



Check for
updates

Versi 1.0

RANGKA KERJA PRIVASI NIST: ALAT UNTUK MENAMBAHBAIK PRIVASI MELALUI PENGURUSAN RISIKO PERUSAHAAN

16 Januari 2020

Kandungan dokumen ini tidak mempunyai kuasa dan kesan undang-undang serta tidak bertujuan untuk mengikat orang ramai dalam apa cara sekalipun.



<https://doi.org/10.6028/NIST.CSWP.10.may>

Translated by Associate Prof. Ir. Dr. Mohd Fared Abdul Khir CISSP, NCSP. & Nur Insyirah Mohd Fared. Reviewed by TaikaTranslations LLC. Official U.S. Government translation.

The official English language version of this publication is available free of charge from the National Institute of Standards and Technology (NIST): <https://doi.org/10.6028/NIST.CSWP.10>.

Ringkasan eksekutif

Selama lebih daripada dua dekad, Internet dan teknologi maklumat yang berkaitan telah memacu inovasi, nilai ekonomi dan peningkatan yang belum pernah berlaku sebelum ini dalam perkhidmatan sosial. Banyak manfaat ini didorong oleh data tentang individu, yang mengalir melalui ekosistem yang kompleks. Akibatnya, individu mungkin tidak dapat memahami kemungkinan akibat terhadap privasi mereka semasa mereka berinteraksi dengan sistem, produk dan perkhidmatan. Pada masa yang sama, organisasi mungkin tidak menyedari sepenuhnya akibat-akibat ini untuk individu, masyarakat, atau perusahaan mereka, yang boleh menjelaskan jenama mereka, keuntungan mereka dan prospek pertumbuhan masa depan mereka.

Berikutnya proses berasaskan konsensus yang telus termasuk pihak berkepentingan swasta dan awam untuk menghasilkan alat sukarela ini, Institut Piawaian dan Teknologi Kebangsaan (NIST) sedang menerbitkan Rangka Kerja Privasi ini: Alat untuk Meningkatkan Privasi melalui Pengurusan Risiko Perusahaan (Rangka Kerja Privasi), untuk membolehkan amalan kejuruteraan privasi lebih baik yang menyokong privasi melalui konsep reka bentuk dan membantu organisasi melindungi privasi individu. Rangka Kerja Privasi ini boleh menyokong organisasi dalam:

- Membina kepercayaan pelanggan dengan menyokong pembuatan keputusan beretika dalam reka bentuk atau penggunaan produk dan perkhidmatan yang mengoptimumkan penggunaan data yang berfaedah sambil meminimumkan akibat buruk terhadap privasi individu dan masyarakat secara keseluruhan;¹
- Memenuhi kewajipan pematuhan semasa, serta produk dan perkhidmatan kalis masa hadapan bagi memenuhi kewajipan ini dalam persekitaran teknologi dan dasar yang berubah; dan
- Memudahkan komunikasi tentang amalan privasi dengan individu, rakan kongsi perniagaan, penilai dan pengawal selia.

Mendapatkan faedah daripada data sambil mengurus risiko terhadap privasi individu secara serentak, adalah tindakan yang tidak sesuai dilaksanakan secara penyelesaian satu saiz untuk semua (one-size-fits-all). Seperti membina rumah, di mana pemilik rumah membuat pilihan susun atur dan reka bentuk sambil bergantung kepada asas binaan yang telah sedia direka dengan baik, perlindungan privasi juga haruslah membenarkan pilihan individu, selama mitigasi risiko privasi yang efektif telah sedia direka bentuk di dalam produk dan perkhidmatan tersebut. Rangka Kerja Privasi—melalui pendekatan berasaskan risiko dan hasil— adalah cukup fleksibel untuk menangani keperluan privasi yang pelbagai, membolehkan penyelesaian yang lebih inovatif dan efektif yang boleh membawa kepada hasil yang lebih baik untuk individu dan organisasi, dan kekal terkini dengan trend teknologi, seperti kecerdasan buatan (AI) dan Internet Benda (IoT).

Rangka Kerja Privasi ini mengikuti struktur [Rangka Kerja untuk Meningkatkan Infrastruktur Keselamatan Siber Kritikal \(Rangka Kerja Keselamatan Siber\)](#) [1] untuk memudahkan penggunaan kedua-dua rangka kerja secara bersama. Seperti Rangka Kerja Keselamatan Siber, Rangka Kerja Privasi ini terdiri daripada tiga bahagian: Teras, Profil dan Peringkat Pelaksanaan. Setiap komponen memperkuuh pengurusan risiko privasi melalui hubungan antara pemacu perniagaan dan misi, peranan dan tanggungjawab organisasi serta aktiviti perlindungan privasi.

- Teras membolehkan dialog—from peringkat eksekutif hingga peringkat pelaksanaan/operasi—tentang aktiviti perlindungan privasi yang penting dan hasil yang

¹ Tiada standard yang berobjektifkan membuat keputusan beretika; ia berasaskan norma, nilai, dan tuntutan undang-undang dalam masyarakat tertentu

diinginkan.

- Profil membolehkan penentuan keutamaan ke atas hasil dan aktiviti yang paling memenuhi nilai privasi organisasi, keperluan misi atau perniagaan dan risiko.
- Peringkat Pelaksanaan menyokong pembuatan keputusan dan komunikasi tentang kecukupan proses dan sumber organisasi untuk mengurus risiko privasi.

Ringkasnya, Rangka Kerja Privasi bertujuan untuk membantu organisasi membina asas privasi yang lebih baik dengan membawa risiko privasi selaras dengan portfolio risiko perusahaan mereka yang lebih luas.

Penghargaan

Penerbitan ini adalah hasil usaha sama antara NIST dan pihak berkepentingan organisasi dan individu dalam sektor awam dan swasta. Dalam membangunkan Rangka Kerja Privasi, NIST telah bergantung kepada tiga bengkel awam, permintaan untuk maklumat (RFI), permintaan untuk ulasan (RFC), lima webinar dan ratusan interaksi langsung dengan pihak berkepentingan.² NIST mengiktiraf dan berterima kasih kepada semua pihak yang telah menyumbang kepada penerbitan ini.

² Arkib pembangunan lengkap boleh didapati di <https://www.nist.gov/privacy-framework>.

Isi Kandungan

<i>Ringkasan Eksekutif.....</i>	<i>i</i>
<i>Penghargaan</i>	<i>ii</i>
1.0 Pengenalan Rangka Kerja Privasi	1
1.1 Gambaran Keseluruhan Rangka Kerja Privasi.....	2
1.2 Pengurusan Risiko Privasi	3
1.2.1 Keselamatan Siber dan Pengurusan Risiko Privasi.....	3
1.2.2 Penilaian Risiko Privasi.....	5
1.3 Gambaran Keseluruhan Dokumen.....	6
2.0 Asas Rangka Kerja Privasi	6
2.1 Teras	6
2.2 Profil.....	8
2.3 Peringkat Pelaksanaan.....	9
3.0 Cara Menggunakan Rangka Kerja Privasi	9
3.1 Pemetaan kepada Rujukan Bermaklumat	10
3.2 Memperkuuh Kebertanggungjawapan	11
3.3 Menubuhkan atau Menambah Baik Program Privasi	12
3.4 Menggunakan Kitaran Hayat Pembangunan Sistem	13
3.5 Menggunakan dalam Ekosistem Pemprosesan Data.....	14
3.6 Memaklumkan Keputusan Membeli.....	15
Rujukan	16
Lampiran A: Teras Rangka Kerja Privasi	18
Lampiran B: Glosari.....	30
Lampiran C: Akronim.....	34
Lampiran D: Amalan Pengurusan Risiko Privasi	35
Lampiran E: Takrifan Peringkat Pelaksanaan.....	41

Senarai Rajah

Rajah 1: Teras, Profil dan Peringkat Pelaksanaan.....	2
Rajah 2: Keselamatan Siber dan Hubungan Risiko Privasi	3
Rajah 3: Hubungan Antara Risiko Privasi dan Risiko Organisasi	4
Rajah 4: Struktur Teras Rangka Kerja Privasi.....	6
Rajah 5: Menggunakan Fungsi untuk Menguruskan Risiko Keselamatan Siber dan Privasi	7
Rajah 6: Hubungan Antara Teras dan Profil	8
Rajah 7: Nosional Kerjasama dan Aliran Komunikasi Dalam Organisasi	11
Rajah 8: Perhubungan Ekosistem Pemprosesan Data	14

Senarai Jadual

Jadual 1: Fungsi Rangka Kerja Privasi dan Pengecam Unik Kategori	20
Jadual 2: Teras Rangka Kerja Privasi	21
Jadual 3: Kejuruteraan Privasi dan Objektif Keselamatan	38

1.0 Pengenalan Rangka Kerja Privasi

Selama lebih daripada dua dekad, Internet dan teknologi maklumat yang berkaitan telah memacu inovasi, nilai ekonomi dan akses kepada perkhidmatan sosial, yang tidak pernah berlaku sebelum ini. Banyak faedah ini didorong oleh *data tentang individu*, yang mengalir melalui sebuah ekosistem yang kompleks. Akibatnya, seseorang individu mungkin tidak dapat memahami potensi kesan terhadap privasi mereka semasa mereka berinteraksi dengan sistem, produk dan perkhidmatan. Organisasi mungkin turut sama tidak menyedari sepenuhnya akibat-akibat tersebut. Kegagalan mengurus *risiko privasi* boleh mendatangkan kesan buruk secara langsung pada peringkat individu dan masyarakat, dengan kesan susulan pada jenama organisasi, keuntungan dan prospek pertumbuhan masa depan. Mencari cara untuk terus memperoleh manfaat daripada *pemprosesan data* sambil melindungi privasi individu secara serentak adalah mencabar dan tidak sesuai dengan penyelesaian satu saiz untuk semua.

Privasi adalah mencabar kerana ia bukan sahaja konsep yang merangkumi semua yang membantu melindungi nilai penting seperti autonomi dan maruah manusia, tetapi juga cara untuk mencapainya boleh berbeza-beza.³ Sebagai contoh, privasi boleh dicapai melalui pengasingan, mengehadkan pemerhatian atau kawalan individu terhadap aspek identiti mereka (cth., badan, data, reputasi).⁴ Selain itu, autonomi dan maruah manusia bukanlah binaan yang tetap dan boleh diukur; mereka ditapis melalui kepelbagaian budaya dan perbezaan individu. Sifat privasi yang luas dan berubah-ubah ini menjadikannya sukar untuk berkomunikasi dengan jelas tentang risiko privasi dalam dan antara organisasi serta dengan individu. Apa yang tiada ialah bahasa bersama dan alat praktikal yang cukup fleksibel untuk menangani keperluan privasi yang pelbagai.

Rangka Kerja Privasi NIST sukarela ini: Alat untuk Meningkatkan Privasi melalui Pengurusan Risiko Perusahaan (Rangka Kerja Privasi) adalah bertujuan untuk digunakan secara meluas oleh organisasi dari semua saiz dan agnostik kepada mana-mana teknologi, sektor, undang-undang atau bidang kuasa tertentu. Menggunakan pendekatan umum—boleh disesuaikan dengan mana-mana peranan organisasi dalam *ekosistem pemprosesan data*—tujuan Rangka Kerja Privasi ini adalah untuk membantu organisasi mengurus risiko privasi dengan cara:

- Mengambil kira privasi semasa mereka, mereka bentuk dan menggunakan sistem, produk dan perkhidmatan yang memberi kesan kepada individu;
- Berkomunikasi tentang amalan privasi mereka; dan
- Menggalakkan kerjasama tenaga kerja merentas organisasi—contohnya, dalam kalangan eksekutif, undang-undang dan teknologi maklumat (IT)—melalui pembangunan Profil, pemilihan Peringkat dan pencapaian hasil.

³ Autonomi dan maruah adalah konsep yang termaktub dalam Deklarasi Universal Hak Asasi Manusia Pertubuhan Bangsa-Bangsa Bersatu di <https://www.un.org/en/universal-declaration-human-rights/>.

⁴ Terdapat banyak penerbitan yang memberikan penerangan mendalam tentang latar belakang privasi atau aspek konsep yang berbeza. Untuk dua contoh, lihat Solove D (2010) *Understanding Privacy* (Harvard University Press, Cambridge, MA), <https://ssrn.com/abstract=1127888>; dan Selinger E, Hartzog W (2017) *Obscurity and Privacy, Spaces for the Future: A Companion to Philosophy of Technology*, eds Pitt J, Shew A (Taylor & Francis, New York, NY), Chapter 12, 1st Ed., <https://doi.org/10.4324/9780203735657>.

1.1 Gambaran Keseluruhan Rangka Kerja Privasi

Seperti yang ditunjukkan dalam **Rajah 1**, Rangka Kerja Privasi terdiri daripada tiga bahagian: Teras, Profil dan Peringkat Pelaksanaan.

Setiap komponen memperkuuh cara organisasi mengurus risiko privasi melalui hubungan antara pemacu perniagaan atau misi, peranan dan tanggungjawab organisasi serta aktiviti perlindungan privasi. Seperti yang dijelaskan lebih lanjut dalam seksyen 2:

- Teras ialah satu set aktiviti dan hasil perlindungan privasi yang membolehkan aktiviti dan hasil perlindungan privasi yang telah ditentukan keutamaannya, disampaikan merentasi sesebuah organisasi daripada peringkat eksekutif ke peringkat pelaksanaan/operasi. Teras dibahagikan lagi kepada Kategori dan Subkategori utama—yang merupakan hasil diskret—untuk setiap Fungsi.
- *Profil* mewakili aktiviti privasi semasa organisasi atau hasil yang diingini. Untuk membangunkan Profil, organisasi boleh menyemak semua hasil dan aktiviti dalam Teras untuk menentukan yang mana paling penting untuk difokuskan berdasarkan pemacu perniagaan atau misi, peranan ekosistem pemprosesan data, jenis pemprosesan data dan keperluan privasi individu. Organisasi boleh mencipta atau menambah Fungsi, Kategori dan Subkategori mengikut keperluan. Profil boleh digunakan untuk mengenal pasti peluang untuk meningkatkan postur privasi dengan membandingkan Profil "Semasa" (keadaan "sebagaimana adanya") dengan Profil "Sasaran" (keadaan "untuk menjadi"). Profil boleh digunakan untuk menjalankan penilaian kendiri dan untuk berkomunikasi dalam organisasi atau antara organisasi tentang cara risiko privasi diuruskan.
- *Peringkat Pelaksanaan* ("Peringkat") menyediakan titik rujukan tentang cara organisasi melihat risiko privasi dan sama ada ia mempunyai proses dan sumber yang mencukupi untuk mengurus risiko tersebut. Peringkat mencerminkan perkembangan daripada tindak balas tidak formal dan reaktif kepada pendekatan yang tangkas (*agile*) dan termaklum risiko (*risk informed*). Apabila memilih Peringkat, organisasi harus mempertimbangkan Profil Sasarannya dan bagaimana pencapaian boleh disokong atau dihalang oleh amalan pengurusan risiko semasanya, tahap integrasi risiko privasi ke dalam portfolio pengurusan risiko perusahaannya, hubungan ekosistem pemprosesan datanya, dan komposisi tenaga kerja dan program latihannya.

