuan-tujuan manajemen risiko privasi yang diinginkan. Perbedaan antara kedua Profil ini memungkinkan organisasi untuk mengidentifikasi kesenjangan yang ada, mengembangkan rencana tindakan untukperbaikan, dan mengukur sumber daya yang akan dibutuhkan (misalnya, staf, pendanaan) untuk mencapai hasil privasi. Hal ini membentuk dasar rencana organisasi untuk mengurangi beban biaya efektif terhadap risiko privasi, dan memprioritaskan persoalan. Profil-profil juga bisa membantu risiko dalam berkomunikasi didalam dan diantara organisasi-organisasi dengan cara membantu organisasi mengerti dan bisa membandingkan hasil privasi yang ada sekarang dan yang diharapkan Kerangka Kerja Privasi tidak menentukan satu model Profil untuk Profil yang memungkinkan penerapan yang fleksibel.



Gambar 5: Hubungan antara Inti dan Profil

Di bawah pendekatan berbasis risiko Kerangka Kerja Privasi, organisasi mungkin tidak perlu mencapai setiap hasil atau aktivitas yang tercerminkan dalam Intinya. Saat mengembangkan Profil, organisasi dapat memilih atau menyesuaikan Fungsi, Kategori, dan Subkategori untuk kebutuhan spesifiknya, termasuk mengembangkan tambahan Fungsi, Kategori, dan Subkategorinya sendiri untuk memperhitungkan risiko unik organisasi tersebut. Sebuah organisasi menentukan kebutuhan ini dengan mempertimbangkan misi atau tujuan bisnis, nilai-nilai privasi, dan toleransi risiko; peran dalam ekosistem pemrosesan data atau sektor industri; persyaratan hukum atau peraturan dan praktik terbaik industri; prioritas dan sumber daya manajemen risiko; dan kebutuhan privasi individu yang secara langsung atau tidak langsung dilayani atau dipengaruhi oleh sistem, produk, atau layanan organisasi.

Seperti yang diilustrasikan dalam **Gambar 6,** tidak ada urutan khusus untuk pengembangan Profil. Sebuah organisasi pertama-tama dapat mengembangkan Target dari Profil untuk fokus pada hasil yang diinginkan untuk privasi, kemudian mengembangkan Profil Saat Ini untuk mengidentifikasi kesenjangan; alternatifnya, sebuah organisasi dapat memulai dengan mengidentifikasi aktivitasnya saat ini, dan kemudian mempertimbangkan bagaimana menyesuaikan aktivitas tersebut untuk Profil Targetnya. Sebuah organisasi dapat memilih untuk mengembangkan beberapa Profil untuk peran, sistem, produk, atau layanan yang berbeda, atau kategori individu (misalnya, karyawan, pemakai) untuk memungkinkan

prioritas yang lebih baik dari kegiatan dan hasil di mana mungkin ada tingkat risiko privasi yang berbeda. Organisasi-organisasi di sektor industri tertentu atau dengan peran serupa dalam ekosistem pemrosesan data dapat berkoordinasi untuk mengembangkan Profil bersama.

2.3 Tingkat-Tingkat Implementasi

'Tingkatan-tingkatan (tiers)' mendukung pengambilan keputusan organisasi tentang bagaimana mengelola risiko privasi dengan mempertimbangkan sifat risiko privasi yang ditimbulkan oleh sistem, produk, atau layanan organisasi, kecukupan proses, dan sumber daya yang dimiliki organisasi untuk mengelola risiko tersebut. Saat menyusun Tingkatan, sebuah organisasi harus mempertimbangkan Profil Targetnya dan bagaimana pencapaian dapat didukung atau dihambat oleh praktik manajemen risiko saat ini,tingkatan integrasi risiko privasi ke dalam portofolio usaha manajemen risiko, hubungan dengan ekosistem pemrosesan datanya, dan komposisi tenaga kerja, serta program pelatihannya.

Ada empat konsep Tingkatan-Tingkatan (tiers) yang berbeda, Parsial (Tingkat 1), Risiko dari Informasi(Tingkat 2), Pengulangan (Tingkat 3), dan Adaptif (Tingkat 4) - penjelasannya ada di Lampiran E. Tingkatan mewakilikemajuan, meskipun bukan merupakan sebuah kewajiban. Meskipun organisasi di Tingkat 1 kemungkinan akan mendapat manfaat dari perpindahan ke Tingkat 2, tidak semua organisasi perlu mencapai Tingkat 3 atau 4 (atau mungkin hanya fokus pada area tertentu dari Tingkat-Tingkat ini). Kemajuan ke Tingkat yang lebih tinggi bisa sesuai bila pada saat proses atau sumber daya organisasi pada Tingkat saat ini mungkin tidak cukup untuk membantu mengelola risiko privasinya.

Suatu organisasi dapat menggunakan Tingkatan-tingkatan untuk berkomunikasi secara internal tentang alokasi sumber daya yang diperlukan untuk peningkatan ke Tingkat yang lebih tinggi atau sebagai tolok ukur umum untuk mengukur kemajuan dalam kemampuannya untuk mengelola risiko privasi. Sebuah organisasi juga dapat menggunakan Tingkatan-tingkatan untuk memahami skala sumber daya dan proses dari organisasi lain dalam ekosistem pemrosesan data dan bagaimana mereka selaras dengan prioritas pengelolaan risiko privasi organisasi tersebut. Meskipun demikian, keberhasilan implementasi Kerangka Kerja Privasi didasarkan pada pencapaian hasil yang dijelaskan dalam Profil Target organisasi, bukan pada penentuan Tingkatan.

3.0 Bagaimana Menggunakan Kerangka Kerja Privasi

Sebagai instrumen manajemen risiko, Kerangka Kerja Privasi dapat membantu sebuah organisasi dalam mengoptimalkan manfaat pemakaian data dan pengembangan sistem, produk, dan layanan inovatif sekaligus meminimalkan konsekuensi yang merugikan individu. Kerangka Kerja Privasi dapat membantu organisasi menjawab pertanyaan mendasar tentang, "Bagaimana kami mempertimbangkan dampaknya terhadap individu saat kami mengembangkan sistem, produk, dan layanan kami?" Untuk memperhitungkan kebutuhan unik suatu organisasi, pemakaian Kerangka Kerja Privasi bersifat fleksibel, meskipun dirancang untuk melengkapi bisnis yang sudah ada dan pengembangan sistem operasi. Keputusan tentang bagaimana penerapannya sepenuhnya diserahkan kepada organisasi pelaksana. Misalnya, organisasi mungkin sudah memiliki proses manajemen risiko privasi yang kuat, tetapi dapat menggunakan lima Fungsi Inti sebagai cara yang singkat untuk menganalisis dan mengartikulasikan setiap celah. Alternatifnya, sebuah organisasi yang ingin membuat program privasi, dapat menggunakan Kategori dan Subkategori Inti sebagai referensi. Organisasi-organisasi lain dapat membandingkan Profil-profil atau Tingkatan-tingkatan untuk menyelaraskan prioritas manajemen risiko privasi di berbagai peran dalam ekosistem pemrosesan data. Berbagai cara dimana Kerangka Kerja Privasi dapat digunakan oleh berbagai organisasi seharusnya bisa mencegah masalah yang berkaitan dengan 'kepatuhan pada Kerangka

Kerja Privasi' sebagai konsep yang seragam atau dapat dijadikan referensi eksternal. Subbagian berikutnya menyajikan beberapa opsi untuk penggunaan Kerangka Kerja Privasi.

3.1 Memetakan ke Referensi Informatif

Referensi informatif adalah pemetaan ke Subkategori untuk memberikan dukungan implementasi, termasuk pemetaan instrumen-instrumen, panduan teknis, standar, hukum, peraturan dan praktik terbaik. Persilangan yang memetakan ketentuan standar, hukum dan peraturan ke dalam Subkategori dapat membantu organisasi-organisasi menentukan kegiatan atau hasil mana yang diprioritaskan untuk memfasilitasi kepatuhan tersebut. Kerangka Kerja Privasi adalah teknologi yang netral, tetapi mendukung inovasi teknologi karena organisasi atau sektor industri manapun dapat mengembangkan pemetaan ini seiring dengan perkembangan kebutuhan teknologi dan bisnis yang terkait. Dengan mengandalkan standar, pedoman, dan praktik berbasis konsensus, instrumen dan metode yang tersedia untuk mencapai hasil privasi yang positif dapat diperluas lintas batas dan mengakomodasi sifat global yang alamiah dari risiko privasi. Pemakaian standar yang ada dan yang akan muncul memungkinkan untuk memperluas skala ekonomi dan mendorong pengembangan sistem, produk, dan layanan yang memenuhi kebutuhan pasar yang tertentu serta memperhatikan kebutuhan-kebutuhan privasi individu-individu.

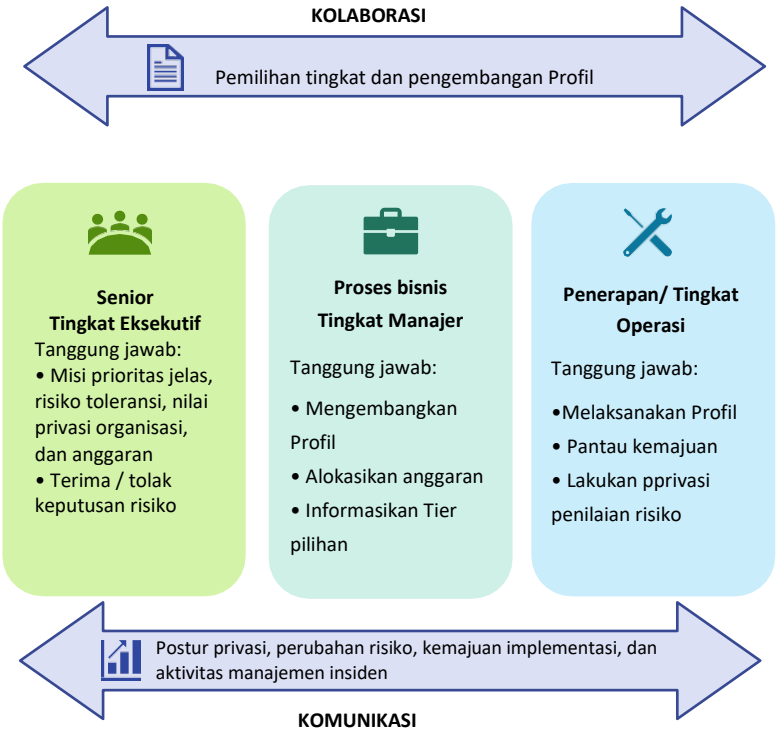
Kesenjangan dalam pemetaan juga dapat digunakan untuk mengidentifikasi dimana standar-standar, pedoman-pedoman, dan praktik-praktik tambahan atau yang sudah direvisi akan membantu organisasi untuk menangani kebutuhan mendesak yang muncul. Sebuah organisasi yang menerapkan Sub Kategori tertentu, atau mengembangkan Subkategori baru, mungkin akan menemukan bahwa ada panduan yang tidak memadai untuk aktivitas atau hasil yang terkait. Untuk memenuhi kebutuhan itu, sebuah organisasi mungkin berkolaborasi dengan para pemimpin di bidang teknologi dan/atau organisasi standar untuk menyusun, mengembangkan, dan mengkoordinasikan standar, pedoman, atau praktik.

Repositori referensi informatif dapat diperoleh melalui https://www.nist.gov/privacy-framework. Sumber ini dapat mendukung pemakaian Kerangka Kerja Privasi oleh organisasi dan pencapaian praktik privasi yang lebih baik.

3.2 Memperkuat Akuntabilitas

Akuntabilitas umumnya dianggap sebagai sebuah kunci dari prinsip privasi, meskipun secara konseptual tidak hanya unik untuk privasi.[13] Akuntabilitas terjadi di seluruh organisasi, dan dapat diekspresikan pada berbagai tingkat perpindahan, misalnya sebagai sebuah nilai budaya, kebijakan pemerintahan dan prosedur-prosedur, atau sebagai hubungan yang bisa dilacak antara *persyaratan* dan *kontrol privasi.*

Manajemen risiko privasi dapat menjadi sarana untuk mendukung akuntabilitas di semua tingkat organisasi karena menghubungkan para eksekutif senior - yang dapat mengkomunikasikan nilai-nilai privasi dan risiko yang dapat ditoleransi - kepada mereka yang berada di tingkat manajer bisnis/ pelaksana, yang bisa berkolaborasi dalam pengembangan dan implementasi kebijakan-kebijakan kepemimpinan dan prosedur-prosedur yang mendukung nilai-nilai privasi organisasi. Kebijakan dan prosedur ini kemudian dapat dikomunikasikan kepada mereka yang berada di tingkat implementasi/operasional, yang berkolaborasi dalam menentukan persyaratan privasi yang mendukung bentuk kebijakan dan prosedur dalam sistem, produk, dan layanan organisasi. Pekerja di level implementasi/ operasional juga memilih, menerapkan, dan mengakses kontrol-kontrol sebagai tindakan teknis dan kebijakan untuk memenuhi persyaratan privasi, dan melaporkan kemajuan, kesenjangan dan kekurangan, manajemen insiden, serta mengubah risiko privasi hingga mereka di level manajer bisnis/pelaksana dan para eksekutif senior dapat lebih memahami dan merespons dengan tepat.