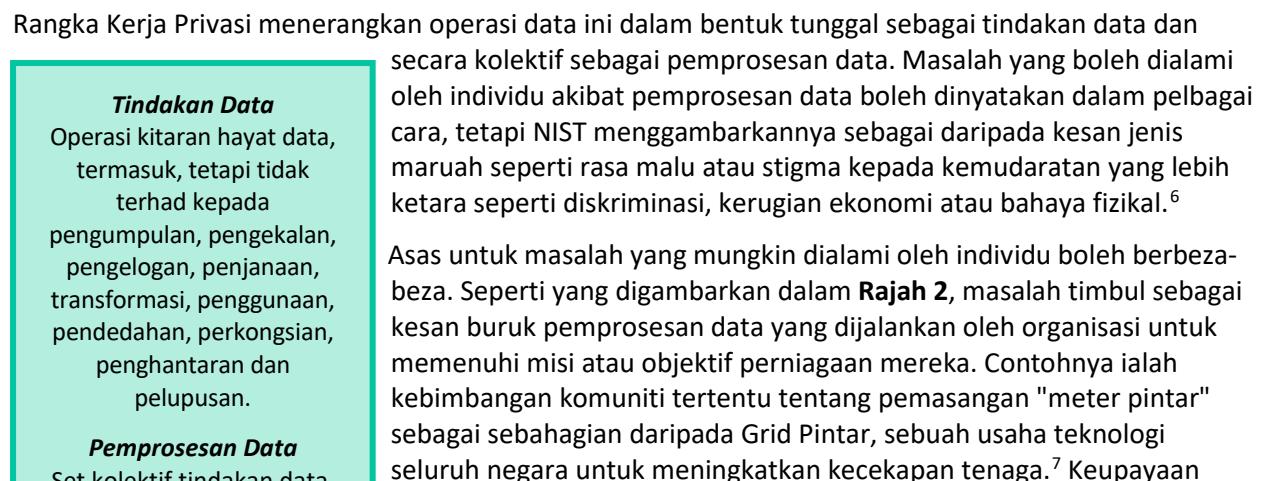


1.2 Pengurusan Risiko Privasi

Walaupun sesetengah organisasi mempunyai pemahaman yang kukuh tentang *pengurusan risiko privasi*, pemahaman umum tentang banyak aspek topik ini masih belum meluas.⁵ Untuk menggalakkan pemahaman yang lebih luas, seksyen ini merangkumi konsep dan pertimbangan yang boleh digunakan oleh organisasi untuk membangun, menambah baik atau berkomunikasi mengenai pengurusan risiko privasi. Lampiran D menyediakan maklumat tambahan tentang amalan pengurusan risiko privasi utama.

1.2.1 Keselamatan Siber dan Pengurusan Risiko Privasi

Sejak dikeluarkan pada 2014, Rangka Kerja Keselamatan Siber telah membantu organisasi berkomunikasi dan mengurus risiko keselamatan siber. [1]. Walau pun mengurus risiko keselamatan siber menyumbang kepada pengurusan risiko privasi, ia tidak mencukupi, kerana risiko privasi juga boleh timbul dengan cara yang tidak berkait dengan insiden keselamatan siber, seperti yang digambarkan dalam **Rajah 2**. Mempunyai pemahaman umum tentang asal-usul berbeza keselamatan siber dan risiko privasi adalah penting dalam menentukan penyelesaian yang paling berkesan untuk menangani risiko tersebut. Pendekatan Rangka Kerja Privasi ini terhadap risiko privasi adalah dengan mempertimbangkan peristiwa privasi sebagai masalah yang mungkin dialami individu, yang timbul daripada operasi sistem, produk atau perkhidmatan melibatkan data, sama ada dalam bentuk digital atau bukan digital, melalui kitaran hayat lengkap daripada pengumpulan data hingga pelupusan.



⁵ Lihat *Summary Analysis of the Responses to the NIST Privacy Framework Request for Information* [2] di m. 7

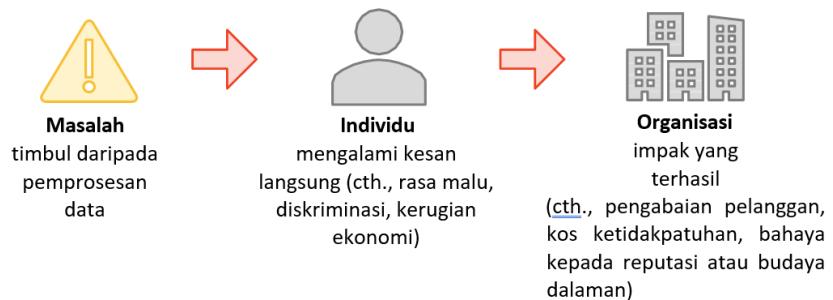
⁶ NIST telah mencipta katalog ilustrasi masalah untuk digunakan dalam penilaian risiko privasi. Lihat *NIST Privacy Risk Assessment Methodology* [3]. Organisasi lain mungkin telah mencipta kategori masalah lain, atau mungkin merujuknya sebagai akibat buruk atau bahaya.

⁷ Lihat, sebagai contoh, NIST Interagency or Internal Report (IR) 7628 Revision 1 Volume 1, *Guidelines for Smart Grid Cybersecurity: Volume 1 – Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements* at [4] m. 26.

meter ini untuk mengumpul, merekod dan mengedarkan maklumat yang sangat terperinci tentang penggunaan elektrik isi rumah boleh memberikan gambaran tentang tingkah laku orang ramai di dalam rumah mereka.⁸ Meter beroperasi seperti yang diinginkan, tetapi pemprosesan data boleh menyebabkan orang berasa diawasi.

Dalam dunia yang semakin terhubung, beberapa masalah boleh timbul hanya daripada interaksi individu dengan sistem, produk dan perkhidmatan, walaupun apabila data yang diproses tidak dikaitkan secara langsung dengan individu yang boleh dikenal pasti. Contohnya, teknologi bandar pintar boleh digunakan untuk mengubah atau mempengaruhi tingkah laku orang seperti di mana atau cara mereka bergerak melalui bandar.⁹ Masalah juga boleh timbul apabila terdapat kehilangan kerahsiaan, integriti atau ketersediaan pada satu ketika dalam pemprosesan data, seperti kecurian data oleh penyerang luar atau akses atau penggunaan data yang tidak dibenarkan oleh pekerja. **Rajah 2** menunjukkan jenis peristiwa privasi berkaitan keselamatan siber ini sebagai pertindihan antara risiko privasi dan keselamatan siber.

Sebaik sahaja organisasi boleh mengenal pasti kemungkinan sebarang masalah tertentu yang timbul daripada pemprosesan data, yang Rangka Kerja Privasi merujuk sebagai *tindakan data bermasalah*, ia boleh menilai kesan sekiranya tindakan data bermasalah berlaku. Penilaian impak ini adalah tempat risiko privasi dan risiko organisasi bersilang. Individu, sama ada secara bersendirian atau berkumpulan (termasuk di peringkat masyarakat) mengalami kesan langsung masalah. Akibat daripada masalah yang dialami individu, organisasi mungkin mengalami kesan seperti kos ketidakpatuhan, kehilangan hasil yang timbul daripada pengabaian produk dan perkhidmatan pelanggan atau kemudaratannya kepada reputasi jenama luaran atau budaya dalamannya. Organisasi biasanya menguruskan jenis impak ini pada peringkat pengurusan risiko perusahaan; dengan menghubungkan masalah yang dialami individu kepada impak organisasi yang difahami dengan baik ini, organisasi boleh membawa risiko privasi kepada setara dengan risiko lain yang mereka uruskan dalam portfolio mereka yang lebih luas dan mendorong pembuatan keputusan yang lebih termaklum tentang peruntukan sumber untuk mengukuhkan program privasi. **Rajah 3** menggambarkan hubungan ini antara risiko privasi dan risiko organisasi.



Rajah 3: Hubungan Antara Risiko Privasi dan Risiko Organisasi

⁸ Lihat NIST IR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* at [5] m. 2. Untuk jenis risiko privasi tambahan yang dikaitkan dengan kesan buruk ke atas individu pemprosesan data, lihat Lampiran E NIST IR 8062.

⁹ Lihat Newcombe T (2016) Security, Privacy, Governance Concerns About Smart City Technologies Grow. *Government Technology*. Boleh didapati di <http://www.govtech.com/Security-Privacy-Governance-Concerns-About-Smart-City-Technologies-Grow.html>.

1.2.2 Penilaian Risiko Privasi

Pengurusan risiko privasi ialah satu set proses merentas organisasi yang membantu organisasi memahami cara sistem, produk dan perkhidmatan mereka boleh menimbulkan masalah kepada individu dan cara membangunkan penyelesaian yang berkesan untuk mengurus risiko tersebut. *Penilaian risiko privasi* ialah sub-proses untuk mengenal pasti dan menilai risiko privasi tertentu. Secara umum, penilaian risiko privasi menghasilkan maklumat yang boleh membantu organisasi untuk menimbang faedah pemprosesan data berbanding risiko dan untuk menentukan tindak balas yang sesuai—kadangkala dirujuk sebagai perkadaran.¹⁰ Organisasi boleh memilih untuk mengutamakan dan bertindak balas terhadap risiko privasi dengan cara yang berbeza, bergantung pada potensi kesan kepada individu dan kesan yang terhasil kepada organisasi. Pendekatan tindak balas termasuk:¹¹

- Mengurangkan risiko (cth., organisasi mungkin boleh menggunakan langkah teknikal dan/atau dasar pada sistem, produk atau perkhidmatan yang meminimumkan risiko ke tahap yang boleh diterima);
- Memindahkan atau berkongsi risiko (cth., kontrak ialah cara berkongsi atau memindahkan risiko kepada organisasi lain, notis privasi dan mekanisme persetujuan ialah cara berkongsi risiko dengan individu);
- Mengelakkan risiko (cth., organisasi mungkin menentukan bahawa risiko melebihi manfaat, dan melepaskan atau menamatkan pemprosesan data); atau
- Menerima risiko (cth., organisasi mungkin menentukan bahawa masalah untuk individu adalah minimum atau tidak mungkin berlaku, oleh itu manfaatnya melebihi risiko, dan tidak perlu melabur sumber dalam mitigasi).

Penilaian risiko privasi amat penting kerana, seperti yang dinyatakan di atas, privasi ialah syarat yang melindungi pelbagai nilai. Kaedah untuk melindungi nilai-nilai ini mungkin berbeza, dan lebih-lebih lagi, mungkin dalam ketegangan antara satu sama lain. Bergantung kepada objektifnya, jika organisasi cuba mencapai privasi dengan mengehadkan pemerhatian, ini mungkin membawa kepada pelaksanaan langkah seperti seni bina data teragih atau teknik kriptografi yang meningkatkan privasi yang menyembunyikan data walaupun daripada organisasi. Jika organisasi juga cuba untuk membolehkan kawalan individu, langkah-langkah itu mungkin bercanggah. Contohnya, jika individu meminta akses kepada data, organisasi mungkin tidak dapat menghasilkan data jika data telah diedarkan atau disulitkan dengan cara yang tidak boleh diakses oleh organisasi. Penilaian risiko privasi boleh membantu organisasi memahami dalam konteks tertentu nilai yang perlu dilindungi, kaedah untuk digunakan dan cara mengimbangi pelaksanaan pelbagai jenis langkah.

Akhir sekali, penilaian risiko privasi membantu organisasi membezakan antara risiko privasi dan risiko pematuhan. Mengenal pasti sama ada pemprosesan data boleh menimbulkan masalah kepada individu, walaupun organisasi mungkin mematuhi sepenuhnya undang-undang atau peraturan yang berkenaan, boleh membantu dalam membuat keputusan beretika dalam reka bentuk atau penggunaan sistem, produk dan perkhidmatan. Walaupun tiada piawaian objektif untuk membuat keputusan beretika, ia berdasarkan norma, nilai dan jangkaan undang-undang dalam masyarakat tertentu. Ini memudahkan pengoptimuman penggunaan data yang berfaedah sambil meminimumkan akibat buruk terhadap privasi individu dan masyarakat secara keseluruhan, serta mengelakkan kehilangan kepercayaan yang merosakkan reputasi organisasi, memperlambangkan penerimaan atau menyebabkan pengabaian produk

¹⁰ Lihat European Data Protection Supervisor (2019) *Necessity & Proportionality*. Boleh didapati di https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en.

¹¹ Lihat NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* [6].

dan perkhidmatan.

Lihat Lampiran D untuk mendapatkan maklumat lanjut tentang aspek operasi penilaian risiko privasi.

1.3 Gambaran Keseluruhan Dokumen

Baki dokumen ini mengandungi seksyen dan lampiran berikut:

- **Seksyen 2** menerangkan komponen Rangka Kerja Privasi: Teras, Profil dan Peringkat Pelaksanaan.
- **Seksyen 3** membentangkan contoh bagaimana Rangka Kerja Privasi boleh digunakan.
- **Seksyen Rujukan** menyenaraikan rujukan untuk dokumen.
- **Lampiran A** membentangkan Teras Rangka Kerja Privasi dalam format jadual: Fungsi, Kategori dan Subkategori.
- **Lampiran B** mengandungi glosari istilah yang dipilih.
- **Lampiran C** menyenaraikan akronim yang digunakan dalam dokumen ini.
- **Lampiran D** mempertimbangkan amalan utama yang menyumbang kepada pengurusan risiko privasi yang berjaya.
- **Lampiran E** mentakrifkan Peringkat Pelaksanaan.

2.0 Asas Rangka Kerja Privasi

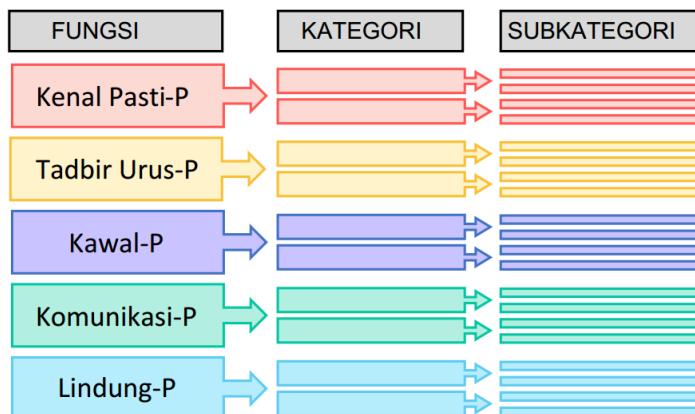
Rangka Kerja Privasi menyediakan bahasa bersama untuk memahami, mengurus dan menyampaikan risiko privasi dengan pihak berkepentingan dalaman dan luaran. Ia boleh disesuaikan dengan mana-mana peranan organisasi dalam ekosistem pemprosesan data. Ia boleh digunakan untuk membantu mengenal pasti dan mengutamakan tindakan untuk mengurangkan risiko privasi, dan ia merupakan alat untuk menyelaraskan pendekatan dasar, perniagaan dan teknologi untuk mengurus risiko tersebut.

2.1 Teras

Ditetapkan dalam Lampiran A, Teras menyediakan set aktiviti dan hasil yang semakin terperinci yang membolehkan dialog tentang mengurus risiko privasi. Seperti yang digambarkan dalam **Rajah 4**, Teras terdiri daripada Fungsi, Kategori dan Subkategori.

Elemen Teras berfungsi bersama:

- *Fungsi* menganjurkan aktiviti privasi asas pada tahap tertinggi mereka. Ia membantu organisasi dalam menyatakan pengurusan risikonya dengan memahami dan mengurus pemprosesan data, membolehkan keputusan *pengurusan risiko*, menentukan cara berinteraksi dengan individu, dan menambah baik dengan belajar daripada aktiviti sebelumnya. Ia tidak bertujuan untuk membentuk laluan bersiri atau membawa kepada keadaan akhir statik yang dikehendaki. Sebaliknya, Fungsi harus dilakukan secara serentak dan berterusan untuk membentuk atau meningkatkan budaya operasi yang menangani sifat dinamik risiko privasi.
- *Kategori* ialah pembahagian Fungsi kepada kumpulan hasil privasi yang berkait rapat

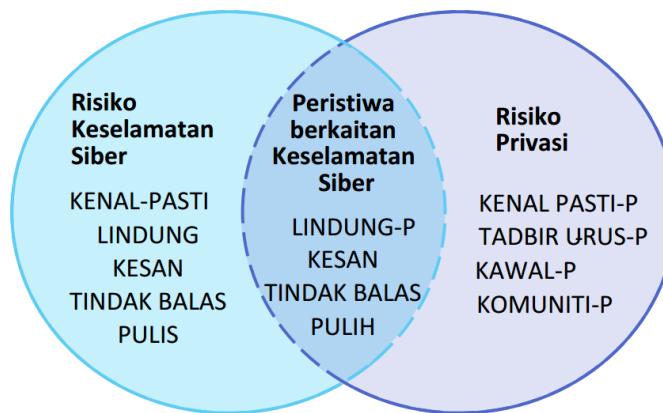


Rajah 4: Struktur Teras Rangka Kerja Privasi

dengan keperluan program dan aktiviti tertentu.

- *Subkategori* membahagikan lagi Kategori kepada hasil khusus aktiviti teknikal dan/atau pengurusan. Mereka menyediakan satu set hasil yang walaupun tidak menyeluruh, membantu menyokong pencapaian hasil dalam setiap Kategori.

Lima Fungsi, Kenal Pasti-P, Tadbir Urus-P, Kawal-P, Komunikasi-P, dan Lindung-P, yang ditakrifkan di bawah, boleh digunakan untuk mengurus risiko privasi yang timbul daripada pemprosesan data.¹² Lindung-P tertumpu secara khusus pada mengurus risiko yang berkaitan dengan peristiwa privasi berkaitan keselamatan siber (cth., *pelanggaran privasi*). [Rangka Kerja Keselamatan Cyber](#), walaupun bertujuan untuk merangkumi semua jenis insiden keselamatan siber, boleh dimanfaatkan untuk menyokong lagi pengurusan risiko yang berkaitan dengan peristiwa privasi berkaitan keselamatan siber dengan menggunakan Fungsi Kesan, Tindak Balas dan Pulih. Sebagai alternatif, organisasi boleh menggunakan kelima-lima Fungsi Rangka Kerja Keselamatan Siber bersama-sama dengan Kenal Pasti-P, Tadbir Urus-P, Kawal-P dan Komunikasi-P untuk menangani risiko privasi dan keselamatan siber secara kolektif. **Rajah 5** menggunakan rajah Venn daripada seksyen 1.2.1 untuk menunjukkan bagaimana Fungsi daripada kedua-dua rangka kerja boleh digunakan dalam kombinasi yang berbeza-beza untuk mengurus aspek privasi dan risiko keselamatan siber yang berbeza. Lima Fungsi Rangka Kerja Privasi ditakrifkan seperti berikut:



Rajah 5: Menggunakan Fungsi untuk Menguruskan Risiko Keselamatan Siber dan Privasi

- *Kenal Pasti-P* – Membangunkan pemahaman organisasi untuk mengurus risiko privasi bagi individu yang timbul daripada pemprosesan data.

Aktiviti dalam Fungsi Kenal Pasti-P adalah asas untuk penggunaan Rangka Kerja Privasi yang berkesan. Menginventori keadaan di mana data diproses, memahami kepentingan privasi individu secara langsung atau tidak langsung disampaikan atau terjejas oleh organisasi, dan menjalankan penilaian risiko membolehkan organisasi memahami persekitaran perniagaan di mana ia beroperasi dan mengenal pasti serta mengutamakan risiko privasi.

- *Tadbir Urus-P* – Membangunkan dan melaksanakan struktur tadbir urus organisasi untuk membolehkan pemahaman berterusan tentang keutamaan pengurusan risiko organisasi yang dimaklumkan oleh risiko privasi.

Fungsi Tadbir Urus-P adalah asas yang sama, tetapi memberi tumpuan kepada aktiviti peringkat organisasi seperti mewujudkan nilai dan dasar privasi organisasi, mengenal pasti keperluan undang-undang/kawal selia, dan memahami *toleransi risiko* organisasi yang membolehkan organisasi memfokus dan mengutamakan usahanya, selaras dengan strategi pengurusan risiko dan keperluan perniagaan.

- *Kawal-P* – Membangunkan dan melaksanakan aktiviti yang sesuai untuk membolehkan

¹² “-P” di hujung setiap nama Fungsi menunjukkan bahawa ia adalah daripada Rangka Kerja Privasi untuk mengelakkan kekeliruan dengan Fungsi Rangka Kerja Keselamatan Siber.

organisasi atau individu mengurus data dengan butiran yang mencukupi untuk mengurus risiko privasi

Fungsi Kawal-P mempertimbangkan pengurusan pemprosesan data dari sudut pandangan kedua-dua organisasi dan individu.

- *Komunikasi-P* – Membangunkan dan melaksanakan aktiviti yang sesuai untuk membolehkan organisasi dan individu mempunyai pemahaman yang boleh dipercayai dan terlibat dalam dialog tentang cara data diproses dan risiko privasi yang berkaitan.

Fungsi Komunikasi-P menyedari bahawa kedua-dua organisasi dan individu mungkin perlu mengetahui cara data diproses untuk mengurus risiko privasi dengan berkesan.

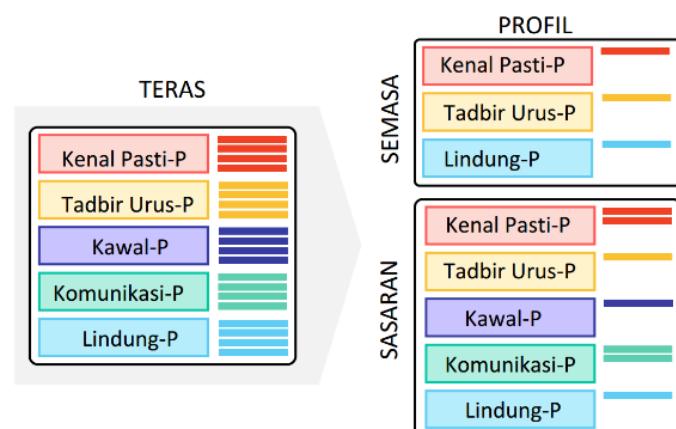
- *Lindung-P* – Membangunkan dan melaksanakan perlindungan pemprosesan data yang sesuai.

Fungsi Lindung-P meliputi perlindungan data untuk mengelakkan peristiwa privasi berkaitan keselamatan siber, pertindihan antara pengurusan risiko privasi dan keselamatan siber.

2.2 Profil

Profil ialah pilihan Fungsi, Kategori dan Subkategori tertentu daripada Teras, yang diutamakan oleh organisasi untuk membantunya mengurus risiko privasi. Profil boleh digunakan untuk menerangkan keadaan semasa dan keadaan sasaran yang dikehendaki bagi aktiviti privasi tertentu. Profil Semasa menunjukkan hasil privasi yang sedang dicapai oleh organisasi, manakala Profil Sasaran menunjukkan hasil yang diperlukan untuk mencapai matlamat pengurusan risiko privasi yang dikehendaki. Perbezaan antara kedua-dua Profil membolehkan organisasi mengenal pasti jurang, membangunkan pelan tindakan untuk penambahbaikan dan mengukur sumber yang diperlukan (cth., kakitangan, pembentangan) untuk mencapai hasil privasi. Ini membentuk asas perancangan organisasi untuk mengurangkan risiko privasi dengan cara yang kos efektif dan diutamakan. Profil juga boleh membantu dalam menyampaikan risiko dalam dan antara organisasi dengan membantu organisasi memahami dan membandingkan keadaan semasa dan hasil privasi yang dikehendaki.

Rangka Kerja Privasi tidak menetapkan templat Profil untuk membolehkan fleksibiliti dalam pelaksanaan. Apabila membangunkan Profil, organisasi boleh memilih atau menyesuaikan Fungsi, Kategori dan Subkategori mengikut keperluan khususnya, termasuk membangunkan Fungsi, Kategori dan Subkategori tambahannya sendiri untuk mengambil kira risiko organisasi yang unik. Organisasi menentukan keperluan ini dengan mempertimbangkan misi atau objektif perniagaannya, nilai privasi dan toleransi risiko; peranan dalam ekosistem pemprosesan data atau sektor industri; keperluan undang-undang/kawal selia dan amalan terbaik industri; keutamaan dan sumber pengurusan risiko; dan keperluan privasi individu yang secara langsung atau tidak langsung dilayan atau dipengaruhi oleh sistem, produk atau perkhidmatan organisasi.



Rajah 6: Hubungan di antara Teras dan Profil

Seperti yang digambarkan dalam **Rajah 6**, tiada susunan khusus pembangunan Profil. Organisasi boleh membangunkan Profil Sasaran terlebih dahulu untuk menumpukan pada hasil yang diingini untuk

privasi dan kemudian membangunkan Profil Semasa untuk mengenal pasti jurang; sebagai alternatif, sesebuah organisasi boleh bermula dengan mengenal pasti aktiviti semasanya dan kemudian mempertimbangkan cara melaraskan aktiviti ini untuk Profil Sasarannya. Organisasi boleh memilih untuk membangunkan berbilang Profil untuk peranan, sistem, produk atau perkhidmatan yang berbeza, atau kategori individu (cth., pekerja, pelanggan) untuk membolehkan keutamaan aktiviti dan hasil yang lebih baik di mana mungkin terdapat tahap risiko privasi yang berbeza.

2.3 Peringkat Pelaksanaan

Peringkat menyokong pembuatan keputusan organisasi tentang cara mengurus risiko privasi dengan mengambil kira sifat risiko privasi yang ditimbulkan oleh sistem, produk atau perkhidmatan organisasi dan kecukupan proses serta sumber yang ada pada organisasi untuk mengurus risiko tersebut. Apabila memilih Peringkat, organisasi harus mempertimbangkan Profil Sasarannya dan bagaimana pencapaian boleh disokong atau dihalang oleh amalan pengurusan risiko semasanya, tahap integrasi privasi risiko ke dalam portfolio pengurusan risiko perusahaannya, hubungan ekosistem pemprosesan datanya serta komposisi tenaga kerja dan program latihannya.

Terdapat empat Peringkat yang berbeza, Separa (Peringkat 1), Risiko Termaklum (Peringkat 2), Boleh Ulang (Peringkat 3) dan Peringkat Mudah Suai (Peringkat 4), yang perihalannya terdapat dalam Lampiran E. Peringkat mewakili satu perkembangan, walaupun bukan sesuatu yang wajib. Walaupun organisasi di Peringkat 1 berkemungkinan akan mendapat manfaat dengan berpindah ke Peringkat 2, tidak semua organisasi perlu mencapai Peringkat 3 atau 4 (atau mungkin hanya menumpukan pada bidang tertentu dalam Peringkat ini). Kemajuan ke Peringkat yang lebih tinggi adalah sesuai apabila proses atau sumber organisasi pada Peringkat semasa mungkin tidak mencukupi untuk membantunya mengurus risiko privasinya.