Gambar 7: Kolaborasi Nosional dan Arus Komunikasi Dalam Organisasi

Gambar 7 memberikan sebuah gambaran grafis dari komunikasi dan kolaborasi dua arah dan bagaimana elemen Kerangka Kerja Privasi dapat digabungkan untuk memfasilitasi proses. Dengan cara ini, organisasi-organisasi dapat menggunakan Kerangka Kerja Privasi sebagai instrumen untuk mendukung akuntabilitas. Mereka juga dapat menggunakan Kerangka Kerja Privasi dalam hubungannya dengan kerangka kerja dan panduan lain yang dapat memberikan praktik tambahan untuk mencapai

[13] Lihat, misalnya, Organisation for Economic Co-operation and Development (OECD) (2013) *Panduan OECD tentang Perlindungan Privasi dan Arus Lintas Batas Data Pribadi,* Tersedia di https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm; Organisasi Internasional untuk Standardisasi (ISO) / Komisi Elektroteknik Internasional (IEC) (2011) *ISO / IEC 29100: 2011 - Teknologi informasi - Teknik keamanan - Kerangka kerja kerja privasi (*ISO, Jenewa, Swiss), tersedia di https://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip ; dan Alliance of Automobile Manufacturers, Inc., Association of Global Automakers, Inc. (2014) *Prinsip Perlindungan Privasi Konsumen: Prinsip Privasi untuk Teknologi dan Layanan Kendaraan,* Tersedia di https://autoalliance.org/wp-content / uploads / 2017/01 / Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf .

akuntabilitas di dalam dan di antara organisasi-organisasi.[14]

3.3 Menyusun atau Meningkatkan Program Privasi

Dengan menggunakan model sederhana "sedia, siap, jalan", Kerangka Kerja Privasi dapat mendukung pembuatan program privasi baru atau peningkatan program yang sudah ada. Saat sebuah organisasi melewati fase-fase ini, organisasi tersebut dapat menggunakan referensi informatif untuk memberikan panduan dalam memprioritaskan atau mencapai hasil-hasil. Lihat bagian 3.1 untuk informasi lebih lanjut tentang referensi informatif. Informasi tambahan dan referensi dapat ditemukan di https://www.nist.gov/privacy-framework .

Bersedia

Manajemen risiko privasi yang efektif membutuhkan organisasi untuk memahami misi atau lingkungan bisnisnya; lingkungan hukumnya; toleransi risikonya; dan berbagai risiko privasi yang ditimbulkan oleh sistem, produk, atau layanannya; dan perannya dalam ekosistem pemrosesan data. Sebuah organisasi dapat menggunakan Fungsi Pengidentifikasian-P dan Pengendalian-P untuk "bersedia" dengan meninjau Kategori dan Subkategori, dan mulai mengembangkan Profil Saat Ini dan Profil Target.[15] Kegiatan dan hasil seperti menetapkan nilai dan kebijakan privasi organisasi, menentukan dan mengungkapkan toleransi risiko organisasi, dan melakukan penilaian risiko privasi (lihat Lampiran D untuk informasi lebih lanjut tentang penilaian risiko privasi) memberikan dasar untuk melengkapi Profil di level "Siap" dibawah ini.

Metode Sederhana untuk Membangun atau Meningkatkan Program Privasi

Sedia: gunakan Fungsi Identifikasi-P dan Pengendalian-P untuk bersedia."

Siap: "Bersiap" rencana tindakan berdasarkan perbedaan antara Saat ini dan Profil Target.

Jalan: "Maju jalan" dengan menerapkan tindakan rencana.

Bersiap

Sebuah organisasi melengkapi Profil Saat Ini dengan menunjukkan hasil Kategori dan Subkategori apa dari Fungsi yang tersisa yang sedang dicapai. Jika suatu hasil tercapai sebagian, maka fakta ini akan mendukung langkah selanjutnya dengan memberikan informasi Dasar. Diinformasikan oleh aktivitas di bawah Identifikasi danKepemimpinan, seperti nilai dan kebijakan privasi organisasi, toleransi risiko organisasi, dan hasil penilaian risiko privasi, sebuah organisasi melengkapi Profil Targetnya dengan berfokus pada penilaian Kategori dan Subkategori yang menjelaskan hasil privasi yang diinginkan. Sebuah organisasi juga dapat mengembangkan Fungsi, Kategori, dan Subkategori tambahannya sendiri untuk memperhitungkan risiko organisasi yang unik. Hal ini juga dapat mempertimbangkan pengaruh dan persyaratan pemangku kepentingan eksternal seperti pemakai bisnis dan mitra saat membuat Profil Target. Suatu organisasi dapat mengembangkan beberapa Profil untuk mendukung berbagai lini bisnis atau prosesnya, yang mungkin memiliki kebutuhan bisnis yang berbeda dan kaitannya dengan risiko yang bisa ditoleransi.

[14]Lihat, misalnya, NIST SP 800-37, Rev.2, *Kerangka kerja Kerja Manajemen Risiko untuk Sistem Informasi dan Organisasi: Pendekatan Siklus Hidup Sistem untuk Keamanan dan Privasi* [7]; dan Organisasi untuk Kemajuan Standar Informasi Terstruktur (OASIS) (2016) Model Referensi dan Metodologi Manajemen Privasi (PMRM) Versi 1.0, https://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.pdf .

[15] Untuk informasi tambahan, lihat langkah "Mempersiapkan", Bagian 3.1, NIST SP 800-37, Rev. 2 [7].

Sebuah organisasi membandingkan Profil Saat Ini dan Profil Target untuk menentukan kesenjangan di antara keduanya. Selanjutnya, organisasi tersebut membuat rencana tindakan yang diprioritaskan untuk mengatasi kesenjangan — seperti mencerminkan pembawa misi bisnis, biaya dan manfaat, serta risiko — untuk mencapai hasil dalam Profil Target. Sebuah organisasi yang menggunakan Kerangka Kerja Keamanan Siber dan Kerangka Kerja Privasi bersama-sama dapat mengembangkan rencana tindakan yang terintegrasi. Yang kemudian, menentukan sumber daya, termasuk pendanaan dan kebutuhan tenaga kerja yang diperlukan untuk mengatasi kesenjangan, yang dapat menginformasikan pemilihan Tingkatan yang sesuai. Pemakaian Profil dengan cara ini mendorong sebuah organisasi untuk membuat keputusan yang tepat tentang aktivitas privasi, mendukung manajemen risiko, dan memungkinkan sebuah organisasi untuk melakukan perbaikan dengan biaya yang hemat dan peningkatan yang sesuai dengan target.

Berjalan

Dengan konsep rencana tindakan 'bersedia', sebuah organisasi memprioritaskan tindakan mana yang harus diambil untuk mengatasi setiap kesenjangan, dan kemudian menyesuaikan praktik privasi saat ini untuk mencapai Profil Target.[16]

Suatu organisasi dapat melalui fase-fase yang tidak berhubungan langsung sesuai kebutuhan untuk terus menilai dan meningkatkan postur privasinya. Misalnya, sebuah organisasi mungkin menemukan bahwa pengulangan fase 'bersedia' lebih sering meningkatkan kualitas penilaian risiko privasi. Selain itu, organisasi dapat memantau kemajuan melalui pembaharuan berulang-ulang pada Profil Saat Ini atau Profil Target untuk menyesuaikan dengan risiko yang berubah, kemudian membandingkan Profil Saat Ini dengan Profil Target.

3.4 Menerapkan Siklus Hidup Pengembangan Sistem

Profil Target dapat diselaraskan dengan fase siklus hidup pengembangan sistem atau "*System Development Life Cycle*" (SDLC) dari rencana, desain, pembuatan/pembelian, penerapan, pengoperasian, dan penonaktifan untuk mendukung pencapaian hasil privasi yang diprioritaskan.[17] Dimulai dengan 'fase rencana', hasil privasi yang diprioritaskan dapat diubah menjadi kemampuan dan persyaratan privasi untuk sistem, dengan menyadari bahwa persyaratan cenderung akan berkembang selama sisa siklus hidup. Tonggak penting dari 'fase desain' adalah mensahkan kapabilitas dan persyaratan privasi yang sesuai dengan kebutuhan dan risiko yang bisa ditoleransi dari organisasi seperti yang dinyatakan dalam Profil Target. Profil Target yang sama dapat berfungsi sebagai daftar internal untuk dinilai saat 'fase menerapkan' sistem untuk memverifikasi bahwa semua kemampuan dan persyaratan privasi diterapkan. Hasil privasi yang ditentukan dengan menggunakan Kerangka Kerja Privasi kemudian harus berfungsi sebagai dasar untuk 'fase pengoperasian' sistem yang sedang berjalan. Hal ini termasuk penilaian ulang pada waktu-waktu tertentu, menangkap hasil di Profil Saat Ini, untuk memverifikasi bahwa kemampuan dan persyaratan privasi masih terpenuhi.

Penilaian risiko privasi biasanya berfokus pada siklus hidup data, tahapan yang dilalui data, seringkali digolongkan dalam bentuk fase aktivitas pembuatan atau pengumpulan, pemrosesan, penyebaran,

[16] NIST SP 800-37, Rev. 2 [7] memberikan informasi tambahan tentang langkah-langkah untuk melaksanakan rencana tindakan, termasuk pemilihan kontrol, implementasi, dan penilaian untuk menutup setiap celah.

[17] Di dalam SDLC, organisasi dapat menggunakan berbagai metodologi pengembangan (misalnya air terjun, spiral, atau gesit).

pemakaian, penyimpanan, danpenempatan, termasuk fase aktivitas penghancuran dan penghapusan. Menyelaraskan SDLC dan siklus hidup data dengan mengidentifikasi dan memahami bagaimana data diproses selama semua tahapan SDLC membantu organisasi untuk mengelola risiko privasi dengan lebih baik dan menginformasikan pemilihan dan penerapan kontrol privasi untuk memenuhi persyaratan privasi.

3.5 Pemakaian dalam Ekosistem Pemrosesan Data

Faktor kunci dalam pengelolaan risiko privasi adalah peran entitas dalam ekosistem pemrosesan data, yang dapat mempengaruhi tidak hanya kewajiban hukumnya, tetapi juga tindakan yang mungkin diambil untuk mengelola risiko privasi. Seperti yang digambarkan dalam **Gambar 8,** ekosistem pemrosesan data mencakup serangkaian entitas dan peran yang mungkin memiliki multi-arah yang kompleks hubungannya satu sama lain dan individu-individu. Kompleksitas dapat meningkat saat entitas didukung oleh rantai sub-entitas; misalnya, penyedia layanan mungkin didukung oleh serangkaian penyedia layanan lainnya, atau produsen mungkin memiliki beberapa penyedia-penyedia komponen lainnya. **Gambar 8** menampilkan entitas yang memiliki peran yang berbeda, tetapi beberapa mungkin memiliki peran yang beragam, seperti sebuah organisasi yang menyediakan layanan untuk organisasi lain dan menyediakan produk ritel untuk konsumen. Peran dalam **Gambar 8** dimaksudkan sebagai konsep klasifikasi abstrak. Dalam praktiknya, peran entitas dapat dikodifikasi secara hukum — misalnya, beberapa peraturan perundang-undangan mengklasifikasikan organisasi-organisasi sebagai pengendali data atau prosesor data — atau klasifikasi dapat diturunkan dari penunjukan sektor industri.

Gambar 6 Hubungan-Hubungan Ekosistem Pemrosesan Data

Dengan mengembangkan satu atau lebih Profil yang relevan dengan perannya, suatu entitas dapat menggunakan Kerangka Kerja Privasi untuk mempertimbangkan cara mengelola risiko privasi tidak hanya terkait dengan prioritasnya sendiri, tetapi juga dalam kaitannya dengan bagaimana pengukuran dapat mempengaruhi manajemen risiko privasi dari entitas ekosistem pemrosesan data yang lain. Sebagai contoh:

- Sebuah organisasi yang membuat keputusan tentang cara pengumpulan dan pemakaian data tentang individu dapat menggunakan Profil untuk menyatakan persyaratan privasi kepada penyedia layanan eksternal (misalnya, penyedia cloud tempat ia mengunggah data); penyedia layanan eksternal yang memproses data dapat menggunakan profilnya untuk mendemonstrasikan tindakan yang diadopsi untuk memproses data sesuai dengan kewajiban kontrak.

- Suatu organisasi dapat menyatakan postur privasinya melalui Profil Saat Ini untuk melaporkan

hasil atau untuk membandingkan dengan persyaratan akuisisi.

- Sektor industri dapat membuat Profil umum yang dapat digunakan oleh anggotanya untuk menyesuaikan Profil mereka sendiri.

- Sebuah industri manufaktur dapat menggunakan Profil Target untuk menentukan kemampuan untuk membangun produknya sehingga pemakai bisnisnya dapat memenuhi kebutuhan privasi pengguna akhir.

- Penyedia/pengembang teknologi dapat menggunakan Profil Target untuk mempertimbangkan bagaimana merancang aplikasi yang memungkinkan perlindungan privasi saat digunakan dalam lingkungan sistem organisasi lain.