Organisasi boleh menggunakan Peringkat untuk berkomunikasi secara dalaman tentang peruntukan sumber yang diperlukan untuk maju ke Peringkat yang lebih tinggi atau sebagai penanda aras umum untuk mengukur kemajuan dalam keupayaannya mengurus risiko privasi. Organisasi juga boleh menggunakan Peringkat untuk memahami skala sumber dan proses organisasi lain dalam ekosistem pemprosesan data dan cara ia sejajar dengan keutamaan pengurusan risiko privasi organisasi. Namun begitu, kejayaan pelaksanaan Rangka Kerja Privasi adalah berdasarkan pencapaian hasil yang diterangkan dalam Profil Sasaran organisasi dan bukan berdasarkan penentuan Peringkat.

3.0 Cara Menggunakan Rangka Kerja Privasi

Apabila digunakan sebagai alat pengurusan risiko, Rangka Kerja Privasi boleh membantu organisasi dalam usahanya untuk mengoptimumkan penggunaan data yang berfaedah dan pembangunan sistem, produk dan perkhidmatan yang inovatif sambil meminimumkan akibat buruk bagi individu. Rangka Kerja Privasi boleh membantu organisasi menjawab soalan asas, "Bagaimakah kami mempertimbangkan kesan kepada individu semasa kami membangunkan sistem, produk dan perkhidmatan kami?" Untuk mengambil kira keperluan unik sesebuah organisasi, penggunaan Rangka Kerja Privasi adalah fleksibel, walaupun ia direka bentuk untuk melengkapkan operasi pembangunan sistem dan perniagaan sedia ada. Keputusan tentang cara menerapkannya diserahkan kepada organisasi pelaksana. Sebagai contoh, organisasi mungkin sudah mempunyai proses pengurusan risiko privasi yang mantap, tetapi mungkin menggunakan lima Fungsi Teras sebagai cara yang diperkemas untuk menganalisis dan menyatakan sebarang jurang. Sebagai alternatif, organisasi yang ingin mewujudkan program privasi boleh menggunakan Kategori Teras dan Subkategori sebagai rujukan. Organisasi lain mungkin membandingkan Profil atau Peringkat untuk menyelaraskan keutamaan pengurusan risiko privasi merentas peranan berbeza dalam ekosistem pemprosesan data. Kepelbagaiannya cara Rangka Kerja Privasi boleh digunakan oleh organisasi seharusnya tidak menggalakkan tanggapan "pematuhan dengan

"Rangka Kerja Privasi" sebagai konsep seragam atau boleh dirujuk secara luaran. Subseksyen yang berikut menunjukkan beberapa pilihan untuk penggunaan Rangka Kerja Privasi.

3.1 Pemetaan kepada Rujukan Bermaklumat

Rujukan bermaklumat ialah pemetaan kepada Subkategori untuk menyediakan sokongan pelaksanaan, termasuk pemetaan alatan, panduan teknikal, piawaian, undang-undang, peraturan dan amalan terbaik. Lintasan yang memetakan peruntukan piawaian, undang-undang dan peraturan kepada Subkategori boleh membantu organisasi menentukan aktiviti atau hasil yang perlu diutamakan untuk memudahkan pematuhan. Rangka Kerja Privasi adalah teknologi neutral, tetapi ia menyokong inovasi teknologi kerana mana-mana organisasi atau sektor industri boleh membangunkan pemetaan ini apabila teknologi dan keperluan perniagaan yang berkaitan berkembang. Dengan bergantung pada piawaian, garis panduan dan amalan berasaskan konsensus, alat dan kaedah yang tersedia untuk mencapai hasil privasi yang positif boleh merentasi sempadan dan menampung sifat global risiko privasi. Penggunaan piawaian sedia ada dan yang baharu muncul akan membolehkan ekonomi skala dan memacu pembangunan sistem, produk dan perkhidmatan yang memenuhi keperluan pasaran yang dikenal pasti sambil mengambil kira keperluan privasi individu.

Jurang dalam pemetaan juga boleh digunakan untuk mengenal pasti di mana piawaian, garis panduan dan amalan tambahan atau yang disemak semula akan membantu organisasi menangani keperluan yang muncul. Jurang dalam pemetaan juga boleh digunakan untuk mengenal pasti di mana piawaian, garis panduan dan amalan tambahan atau yang disemak semula akan membantu organisasi menangani keperluan yang muncul. Organisasi yang melaksanakan Subkategori tertentu atau membangunkan Subkategori baharu, mungkin mendapat bahawa terdapat panduan yang tidak mencukupi untuk aktiviti atau hasil yang berkaitan. Untuk menangani keperluan itu, organisasi mungkin bekerjasama dengan pemimpin teknologi dan/atau badan piawai untuk merangka, membangun dan menyelaraskan piawaian, garis panduan atau amalan.

Repositori rujukan bermaklumat boleh didapati di <https://www.nist.gov/privacy-framework>. Sumber ini boleh menyokong penggunaan Rangka Kerja Privasi oleh organisasi dan pencapaian amalan privasi yang lebih baik.

3.2 Memperkuuh Akauntabiliti

Kebertanggungjawapan secara amnya dianggap sebagai prinsip privasi yang utama, walaupun secara konsep ia bukan unik untuk privasi.¹³ Kebertanggungjawapan berlaku di seluruh organisasi dan ia boleh dinyatakan pada tahap pengabstrakan yang berbeza-beza, contohnya sebagai nilai budaya, sebagai dasar dan prosedur tadbir urus, atau sebagai hubungan

kebolehkesanan antara *keperluan privasi dan kawalan*. Pengurusan risiko privasi boleh menjadi cara untuk menyokong kebertanggungjawapan di semua peringkat organisasi kerana ia menghubungkan eksekutif kanan, yang boleh menyampaikan nilai privasi dan toleransi risiko organisasi, kepada mereka di peringkat pengurus perniagaan/proses, yang boleh bekerjasama dalam pembangunan dan pelaksanaan dasar serta prosedur tadbir urus yang menyokong nilai privasi organisasi. Polisi dan prosedur ini kemudiannya boleh disampaikan kepada mereka di peringkat pelaksanaan/operasi, yang bekerjasama dalam menentukan keperluan privasi yang menyokong pernyataan dasar dan prosedur dalam sistem, produk dan perkhidmatan organisasi. Kaitangan di peringkat pelaksanaan/operasi juga memilih, melaksana dan menilai kawalan sebagai langkah teknikal dan dasar yang memenuhi keperluan privasi, dan melaporkan kemajuan, jurang dan kekurangan, pengurusan insiden dan mengubah risiko privasi supaya mereka yang berada di dalam perniagaan/peringkat pengurus proses dan eksekutif kanan boleh lebih memahami dan bertindak balas dengan sewajarnya.

Rajah 7 menyediakan gambaran grafik kerjasama dan komunikasi dua hala ini dan bagaimana elemen Rangka Kerja Privasi boleh digabungkan untuk memudahkan proses. Dengan cara ini, organisasi boleh menggunakan Rangka Kerja Privasi sebagai alat untuk menyokong akauntabiliti. Mereka juga boleh menggunakan Rangka Kerja Privasi bersama-sama dengan rangka kerja dan panduan lain yang



Rajah 7: Cadangan Kerjasama dan Aliran Komunikasi Dalam Organisasi

¹³ Lihat, cth., Organisation for Economic Co-operation and Development (OECD) (2013) *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, boleh didapati di <https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>; International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) (2011) *ISO/IEC 29100:2011 – Information technology – Security techniques – Privacy framework* (ISO, Geneva, Switzerland), boleh didapati 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) *Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services*, boleh didapati di https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf.

menyediakan amalan tambahan untuk mencapai akauntabiliti dalam dan antara organisasi.¹⁴

3.3 Menubuhkan atau Menambah baik Program Privasi

Menggunakan model mudah fasa "sedia, tetapkan, maju", Rangka Kerja Privasi boleh menyokong penubuhan program privasi baharu atau penambahbaikan program sedia ada. Semasa sesebuah organisasi melalui fasa ini, ia mungkin menggunakan rujukan bermaklumat untuk memberikan panduan tentang mengutamakan atau mencapai hasil. Lihat seksyen 3.1 untuk maklumat lanjut tentang rujukan bermaklumat. Selain itu, repositori boleh didapati di <https://www.nist.gov/privacy-framework>.

Sedia

Pengurusan risiko privasi yang berkesan memerlukan organisasi memahami misi atau persekitaran perniagaannya; persekitaran undang-undangnya; toleransi risikonya; risiko privasi yang ditimbulkan oleh sistem, produk atau perkhidmatannya; dan peranannya dalam ekosistem pemprosesan data. Organisasi boleh menggunakan Fungsi Kenal Pasti-P and Tadbir Urus-P untuk "bersedia" dengan menyemak Kategori dan Subkategori, dan mula membangunkan Profil Semasa dan Profil Sasarannya.¹⁵ Aktiviti dan hasil seperti mewujudkan nilai dan dasar privasi organisasi, menentukan dan menyatakan toleransi risiko organisasi, dan menjalankan penilaian risiko privasi (lihat Lampiran D untuk maklumat lanjut tentang penilaian risiko privasi) menyediakan asas untuk melengkapkan Profil dalam "Tetapkan".

Kaedah Ringkas untuk Menubuhkan atau Menambah baik Program Privasi

Sedia: gunakan Fungsi Kenal Pasti-P and Tadbir Urus-P untuk "sedia".

Tetapkan: "tetapkan" pelan tindakan berdasarkan perbezaan antara Profil Semasa dan Sasaran.

Maju: "maju" ke hadapan dengan melaksanakan pelan tindakan

Tetapkan

Organisasi melengkapkan Profil Semasanya dengan menunjukkan hasil Kategori dan Subkategori daripada Fungsi selebihnya yang sedang dicapai. Jika sebahagian hasil dicapai, mencatat fakta ini akan membantu menyokong langkah seterusnya dengan menyediakan maklumat asas. Dimaklumkan oleh aktiviti di bawah Kenal Pasti dan Tadbir Urus, seperti nilai dan dasar privasi organisasi, toleransi risiko organisasi dan keputusan penilaian risiko privasi, organisasi melengkapkan Profil Sasarannya yang memfokuskan pada penilaian Kategori dan Subkategori yang menerangkan hasil privasi yang diingini. Organisasi juga boleh membangunkan Fungsi, Kategori dan Subkategori tambahannya sendiri untuk mengambil kira risiko organisasi yang unik. Ia juga mungkin mempertimbangkan pengaruh dan keperluan pihak berkepentingan luar seperti pelanggan dan rakan kongsi perniagaan apabila membuat Profil Sasaran. Organisasi boleh membangunkan berbilang Profil untuk menyokong barisan atau proses perniagaan yang berbeza, yang mungkin mempunyai keperluan perniagaan yang berbeza dan toleransi risiko yang berkaitan.

Organisasi membandingkan Profil Semasa dan Profil Sasaran untuk menentukan jurang. Seterusnya, ia mewujudkan pelan tindakan yang diutamakan untuk menangani jurang—mencerminkan pamacu misi, kos dan faedah serta risiko—untuk mencapai hasil dalam Profil Sasaran. Organisasi yang menggunakan

¹⁴ Lihat, cth., NIST SP 800-37, Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [7]; dan Organization for the Advancement of Structured Information Standards (OASIS) (2016) Privacy Management Reference Model and Methodology (PMRM) Version 1.0, <https://docs.oasis-open.org/pmrpm/PMRM/v1.0/PMRM-v1.0.pdf>.

¹⁵ Untuk maklumat tambahan, lihat Langkah "Sedia", Seksyen 3.1, NIST SP 800-37, Rev. 2 [7].

Rangka Kerja Keselamatan Siber dan Rangka Kerja Privasi bersama-sama, boleh membangunkan pelan tindakan bersepada. Ia kemudiannya menentukan sumber, termasuk pembiayaan dan keperluan tenaga kerja, yang diperlukan untuk menangani jurang, yang boleh memaklumkan pemilihan Peringkat yang sesuai. Menggunakan Profil dengan cara ini menggalakkan organisasi membuat keputusan termaklum tentang aktiviti privasi, menyokong pengurusan risiko, dan membolehkan organisasi melakukan penambahbaikan bersasaran keberkesanan kos.

Maju

Dengan pelan tindakan "ditetapkan", organisasi mengutamakan tindakan yang perlu diambil untuk menangani sebarang jurang dan kemudian melaraskan amalan privasi semasanya untuk mencapai Profil Sasaran.¹⁶

Organisasi boleh melalui fasa-fasa tersebut secara tidak berurutan mengikut keperluan untuk terus menilai dan memperbaiki postur privasinya. Sebagai contoh, organisasi mungkin mendapati pengulangan fasa Sedia yang lebih kerap, meningkatkan kualiti penilaian risiko privasi. Tambahan pula, organisasi boleh memantau kemajuan melalui kemas kini berulang kepada Profil Semasa atau Profil Sasaran untuk menyesuaikan diri dengan perubahan risiko, seterusnya membandingkan Profil Semasa dengan Profil Sasaran.

3.4 Menggunakan Kitaran Hayat Pembangunan Sistem

Profil Sasaran boleh diselaraskan dengan fasa kitaran hayat pembangunan sistem (SDLC) perancangan, reka bentuk, bina/beli, gunakan, kendalikan dan penyahtaulian untuk menyokong pencapaian hasil privasi yang diutamakan.¹⁷ Bermula dengan fasa perancangan, hasil privasi yang diutamakan boleh diubah menjadi keupayaan dan keperluan privasi untuk sistem, dengan menyedari bahawa keperluan berkemungkinan akan berubah semasa baki kitaran hayat. Pencapaian penting dalam fasa reka bentuk ialah mengesahkan bahawa keupayaan dan keperluan privasi sepadan dengan keperluan dan toleransi risiko sesebuah organisasi seperti yang dinyatakan dalam Profil Sasaran. Profil Sasaran yang sama boleh berfungsi sebagai senarai dalaman untuk dinilai apabila menggunakan sistem untuk mengesahkan bahawa semua keupayaan dan keperluan privasi dilaksanakan. Hasil privasi yang ditentukan dengan menggunakan Rangka Kerja Privasi hendaklah berfungsi sebagai asas untuk operasi berterusan sistem. Ini termasuk penilaian semula sekali-sekala, mendapatkan keputusan dalam Profil Semasa, untuk mengesahkan bahawa keupayaan dan keperluan privasi masih dipenuhi.