Kerangka Kerja Privasi menyediakan bahasa umum untuk mengomunikasikan persyaratan privasi dengan entitas dalam ekosistem pemrosesan data. Khususnya kebutuhan akan komunikasi ini sangat penting ketika ekosistem pemrosesan data melintasi batas nasional, seperti dengan transfer data internasional. Praktik-praktik organisasi yang mendukung komunikasi seperti ini dapat mencakup:

- Menentukan persyaratan privasi;

- Memberlakukan persyaratan privasi melalui perjanjian formal (misalnya, kontrak, kerangka kerja multi-pihak);

- Mengomunikasikan bagaimana persyaratan privasi tersebut akan diverifikasi dan divalidasi;

- Memverifikasi bahwa persyaratan privasi dipenuhi melalui berbagai metodologi penilaian; dan

- Mengatur dan mengelola kegiatan-kegiatan di atas ini.

3.6 Menginformasikan Proses Pengambilan Keputusan Untuk Pembelian

Karena baik Profil Saat Ini atau Profil Target dapat dipakai untuk membuat daftar prioritas dari persyaratan privasi, profil-profil ini juga dapat digunakan untuk menginformasikan keputusan berkenaan dengan pembelian produk atau pemakaian layanan. Dengan terlebih dahulu memilih hasil yang cocok dengan tujuan privasinya, selanjutnya organisasi kemudian dapat melakukan evaluasi pada sistem, produk, atau layanan mitra dari hasil ini. Contohnya, jika sebuah perangkat dibeli untuk pemantauan terhadap pemanfaatan hutan, *kemampuan untuk pengelolaan* penting untuk mendukung kemampuan meminimalkan pemrosesan data tentang orang-orang yang menggunakan hutan tersebut, dan mendorong evaluasi manufaktur perangkat berkaitan dengan sub kategori yang ada pada Inti (misalnya, CT.DP-P4: konfigurasi sistem atau perangkat memperbolehkan pengumpulan atau pengungkapan yang selektif dari *elemen-elemen data).*

Dalam keadaan yang tidak memungkinkan untukmemberlakukan prioritas untuk persyaratan privasi pada penyedia, maka tujuannya seharusnya agar pembuatan keputusan untuk pembelian berdampak baik pada para penyedia barang, dengan mempertimbangkan daftar persyaratan privasi yang ditentukan. Seringkali, hal ini berarti ada beberapa saatkemungkinan pilihan-pilihan yang mana lebih baik, membandingkan beberapa produk atau layanan dengan jaraknya diketahui terhadap Profil. Jika sistem, produk, atau layanan yang dibeli tidak memenuhi semua tujuan yang dijelaskan dalam Profil, organisasi dapat mengatasi risiko yang tertinggal dengan melakukan tindakan mitigasi atau penanganan lainnya.

Referensi

1) Institut Nasional Standar dan Teknologi (2018) Kerangka Kerja untuk Meningkatkan Keamanan Siber Infrastruktur Kritis, Versi 1.1. (Institut Nasional Standar dan Teknologi, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018
2) Institut Nasional Standar dan Teknologi (2019) Analisis Ringkasan Tanggapan terhadap Permintaan Kerangka Kerja Privasi NIST untuk Informasi. (Institut Nasional Standar dan Teknologi, Gaithersburg, MD). https://www.nist.gov/sites/default/files/documents/2019/02/27/rfi_response_analysis_privacyframework_2.27.19.pdf
3) Institut Nasional Standar dan Teknologi (2019) NIST Privacy Risk Assessment Methodology (PRAM). (Institut Nasional Standar dan Teknologi, Gaithersburg, MD). https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources
4) Panel Interoperabilitas Smart Grid — Smart Grid Cybersecurity Committee (2014) Panduan untuk Keamanan Siber Smart Grid: Volume 1 - Strategi, Arsitektur, dan Persyaratan Tingkat Tinggi Smart Grid. (Institut Nasional Standar dan Teknologi Gaithersburg, MD), NIST Antar Lembaga atau Laporan Internal (IR) 7628, Rev. 1, Vol. 1. https://doi.org/10.6028/NIST.IR.7628r1
5) Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017) Pengantar Teknik Privasi dan Manajemen Risiko dalam Sistem Federal. (Institut Nasional Standar dan Teknologi, Gaithersburg, MD), NIST Antar Lembaga atau Laporan Internal (IR) 8062. https://doi.org/10.6028/NIST.IR.8062
6) Joint Task Force Transformation Initiative (2011) Mengelola Risiko Keamanan Informasi: Tampilan Organisasi, Misi, dan Sistem Informasi. (Institut Nasional Standar dan Teknologi, Gaithersburg, MD). Publikasi Khusus NIST (SP) 800-39. https://doi.org/10.6028/NIST.SP.800-39
7) Satuan Tugas Bersama (2018) Kerangka Kerja Manajemen Risiko untuk Sistem Informasi dan Organisasi: Pendekatan Siklus Hidup Sistem untuk Keamanan dan Privasi. (Institut Nasional Standar dan Teknologi, Gaithersburg, MD), Publikasi Khusus NIST (SP) 800-37 Rev.2. https://doi.org/10.6028/NIST.SP.800-37r2.
8) Grassi PA, Garcia ME, Fenton JL (2017) Pedoman Identitas Digital. (Institut Nasional Standar dan Teknologi, Gaithersburg, MD), Publikasi Khusus NIST (SP) 800-63-3, Termasuk pembaruan per 1 Desember 2017. https://doi.org/10.6028/NIST.SP.800-63
9) Office of Management and Budget (2017) Mempersiapkan dan Menanggapi Pelanggaran Informasi Identitas Pribadi. (Gedung Putih, Washington, DC), OMB Memorandum-17-12, 3 Januari 2017. Tersedia di https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf
10) Joint Task Force Transformation Initiative (2013) Kontrol Keamanan dan Privasi untuk Sistem dan Organisasi Informasi Federal. (Institut Nasional Standar dan Teknologi, Gaithersburg, MD), Publikasi Khusus NIST (SP) 800-53, Rev. 4, Termasuk pembaruan per Januari 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4
11) Grassi PA, Lefkovitz NB, Nadeau EM, Galluzzo RJ, Dinh AT (2018) Atribut Metadata: Skema yang Diusulkan untuk Mengevaluasi Atribut Federasi. (Institut Nasional Standar dan Teknologi, Gaithersburg, MD), NIST Antar Lembaga atau Laporan Internal (IR) 8112.

https://doi.org/10.6028/NIST.IR.8112

12) Joint Task Force Transformation Initiative (2012) Guide for Conducting Risk Assessment. (Institut Nasional Standar dan Teknologi, Gaithersburg, MD), Publikasi Khusus NIST (SP) 800-30, Rev.1. https://doi.org/10.6028/NIST.SP.800-30r1

13) "Definisi," Judul 44 *Kode AS,* Detik. 3542. 2011 ed.

https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44-chap35- subchapIII-sec3542

Lampiran A: Inti Kerangka Kerja Privasi

Dalam lampiran ini menjelaskan Inti: sebuah tabel dari fungsi-fungsi, kategori-kategori, dan subkategori-subkategori yang mendeskripsikan aktivitas-aktivitas dan hasil-hasil spesifik yang dapat membantu dalam pelaksanaan dan manajemen risiko, saat sistem, produk, dan layanan sedang memproses data.

Catatan Untuk Para Pengguna

Pendekatan berbasis risiko:

- **Sebuah Inti tidak hanya sebuah daftar tindakan-tindakan untuk bekerja. Sebuah organisasi memilih subkategori yang konsisten dengan strategi risiko dalam perlindungan data privasi individu sesuai dengan deskripsi kategori**. Sebuah organisasi mungkin tidak perlu meraih setiap hasil atau melakukan aktivitas yang tergambar pada Inti. Hal ini diharapkan sebuah organisasi akan menggunakan profil untuk memilih dan memprioritaskan Fungsinya, Kategori, dan Subkategori yang memenuhi kebutuhan spesifiknya dengan mempertimbangkan tercapainya tujuan-tujuan ,peran-perannya dalam ekosistem pemrosesan data atau sektor industri, legalitas/persyaratan hukum danpraktik terbaik industri, prioritas dalam manajemen risiko, dan keperluan privasi dari individu yang secara langsung maupun tidak langsung terlayani atau terdampak oleh sebuah sistem, produk, dan pelayanan organisasi.

- Bukan sebuah kewajiban untuk meraih hasil secara keseluruhan. Suatu organisasi dapat menggunakan Profil-profilnya untuk menggambarkan sebuah pencapaian sebagian dari suatu hasil, karena tidak semua aspek hasil mungkin relevan untuk mengelola risiko privasi, atau sebuah organisasi yang mungkin menggunakan Profil Target yang dapat menggambarkan sebuah aspek hasil yang sebenarnya tidak memiliki kemampuan untuk mencapainya.

- Mungkin perlu untuk mempertimbangkan beberapa hasil dari kombinasi untuk mengelola risiko privasi dengan benar dan tepat. Contoh, sebuah organisasi yang merespon pada sebuah permintaan individu-individu untuk melakukan akses pada data dapat memilih pada profilnya diantara Subkategori CT.DM-P1: "Elemen-elemen data dapat diakses untuk ditinjau" dan Kategori "Manajemen Identitas, Keaslian, dan Kontrol Akses" (PR.AC-P) untuk memastikan bahwa hanya individu yang terkait dengan data yang sesuai untuk mendapatkan akses yang diminta.

Implementasi: Format tabel dari Inti tidak cenderung menyarankan sebuah ketertiban implementasi spesifik atau menyiratkan tahapan dari pentingnya antara Fungsi-fungsi, Kategori-kategori, dan Subkategori-subkategori. Pada saat Implementasinya mungkin saja tidak terlalu penting, simultan, atau berulang, tergantung pada tahap SDLC, status program privasi, skala tenaga kerja, atau pemegang peran organisasi dalam ekosistem pemrosesan data. Sebagai tambahan, Inti tidak seharusnya menyeluruh, ia dapat diperluas, memungkinkan organisasi-organisasi, sektor-sektor, dan entitas-entitas lain untuk menyesuaikan atau menambahkan Fungsi, Kategori, dan Subkategori ke Profil mereka.

Beberapa Peran:

- **Peran-peran ekosistem**: Inti dimaksudkan agar dapat digunakan oleh suatu organisasi atau entitas terlepas dari perannya dalam ekosistem pemrosesan data. Meskipun

Kerangka Kerja privasi tidak mengklasifikasikan peran ekosistem, sebuah organisasi harus meninjau Inti dalam sudut pandang ekosistem. Peran organisasi dapat dikodifikasi secara hukum - misalnya, beberapa undang-undang mengklasifikasikan organisasi-organisasi sebagai pengontrol atau pemroses data - atau klasifikasi-klasifikasi dapat diturunkan dari ciri khas industri. Karena pada elemen-elemen Inti tidak ditetapkan oleh peran ekosistem,sebuah organisasi dapat menggunakan Profilnya untuk memilih Fungsi, Kategori, dan Subkategori yang sesuai dengan perannya.

- **Peran Organisasi**: Bagian berbeda dari tenaga kerja pada organisasi mungkin mengambil tanggung jawab dari Kategori atau Sub kategori yang berbeda. Misalnya, departemen legal mungkin bertanggung jawab dalam pelaksanaan aktivitas di bawah "Kebijakan, Proses, dan Prosedur Tata Kelola" sementara departemen Teknologi Informasi (TI) mengemban tugas untuk "Inventaris dan Pemetaan". Idealnya, Inti mendorong kolaborasi lintas organisasi untuk pengembangan Profil dan hasil-hasil pencapaian.

Perluasan: Dalam aspek-aspek tertentu memungkinkan lahirnya sebuah kata yang memiliki arti beberapa (ambigu). Contohnya, istilah “dikomunikasikan” atau “diungkapkan” dengan tidak menyertakan kepada siapa kata-kata tersebut dilontarkan. Ketidakjelasan arti ini disengaja untuk skala yang luas bagi organisasi-organisasi dengan berbagai kasus yang berbeda untuk menentukan hal apa yang tepat atau dibutuhkan dalam sebuah konteks tertentu.

Sumber: Tulisan yang berdiri sendiri ini merupakan Inti yang bersumber dari https://www.nist.gov/privacy-framework.

Penjelasan peraturan keamanan siber:

- Seperti yang sebelumnya telah disebutkan pada bagian 2.1, organisasi-organisasi dapat menggunakan lima dari fungsi kerangka kerja privasi, antara lain, Pengidentifikasian-P, Pengendalian-P, Pengontrolan-P, Pengkomunikasian-P, dan Perlindungan-P, dengan mengatur risiko privasi yang timbul saat pemrosesan data. Perlindungan-P ini secara khusus memiliki fokus pada pengaturan dari risiko yang memiliki hubungan dengan keamanan keprivasian. (contohnya, pelanggaran pada privasi seseorang). Untuk lebih jauh mendukung pengaturan risiko yang berkaitan dengan kegiatan keamanan privasi, sebuah organisasi bisa memilih tiga fungsi antara lain yaitu: Deteksi, Respon, dan Pemulihan fungsi pada Kerangka Kerja Keamanan Siber. Dengan alasan ini, ketiga fungsi ini dapat dilihat pada **tabel 1** berwarna abu-abu. Alternatifnya, organisasi-organisasi dapat menggunakan semua dari kelima fungsi keamanan siber yang berhubungan dengan Pengidentifikasian-P, Pengendalian-P, Pengontrolan-P, Pengkomunikasian-P, dan Perlindungan-P, secara bersamaan berfokus pada risiko privasi dan keamanan. Bisa dilihat pada **gambar ke 5** sebagai contoh ilustrasi mengenai bagaimana Fungsi-fungsi dari kedua kerangka kerja dapat digunakan dalam berbagai kombinasi untuk mengatur aspek-aspek yang berbeda dari privasi dan risiko-risiko keamanan siber.