Penilaian risiko privasi biasanya menumpukan pada kitaran hayat data, peringkat yang melaluinya data lalu, selalunya dicirikan sebagai penciptaan atau pengumpulan, pemprosesan, penyebaran, penggunaan, penyimpanan dan pelupusan, termasuk pemusnahan dan pemadaman. Menjajarkan SDLC dan kitaran hayat data dengan mengenal pasti dan memahami cara data diproses semasa semua peringkat SDLC membantu organisasi mengurus risiko privasi dengan lebih baik dan memaklumkan pemilihan dan pelaksanaan kawalan privasi untuk memenuhi keperluan privasi.

¹⁶ NIST SP 800-37, Rev. 2 [7] menyediakan maklumat tambahan tentang langkah untuk melaksanakan pelan tindakan, termasuk pemilihan kawalan, pelaksanaan dan penilaian untuk menutup sebarang jurang.

¹⁷ Dalam SDLC, organisasi boleh menggunakan pelbagai metodologi pembangunan (e.g., waterfall, spiral, or agile).

3.5 Menggunakan dalam Ekosistem Pemprosesan Data

shoFaktor utama dalam pengurusan risiko privasi ialah peranan entiti dalam ekosistem pemprosesan data, yang boleh menjelaskan bukan sahaja kewajipan undang-undangnya, tetapi juga langkah yang mungkin diambil untuk mengurus risiko privasi. Seperti yang digambarkan dalam **Rajah 8**, ekosistem pemprosesan data merangkumi pelbagai entiti dan peranan yang mungkin mempunyai hubungan yang kompleks dan berbilang hala antara satu sama lain dan individu. Kerumitan boleh meningkat apabila entiti disokong oleh rantaian sub-entiti; contohnya, pembekal perkhidmatan mungkin disokong oleh satu siri pembekal perkhidmatan, atau pengeluar mungkin mempunyai berbilang pembekal komponen. **Rajah 8** memaparkan entiti sebagai mempunyai peranan yang berbeza, tetapi sesetengahnya mungkin mempunyai berbilang peranan seperti organisasi menyediakan perkhidmatan kepada organisasi lain dan menyediakan produk runcit kepada pengguna. Peranan dalam **Rajah 8** bertujuan untuk menjadi cadangan klasifikasi. Dalam amalan sebenar, peranan entiti mungkin dikodkan secara sah—contohnya, sesetengah undang-undang mengklasifikasikan organisasi sebagai pengawal data atau pemproses data—atau klasifikasi mungkin diperoleh daripada penetapan sektor industri.

Dengan membangunkan satu atau lebih Profil yang berkaitan dengan peranannya, entiti boleh menggunakan Rangka Kerja Privasi untuk mempertimbangkan cara mengurus risiko privasi bukan sahaja berkaitan dengan keutamaannya sendiri, tetapi juga berhubung dengan cara langkah yang mungkin diambil, memberi kesan terhadap pengurusan risiko privasi kepunyaan entiti ekosistem pemprosesan data lain. Sebagai contoh:

- Organisasi yang membuat keputusan tentang cara mengumpul dan menggunakan data tentang individu boleh menggunakan Profil untuk menyatakan keperluan privasi kepada pembekal perkhidmatan luaran (mis., pembekal awam yang mengeksport datanya); pembekal perkhidmatan luar yang memproses data boleh menggunakan Profilnya untuk menunjukkan langkah-langkah yang telah diterima pakai untuk memproses data selaras dengan kewajipan kontrak.
- Organisasi boleh menyatakan postur privasinya melalui Profil Semasa untuk melaporkan keputusan atau membandingkan dengan keperluan pemerolehan.
- Sektor industri boleh mewujudkan Profil biasa yang boleh digunakan oleh ahlinya untuk menyesuaikan Profil mereka sendiri.
- Pengilang boleh menggunakan Profil Sasaran untuk menentukan kebolehan membina ke dalam produknya agar pelanggan perniagaannya boleh memenuhi keperluan privasi pengguna akhir mereka.
- Pembangun boleh menggunakan Profil Sasaran untuk mempertimbangkan cara mereka bentuk aplikasi yang membolehkan perlindungan privasi apabila digunakan dalam persekitaran sistem organisasi lain.



Rajah 8: Hubungan Ekosistem Pemprosesan Data

Organisasi menyediakan perkhidmatan kepada organisasi lain dan menyediakan produk runcit kepada pengguna. Peranan dalam **Rajah 8** bertujuan untuk menjadi cadangan klasifikasi. Dalam amalan sebenar, peranan entiti mungkin dikodkan secara sah—contohnya, sesetengah undang-undang mengklasifikasikan organisasi sebagai pengawal data atau pemproses data—atau klasifikasi mungkin diperoleh daripada penetapan sektor industri.

Rangka Kerja Privasi menyediakan bahasa yang sama untuk menyampaikan keperluan privasi dengan entiti dalam ekosistem pemprosesan data. Keperluan untuk komunikasi ini boleh menjadi ketara terutamanya apabila ekosistem pemprosesan data merentas sempadan negara, seperti dengan pemindahan data antarabangsa. Amalan organisasi yang menyokong komunikasi mungkin termasuk:

- Menentukan keperluan privasi;
- Menggubal keperluan privasi melalui perjanjian rasmi (cth., kontrak, rangka kerja berbilang pihak);
- Berkommunikasi bagaimana keperluan privasi tersebut akan disahkan dan disahkan;
- Mengesahkan bahawa keperluan privasi dipenuhi melalui pelbagai metodologi penilaian; dan
- Mentadbir dan mengurus aktiviti di atas.

3.6 Memaklumkan Keputusan Membeli

Memandangkan sama ada Profil Semasa atau Sasaran boleh digunakan untuk menjana senarai keutamaan keperluan privasi, Profil ini juga boleh digunakan untuk memaklumkan keputusan tentang membeli produk dan perkhidmatan. Dengan terlebih dahulu memilih hasil yang berkaitan dengan matlamat privasinya, organisasi kemudiannya boleh menilai sistem, produk atau perkhidmatan rakan kongsi terhadap hasil ini. Contohnya, jika peranti dibeli untuk pemantauan alam sekitar hutan, *kebolehurusan* mungkin penting untuk menyokong keupayaan untuk meminimumkan pemprosesan data tentang orang yang menggunakan hutan dan harus mendorong penilaian pengilang terhadap Subkategori yang berkenaan dalam Teras (cth., CT .DP-P4: konfigurasi sistem atau peranti membenarkan pengumpulan atau pendedahan *elemen data* terpilih).

Dalam keadaan yang mungkin tidak boleh untuk mengenakan satu set keperluan privasi ke atas pembekal, objektifnya adalah untuk membuat keputusan pembelian terbaik di kalangan berbilang pembekal, memandangkan senarai keperluan privasi yang ditentukan dengan teliti. Selalunya, ini bermakna beberapa tahap pertukaran, membandingkan berbilang produk atau perkhidmatan dengan jurang yang diketahui dengan Profil. Jika sistem, produk atau perkhidmatan yang dibeli tidak memenuhi semua objektif yang diterangkan dalam Profil, organisasi boleh menangani baki risiko melalui langkah mitigasi atau tindakan pengurusan lain.

Rujukan

- [1] Institut Standard dan Teknologi Kebangsaan (2018) Rangka Kerja untuk Menambah Baik Keselamatan Siber Infrastruktur Kritis, Versi 1.1 (Institut Standard dan Teknologi, Gaithersburg, MD).
<https://doi.org/10.6028/NIST.CSWP.04162018>
- [2] Institut Standard dan Teknologi Kebangsaan (2019) Ringkasan Analisis Respons kepada Permintaan Maklumat Rangka Kerja Privasi NIST. (Institut Standard dan Teknologi Kebangsaan, Gaithersburg, MD). https://www.nist.gov/sites/default/files/documents/2019/02/27/rfi_response_analysis_privacyframework_2.27.19.pdf
- [3] Institut Standard dan Teknologi Kebangsaan (2019) Metodologi Penilaian Risiko Privasi NIST (PRAM). (Institut Standard dan Teknologi Kebangsaan, Gaithersburg, MD).
<https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources>
- [4] Panel Saling Kendali Grid Pintar—Jawatankuasa Keselamatan Siber Grid Pintar (2014) Garis Panduan untuk Keselamatan Siber Grid Pintar: Jilid 1 – Keperluan Strategi, Seni bina dan Peringkat Tinggi Keselamatan Siber Grid Pintar. (Institut Standard dan Teknologi Kebangsaan, Gaithersburg, MD), Silang Agensi atau Laporan Dalaman (IR) 7628 NIST, Ruj. 1, Jilid. 1.
<https://doi.org/10.6028/NIST.IR.7628r1>
- [5] Brooks SW, Garcia ME, Lefkovitz NB, Lightman S, Nadeau EM (2017) Pengenalan kepada Kejuruteraan Privasi dan Pengurusan Risiko dalam Sistem Persekutuan.. (Institut Standard dan Teknologi Kebangsaan, Gaithersburg, MD), Silang Agensi atau Laporan Dalaman (IR) 8062 NIST.
<https://doi.org/10.6028/NIST.IR.8062>
- [6] Inisiatif Transformasi Pasukan Petugas Bersama (2011) Menguruskan Risiko Keselamatan Maklumat: Organisasi, Misi dan Paparan Sistem Maklumat. (Institut Standard dan Teknologi Kebangsaan, Gaithersburg, MD). Penerbitan Khas (SP) NIST 800-39.
<https://doi.org/10.6028/NIST.SP.800-39>
- [7] Pasukan Petugas Bersama (2018) Rangka Kerja Pengurusan Risiko untuk Sistem Maklumat dan Organisasi: Pendekatan Kitara Hidup Sistem untuk Keselamatan dan Privasi. (Institut Standard dan Teknologi Kebangsaan, Gaithersburg, MD), Penerbitan Khas (SP) NIST 800-37 Ruj. 2.
<https://doi.org/10.6028/NIST.SP.800-37r2>
- [8] Grassi PA, Garcia ME, Fenton JL (2017) Garis Panduan Identiti Digital. (Institut Standard dan Teknologi Kebangsaan, Gaithersburg, MD), Penerbitan Khas (SP) NIST 800-63-3, Termasuk kemas kini setakat 1 Disember 2017. <https://doi.org/10.6028/NIST.SP.800-63-3>
- [9] Pejabat Pengurusan dan Belanjawan (2017) Menyediakan dan Memberikan Respons kepada Pelanggaran Maklumat Peribadi Boleh Dikenal Pasti. (White House, Washington, DC), OMB Memorandum M-17-12, 3 Januari 2017. Tersedia di
https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf
- [10] Inisiatif Transformasi Pasukan Petugas Bersama (2013) Kawalan Keselamatan dan Privasi untuk Sistem Maklumat Persekutuan dan Organisasi. (Institut Standard dan Teknologi Kebangsaan, Gaithersburg, MD), Penerbitan Khas (SP) NIST 800-53, Ruj. 4, Termasuk kemas kini setakat 22 Januari 2015. <https://doi.org/10.6028/NIST.SP.800-53r4>
- [11] Grassi PA, Lefkovitz NB, Nadeau EM, Galluzzo RJ, Dinh AT (2018) Metadata Atribut: Skema Dicadangkan untuk Menilai Atribut Persekutuan. (Institut Standard dan Teknologi Kebangsaan, Gaithersburg, MD), Silang Agensi atau Laporan Dalaman (IR) NIST 8112.
<https://doi.org/10.6028/NIST.IR.8112>

- [12] Inisiatif Transformasi Pasukan Petugas Bersama (2012) Panduan untuk Menjalankan Penilaian Risiko.(Institut Standard dan Teknologi Kebangsaan, Gaithersburg, MD), Penerbitan Khas (SP) NIST800-30, Ruj. 1. <https://doi.org/10.6028/NIST.SP.800-30r1>
- [13] “Definisi,” Tajuk Kod A.S 44, Bahagian. 3542. 2011 ed.
<https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3542>

Lampiran A: Teras Rangka Kerja Privasi

Lampiran ini membentangkan Teras: jadual Fungsi, Kategori dan Subkategori yang menerangkan aktiviti dan hasil tertentu yang boleh menyokong pengurusan risiko privasi apabila sistem, produk dan perkhidmatan sedang memproses data.

Nota kepada Pengguna

Pendekatan Berasaskan Risiko:

- **Teras bukan senarai semak tindakan yang perlu dilakukan. Organisasi memilih Subkategori selaras dengan strategi risikonya untuk melindungi privasi individu, seperti yang dinyatakan dalam penyata Kategori.** Organisasi mungkin tidak perlu mencapai setiap hasil atau aktiviti yang ditunjukkan dalam Teras. Adalah diharapkan bahawa organisasi akan menggunakan Profil untuk memilih dan mengutamakan Fungsi, Kategori dan Subkategori yang paling memenuhi keperluan khususnya dengan mempertimbangkan matlamat, peranannya dalam amalan terbaik ekosistem pemprosesan data atau sektor industri, keperluan undang-undang/kawal selia dan industri, keutamaan pengurusan risiko dan keperluan privasi individu yang secara langsung atau tidak langsung dilayan atau dipengaruhi oleh sistem, produk atau perkhidmatan organisasi.
- Tidak wajib untuk mencapai sesuatu hasil secara keseluruhannya. Organisasi boleh menggunakan Profilnya untuk menyatakan pencapaian separa dari hasil, kerana mungkin tidak semua aspek hasil adalah relevan untuknya menguruskan risiko privasi, atau organisasi boleh menggunakan Profil Sasaran untuk menyatakan aspek hasil yang ia tidak mempunyai keupayaan untuk mencapainya pada masa ini.
- Mungkin perlu untuk mempertimbangkan pelbagai hasil dalam kombinasi untuk mengurus risiko privasi dengan sewajarnya. Sebagai contoh, organisasi yang bertindak balas kepada permintaan individu untuk akses data boleh memilih sebagai Profilnya kedua-dua Subkategori CT.DM-P1: “Elemen data boleh diakses untuk semakan” dan Kategori “Pengurusan Identiti, Pengesahan dan Kawalan Akses” (PR.AC-P) untuk memastikan bahawa hanya individu yang mempunyai data berkenaan mendapat akses.