- Fungsi, Kategori, dan Subkategori tertentu memiliki suatu hal yang identik yang dapat diadaptasi dari kerangka kerja keamanan siber. Berikutnya, hal ini dapat digunakan dalam mengidentifikasi hubungan ini dalam **table 2.** Hubungan persilangan antara kedua kerangka kerja ini dapat dilihat pada https://www.nist.gov/privacy-framework.

Fungsi-fungsi, Kategori-kategori, atau Subkategori-subkategori berada di dalam Kerangka Kerja Keamanan Siber, akan tetapi pasal–pasal dari peraturan ini diadaptasikan untuk Kerangka Kerja Privasi.

Kategori atau subkategori identik dengan Kerangka Kerja Keamanan Siber.

Identifikasi-Identifikasi Inti: Untuk kemudahan pemakaian, pada setiap komponen dari Inti diberikan pengenalan yang khusus. Fungsinya dan Kategorinya masing-masing memiliki tanda pengenal yang berupa penanda huruf yang khusus berdasarkan abjad, seperti yang bisa dilihat pada **tabel 1.** Subkategori dalam masing-masing kategori memiliki tambahan penomoran ke dalam penanda huruf berdasarkan abjad, pengidentifikasian yang unik dari masing-masing subkategori yang termasuk pada **tabel 2**.

Tabel 1 Inti, Fungsi, Kategori Dari Pengat Privas

Fungsi khusus pengenalan	Fungsi	Kategori dan kode	Kategori
ID-P	Identifikasi-P	ID.IM-P	Inventarisasi dan pemetaan
		ID.BE-P	Lingkungan bisnis
		ID.RA-P	Penilaian risiko
		ID.DE-P	Manajemen Risiko Ekosistem Pemrosesan Data
GV-P	Pengendalian-P	GV.PO-P	Kebijakan pemerintahan, Pemrosesan, dan prosedur
		GV.RM-P	Strategi manajemen risiko
		GV.AT-P	Kesadaran dan pelatihan
		GV.MT-P	Peninjauan dan pemantauan
CT-P	Kontrol-P	CT.PO-P	Kebijakan pemrosesan data, pemrosesan, dan prosedur
		CT.DM-P	Manajemen pemrosesan data
		CT.DP-P	Pemrosesan Terpisah
CM-P	Komunikasi-P	CM.PO-P	Komunikasi dalam kebijakan, pemrosesan, dan prosedur
		CM.AW-P	Kesadaran pemrosesan data
PR-P	Perlindungan-P	PR.PO-P	Kebijakan, pemrosesan, dan prosedur perlindungan data
		PR.AC-P	Manajemen identitas, otentikasi, dan kontrol pada akses
		PR.DS-P	Keamanan Data
		PR.MA-P	Perawatan
		PR.PT-P	Teknologi yang memiliki fungsi sebagai pelindung
DE	Deteksi	DE.AE	Kejanggalan dan kejanggalan-kejanggalan
		DE.CM	Pemantauan Keamanan Berkelanjutan
		DE.DP	Proses-proses Pendeteksian
RS	Respon	RS.RP	Perencanaan Respon
		RS.CO	Komunikasi-komunikasi
		RS.AN	Analisis-analisis
		RS.MI	Mitigasi
		RS.IM	Pengembangan-pengembangan
RC	Pemulihan	RC.RP	Rencana Pemulihan
		RC.IM	Pengembangan-pengembangan
		RC.CO	Komunikasi-komunikasi

Tabel 2 Inti Perlindungan Privasi

Fungsi	Kategori	Subkategori
PENGIDENTIFIKASIAN-P (ID-P): Mengembangkan pemahaman atas risiko yang timbul dari pemrosesan data individu - individu.	**Inventarisasi dan Pemetaan (ID.IM-P)** pemrosesandari sistem-sistem elektronik, produk dan layanan yang dipahami serta memberikan informasi pengelolaan risiko privasi.	**ID.IM-P1:** Sistem-sistem/Produk-produk/Layanan-layanan inventari data.
		ID.IM-P2: Pemilik-pemilik atau operator-operator (seperti organisasi atau pihak ketiga dalam penyedia-penyedia, rekanan, pemakai-pemakai dan pengembang-pengembang) dan peran-peran mereka dalam mengenai sistem-sistem, produk-produk, layanan-layanan dan komponen-komponen (seperti, internal atau eksternal), pemrosesan data tersebut diinventarisasi.
		ID.IM-P3: kategori-kategori individu-individu (seperti para pemakai, karyawan atau calon karyawan, dan konsumen) data yang dimilikinya sedang diproses dan diinventarisasi.
		ID.IM-P4: Aktivitas-aktivitas data dilakukan oleh sistem-sistem/produk-produk/layanan-layanan yang diinventarisasi.
		ID.IM-P5: Tujuan-tujuan untuk aktivitas-aktivitas data yang diinventarisasi.
		ID.IM-P6: Elemen-elemen data dalam aktivitas-aktivitas data yang diinventarisasi.
		ID.IM-P7: lingkungan pemrosesan data yang teridentifikasi (seperti lokasi geografis, kondisi internal, komputasi awan, dan pihak-pihak ketiga)
		ID.IM-P8: Pemrosesan data dipetakan, digambarkan aksi-aksi data dan terhubung dengan elemen-elemen data untuk sistem-sistem/produk-produk dan layanan-layanan, termasuk komponen-komponen, seperti: peran-peran dari pemilik-pemilik/operator-operator komponen dan interaksi-interaksi individu atau pihak-pihak ketiga dengan sistem-sistem/produk-produk/layanan-layanan.
	Lingkungan Bisnis (ID.BE-P): Misi, tujuan-tujuan, para pemangku kepentingan, dan	**ID.BE-P1:** Peran-peran organisasi dalam ekosistem pemrosesan data diidentifikasi dan dikomunikasikan

		aktivitas organisasi dapat dipahami dan diprioritaskan; informasi ini digunakan untuk menginformasikan peran-peran, pertanggungjawaban privasi dan keputusan-keputusan manajemen risiko.	**ID.BE-P2:** Prioritas-prioritas untuk misi, tujuan-tujuan dan aktivitas-aktivitas organisasi disusun dan dikomunikasikan.
			ID.BE-P3: Sistem-sistem, produk-produk, dan layanan-layanan yang mendapat prioritas dukungan organisasi diidentifikasi dan dikomunikasikan persyaratan-persyaratan kuncinya.
		Penilaian Risiko (ID.RA-P): Organisasi memahami risiko privasi terkait individu-individu dan bagaimana risiko privasi ini dibuat untuk dapat menindaklanjuti dampak pada operasi-operasi organisasi, termasuk misi, fungsi-fungsi, prioritas-prioritas manajemen risiko yang lain (misalnya, kepatuhan, keuangan), reputasi, tenaga kerja, dan kultur.	**ID.RA-P1:** Faktor–faktor kontekstual yang terkait dengan sistem-sistem/produk-produk/layanan-layanan dan aktivitas-aktivitas data yang diidentifikasi (seperti, demografi individu-individu dan kepentingan-kepentingan privasi atau persepsi-persepsi, kesensitifan data dan/atau tipe-tipe, visibilitas dari pemrosesan data untuk individu-individu atau pihak ketiga).
			ID.RA-P2: Analisis dari data yang masuk maupun keluar diidentifikasi dan dievaluasi agar tidak ada ketidak jelasan. .
			ID.RA-P3: Aktivitas-aktivitas data bermasalah dan masalah terkait yang diidentifikasi.
			ID.RA-P4: Permasalahan yang akan timbul dalam pemrosesan data menjadi penentuan akan penanganan risiko nantinya.
			ID.RA-P5: Respon-respon dari risiko diidentifikasi, diprioritaskan, dan diimplementasikan.
		Ekosistem Pengolahan Data Manajemen Risiko (ID.DE-P): Prioritas-prioritas, kendala-kendala, risiko toleransi, dan anggapan-anggapan disusun dan digunakan untuk mendukung anggapan, dijalankan untuk mendukung pengambilan keputusan risiko sesuai dengan manajemen risiko privasi dan ketiga bagian dalam ekosistem pengolahan data. Organisasi menjalankan dan mengimplementasi pemrosesan untuk identifikasi, menilai dan mengatur risiko privasi dalam pengolahan data.	**ID.DE-P1:** Mengidentifikasi, menjalankan, menilai, mengatur pada Kebijakan ekosistem pengolahan data manajemen risiko, pemrosesan, dan prosedur. Sesuai persetujuan pemangku organisasi.
			ID.DE-P2: Ekosistem pemrosesan data (seperti, layanan-layanan, penyedia-penyedia, pemakai-pemakai, rekanan, produsen, pengembang-pengembang aplikasi) yang diidentifikasi, diprioritaskan, dan dinilai dari proses risiko privasi.
			ID.DE-P3: Kontrak-kontrak berkenaan dengan bagian-bagian ekosistem pemrosesan data digunakan pada implementasi yang sesuai design untuk memenuhi objektivitas dari program privasi milik organisasi.
			ID.DE-P4: Kerangka kerja-kerangka kerja antar aplikasi dengan protokol yang disepakati bersama atau pendekatan-pendekatan multi bagian untuk digunakan memanajemen ekosistem pemrosesan data risiko

			privasi.
			ID.DE-P5: Bagian-bagian dari ekosistem pemrosesan data rutin diaudit, dites, atau dievaluasi untuk memastikan pemenuhan kontrak, kerangka kerja antar aplikasi dengan protokol yang disepakati bersama, atau kewajiban lainnya.

	Fungsi	**Kategori**	**Subkategori**
	Pengendalian-P (GV-P): Pengembangan dan pengimplementasian struktur pada organisasi untuk pemahaman manajemen risiko organisasi yang bersumber pada risiko privasi.	**Kebijakan Pengendalian, Proses, dan Prosedur (GV.PO-P):** Kebijakan-kebijakan, pemrosesan-pemrosesan, dan prosedur-prosedur untuk mengatur dan memantau regulasi dari organisasi, legalitas, risiko, lingkungan dan operasional yang memahami manajemen dari risiko privasi.	**GV.PO-P1:** Nilai-nilai dan kebijakan-kebijakan dari privasi organisasi (misalnya, pengkondisian pada pemrosesan data atau periode retensi, pada pengolahan data berdasarkan pemrosesan hak-hak individu) dijalankan dan dikomunikasikan.
			GV.PO-P2: Pemrosesan-pemrosesan yang melibatkan nilai-nilai privasi organisasi dengan pengembangan sistem-sistem/produk-produk/layanan, dan operasi-operasi yang dijalankan.
			GV.PO-P3: Tenaga kerja memiliki peran dan tanggung jawab dalam menjalankan fungsinya dengan menghormati data privasi.
			GV.PO-P4: Peran-peran dan tanggung jawab-tanggung jawab yang dikoordinasikan dan diselaraskan dengan pihak ketiga (seperti, penyedia layanan, pemakai-pemakai, dan rekanan).
			GV.PO-P5: Legalitas, regulasi dan persyaratan-persyaratan kontraktual merujuk pada pemahaman dan pengaturan berkenaan privasi.
			GV.PO-P6: Pengendalian dan kebijakan manajemen risiko serta prosedurnya bertujuan untuk risiko privasi.
		Strategi Manajemen Risiko (GV.RM-P): Prioritas-prioritas, kendala-kendala, toleransi-toleransi risiko, dan asumsi-asumsi dari organisasi, dijalankan sesuai dengan kegunaannya untuk mendukung pemutusan risiko.	**GV.RM-P1:** Proses manajemen risiko, dijalankan, diatur dan disetujui oleh pemangku jabatan pada organisasi.
			GV.RM-P2: Organisasi memiliki toleransi yang kuat terhadap kemungkinan serangan atau kebocoran data.
			GV.RM-P3: Penentuan dari organisasi dari risiko toleransi diinformasikan dari peran-peran dalam ekosistem pemrosesan data - .