Pelaksanaan: Format jadual Teras tidak bertujuan untuk mencadangkan susunan pelaksanaan tertentu atau membayangkan tahap kepentingan antara Fungsi, Kategori dan Subkategori. Pelaksanaan mungkin tidak berurutan, serentak atau berulang, bergantung pada peringkat SDLC, status program privasi, skala tenaga kerja atau peranan organisasi dalam ekosistem pemprosesan data. Di samping itu, Teras tidak menyeluruh; ia boleh diperluaskan, membenarkan organisasi, sektor dan entiti lain menyesuaikan atau menambah Fungsi, Kategori dan Subkategori tambahan pada Profil mereka.

Peranan:

- **Peranan Ekosistem:** Teras bertujuan untuk boleh digunakan oleh mana-mana organisasi atau entiti tanpa mengira peranannya dalam ekosistem pemprosesan data. Walaupun Rangka Kerja Privasi tidak mengklasifikasikan peranan ekosistem, organisasi harus menyemak Teras dari sudut pandangannya dalam ekosistem. Peranan organisasi mungkin dikodkan secara sah—contohnya, sesetengah undang-undang mengklasifikasikan organisasi sebagai pengawal data atau pemproses data—atau klasifikasi mungkin diperoleh daripada penetapan industri. Memandangkan elemen Teras tidak diberikan oleh peranan ekosistem, organisasi boleh menggunakan Profilnya untuk memilih Fungsi, Kategori dan Subkategori yang berkaitan dengan peranannya.
- **Peranan Organisasi:** Bahagian berlainan tenaga kerja organisasi mungkin bertanggungjawab untuk Kategori atau Subkategori yang berbeza. Sebagai contoh, jabatan undang-undang

mungkin bertanggungjawab untuk menjalankan aktiviti di bawah "Dasar Tadbir Urus, Proses dan Prosedur" semasa jabatan IT sedang mengusahakan "Inventori dan Pemetaan." Sebaik-baiknya, Teras menggalakkan kerjasama merentas organisasi untuk membangunkan Profil dan mencapai hasil.

Boleh Skala: Aspek tertentu hasil mungkin dinyatakan dengan samar-samar. Sebagai contoh, hasil mungkin termasuk istilah seperti "disampaikan" atau "didedahkan" tanpa menyatakan kepada siapa penyampaian atau pendedahan itu dibuat. Kekaburan itu disengajakan untuk membolehkan pelbagai organisasi dengan kes penggunaan berbeza untuk menentukan perkara yang sesuai atau diperlukan dalam konteks tertentu.

Repositori Sumber: Sumber kendiri yang boleh memberikan lebih banyak maklumat tentang cara mengutamakan atau mencapai hasil boleh didapati di <https://www.nist.gov/privacy-framework>.

Penjajaran Rangka Kerja Keselamatan Siber:

- Seperti yang dinyatakan dalam seksyen 2.1, organisasi boleh menggunakan lima Fungsi Rangka Kerja Privasi—Kenal Pasti-P, Tadbir Urus-P, Kawal-P, Komunikasi-P dan Lindung-P—untuk mengurus risiko privasi yang timbul daripada pemprosesan data. Lindung-P tertumpu secara khusus pada mengurus risiko yang berkaitan dengan acara privasi berkaitan keselamatan (cth., pelanggaran privasi). Untuk menyokong lagi pengurusan risiko yang berkaitan dengan acara privasi berkaitan keselamatan, organisasi boleh memilih untuk menggunakan Fungsi Kesan, Balas dan Pulih daripada [Rangka Kerja Keselamatan Siber](#). Atas sebab ini, Fungsi ini disertakan dalam **Jadual 1**, tetapi dikelabukan. Sebagai alternatif, organisasi boleh menggunakan kelima-lima Fungsi Rangka Kerja Keselamatan Siber bersama-sama dengan Kenal Pasti-P, Tadbir Urus-P, Kawal-P dan Komunikasi-P untuk menangani risiko privasi dan keselamatan secara kolektif. Lihat **Rajah 5** untuk contoh yang digambarkan tentang bagaimana Fungsi daripada kedua-dua rangka kerja boleh digunakan dalam kombinasi yang berbeza-beza untuk mengurus aspek privasi dan risiko keselamatan siber yang berbeza.
- Fungsi, Kategori atau Subkategori tertentu mungkin sama atau telah disesuaikan daripada Rangka Kerja Keselamatan Siber. Legenda berikut boleh digunakan untuk mengenal pasti perhubungan ini dalam **Jadual 2**. Satu lintasan lengkap antara dua rangka kerja boleh didapati dalam repositori sumber di <https://www.nist.gov/privacy-framework>.
 - Fungsi, Kategori atau Subkategori sejajar dengan Rangka Kerja Keselamatan Siber, tetapi teks telah disesuaikan untuk Rangka Kerja Privasi
 - Kategori atau Subkategori adalah sama dengan Rangka Kerja Keselamatan Siber

Pengecam Teras: Untuk kemudahan penggunaan, setiap komponen Teras diberikan pengecam unik. Fungsi dan Kategori masing-masing mempunyai pengecam abjad yang unik, seperti yang ditunjukkan dalam **Jadual 1**. Subkategori dalam setiap Kategori mempunyai nombor yang ditambahkan pada pengecam abjad; pengecam unik untuk setiap Subkategori disertakan dalam **Jadual 2**.

Jadual 1: Fungsi Rangka Kerja Privasi dan Pengecam Unik Kategori

Pengecam Unik Fungsi	Fungsi	Pengecam Unik Kategori	Kategori
ID-P	Kenal Pasti-P	ID.IM-P	Inventori dan Pemetaan
		ID.BE-P	Persekuturan Perniagaan
		ID.RA-P	Penilaian Risiko
		ID.DE-P	Pengurusan Risiko Ekosistem Pemprosesan Data
GV-P	Tadbir Urus-P	GV.PO-P	Dasar, Proses dan Prosedur Tadbir Urus
		GV.RM-P	Strategi Pengurusan Risiko
		GV.AT-P	Kesedaran dan Latihan
		GV.MT-P	Pemantauan dan Semakan
CT-P	Kawal-P	CT.PO-P	Dasar, Proses dan Prosedur Pemprosesan Data
		CT.DM-P	Pengurusan Pemprosesan Data
		CT.DP-P	Pemprosesan Terpisah
CM-P	Komunikasi-P	CM.PO-P	Dasar, Proses dan Prosedur Komunikasi
		CM.AW-P	Kesedaran Pemprosesan Data
PR-P	Lindung-P	PR.PO-P	Dasar, Proses dan Prosedur Perlindungan Data
		PR.AC-P	Pengurusan Identiti, Pengesahan dan Kawalan Akses
		PR.DS-P	Keselamatan Data
		PR.MA-P	Penyelenggaraan
		PR.PT-P	Teknologi Perlindungan
DE	Kesan	DE.AE	Anomali dan Peristiwa
		DE.CM	Pemantauan Berterusan Keselamatan
		DE.DP	Proses Pengesahan
RS	Tindak Balas	RS.RP	Perancangan Tindak Balas
		RS.CO	Komunikasi
		RS.AN	Analisis
		RS.MI	Pengurangan
		RS.IM	Penambahbaikan
RC	Pulih	RC.RP	Perancangan Pemulihan
		RC.IM	Penambahbaikan
		RC.CO	Komunikasi

Jadual 2: Teras Rangka Kerja Privasi

Fungsi	Kategori	Subkategori
KENAL PASTI-P (ID-P): Membangunkan pemahaman organisasi untuk mengurus risiko privasi bagi individu yang timbul daripada pemprosesan data.	Inventori dan Pemetaan (ID.IM-P): <u>Pemprosesan data</u> oleh sistem, produk atau perkhidmatan difahami dan memaklumkan pihak pengurusan <u>risiko privasi</u> .	<p>ID.IM-P1: Sistem/produk/perkhidmatan yang memproses <u>data</u> diinventori.</p> <p>ID.IM-P2: Pemilik atau pengendali (cth., organisasi atau pihak ketiga seperti penyedia perkhidmatan, rakan kongsi, pelanggan dan pembangun) dan peranan mereka berkenaan dengan sistem/produk/perkhidmatan dan komponen (cth., dalaman atau luaran) yang memproses data diinventori.</p> <p>ID.IM-P3: Kategori <u>individu</u> (cth., pelanggan, pekerja atau bakal pekerja, pengguna) yang datanya sedang diproses diinventori.</p> <p>ID.IM-P4: <u>Tindakan data</u> sistem/produk/perkhidmatan diinventori.</p> <p>ID.IM-P5: Tujuan untuk tindakan data diinventori.</p> <p>ID.IM-P6: <u>Elemen data</u> dalam tindakan data diinventori.</p> <p>ID.IM-P7: Persekitaran pemprosesan data dikenal pasti (cth., lokasi geografi, dalaman, awan, pihak ketiga).</p> <p>ID.IM-P8: Pemprosesan data dipetakan, menggambarkan tindakan data dan elemen data yang berkaitan untuk sistem/produk/perkhidmatan, termasuk komponen; peranan pemilik/pengendali komponen; dan interaksi individu atau pihak ketiga dengan sistem/produk/perkhidmatan.</p>
	Persekitaran Perniagaan (ID.BE-P): Misi, objektif, pihak berkepentingan, dan aktiviti organisasi difahami dan diberi keutamaan; maklumat ini digunakan untuk memaklumkan privasi peranan, tanggungjawab, dan keputusan <u>pengurusan risiko</u> .	<p>ID.BE-P1: Peranan organisasi dalam <u>ekosistem pemprosesan data</u> dikenal pasti dan disampaikan.</p> <p>ID.BE-P2: Keutamaan untuk misi, objektif dan aktiviti organisasi diwujudkan dan disampaikan.</p> <p>ID.BE-P3: Sistem/produk/perkhidmatan yang menyokong keutamaan organisasi dikenal pasti dan keperluan utama disampaikan.</p>

Fungsi	Kategori	Subkategori
	<p>Penilaian risiko (ID.RA-P): Organisasi memahami risiko privasi kepada individu dan bagaimana risiko privasi tersebut boleh menimbulkan kesan susulan pada operasi organisasi, termasuk misi, fungsi, keutamaan pengurusan risiko lain (cth., pematuhan, kewangan), reputasi, tenaga kerja dan budaya.</p>	<p>ID.RA-P1: Faktor kontekstual yang berkaitan dengan sistem/produk/perkhidmatan dan tindakan data dikenal pasti (cth., kepentingan atau persepsi demografi dan privasi individu, kepekaan dan/atau jenis data, keterlihatan pemprosesan data kepada individu dan pihak ketiga).</p> <p>ID.RA-P2: Input dan output analitik data dikenal pasti dan dinilai sama ada memihak kepada sesuatu pihak</p> <p>ID.RA-P3: Tindakan data bermasalah yang berpotensi dan masalah yang berkaitan dikenal pasti.</p> <p>ID.RA-P4: Tindakan data bermasalah, kemungkinan dan impak digunakan untuk menentukan dan mengutamakan risiko.</p> <p>ID.RA-P5: Tindak balas risiko dikenal pasti, diberi keutamaan, dan dilaksanakan.</p>
	<p>Pengurusan Risiko Ekosistem</p> <p>Pemprosesan Data (ID.DE-P): Keutamaan organisasi, kekangan, toleransi risiko, dan andaian diwujudkan dan digunakan untuk menyokong keputusan risiko yang berkaitan dengan pengurusan risiko privasi dan pihak ketiga dalam ekosistem pemprosesan data. Organisasi telah menubuhkan dan melaksanakan proses untuk mengenal pasti, menilai dan mengurus risiko privasi dalam ekosistem pemprosesan data.</p>	<p>ID.DE-P1: Dasar, proses dan prosedur pengurusan risiko ekosistem pemprosesan data dikenal pasti, diwujudkan, dinilai, diurus dan dipersetujui oleh pihak berkepentingan organisasi..</p> <p>ID.DE-P2: Pihak ekosistem pemprosesan data (cth., pembekal perkhidmatan, pelanggan, rakan kongsi, pengeluar produk, pembangun aplikasi) dikenal pasti, diberi keutamaan dan dinilai menggunakan proses penilaian risiko privasi.</p> <p>ID.DE-P3: Kontrak dengan pihak ekosistem pemprosesan data digunakan untuk melaksanakan langkah-langkah yang sesuai yang direka bentuk untuk memenuhi objektif program privasi organisasi.</p> <p>ID.DE-P4: Rangka kerja saling boleh kendali (<i>interoperability framework</i>) atau pendekatan berbilang pihak yang serupa digunakan untuk mengurus privasi ekosistem pemprosesan data risiko.</p>

		ID.DE-P5: Pihak ekosistem pemprosesan data dinilai secara rutin menggunakan audit, keputusan ujian, atau bentuk penilaian lain untuk mengesahkan bahawa mereka memenuhi kontrak, rangka kerja saling boleh kendali, atau kewajipan lain.
--	--	---

Fungsi	Kategori	Subkategori
TADBIR URUS-P (GV-P): Membangunkan dan melaksanakan struktur tadbir urus organisasi untuk membolehkan pemahaman berterusan tentang keutamaan pengurusan risiko organisasi yang dimaklumkan oleh risiko privasi.	Dasar, Proses dan Prosedur Tadbir Urus (GV.PO-P): Dasar, proses dan prosedur untuk mengurus dan memantau keperluan kawal selia, undang-undang, risiko , alam sekitar dan operasi organisasi difahami dan memaklumkan pengurusan risiko privasi .	GV.PO-P1: Nilai dan dasar privasi organisasi (cth., syarat pemprosesan data seperti penggunaan data atau tempoh pengekalan, hak prerogatif individu berkenaan dengan pemprosesan data) diwujudkan dan disampaikan. GV.PO-P2: Proses untuk menerapkan nilai privasi organisasi dalam pembangunan dan operasi sistem/produk/perkhidmatan diwujudkan dan dilaksanakan. GV.PO-P3: Peranan dan tanggungjawab untuk tenaga kerja ditetapkan dengan mengambil kira privasi. GV.PO-P4: Peranan dan tanggungjawab privasi diselaraskan dan dijajarkan dengan pihak berkepentingan pihak ketiga (cth., penyedia perkhidmatan, pelanggan, rakan kongsi). GV.PO-P5: Keperluan undang-undang, kawal selia dan kontrak mengenai privasi difahami dan diuruskan. GV.PO-P6: Tadbir urus dan dasar, proses serta prosedur pengurusan risiko menangani risiko privasi.
	Strategi Pengurusan Risiko (GV.RM-P): Keutamaan, kekangan, toleransi risiko , dan andaian organisasi ditetapkan dan digunakan untuk menyokong keputusan risiko operasi.	GV.RM-P1: Proses pengurusan risiko ditubuhkan, diurus dan dipersetujui oleh pihak berkepentingan organisasi. GV.RM-P2: Toleransi risiko organisasi ditentukan dan dinyatakan dengan jelas. GV.RM-P3: Penentuan toleransi risiko organisasi dimaklumkan oleh peranannya dalam ekosistem pemprosesan data .
	Kesedaran dan Latihan (GV.AT-P): Tenaga kerja organisasi dan pihak ketiga	GV.AT-P1: Tenaga kerja dimaklumkan dan dilatih mengenai peranan dan tanggungjawabnya.