		Kewaspadaan dan Pelatihan (GV.AT-P): Tenaga kerja dan organisasi eksternal bekerjasama pada pengolahan data yang tersedia dalam pendidikan kesadaran privasi, terlatih untuk menjalankan tugas yang berkaitan dengan kewajiban mereka konsisten dengan kebijakan, proses dan kesepakatan dan nilai-nilai privasi organisasi	**GV.AT-P1:** Tenaga kerja diinformasikan dan dilatih untuk bertanggung jawab dalam menjalankan peran-perannya.
			GV.AT-P2: Eksekutif organisasi harus mengerti akan peranan dan tanggung jawabnya.
			GV.AT-P3: Pejabat pelindung data mengerti akan peranan dan tanggung jawabnya.
			GV.AT-P4: Ketiga pihak (Penyedia layanan, Pekerja, Pemakai, dan rekanan) mengetahui peranan dan tanggung jawabnya masing-masing.
		Pemantauan dan peninjauan (GV.MT-P): Kebijakan-kebijakan, pemrosesan-pemrosesan, dan prosedur-prosedur untuk peninjauan terus-menerus yang bisa dimengerti dan diinformasikan ke pengelolaan risiko privasi.	**GV.MT-P1:** Re-evaluasi yang rutin terhadap manajemen risiko dan sebagai faktor utama, termasuk lingkungan bisnis organisasi (seperti pengenalan teknologi baru), kepemimpinan (seperti kewajiban legal, toleransi risiko), proses data dan perubahan sistem/produk.jasa
			GV.MT-P2: Nilai-nilai dari privasi, kebijakan-kebijakan, serta pelatihan dipantau dan dibaharui untuk pengkomunikasian.
			GV.MT-P3: Kebijakan-kebijakan, pemrosesan-pemrosesan, dan prosedur-prosedur untuk menilai pemenuhan persyaratan-persyaratan legalitas dan kebijakan-kebijakan privasi yang dibuat dan dijalankan.
			GV.MT-P4: Kebijakan-kebijakan, pemrosesan-pemrosesan, dan prosedur-prosedur untuk pengkomunikasian kemajuan dalam manajemen risiko privasi yang dijalankan.
			GV.MT-P5: Kebijakan-kebijakan, pemrosesan-pemrosesan, dan prosedur-prosedur yang dijalankan untuk menerima, menganalisis, dan merespon problematika aktivitas-aktivitas data dari sumber-sumber internal dan eksternal (contoh, penemuan internal, riset-riset privasi, peristiwa-peristiwa professional).
			GV.MT-P6: Kebijakan, pengelolaan, dan prosedur dipelajari dari masalah aktivitas data.
			GV.MT-P7: Kebijakan-kebijakan, pemrosesan-pemrosesan, dan prosedur-prosedur untuk menerima, melacak, dan merespon aduan atau pertanyaan dari individu mengenai praktik dari organisasi dibuat

			dan dijalankan..
	Kontrol-P (CT-P): Pengembangan dan pengimplementasian aktivitas yang pantas untuk organisasi - organisasi atau individu - individu dalam mengatur data dengan perincian yang memadai untuk pengelolaan risiko-risiko privasi.	**Kebijakan pemrosesan data dan prosedur (CT.PO-P):** Kebijakan-kebijakan, pemrosesan-pemrosesan, dan prosedur-prosedur dijaga dan digunakan untuk mengelola pemrosesan data (misalnya, tujuan, cakupan, peran-peran tanggung jawab-tanggung jawab dalam ekosistem pemrosesan data, dan komitmen manajemen), konsisten dengan strategi risiko organisasi untuk melindungi privasi individu.	**CT.PO-P1:** Kebijakan-kebijakan, pemrosesan-pemrosesan, dan prosedur-prosedur mengizinkan pengolahan data (Misalnya, keputusan-keputusan organisasi, kesepakatan individual), mencabut otoritarisasi-otoritarisasi, dan memelihara otorisasi-otorisasi yang dibuat dan dijalankan.
			CT.PO-P2: Kebijakan-kebijakan, pemrosesan-pemrosesan, dan prosedur-prosedur memungkinkan mengulas data, mentransfer, membagi, merubah, serta menghapus juga dibuat dan dijalankan (misalnya, mempertahankan kualitas data, manajemen retensi data).
			CT.PO-P3: Kebijakan-kebijakan, pemrosesan-pemrosesan, dan prosedur-prosedur memungkinkan preferensi-preferensi pemrosesan data individu serta permintaan-permintaan dibuat dan dijalankan.
			CT.PO-P4: Siklus masa data untuk mengatur agar selaras dan diimplementasi dengan pengembangan sistem masa siklus untuk mengatur sistem-sistem.
		Pengelolaan pengolahan data (CT.DM-P): Data yang dikelola konsisten dengan strategi risiko organisasi untuk melindungi privasi individu, menambah daya pengelolaan, dan memungkin penerapan prinsip-prinsip privasi (misalnya, partisipasi individu, kualitas data, minimisasi data).	**CT.DM-P1:** Element-element data dapat diakses untuk ditinjau.
			CT.DM-P2: Dapat melakukan penyingkapan dan transmisi data.
			CT.DM-P3: Data dapat diubah sesuai keperluan.
			CT.DM-P4: Memungkinkan data dapat dihapus.
			CT.DM-P5: Data dapat dimusnahkan merujuk pada kebijakan.
			CT.DM-P6: Data ditransmisi dalam format-format standar.
			CT.DM-P7: Izin mekanisme dalam transmisi proses data berkenaan dengan nilai-nilai dari data tersebut dibuat dan dijalankan..

			CT.DM-P8: Audit/catan-catatan histori ditentukan, didokumentasikan, diimplementasi, dan ditinjau dalam kebijakan berdasarkan prinsip minimalisasi data.
			CT.DM-P9: Menerapkan tindakan yang dapat mengelola data yang diproses, dinilai, dan diuji.
			CT.DM-P10: Pemangku jabatan memasukkan preferensi privasi pada desain algoritma yang objektif dan hasilnya dievaluasi dengan preferensi ini.
		Pemrosesan Terpisah (CT.DP-P): Solusi pemrosesan data meningkatkan diasosiasi yang konsisten dengan strategi risiko organisasi untukperlindungan privasi individu dan penerapan prinsip-prinsip privasi, seperti meminimalisasi data.	**CT.DP-P1:** Data diproses dan dibatasi pada pengamatan dan keterkaitan (misalnya, aktivitas data pada perangkat lokal, privasi dijaga melalui kriptografi).
			CT.DP-P2: Data diproses dengan batasan identifikasi dari individu-individu (misalnya, teknik identifikasi ulang privasi,upaya mengubah sebuah nilai/value menjadi aset digital).
			CT.DP-P3: Data diproses pada pembatasan formulasi dari kesimpulan mengenai tingkah laku individu atau aktivitasnya.
			CT.DP-P4: Sistem atau perangkat yang terkonfigurasi memungkinkan pengumpulan atau menyeleksi pengungkapan elemen data.
			CT.DP-P5: Menggantikan atribut referensi menjadi atribut nilai-nilai.
	Pengkomunikasian-P (CM-P): Menerapkan dan mengembangkan aktivitas yang sesuai yang memungkinkan organisasi memiliki pengertian yang bisa diandalkan dan terlibat dalam diskusi tentang pemrosesan data dan risiko privasi yang terkait	**Kebijakan, Proses, dan Prosedur Komunikasi (CM.PO-P):** Kebijakan, pengolahan, dan prosedur dijaga dan digunakan untuk meningkatkan transparansi dari praktik pengolahan data organisasi (seperti tujuan, lingkup kerja, peran-peran dan tanggungjawab dalam ekosistem pemrosesan data dan komitmen pengelolaan) dan risiko privasi terkait.	**CM.PO-P1:** Penerapan transparan prosedur untuk pemberitahuan tujuan dan praktik dan data privasi terkait sudah dibuat dan dijalanakan.
			CM.PO-P2: Peran dan tanggung jawab (misalnya, Publik relasi) untuk mengkomunikasikan tujuan pemrosesan data, praktik-praktik dan risiko privasi terkait sudah dibuat.
		Kesadaran dalam Pemrosesan Data (CM.AW-P): Individu-individu dan organisasi yang memiliki pengetahuan yang dapat diandalkan mengenai praktik	**CM.AW-P1:** Mekanisme (misalnya seperti pemberitahuan, internal atau laporan publik) untuk pengkomunikasian tujuan pemrosesan data, praktik-praktik, risiko privasi terkait dan pilihan untuk memungkinkan preferensi pemrosesan data individu Dan permintaan

		pengolahan data dan risiko privasi terkait, dengan mekanisme yang efektif digunakan dan dijaga untuk meningkatkan prediksi yang konsisten dengan strategi risiko organisasi untuk melindungi privasi individu.	ini sudah dibuat dan dijalankan.
			CM.AW-P2: Mekanisme untuk memperoleh masukan dari individu (misalnya survei atu fokus grup) tentang pemrosesan data dan risiko privasi terkait sudah dibuat dan dijalankan..
			CM.AW-P3: Desain/sistem /layanan memungkinkan untuk visibilitas dari data yang diproses.
			CM.AW-P4: Memiliki akses dari catatan pengungkapan dan pembagian data dan bisa diakses untuk peninjauan ulang atau transmisi/pengungkapan data
			CM.AW-P5: Untuk setiap perbaikan dan pemusnahan data harus dikomunikasikan ke individu atau organisasi (misalnya sumber data) dalam ekosistem pemrosesan data.
			CM.AW-P6: Data asal atau turunannya dipertahankan guna peninjauan atau pengungkapan data
			CM.AW-P7: Individu yang terkena dampak dan organisasi akan diberi diinformasikan jika datanya dibobol atau dirusak.
			CM.AW-P8: Individu-individu difasilitasi dengan mekanisme yang mitigasi (monitor kredit, persetujuan penarikan, perubahan atau penghilangan data) untuk mengatasi dampak dari problematika aktivitas data.
	Perlindungan-P (PR-P): Penerapan dan pengembangan yang sesuai dalam menjaga	**Kebijakan dan Prosedur perlindungan data (PR.PO-P):** Keamanan dan kebijakan privasi (misalnya tujuan, cakupan, peran dan tanggungjawab dalam ekosistem pemrosesan data dan penegelolaan komitmen), proses-proses dan prosedur-prosedur dijaga dan dipakai untuk pengelolaan perlindungan data	**PR.PO-P1:** Garis dasar dari konfigurasi teknologi informasi dengan menciptakan dan merawat penggabungan dari prinsip-prinsip keamanan (mislanya konsep fungsional yang paling sedikit).

	pemrosesan data.		**PR.PO-P2:** Proses dan kontrol perubahan konfigurasi sudah dibuat dan dijalankan
			PR.PO-P3: Cadangan informasi disusun, dijaga dan dites
			PR.PO-P4: Peraturan serta kebijakan mengenai lingkungan operasi fisik untuk organisasi dapat dipenuhi
			PR.PO-P5: Proses perlindungan diperbaiki.
			PR.PO-P6: Efektivitas perlindungan teknologi dibagikan
			PR.PO-P7: Rencana tanggapan (Tanggapan insidental dan Keberlanjutan Bisnis) dan rencana pemulihan (Pemulihan Insidental dan Pemulihan karena Kesalahan) sudah ada, dijalankan dan dikelola.
			PR.PO-P8: Tanggapan dan pemulihan telah diuji.
			PR.PO-P9: Prosedur privasi juga masuk dalam praktik ketenagakerjaan (misalnya paham permasalahan, tenaga yang sudah lewat penyaringan)
			PR.PO-P10: Rencan pengelolaan yang mudah dirubah disusun dan dijalankan
		Identitas manajemen, Autentikasi, dan Kontrol Akses (PR.AC-P): Akses terhadap data dan perangkat terbatas pada individu, proses dan perangkat berwenang dan dikelola konsisten dengan risiko yang terkontrol dari akses yang tidak legal.	**PR.AC-P1:** Untuk identitas dan kredensial yang dikeluarkan, diatur, diverifikasi, dicabut, dan diaudit Oleh individu, proses dan perangkat berwenang
			PR.AC-P2: Akses fisik ke data dan perangkat bisa dikelola
			PR.AC-P3: Pengaturan akses dari jarak jauh bisa dikelola
			PR.AC-P4: Ijin dan kewenangan akses bisa dikelola, digabungkan dengan hak mengakses berdasarkan tingkatan dan pembagian tugas.
			PR.AC-P5: Perlindungan pada jaringan integritas, seperti pemisahan jaringan dan segmentasi jaringan.
			PR.AC-P6: Individu-individu dan perangkat-perangkat dibuktikan dengan surat kepercayaan dan autentikasi sepadan dengan risiko transaksi. (misalnya, keamanan individual dan risiko privasi dan risiko-risiko organisasi lainnya).

		Sekuriti Data (PR.DS-P): Data diatur secara konsisten oleh organisasi dengan strategi pengelolaan risiko untuk keamanan privasi individu dan menjaga kerahasiaan, integritas dan ketersediaan data	**PR.DS-P1:** Perlindungan terhadap data yang disimpan
			PR.DS-P2: Perlindungan data pada fase transisi.
			PR.DS-P3: Sistem-sistem, produk-produk,atau pelayan-pelayanan data dapat diatur dengan menghapus, mengirim atau memposisi ulang data tersebut.
			PR.DS-P4: Kapasitas yang memadai untuk memastikan ketersediaan data
			PR.DS-P5: Perlindungan terhadap kebocoran data.
			PR.DS-P6: Mekanisme integritas pemeriksaan digunakan untuk memverifikasi, perangkat lunak, komponen elektronik yang berisi instruksi-instruksi dan informasi yang berintegritas.
			.
			PR.DS-P7: Pengembangan dan uji coba lingkungan sistem dipisahkan dari lingkungan produksi.
			PR.DS-P8: Integritas dari mekanisme yang baik dalam verifikasi perangkat keras.
		Pemeliharaan (PR.MA-P): Pemeliharaan sistem dan perbaikan dijalankan konsisten dengan kebijakan, proses dan prosedur.	**PR.MA-P1:** Perawatan dan perbaikan pada aset organisasi dijalankan, terdaftar, dengan peralatan yang diakui dan bisa dikontrol
			PR.MA-P2: Pengontrolan dari jauh dari aset organisasi diakui, terdaftar, dan dijalankan dengan cara yang bisa mencegah akses yang tidak diizinkan.
		Perlindungan Teknologi (PR.PT-P): Solusi keamanan teknik dikelola untuk memastikan keamanan dan ketahanan produk dan data terkait, konsisten dengan kebijakan terkait, proses-proses, prosedur dan kesepakatan-kesepakatan..	**PR.PT-P1:** Media yang dapat dipindahkan dilindungi dan pemakaiannya dibtasi dengan merujuk pada kebijakan.
			PR.PT-P2: Prinsip dari fungsional tergabung dari konfigurasi sistemuntuk memenuhi hanya kebutuhan esensial.
			PR.PT-P3: Komunikasi dan kontrol dari jaringan dilindungi.
			PR.PT-P4: Mekanisme (misalnya kegagalan dalam keamanan, keseimbangan beban data, penggantian hard-drive karena kerusakan) dijalankan untuk mencapai persyaratan dalam situasi normal maupun tidak normal.