	<p>yang terlibat dalam pemprosesan data diberikan pendidikan kesedaran privasi dan dilatih untuk melaksanakan tugas dan tanggungjawab berkaitan privasi mereka selaras dengan dasar, proses, prosedur dan perjanjian serta nilai privasi organisasi.</p>	<p>GV.AT-P2: Eksekutif kanan memahami peranan dan tanggungjawab mereka.</p> <p>GV.AT-P3: Kakitangan privasi memahami peranan dan Tanggungjawab mereka.</p> <p>GV.AT-P4: Pihak ketiga (mis., penyedia perkhidmatan, pelanggan, rakan kongsi) memahami peranan dan tanggungjawab mereka.</p>
--	--	---

Fungsi	Kategori	Subkategori
	<p>Pemantauan dan Semakan (GV.MT-P): Dasar, proses dan prosedur untuk semakan berterusan terhadap postur privasi organisasi difahami dan memaklumkan pengurusan risiko privasi.</p>	<p>GV.MT-P1: Risiko privasi dinilai semula secara berterusan dan sebagai faktor utama, termasuk persekitaran perniagaan organisasi (cth., pengenalan teknologi baharu), tadbir urus (cth., kewajipan undang-undang, toleransi risiko), pemprosesan data dan perubahan sistem/produk/perkhidmatan.</p> <p>GV.MT-P2: Nilai privasi, dasar dan latihan disemak dan sebarang kemas kini dimaklumkan.</p> <p>GV.MT-P3: Dasar, proses dan prosedur untuk menilai pematuhan dengan keperluan undang-undang dan dasar privasi diwujudkan dan dilaksanakan.</p> <p>GV.MT-P4: Dasar, proses dan prosedur untuk menyampaikan kemajuan dalam mengurus risiko privasi diwujudkan dan dilaksanakan.</p> <p>GV.MT-P5: Dasar, proses dan prosedur diwujudkan dan disediakan untuk menerima, menganalisis dan bertindak balas terhadap tindakan data bermasalah yang didedahkan kepada organisasi daripada sumber dalaman dan luaran (cth., penemuan dalaman, penyelidik privasi, acara profesional).</p> <p>GV.MT-P6: Dasar, proses dan prosedur menggabungkan pengajaran yang dipelajari daripada tindakan data bermasalah.</p> <p>GV.MT-P7: Dasar, proses dan prosedur untuk menerima, menjelak dan bertindak balas terhadap aduan, kebimbangan dan soalan daripada individu tentang amalan privasi organisasi telah ditetapkan dan dilaksanakan.</p>

KAWAL-P (CT-P): Membangun dan melaksanakan aktiviti yang sesuai untuk membolehkan organisasi atau individu mengurus data dengan	<p>Dasar, Proses dan Prosedur Pemprosesan Data (CT.PO-P): Dasar, proses dan prosedur dikekalkan dan digunakan untuk mengurus pemprosesan data (mis., tujuan, skop, peranan dan tanggungjawab dalam ekosistem pemprosesan data, dan komitmen pengurusan) selaras dengan strategi risiko organisasi untuk melindungi privasi individu.</p>	<p>CT.PO-P1: Dasar, proses dan prosedur untuk membenarkan pemprosesan data (cth., keputusan organisasi, persetujuan individu), membatalan kebenaran dan mengekalkan kebenaran ditetapkan dan dilaksanakan.</p> <p>CT.PO-P2: Dasar, proses dan prosedur untuk membolehkan semakan, pemindahan, perkongsian atau pendedahan, pengubahan dan pemadaman data diwujudkan dan dilaksanakan (cth., untuk mengekalkan kualiti data, mengurus data pengekalan)</p> <p>CT.PO-P3: Dasar, proses dan prosedur untuk membolehkan pilihan dan permintaan pemprosesan data individu diwujudkan dan dilaksanakan.</p>
--	---	--

Fungsi	Kategori	Subkategori
kebutiran mencukupi untuk mengurus risiko privasi.	<p>Pengurusan Pemprosesan Data (CT.DM-P): Data diurus selaras dengan strategi risiko organisasi untuk melindungi privasi individu, meningkatkan kebolehurusan, dan membolehkan pelaksanaan prinsip privasi (cth., penyertaan individu, kualiti data, pemminimuman data).</p>	<p>CT.PO-P4: Kitaran hayat data untuk mengurus data diselaraskan dan dilaksanakan dengan kitaran hayat pembangunan sistem untuk mengurus sistem.</p> <p>CT.DM-P1: Elemen data boleh diakses untuk semakan.</p> <p>CT.DM-P2: Elemen data boleh diakses untuk penghantaran atau pendedahan.</p> <p>CT.DM-P3: Elemen data boleh diakses untuk diubah.</p> <p>CT.DM-P4: Elemen data boleh diakses untuk pemadaman.</p> <p>CT.DM-P5: Data dimusnahkan mengikut dasar.</p> <p>CT.DM-P6: Data dihantar menggunakan format piawai.</p> <p>CT.DM-P7: Mekanisme untuk menghantar kebenaran pemprosesan dan nilai data yang berkaitan dengan elemen data diwujudkan dan dilaksanakan.</p> <p>CT.DM-P8: Rekod audit/log ditentukan, didokumenkan, dilaksanakan dan disemak mengikut dasar dan menggabungkan prinsip pemminimuman data.</p> <p>CT.DM-P9: Langkah teknikal yang dilaksanakan untuk mengurus data pemprosesan diuji dan dinilai.</p> <p>CT.DM-P10: Keutamaan privasi pihak berkepentingan disertakan dalam objektif reka bentuk algoritma dan output dinilai berdasarkan keutamaan ini.</p>

	<p>Pemprosesan Terpisah (CT.DP-P): Penyelesaian pemprosesan data meningkatkan kebolehpisahan selaras dengan strategi risiko organisasi untuk melindungi privasi individu dan membolehkan pelaksanaan prinsip privasi (cth., peminimuman data).</p>	<p>CT.DP-P1: Data diproses untuk mengehadkan kebolehan melihat dan menghubung (cth., tindatakan data berlaku pada peranti tempatan, memelihara privasi kriptografi).</p> <p>CT.DP-P2: Data diproses untuk mengehadkan pengenalan individu (cth., teknik privasi nyah pengenalan, penggunaan token).</p> <p>CT.DP-P3: Data diproses untuk mengehadkan rumusan petaabiran tentang tingkah laku atau aktiviti individu (cth., pemprosesan data terpencerar, seni bina teragih).</p> <p>CT.DP-P4: Konfigurasi sistem atau peranti membenarkan pengumpulan terpilih atau pendedahan eleman data.</p> <p>CT.DP-P5: Rujukan atribut digantikan dengan nilai atribut.</p>
--	---	--

Fungsi	Kategori	Subkategori
KOMUNIKASI-P (CM-P): Membangunkan dan melaksanakan aktiviti yang sesuai untuk membolehkan organisasi dan individu mempunyai pemahaman yang boleh dipercayai dan terlibat dalam dialog tentang cara data diproses dan risiko privasi yang berkaitan.	Dasar, Proses dan Prosedur Komunikasi (CM.PO-P): Dasar, proses dan prosedur dikekalkan dan digunakan untuk meningkatkan ketelusan amalan pemprosesan data organisasi (mis., tujuan, skop, peranan dan tanggungjawab dalam ekosistem pemprosesan data , dan pengurusan komitmen) dan risiko privasi yang berkaitan.	<p>CM.PO-P1: Dasar ketelusan, proses dan prosedur untuk menyampaikan tujuan pemprosesan data, amalan dan risiko privasi yang berkaitan telah ditetapkan dan dilaksanakan.</p> <p>CM.PO-P2: Peranan dan tanggungjawab (cth., perhubungan awam) untuk menyampaikan tujuan pemprosesan data, amalan dan risiko privasi yang berkaitan telah ditetapkan.</p>
	Kesedaran Pemprosesan Data (CM.AW-P): Individu dan organisasi mempunyai pengetahuan yang boleh dipercayai tentang amalan pemprosesan data dan risiko privasi yang berkaitan, dan mekanisme yang berkesan digunakan dan dikekalkan untuk meningkatkan kebolehramalan selaras dengan strategi risiko organisasi untuk melindungi privasi individu.	<p>CM.AW-P1: Mekanisme (cth., notis, laporan dalaman atau awam) untuk menyampaikan tujuan pemprosesan data, amalan, risiko privasi yang berkaitan dan pilihan untuk membolehkan pilihan pemprosesan data individu dan permintaan diwujudkan dan disediakan.</p> <p>CM.AW-P2: Mekanisma untuk mendapatkan maklum balas daripada individu (mis., tinjauan atau kumpulan fokus) tentang pemprosesan data dan risiko privasi yang berkaitan telah diwujudkan dan dilaksanakan.</p> <p>CM.AW-P3: Reka bentuk sistem/produk/perkhidmatan membolehkan kebolehlihatan pemprosesan data.</p>

		<p>CM.AW-P4: Rekod pendedahan dan perkongsian data dikekalkan dan boleh diakses untuk semakan atau penghantaran/pendedahan.</p> <p>CM.AW-P5: Pembetulan atau pemadaman data boleh disampaikan kepada individu atau organisasi (cth., sumber data) dalam ekosistem pemprosesan data.</p> <p>CM.AW-P6: Data asal dan terbitan dikekalkan dan boleh diakses untuk semakan atau penghantaran/pendedahan.</p> <p>CM.AW-P7: Individu dan organisasi yang terjejas dimaklumkan tentang pelanggaran privasi atau peristiwa.</p> <p>CM.AW-P8: Individu dibekalkan dengan mekanisme mitigasi (cth., pemantauan kredit, persetujuan pengeluaran, pengubahan atau pemadaman data) untuk menangani kesan tindakan data bermasalah.</p>
LINDUNG-P (PR-P): Membangunkan	Dasar, Proses dan Prosedur Perlindungan Data (PR.PO-P): Dasar keselamatan dan privasi (mis., tujuan, skop, peranan	<p>PR.PO-P1: Konfigurasi garis dasar teknologi maklumat dicipta dan dikekalkan dengan menggabungkan prinsip keselamatan (mis., konsep kefungsian paling sedikit).</p>

Fungsi	Kategori	Subkategori
dan melaksanakan perlindungan pemprosesan data yang sesuai.	dan tanggungjawab dalam ekosistem pemprosesan data dan komitmen pengurusan), proses dan prosedur dikekalkan dan digunakan untuk mengurus perlindungan data .	<p>PR.PO-P2: Proses kawalan perubahan konfigurasi diwujudkan dan disediakan.</p> <p>PR.PO-P3: Sandaran maklumat dijalankan, diselenggara dan diuji.</p> <p>PR.PO-P4: Dasar dan peraturan mengenai persekitaran operasi fizikal untuk aset organisasi dipenuhi.</p> <p>PR.PO-P5: Proses perlindungan dipertingkatkan.</p> <p>PR.PO-P6: Keberkesaan teknologi perlindungan dikongsikan.</p> <p>PR.PO-P7: Pelan tindak balas (Tindak Balas Insiden dan Kesinambungan Perniagaan) dan pelan pemulihan (Pemulihan Insiden dan Pemulihan Bencana) diwujudkan, disediakan dan diuruskan.</p> <p>PR.PO-P8: Pelan tindak balas dan pemulihan diuji.</p> <p>PR.PO-P9: Prosedur privasi disertakan dalam amalan sumber manusia (cth., nyah peruntukan, tapisan kakitangan).</p>

		PR.PO-P10: Pelan pengurusan kerentanan dibangunkan dan dilaksanakan.
	Pengurusan Identiti, Pengesahan dan Kawalan Akses (PR.AC-P): Akses kepada data dan peranti adalah terhad kepada individu , proses dan peranti yang dibenarkan, dan diuruskan selaras dengan penilaian risiko akses tanpa kebenaran.	PR.AC-P1: Identiti dan bukti kelayakan (<i>credential</i>) dikeluarkan, diurus, disahkan, dibatalkan dan diaudit untuk individu, proses dan peranti yang diberi kuasa. PR.AC-P2: Akses fizikal kepada data dan peranti diuruskan. PR.AC-P3: Akses jauh diuruskan. PR.AC-P4: Kebenaran akses dan keizinan diurus, menggabungkan prinsip keistimewaan paling sedikit dan pengasingan tugas. PR.AC-P5: Integriti rangkaian dilindungi (mis., pengasingan rangkaian, pembahagian rangkaian). PR.AC-P6: Individu dan peranti dibuktikan dan terikat kepada bukti kelayakan, dan disahkan setara dengan risiko transaksi (cth., risiko keselamatan dan risiko privasi serta risiko lain organisasi).
	Keselamatan Data (PR.DS-P): Data diurus selaras dengan strategi	PR.DS-P1: Data sedang rehat dilindungi. PR.DS-P2: Data dalam transit dilindungi.