Lampiran B: Daftar-Daftar Istilah

Lampiran ini menjelaskan mengenai istilah - istilah tertentu yang digunakan pada publikasi ini.

Referensi Atribut (NIST SP 800-63-3 [8])	Sebuah pernyataan yang menegaskan properti milik pemakai tanpa harus berisikan identitas informasi, terlepas dari formatnya. Misalnya, untuk atribut “ulang tahun”, referensi bisa jadi “lebih tua dari 18” atau “lahir di bulan Desember”.
Nilai Atribut (NIST SP 800-63-3 [8])	Sebuah pernyataan lengkap yang menegaskan properti milik pemakai, independen dari format. Misalnya, untuk atribut “ulang tahun”, nilainya bisa jadi “12/1/1980” atau “1 Desember 1980”.
Ketersediaan (44 U.S.C. [13])	Memastikan akses dan pemakaian informasi yang tepat waktu serta dapat diandalkan.
Kategori	Pembagian fungsi ke dalam kelompok privasi yang memiliki keterkaitan dengan kebutuhan pada programatik dan aktivitas-aktivitas tertentu.
Pengkomunikasian-P (Fungsi)	Mengembangkan dan menerapkan aktivitas-aktivitas yang sesuai untuk memungkinkan organisasi-organisasi dan individu-individu untuk memiliki pemahaman yang dapat diandalkan dan terlibat dalam dialog tentang bagaimana data diproses dan risiko-risiko privasi terkait.
Kerahasiaan (44 U.S.C. [13])	Mempertahankan pembatasan resmi atas akses dan pengungkapan informasi, termasuk cara untuk melindungi privasi miliki pribadi dan informasi data pribadi
Pengontrolan -P (Fungsi)	Mengembangkan dan menerapkan aktivitas-aktivitas yang memungkinkan organisasi-organisasi atau individu-individu , untuk mengatur data secara jelas dalam rangka manajemen dari risiko privasi.
Inti	Serangkaian aktivitas dan perlindungan privasi, yang mana Inti kerangka kerja ini terdiri dari elemen Fungsi-fungsi, Kategori-kategori, dan Subkategori-subkategori.

Peristiwa Dalam Keamanan Siber (Kerangka kerja untuk Meningkatkan Pengetahuan Pada Instrumen Keamanan Siber [1])	Peristiwa keamanan siber yang telah ditentukan memiliki dampak pada organisasi yang memiliki kapasitas untuk memberikan tanggapan dan pemulihan.
(OMB 17-12 [9])	Suatu kejadian yang (1) akan terjadi dan akan segera membahayakan, tanpa otoritas yang sah, integritas, kerahasiaan, atau ketersediaan informasi atau sistem informasi atau (2) merupakan suatu pelanggaran maupun ancaman langsung dari pelanggaran hukum, kebijakan-kebijakan keamanan, prosedur-prosedur keamanan, atau kebijakan-kebijakan pemakaian.
Data	Sebuah representasi informasi, termasuk format-format digital dan non-digital.

Aktivitas Data (Merujuk pada NIST IR 8062 [5])	Sebuah sistem/produk/layanan data yang beroperasi, yang terlibat akan tetapi tidak terbatas pada pengumpulan, penyimpanan, catatan, transformasi, pemakaian, pengungkapan, pembagian, pentransmisian dan pemusnahan.
Elemen Data	Item terkecil dari informasi data yang berguna.
Pemrosesan Data (Merujuk pada NIST IR 8062 [5])	Kumpulan aktivitas-aktivitas data dalam yaitu pengumpulan, penyimpanan, catatan, pembuatan, transformasi, pemakaian, pengungkapan, berbagi, transmisi, dan pemusnahan.
Ekosistem Pemrosesan Data	Hubungan yang kompleks dan saling bersinergi di antara entitas yang terlibat dalam pembuatan atau penerapan sistem, produk, atau layanan atau komponen-komponen apapun pada pemrosesan data.
Pemisahan (Merujuk pada NIST IR 8062 [5])	Mengaktifkan pemrosesan data atau peristiwa tanpa keterkaitan dengan individu-individu atau perangkat di luar dari persyaratan - persyaratan operasional sistem.
Fungsi	Sebuah komponen inti yang menyediakan tingkat struktur tertinggi yang mengatur aktivitas-aktivitas privasi dasar pada kategori-kategori dan subkategori-subkategori.
Pengendalian-P(Fungsi)	Mengembangkan dan menerapkan struktur tata kelola organisasi untuk memungkinkan pemahaman yang berkelanjutan tentang prioritas manajemen risiko organisasi yang diinformasikan oleh risiko privasi.
Pengidentifikasian-P (Fungsi)	Pendalaman pemahaman pada organisasi untuk mengelola risiko privasi bagi individu-individu yang timbul dari pemrosesan data.
Tingkatan Penerapan	Mengaplikasikan referensi mengenai bagaimana organisasi menyikapi risiko dari privasi dan apakah sebuah organisasi tersebut memiliki pemrosesan dan sumber daya yang memadai untuk mengelola risiko tersebut.

Individual	Seseorang atau sekelompok orang dalam grup, termasuk di tingkat masyarakat.
Keutuhan (44 U.S.C. [13])	Menjaga dari modifikasi atau perusakan informasi yang tidak tepat, dan termasuk memastikan informasi non-penyangkalan dan keaslian.
Turunan	Catatan pemrosesan elemen data, yang mencakup aliran data dan tindakan data yang dilakukan pada elemen data.
Pengelolaan (Merujuk pada NIST IR 8062 [5])	Memiliki kapasitas untuk pengadministrasian data yang jelas, termasuk perubahan, pemusnahan, dan pengungkapan yang selektif.
Metadata (Merujuk pada NIST SP 800-53 [10])	Informasi yang mendeskripsikan karakteristik-karakteristik data itu sendiri. Seperti struktural yang menjelaskan struktur data (misalnya, format data, sintaksis, semantik), dan metadata deskriptif sehingga bisa menjelaskan isi konten-konten data.
Prediksi (Merujuk pada NIST IR 8062 [5])	Membuat asumsi yang dapat diandalkan oleh individu-individu, pemilik-pemilik, dan operator-operator tentang pemrosesan data oleh sistem, produk, atau layanan.
Pelanggaran Privasi (Merujuk pada OMB M-17-12 [9])	Hilangnya kendali, kompromi, pengungkapan tidak sah, akuisisi tidak sah, atau kejadian serupa dimana (1) Orang selain pemakai yang sah mengakses atau berpotensi mengakses data untuk tujuan selain yang berwenang. (2) Pemakai yang berwenang mengakses data selain untuk tujuan yang sah. .
Pengontrolan Privasi (Merujuk pada NIST SP 800-37 [7])	Pengamanan administratif, teknis, dan fisik yang digunakan dalam organisasi untuk memenuhi persyaratan-persyaratan privasi.
Peristiwa pelanggaran Privasi	Terjadinya suatu aktivitas-aktivitas yang berpotensi terjadinya kesalahan pada data.
Syarat – syarat Privasi	Sebuah spesifikasi fungsi dari sistem/produk/layanan fungsionalitas untuk memenuhi hasil privasi yang diinginkan pemangku kepentingan.

Risiko Privasi	Kemungkinan individu-individu akan mengalami masalah akibat pemrosesan data, dan dampaknya jika terjadi.
Penilaian Risiko Privasi	Proses dari manajemen risiko privasi dalam mengidentifikasi dan mengevaluasi risiko privasi.
Pengelolaan Risiko Privasi	Serangkaian proses antara organisasi untuk mengidentifikasi, menilai, dan merespon risiko privasi.
Problematika Dalam Tindakan Data (Merujuk pada NIST IR 8062 [5])	Aktivitas data yang dapat menyebabkan efek buruk pada individu-individu.
Pemrosesan	Lihat pada pengolahan data.
Profil	Pilihan Fungsi, Kategori, dan Subkategori tertentu dari Inti yang telah diprioritaskan oleh organisasi untuk membantu dalam pengelolaan risiko-risiko privasi.
Perlindungan -P (Fungsi)	Pengembangan dan implementasi pengamanan pemrosesan data yang sesuai.
Asal (Merujuk pada NIST IR 8112 [11])	Sumber yang berkaitan dari asal data tersebut.
Risiko (NIST SP 800-30 [12])	Tolak ukur sejauh mana suatu entitas terancam oleh keadaan atau peristiwa yang berfungsi dari, (i) kerugian yang timbul jika perbuatan tersebut terjadi, dan (ii) Kemungkinan terjadinya peristiwa tersebut.
Manajemen Risiko	Proses mengidentifikasi, menilai, dan menanggapi risiko.
Daya Tahan Risiko (NIST SP 800-39 [6])	Tingkatan dari risiko atau tingkatan dari ketidakpastian yang mungkin akan dirasakan oleh organisasi-organisasi.
Subkategori	Pembagian lebih lanjut dari suatu Kategori menjadi hasil khusus dari kegiatan teknis dan/atau manajemen.

Lampiran C: Akronim-Akronim

Lampiran ini menjelaskan dari pemakaian akronim pada publikasi ini.

IEC	International Electrotechnical Commission. (Komisi Elektronik Internasional)
IR	Interagency or Internal Report. (Laporan Internal atau Antar Lembaga)
ISO	International Organization for Standardization. (Organisasi Internasional untuk Standardisasi).
IT	Information Technology. (Teknologi Informasi).
NIST	National Institute of Standards and Technology. (Institut Nasional Standar dan Teknologi).
OASIS	Organization for the Advancement of Structured Information Standards. (Organisasi untuk Standar Kemajuan Informasi Terstruktur).
OECD	Organisation for Economic Co-operation and Development. (Organisasi untuk Kerja Sama Ekonomi dan Pembangunan)
OMB	Office of Management and Budget. (Kantor Manajemen dan Anggaran).
PMRM	Privacy Management Reference Model and Methodology. (Model dan Metodologi Referensi Manajemen Privasi).
PRAM	Privacy Risk Assessment Methodology. (Metodologi Penilaian Risiko Privasi).
RFC	Request for Comment. (Permintaan untuk Komentar).
RFI	Request for Information. (Permintaan untuk informasi).
SDLC	System Development Life Cycle. (Sistem Pengembangan Siklus Hidup m)
SP	Special Publication. (Publikasi Khusus).

Lampiran D: Praktik-Praktik Manajemen Risiko Privasi

Bagian 1.2 mengenalkan pertimbangan-pertimbangan seputar manajemen risiko privasi, termasuk hubungan antara keamanan siber dan risiko privasi, serta peran dari penilaian risiko privasi. Dalam lampiran ini membahas beberapa praktik utama yang memiliki dampak pada keberhasilan manajemen risiko, salah satunya mengatur sumber daya persiapan, menentukan kemampuan privasi, menentukan persyaratan privasi, melakukan penilaian risiko privasi, membuat persyaratan privasi yang bisa dilacak, dan pemantauan untuk mengubah risiko privasi. Referensi pada Kategori dan Subkategori disertakan untuk memfasilitasi pemakaian Inti untuk mendukung praktik-praktik ini; referensi ini muncul dalam tanda kurung.

Mengorganisir Persiapan Sumber Daya

Sumber daya yang sesuai memfasilitasi pengambilan keputusan yang diinformasikan tentang risiko privasi di semua tingkatan dalam organisasi. Sebagai masalah praktis, tanggung jawab untuk mengembangkan berbagai sumber daya yang mungkin dimiliki oleh berbagai komponen organisasi. Oleh karena itu, komponen organisasi bergantung pada sumber daya tertentu mungkin mengetahui bahwa mereka tidakpernah, atau mungkin tidak cukup membahas masalah privasi. Dalam keadaan ini, komponen pembantu dapat mempertimbangkan kegunaan sumber daya dan mencari informasi melalui sumber lain atau membuat keputusan terbaik yang dapat dilakukan dengan informasi yang tersedia. Singkatnya, sumber daya yang baik sangatlah membantu, akan tetapi jika ada kekurangan hal ini tidak boleh menjadi penghalang bagi organisasi untuk mengambil keputusan-keputusan risiko terbaik yang mereka bisa sesuai kemampuan-kemampuan mereka.

Sumber daya berikut, meski tidak menyeluruh, dapat membangun fondasi untuk pengambilan keputusan yang lebih baik.

- **Peran Penugasan manajemen risiko (**GV.PO-P3, GV.PO-P4)

  Membangun dan memungkinkan pemahaman lintas organisasi tentang siapa yang bisa dipercaya dan siapa yang memiliki tanggung jawab atas manajemen risiko privasi serta tugas manajemen risiko lainnya, dalam suatu organisasi untuk mendukung koordinasi dan akuntabilitas yang lebih baik dalam pengambilan keputusan. Selain itu, berbagai perspektif dapat meningkatkan proses pengidentifikasian, penilaian, dan respons terhadap risiko privasi. Tim yang beragam dan lintas fungsi dapat membantu pengidentifikasian risiko yang lebih komprehensif terhadap privasi individu dan untuk memilih rangkaian mitigasi yang lebih luas. Menentukan peran mana yang akan dimasukkan dalam diskusi manajemen risiko bergantung pada konteks dan susunan organisasi, meskipun kolaborasi antara privasi organisasi dan program keamanan siber masih tetap penting. Jika satu individu ditugaskan untuk beberapa peran, mengelola potensi konflik kepentingan harus dipertimbangkan.

- **Strategi manajemen risiko perusahaan** (GV.RM-P)

  Strategi pada manajemen risiko bisnis suatu organisasi di persuahaan membantu dalam penyelarasan misi dan nilai-nilai organisasi dengan toleransi risiko, asumsi-asumsi, kendala-kendala, dan prioritas. Keterbatasan atas sumber daya untuk mencapai misi atau tujuan bisnis dan untuk mengelola secara luas portofolio risiko yang kemungkinan perlu pertukaran timbal balik. Memungkinkan personel yang terlibat dalam proses manajemen risiko privasi untuk lebih memahami toleransi risiko organisasi, bisa membantu memandu keputusan tentang bagaimana mengalokasikan sumber daya dan meningkatkan keputusan seputar

respon risiko.

- **Para pemangku kepentingan utama** (GV.PO-P4, ID.DE-P)

  Para pemangku kepentingan privasi adalah mereka yang memiliki kepentingan atau fokus pada sistem hasil privasi, produk, atau layanan. Misalnya, perhatian-perhatian hukum seperti yang difokuskan apakah pada sistem, produk, atau layanan beroperasi dengan cara yang bisa membuat sebuah organisasi keluar dari kepatuhan dengan hukum atau peraturan privasi dan perjanjian bisnis. Pemilik-pemilik bisnis yang ingin memaksimalkan pemakaian mungkin khawatir tentang hilangnya kepercayaan pada sistem, produk, atau layanan karena privasi yang buruk. Individu-individu yang datanya sedang diproses atau yang berinteraksi dengan sistem, produk, atau layanan akan tertarik untuk tidak mengalami masalah-masalah atau konsekuensi yang merugikan. Memahami pemangku kepentingan dan jenis hasil privasi yang mereka mau akan memfasilitasi desain sistem/produk/layanan yang sesuai dengan kebutuhan pemangku kepentingan.

- **Persyaratan privasi tingkat organisasi (GV.PO-P)**

  Persyaratan privasi pada tingkatan organisasi merupakan cara untuk mengungkapkan kewajiban-kewajiban hukum, nilai-nilai privasi, dan kebijakan-kebijakan yang ingin dipatuhi oleh setiap organisasi. Memahami persyaratan ini adalah kunci utama untuk memastikan bahwa desain sistem/produk/layanan sesuai dengan kewajibannya. Persyaratan privasi tingkat organisasi dapat berasal dari berbagai sumber, termasuk:
  - Lingkungan Hukum (seperti Hukum, Peraturan dan Kontrak);
  - Kebijakan organisasi atau nilai-nilai budaya;
  - Standar yang relevan; dan
  - Prinsip-prinsip privasi

- **Bentuk-bentuk desain sistem/produk/layanan (ID.BE-P3)**

  Bentuk-bentuk desain dapat mengambil berbagai bentuk seperti sistem arsitektur desain atau diagram aliran data. Bentuk-bentuk ini membantu organisasi menentukan bagaimana sistem, produk, dan layanannya akan beroperasi. Oleh karena itu, mereka dapat membantu program privasi memahami bagaimana sistem, produk, dan layanan perlu berfungsi sehingga perangkat kontrol atau ukuran dapat memberikan bantuan agar dapat memilih pengelolaan risiko privasi dan diimplementasikan dengan cara-cara yang terjaga fungsionalitasnya sekaligus menjaga privasi.

- **Peta-peta data (ID.IM-P)**

  Peta-peta data menggambarkan pemrosesan data dan interaksi individu-individu dengan sistem-sistem, produk-produk, dan layanan-layanan. Peta data menunjukkan bagaimana alur pemrosesan data yang mencakup komponen-komponen data apa yang sedang diproses atau yang berinteraksi dengan individu yang mana, pemilik atau operator komponen, dan tindakan data diskrit serta elemen-elemen data tertentu yang sedang diproses. Peta data dapat diilustrasikan dengan cara yang berbeda, dan tingkat detail dapat bervariasi berdasarkan kebutuhan organisasi. Sebuah Peta data dapat digabungkan pada gambaran desain sistem/produk/layanan yang sudah ada untuk kenyamanan dan kemudahan

komunikasi antara komponen-komponen organisasi. Seperti yang dibahas di bawah ini, Peta data adalah gambaran penting dalam penilaian risiko privasi.

Menentukan Kemampuan-Kemampuan Privasi.

Kemampuan privasi dapat digunakan untuk menjelaskan sistem, produk, atau layanan properti atau fitur yang mencapai hasil privasi yang diinginkan (misalnya, "layanan memungkinkan minimalisasi data"). Tujuannya dari keamanankerahasiaan, integritas, dan ketersediaan bersama dengan persyaratan keamanan digunakan untuk menginformasikan kemampuan keamanan sistem, produk, atau layanan. Sebagaimana yang dijelaskan dalam **Tabel 3**, serangkaian tujuan rekayasa privasi tambahan dapat mendukung penentuan kemampuan privasi. Sebuah organisasi juga dapat menggunakan tujuan rekayasa privasi sebagai perangkat prioritas tingkat tinggi. Sistem-sistem, produk-produk, atau layanan-layanan yang kemungkinannya rendah, pengelolaan atau ketidakmampuan bersosialisasi mungkin merupakan sinyal peningkatan risiko privasi yang karena itu membutuhkan penilaian risiko privasi yang lebih komprehensif.
Dalam menentukan kemampuan-kemampuan privasi, sebuah organisasi dapat mempertimbangkan teknis privasi dan tujuan keamanan yang paling penting yang berhubungan dengan misi atau kebutuhan bisnisnya, toleransi risiko, dan persyaratan privasi tingkat organisasi (lihat Mengelola Persiapan Sumber Daya di atas). Tidak semua tujuan mungkin sama pentingnya, atau pertukaran timbal balik mungkin diperlukan di antara mereka. Meskipun kapabilitas privasi menginformasikan penilaian risiko privasi dengan mendukung keputusan prioritas risiko, kemampuan privasi juga dapat diinformasikan oleh penilaian risiko dan disesuaikan untuk mendukung manajemen risiko privasi tertentu atau mengatasi perubahan lingkungan, termasuk perubahan desain pada sistem, produk, atau layanan.

Tabel 3 Rekayasa Privasi dan Tujuan Keamanan. [18]

	Objek	Definisi	Prinsip – Prinsip dalam Inti Kerangka kerja Perlindungan Privasi
Objek Privasi	Prediksi	Mengaktifkan asumsi yang dapat diandalkan oleh individu-individu, pemilik sistem, dan operator-operator tentang data dan pemrosesannya oleh sistem	Pengidentifikasian-P, Pengendalian-P, Pengontrolan-P, Pengkomunikasian-P, dan Perlindungan-P
	Pengelolaan	Memberikan kemampuan untuk administrasi data yang terperinci, termasuk pengumpulan, pengubahan, penghapusan, dan penginformasian selektif	Pengidentifikasian-P, Pengendalian-P, Pengontrolan-P
	Keterpisahan	Memungkinkan pemrosesan data atau peristiwa tanpa keterkaitan dengan individu-individu atau perangkat-perangkat di luar persyaratan operasional sistem	Pengidentifikasian-P, Pengendalian-P, Pengontrolan-P
Tujuan-Tujuan	Kerahasiaan	Mempertahankan pembatasan resmi atas akses dan pengungkapan informasi, termasuk cara untuk melindungi privasi pribadi dan informasi hak milik	Pengidentifikasian-P, Pengendalian-P, Perlindungan-P

[18] Tujuan teknik privasi yaitu merujuk pada NIST IR 8062 [5]. Tujuan keamanan berasal dari NIST SP 800-37, Rev. 2 [7].

Keamanan	Integritas	Menjaga dari modifikasi atau perusakan informasi yang tidak tepat; termasuk memastikan informasi tidak tertolak dan keaslian terjaga	Pengidentifikasian-P, Pengendalian-P, Perlindungan-P
	Ketersediaan	Memastikan akses dan pemakaian informasi yang tepat waktu dan dapat diandalkan	Pengidentifikasian-P, Pengendalian-P, Perlindungan-P

Mendefinisikan Persyaratan Privasi

Persyaratan privasi dengan menentukan cara sistem, produk, atau layanan perlu berfungsi untuk memenuhi hasil privasi yang diinginkan pemangku kepentingan (misalnya, "aplikasi dikonfigurasi untuk memungkinkan pemakai memilih elemen-elemen data tertentu). Untuk menentukan persyaratan privasi, pertimbangkan persyaratan privasi tingkat organisasi (lihat Mengorganisir Persiapan Sumber Daya di atas) dan hasil dari penilaian risiko privasi. Proses ini membantu organisasi untuk menjawab dua pertanyaan: 1) Apa yang bisa sistem, produk, atau layanan lakukan dengan pemrosesan data dan interaksi dengan individu-individu? 2) Apa yang sebaiknya dilakukan? Kemudian sebuah organisasi dapat mengalokasikan sumber daya untuk merancang sistem, produk, atau layanan dengan cara yang bisa mencapai persyaratan yang ditentukan. Pada akhirnya, menentukan persyaratan privasi dapat mengarah pada pengembangan sistem, produk, dan layanan yang lebih memperhatikan privasi individu, dan didasarkan pada keputusan risiko yang diinformasikan.

Melakukan Penilaian Risiko Privasi

Melakukan penilaian risiko privasi membantu organisasi untuk mengidentifikasi risiko privasi yang ditimbulkan oleh sistem, produk, atau layanan, dan memprioritaskannya untuk dapat membuat keputusan yang tepat tentang cara merespon risiko-risiko (ID.RA-P, GV.RM-P). Metodologi untuk melakukan penilaian risiko privasi mungkin berbeda-beda, tetapi organisasi-organisasi harus mempertimbangkan karakteristik-karakteristik berikut:[19]

- **Model Risiko** (ID.RA-P, GV.MT-P1)

  Model-model risiko menentukan faktor risiko yang dinilai dan berhubungan di antara faktor-faktor tersebut.[20] Jika organisasi tidak menggunakan model risiko yang telah ditentukan sebelumnya, sebuah organisasi harus dengan jelas menentukan faktor-faktor risiko mana akan dinilai dan bagaimana hubungan di antara faktor-faktor ini. Meskipun keamanan siber memiliki model risiko yang banyak digunakan berdasarkan faktor risiko ancaman, kerentanan, kemungkinan, dan dampak, tidak ada hanya satu model risiko privasi yang diterima secara umum. NIST telah mengembangkan model risiko privasi untuk menghitung risiko berdasarkan kemungkinan tindakan data yang bermasalah dikalikan dengan dampak tindakan data yang bermasalah; masing-masing dari ketiga faktor-faktor risiko tersebut dijelaskan di bawah ini.

Faktor dalam risiko privasi:

Permasalahan dalam tindakan data | Kemungkinan | Dampak

[19] NIST telah mengembangkan Metodologi Penilaian Risiko Privasi atau *Privacy Risk Assessment Methodology* (PRAM) yang dapat membantu organisasi-organisasi dalam mengidentifikasi, mengakses, dan menanggapi risiko-risiko privacy. Ini terdiri dari satu set lembar kerja yang tersedia di [3].

[20] Lihat NIST SP 800-30, Rev. 1, *Panduan untuk melakukan Penilaian Risiko* [12] di hal. 8.

- Tindakan data bermasalah merupakan tindakan apa pun yang dilakukan sistem untuk memproses data yang dapat mengakibatkan masalah bagi individu-individu. Organisasi-organisasi mempertimbangkan jenis masalah-masalah yang relevan dengan populasi dari individu-individu. Masalah-masalah dapat terjadi dalam bentuk apa pun dan dapat mempertimbangkan pengalaman dari individu-individu.[21]
- Kemungkinan didefinisikan sebagai analisis kontekstual bahwa tindakan data cenderung menciptakan masalah bagi perwakilan sekumpulan individu. Konteks dapat mencakup faktor-faktor organisasi (misalnya, lokasi geografis, persepsi publik tentang organisasi yang berpartisipasi sehubungan dengan privasi), faktor-faktor sistem (misalnya, sifat dan sejarah interaksi individu dengan sistem, visibilitas pemrosesan data kepada individu-individu dan pihak ketiga), atau faktor-faktor individu (misalnya, demografi individu, minat atau persepsi privasi, sensitivitas data).[22] Sebuah Peta data dapat membantu analisis kontekstual ini (lihat Mengorganisir Persiapan Sumber Daya).
- Dampak adalah sebuah analisis biaya jika masalah terjadi. Seperti yang disebutkan di bagian 1.2, organisasi-organisasi tidak mengalami masalah-masalah ini secara langsung. Selain itu, pengalaman individu mungkin subjektif. Dengan demikian, dampak mungkin sulit untuk dinilai secara akurat. Organisasi-organisasi harus mempertimbangkan jalan terbaik untuk menginternalisasi dampak pada individu-individu untuk memberikan prioritas dan menanggapi risiko-risiko privasi dengan tepat.[23]

- **Pendekatan penilaian**

  Pendekatan penilaian adalah mekanisme yang memprioritaskan risiko-risiko yang teridentifikasi. Pendekatan penilaian dapat dikategorikan sebagai kuantitatif, semi-kuantitatif, atau kualitatif.[24] [25]

- **Memprioritaskan risiko (ID.RA-P4)**

  Mengingat batasan yang berlaku dari sumber daya organisasi, organisasi-organisasi memprioritaskan risiko untuk memfasilitasi komunikasi tentang cara merespon.[26]

- **Menanggapi risiko (ID.RA-P5)**

  Seperti yang sudah dijelaskan di bagian 1.2.2, pendekatan respon mencakup mitigasi, transfer/berbagi, penghindaran, atau penerimaan.[27]

[21] Sebagai bagian dari PRAM-nya, NIST telah membuat katalog ilustrasi tindakan-tindakan data yang bermasalah dan masalah-masalah untuk dipertimbangkan [3]. Organisasi-organisasi lain mungkin telah menciptakan rangkaian masalah tambahan, atau mungkin merujuknya sebagai konsekuensi buruk yang merugikan Seor.

[22] Lihat NIST PRAM untuk informasi lebih lanjut tentang faktor kontekstual. Id. di Lembar Kerja 2.

[23] NIST PRAM menggunakan biaya-biaya organisasi seperti biaya ketidakpatuhan, biaya bisnis langsung, biaya reputasi, dan biaya budaya internal sebagai pendorong untuk mempertimbangkan bagaimana menilai dampak individu. Id. di Lembar Kerja 3, Tab dampak.

[24] Lihat NIST SP 800-30, Rev.1, Panduan untuk Melakukan Penilaian Risiko [12] hal 14

[25] NIST PRAM menggunakan pendekatan semi-kuantitatif berdasarkan skala 1-10

[26] NIST PRAM menyediakan berbagai representasi, termasuk sebuah *heat map*. Lihat [3] Lembar Kerja 3.

[27] NIST PRAM menyediakan proses untuk merespon risiko-risiko privasi yang diprioritaskan. Id. di Lembar Kerja 4.

Membuat Persyaratan Privasi Yang Bisa Dilacak

Setelah sebuah organisasi menentukan risiko-risiko mana yang harus dimitigasi, hal ini dapat memperbaiki persyaratan privasi dan kemudian memilih dan menerapkan kontrol (misalnya, teknis, fisik, dan/atau kebijakan) untuk memenuhi persyaratan-persyaratan.[28] Sebuah organisasi dapat menggunakan berbagai sumber untuk memilih kontrol-kontrol, seperti NIST SP 800-53, Kontrol-Kontrol Keamanan dan Privasi untuk Sistem Informasi dan Organisasi-Organisasi.[29] Setelah implementasi, sebuah organisasi secara berulang menilai kontrol untuk keefektifannya dalam memenuhi persyaratan-persyaratan privasi dan mengelola risiko privasi. Dengan cara ini, organisasi menciptakan hal yang bisa dilacak antara kontrol-kontrol dan persyaratan-persyaratan privasi, dan menunjukkan akuntabilitas antara sistem-sistem, produk-produk, dan layanan-layanannya serta tujuan-tujuan privasi organisasinya.

Memantau Perubahan

Manajemen risiko privasi bukanlah proses statis. Sebuah organisasi memantau bagaimana perubahan dalam lingkungan bisnisnya — termasuk hukum-hukum baru dan peraturan-peraturan serta teknologi-teknologi baru — dan perubahan tersebut dikorespondensi kan dengan sistem-sistem, produk-produk, dan layanan-layanan yang dapat mempengaruhi risiko privasi dan secara berulang menggunakan praktik-praktik dalam lampiran ini untuk menyesuaikannya. (GV.MT-P1)

[28] Lihat NIST SP 800-37, Rev. 2 [7].

[29] Lihat NIST SP 800-53 sebagai pembaharuan [10].

Lampiran E: Definisi Tingkat-Tingkat Implementasi

Empat Tingkatan-Tingkatan diringkas dibawah ini didefinisikan dengan empat elemen:

Tingkat 1: Parsial

- **Proses Manajemen Risiko Privasi** - Praktik manajemen risiko privasi pada organisasi tidak diformalkan dan risiko dikelola secara khusus/ad hoc dan kadang kala menjadi masalah yang reaktif. Prioritas dari aktivitas-aktivitas privasi mungkin tidak diinformasikan secara langsung oleh prioritas manajemen risiko organisasi, penilaian-penilaian risiko privasi, atau misi atau tujuan bisnis.

- **Program Manajemen Risiko Privasi Terintegrasi** - Terdapat keterbatasan kesadaran tentang risiko privasi di tingkat organisasi. Organisasi menerapkan manajemen risiko privasi secara tidak teratur, kasus per kasus yang disebabkan oleh beragamnya pengalaman atau informasi yang diperoleh dari sumber-sumber luar. Organisasi mungkin tidak memiliki proses yang memungkinkan berbagi informasi tentang pemrosesan data dan mengakibatkan risiko privasi dalam organisasi.

- **Hubungan-hubungan Ekosistem Pemrosesan Data** - Ada pemahaman yang terbatas tentang peran organisasi dalam ekosistem yang lebih besar sehubungan dengan entitas lain (misalnya, para pembeli, para pemasok, para penyedia layanan, para rekan bisnis, para mitra). Organisasi tidak memiliki proses untuk mengidentifikasi bagaimana risiko privasi dapat menyebar di seluruh ekosistem atau untuk mengkomunikasikan risiko atau persyaratan privasi kepada entitas lain dalam ekosistem.

- **Tenaga kerja** - Beberapa personel mungkin memiliki pemahaman yang terbatas tentang risiko privasi atau proses manajemen risiko privasi, tetapi tidak memiliki tanggung jawab privasi khusus. Jika tersedia, pelatihan privasi bersifat khusus/ad hoc dan kontennya tidak selalu mengikuti praktik-praktik terbaik.

Tingkat 2: Risiko yang diinformasikan

- **Proses Manajemen Risiko Privasi** - Praktik-praktik manajemen risiko disetujui oleh manajemen tetapi mungkin tidak ditetapkan sebagai kebijakan organisasi secaa luas. Prioritas aktivitas-aktivitas privasi diinformasikan secara langsung oleh prioritas-prioritas manajemen risiko organisasi, penilaian risiko privasi, misi, atau tujuan-tujuan bisnis.

- **Program Manajemen Risiko Privasi Terintegrasi** - Ada kesadaran akan risiko privasi di tingkat organisasi, tetapi pendekatan organisasi secara luas untuk mengelola risiko privasi mungkin belum mapan. Informasi tentang pemrosesan data dan risiko privasi yang dihasilkan dibagikan di dalam organisasi secara informal. Pertimbangan privasi dalam tujuan dan program organisasi dapat terjadi di beberapa tetapi tidak semua tingkat organisasi. Penilaian risiko privasi terjadi, tetapi biasanya tidak berulang atau berulang.

- **Hubungan-hubungan Ekosistem Pemrosesan Data** - Ada beberapa pemahaman tentang peran-peran dari organisasi dalam ekosistem yang lebih besar sehubungan dengan entitas lain (misalnya, para pembeli, para pemasok, para penyedia layanan,

para rekan bisnis, para mitra). Organisasi menyadari risiko-risiko ekosistem privasi yang terkait dengan produk dan layanan yang disediakan dan digunakannya, tetapi tidak bertindak secara konsisten atau formal atas risiko tersebut.

- **Tenaga kerja** - Ada personel dengan tanggung jawab privasi tertentu, tetapi mereka mungkin juga memiliki tanggung jawab non-privasi. Pelatihan privasi dilakukan secara teratur untuk personel privasi, meskipun tidak ada proses yang konsisten untuk pembaruan tentang praktik-praktik terbaik.

Tingkat 3: Pengetasan Ulang

- **Proses Manajemen Risiko Privasi** - Praktik manajemen risiko organisasi secara resmi diakui dan dinyatakan sebagai kebijakan. Praktik-praktik privasi organisasi diperbarui secara berkala berdasarkan penerapan proses manajemen risiko terhadap perubahan misi atau tujuan-tujuan bisnis dan perubahan landskap risiko, kebijakan, dan teknologi.

- **Program Manajemen Risiko Privasi Terintegrasi** - Pendekatan organisasi secara luas untuk mengelola risiko privasi. Kebijakan-kebijakan, proses-proses, dan prosedur berdasarkan informasi risikoditentukan, diterapkan sebagaimana dimaksud, dan ditinjau. Metode-metode yang konsisten tdibuat untuk merespons perubahan risiko secara efektif. Organisasi secara konsisten dan akurat memantau risiko privasi. Eksekutif senior yang bertanggungjawab untuk privasi dan non-privasi berkomunikasi secara teratur mengenai risiko privasi. Eksekutif senior memastikan pertimbangan privasi melalui semua lini operasi dalam organisasi.

- **Hubungan-hubungan Ekosistem Pemrosesan Data** - Organisasi harus memahami perannya, ketergantungan, dan tergantungan dalam ekosistem yang lebih besar dan dapat berkontribusi pada pemahaman komunitas yang lebih luas tentang risiko-risiko. Organisasi tersebut menyadari risiko dari kinerja ekosistem privasi tersebut yang berkaitan dengan produk dan layanan yang disediakan dan digunakannya. Selain itu, biasanya bertindak secara formal atas risiko tersebut, termasuk mekanisme seperti perjanjian tertulis untuk mengomunikasikan persyaratan privasi, struktur tata kelola, serta implementasi dan pemantauan kebijakan.

- **Tenaga kerja** - Personel privasi yang berdedikasi memiliki pengetahuan dan keterampilan untuk menjalankan peran dan tanggung jawab mereka. Ada pelatihan privasi rutin dan terkini untuk semua personel.

Tingkat 4: Adaptif

- **Proses Manajemen Risiko Privasi** - Organisasi menyesuaikan praktik privasinya berdasarkan pelajaran yang diperoleh dari peristiwa-peristiwa privasi, dan identifikasi risiko-risiko privasi baru. Melalui proses peningkatan terus menerus yang menggabungkan teknologi dan praktik-praktik privasi canggih, organisasi secara aktif beradaptasi dengan perubahan kebijakan dan landskap teknologi dan merespons secara tepat waktu serta efektif untuk mengembangkan risiko-risiko privasi.

- **Program Manajemen Risiko Privasi Terintegrasi** - Ada pendekatan sebuah organisasi secara luas untuk mengelola risiko privasi yang menggunakan kebijakan-kebijakan, proses-proses, dan prosedur-prosedur berdasarkan risiko untuk menangani tindakan

data yang bermasalah. Hubungan antara risiko privasi dan tujuan organisasi dipahami dengan jelas dan dipertimbangkan saat membuat keputusan. Eksekutif senior memantau risiko privasi dalam konteks yang sama dengan risiko keamanan siber, risiko keuangan, dan risiko organisasi lainnya. Anggaran pada organisasi berdasarkan pada pemahaman tentang pengelolaan risiko saat ini dan keadaan perkiraan kedepan serta toleransi risiko. Unit bisnis menerapkan visi eksekutif dan menganalisis risiko sesuai tingkat sistem dalam konteks toleransi risiko organisasi. Manajemen risiko privasi adalah bagian dari budaya organisasi dan berkembang dari pembelajaran yang didapat dan kesadaran terus-menerus atas pemrosesan data dan risiko privasi yang dihasilkan. Organisasi dapat dengan cepat dan efisien menjelaskan perubahan pada tujuan-tujuan banyak bisnis/misi tentang bagaimana risiko didekati dan dikomunikasikan.

- **Hubungan Ekosistem Pemrosesan Data** - Organisasi memahami peran, ketergantungan, dan tergantungan dalam ekosistem yang lebih besar dan berkontribusi pada pemahaman komunitas yang lebih luas tentang risiko. Organisasi menggunakan informasi waktu nyata atau hampir waktu nyata untuk memahami dan secara konsisten bertindak atas risiko ekosistem privasi yang terkait dengan produk dan layanan yang disediakan dan digunakannya. Sebagai tambahan, ia berkomunikasi secara proaktif, menggunakan mekanisme formal (misalnya, perjanjian-perjanjian) dan mekanisme-mekanisme informal untuk mengembangkan dan memelihara hubungan-hubungan ekosistem yang kuat.

- **Tenaga kerja** - Organisasi memiliki kumpulan keterampilan privasi khusus di seluruh struktur organisasi; personil dengan perspektif yang beragam berkontribusi pada manajemen risiko privasi. Ada pelatihan privasi reguler, terkini, dan khusus untuk semua personel. Personil di semua tingkatan memahami nilai-nilai privasi organisasi dan peran mereka dalam menjaganya.