Fungsi	Kategori	Subkategori
	risiko organisasi untuk melindungi privasi individu dan mengekalkan kerahsiaan , integriti , and ketersediaan .	PR.DS-P3: Sistem/produk/perkhidmatan dan data yang berkaitan diuruskan secara rasmi sepanjang pengalihan keluar, pemindahan dan pelupusan. PR.DS-P4: Kapasiti yang mencukupi untuk memastikan ketersediaan dikekalkan. PR.DS-P5: Perlindungan terhadap kebocoran data dilaksanakan. PR.DS-P6: Mekanisma semakan integriti digunakan untuk mengesahkan integriti perisian, perisian tegar dan maklumat. PR.DS-P7: Persekuturan pembangunan dan ujian adalah berasingan daripada persekitaran pengeluaran. PR.DS-P8: Mekanisme semakan integriti digunakan untuk mengesahkan integriti perkakasan.
	Penyelenggaraan (PR.MA-P):	PR.MA-P1: Penyelenggaraan dan pemberian aset organisasi adalah dilakukan dan dilog, dengan alat yang diluluskan dan dikawal.

	Penyelenggaraan dan pembaikan sistem dilakukan selaras dengan dasar, proses dan prosedur.	<p>PR.MA-P2: Penyelenggaraan jauh aset organisasi diluluskan, dilog dan dilakukan dengan cara yang menghalang akses tanpa kebenaran.</p>
	<p>Teknologi Perlindungan (PR.PT-P): Penyelesaian keselamatan teknikal diuruskan untuk memastikan keselamatan dan daya tahan sistem/produk/perkhidmatan dan data berkaitan, selaras dengan dasar, proses, prosedur dan perjanjian yang berkaitan.</p>	<p>PR.PT-P1: Media boleh tanggal dilindungi dan penggunaannya dihadkan mengikut dasar.</p> <p>PR.PT-P2: Prinsip kefungsian paling sedikit digabungkan dengan mengkonfigurasi sistem untuk menyediakan hanya keupayaan penting.</p> <p>PR.PT-P3: Rangkaian komunikasi dan kawalan dilindungi.</p> <p>PR.PT-P4: Mekanisma (cth., gagal selamat (<i>failsafe</i>), pengimbangan beban, pertukaran panas) dilaksanakan untuk mencapai keperluan daya tahan dalam keadaan normal dan situasi buruk.</p>

Lampiran B: Glosari

Lampiran ini mentakrifkan istilah terpilih yang digunakan untuk tujuan penerbitan ini.

Rujukan Atribut (NIST SP 800-63-3 [8])	Kenyataan yang menetapkan hak milik pelanggan tanpa perlu mengandungi maklumat identiti, bebas daripada format. Contohnya, untuk atribut "hari lahir", rujukan boleh "lebih tua daripada 18 tahun" atau "lahir pada bulan Disember."
Nilai Atribut (NIST SP 800-63-3 [8])	Kenyataan lengkap yang menegaskan sifat pelanggan, bebas daripada format. Sebagai contoh, untuk atribut "hari lahir", nilai boleh menjadi "1/12/1980" atau "1 Disember 1980."
Ketersediaan (44 U.S.C. [13])	Memastikan akses dan penggunaan maklumat yang tepat pada masanya dan boleh dipercayai.
Kategori	Pembahagian Fungsi kepada kumpulan hasil privasi yang berkait rapat dengan keperluan program dan aktiviti tertentu.
Komunikasi-P (Fungsi)	Membangunkan dan melaksanakan aktiviti yang sesuai untuk membolehkan organisasi dan individu mempunyai pemahaman yang boleh dipercayai dan terlibat dalam dialog tentang cara data diproses dan risiko privasi yang berkaitan.
Kerahsiaan (44 U.S.C. [13])	Memelihara sekatan yang dibenarkan ke atas akses dan pendedahan maklumat, termasuk cara untuk melindungi privasi peribadi dan maklumat proprietari.
Kawal-P (Fungsi)	Membangunkan dan melaksanakan aktiviti yang sesuai untuk membolehkan organisasi atau individu mengurus data dengan butiran yang mencukupi untuk mengurus risiko privasi.
Teras	Satu set aktiviti dan hasil perlindungan privasi. Teras Rangka Kerja terdiri daripada tiga elemen: Fungsi, Kategori dan Subkategori.
Insiden Keselamatan Siber	
(Kerangka untuk Meningkatkan Keselamatan Siber Infrastruktur Kritikal [1]) (OMB 17-12 [9])	Peristiwa keselamatan siber yang telah ditentukan untuk memberi kesan kepada organisasi yang mendorong keperluan untuk tindak balas dan pemulihan.
	Kejadian yang (1) sebenarnya atau tidak lama lagi menjaskankan, tanpa kuasa yang sah, integriti, kerahsiaan, atau ketersediaan maklumat atau sistem maklumat; atau (2) merupakan pelanggaran atau ancaman pelanggaran undang-undang, dasar keselamatan, prosedur keselamatan atau dasar
Data	Perwakilan maklumat, termasuk format digital dan bukan digital.

Tindakan Data (Diadaptasi daripada NIST IR 8062 [5])	Operasi kitaran hayat data sistem/produk/perkhidmatan, termasuk, tetapi tidak terhad kepada pengumpulan, pengekalan, pengelogan, penjanaan, transformasi, penggunaan, pendedahan, perkongsian, penghantaran dan pelupusan.
Elemen Data	Item terkecil yang dinamakan dalam data yang menyampaikan maklumat yang bermakna.
Pemprosesan Data (Adapted from NIST IR 8062 [5])	Set tindakan data kolektif (iaitu, kitaran hayat data yang lengkap, termasuk, tetapi tidak terhad kepada pengumpulan, pengekalan, pengelogan, penjanaan, transformasi, penggunaan, pendedahan, perkongsian, penghantaran dan pelupusan).
Ekosistem Pemprosesan Data	Hubungan yang kompleks dan saling berkait antara entiti yang terlibat dalam mencipta atau menggunakan sistem, produk atau perkhidmatan atau mana-mana komponen yang memproses data.
Kebolehpisahan (Diadaptasi daripada NIST IR 8062 [5])	Mendayakan pemprosesan data atau peristiwa tanpa kaitan dengan individu atau peranti di luar keperluan operasi sistem.
Fungsi	Komponen Teras yang menyediakan struktur tahap tertinggi untuk mengatur aktiviti privasi asas ke dalam Kategori dan Subkategori.
Tadbir Urus-P (Fungsi)	Membangunkan dan melaksanakan struktur tadbir urus organisasi untuk membolehkan pemahaman berterusan tentang keutamaan pengurusan risiko organisasi yang dimaklumkan oleh risiko privasi.
Kenal Pasti-P (Fungsi)	Membangunkan pemahaman organisasi untuk mengurus risiko privasi bagi individu yang timbul daripada pemprosesan data.
Peringkat Pelaksanaan	Menyediakan titik rujukan tentang cara organisasi melihat risiko privasi dan sama ada ia mempunyai proses dan sumber yang mencukupi untuk mengurus risiko tersebut.
Individu	Orang perseorangan atau sekumpulan orang, termasuk di peringkat masyarakat.
Integriti (44 U.S.C. [13])	Menjaga daripada pengubahsuaian atau pemusnahaan maklumat yang tidak betul, dan termasuk memastikan tanpa sangkalan (<i>non-repudiation</i>) dan kesahihan maklumat.
Keturunan	Sejarah pemprosesan elemen data, yang mungkin termasuk aliran data titik ke titik dan tindakan data yang dilakukan pada elemen data.
Kebolehurusan (Diadaptasi daripada NIST IR 8062 [5])	Menyediakan keupayaan untuk pentadbiran data secara berbutir (<i>granular</i>), termasuk pengubahan, pemadaman dan pendedahan terpilih.
Metadata (Diadaptasi daripada NIST SP 800-53 [10])	Maklumat yang menerangkan ciri-ciri data. Ini mungkin termasuk, sebagai contoh, metadata struktur yang menerangkan struktur data (iaitu, format data, sintaks, semantik) dan metadata deskriptif yang menerangkan kandungan data.

Kebolehramalan (Diadaptasi daripada NIST IR 8062 [5])	Mendayakan andaian yang boleh dipercayai oleh individu, pemilik dan pengendali tentang data dan pemprosesannya oleh sistem, produk atau perkhidmatan.
Pelanggaran Privasi (Diadaptasi daripada OMB M-17-12 [9])	Kehilangan kawalan, kompromi, pendedahan tanpa kebenaran, pemerolehan tanpa kebenaran, atau sebarang kejadian serupa di mana (1) seseorang selain daripada pengguna yang dibenarkan mengakses atau berpotensi mengakses data atau (2) pengguna yang dibenarkan mengakses data untuk tujuan selain daripada yang dibenarkan.
Kawalan Privasi (Diadaptasi daripada NIST SP 800-37 [7])	Perlindungan pentadbiran, teknikal dan fizikal yang digunakan dalam organisasi untuk memenuhi keperluan privasi.
Peristiwa Privasi	Kejadian atau potensi berlakunya tindakan data bermasalah.
Keperluan Privasi	Spesifikasi untuk fungsi sistem/produk/perkhidmatan untuk memenuhi hasil privasi yang dikehendaki oleh pihak berkepentingan.
Risiko Privasi	Kemungkinan individu akan mengalami masalah akibat daripada pemprosesan data, dan impak sekiranya ia berlaku.
Penilaian Risiko Privasi	Sub-proses pengurusan risiko privasi untuk mengenal pasti dan menilai risiko privasi tertentu.
Pengurusan Risiko Privasi	Satu set proses merentas organisasi untuk mengenal pasti, menilai dan bertindak balas terhadap risiko privasi.
Tindakan Data Bermasalah (Diadaptasi daripada NIST IR 8062 [5])	Tindakan data yang boleh menyebabkan kesan buruk kepada individu.
Memproses	Lihat <i>Pemprosesan Data</i> .
Profil	Pilihan Fungsi, Kategori dan Subkategori tertentu daripada Teras yang diutamakan oleh organisasi untuk membantunya mengurus risiko privasi.
Lindung-P (Fungsi)	Membangunkan dan melaksanakan perlindungan pemprosesan data yang sesuai.
Asal (Diadaptasi daripada NIST IR 8112 [11])	Metadata yang berkaitan dengan asal atau sumber data tertentu.

Risiko (NIST SP 800-30 [12])	Ukuran sejauh mana entiti diancam oleh keadaan atau kejadian yang berpotensi, dan biasanya fungsi: (i) kesan buruk yang akan timbul jika keadaan atau kejadian itu berlaku; dan (ii) kemungkinan berlaku.
Pengurusan Risiko	Proses mengenal pasti, menilai dan bertindak balas terhadap risiko.
Toleransi Risiko (NIST SP 800-39 [6])	Tahap risiko atau tahap ketidakpastian yang boleh diterima oleh organisasi.
Subkategori	Pembahagian selanjutnya Kategori kepada hasil khusus aktiviti teknikal dan/atau pengurusan.

Lampiran C: Akronim

Lampiran ini mentakrifkan akronim terpilih yang digunakan dalam penerbitan ini.

IEC	Suruhanjaya Elektroteknik Antarabangsa
IR	Laporan Antara Agensi atau Dalaman
ISO	International Organization for Standardization
IT	Teknologi Maklumat
NIST	Institut Piawaian dan Teknologi Negara
OASIS	Organisasi untuk Kemajuan Piawaian Maklumat Berstruktur
OECD	Pertubuhan Kerjasama dan Pembangunan Ekonomi
OMB	Pejabat Pengurusan dan Belanjawan
PMRM	Model dan Metodologi Rujukan Pengurusan Privasi
PRAM	Metodologi Penilaian Risiko Privasi
RFC	Request for Comment
RFI	Request for Information
SDLC	Kitaran Hayat Pembangunan Sistem
SP	Penerbitan Khas

Lampiran D: Amalan Pengurusan Risiko Privasi

Seksyen 1.2 memperkenalkan beberapa pertimbangan sekitar pengurusan risiko privasi, termasuk hubungan antara keselamatan siber dan risiko privasi dan peranan penilaian risiko privasi. Lampiran ini mempertimbangkan beberapa amalan utama yang menyumbang kepada pengurusan risiko privasi yang berjaya, termasuk mengatur sumber persediaan, menentukan keupayaan privasi, mentakrifkan keperluan privasi, menjalankan penilaian risiko privasi, mewujudkan keperluan privasi kebolehkesan dan pemantauan untuk mengubah risiko privasi. Rujukan Kategori dan Subkategori disertakan untuk memudahkan penggunaan Teras untuk menyokong amalan ini; rujukan ini muncul dalam kurungan.

Menguruskan Sumber Persediaan

Sumber yang sesuai memudahkan membuat keputusan termaklum tentang risiko privasi di semua peringkat organisasi. Sebagai perkara praktikal, tanggungjawab untuk pembangunan pelbagai sumber mungkin dimiliki oleh komponen organisasi yang berbeza. Oleh itu, komponen organisasi bergantung pada sumber tertentu mungkin mendapati bahawa ia sama ada tidak wujud, atau mungkin tidak menangani privasi dengan secukupnya. Dalam keadaan ini, komponen yang bergantung boleh mempertimbangkan tujuan sumber dan sama ada mencari maklumat melalui sumber lain atau membuat keputusan yang terbaik dengan maklumat yang tersedia. Ringkasnya, sumber yang baik boleh membantu, tetapi sebarang kekurangan tidak seharusnya menghalang komponen organisasi daripada membuat keputusan risiko terbaik mengikut kemampuan mereka.

Sumber berikut, walaupun tidak menyeluruh, membina asas untuk membuat keputusan yang lebih baik.

- **Tugas peranan pengurusan risiko (GV.PO-P3, GV.PO-P4)**

Mewujudkan dan membolehkan pemahaman merentas organisasi tentang siapa yang diberikan kebertanggungjawapan dan siapa yang bertanggungjawab untuk pengurusan risiko privasi serta tugas pengurusan risiko lain dalam organisasi yang menyokong penyelarasan dan kebertanggungjawapan yang lebih baik untuk membuat keputusan. Selain itu, pelbagai perspektif boleh meningkatkan proses mengenal pasti, menilai dan bertindak balas terhadap risiko privasi. Pasukan yang pelbagai dan merentas fungsi boleh membantu mengenal pasti pelbagai risiko yang lebih komprehensif terhadap privasi individu, dan untuk memilih set mitigasi yang lebih luas. Menentukan peranan yang perlu disertakan dalam perbincangan pengurusan risiko bergantung pada konteks dan susunan organisasi, walaupun kerjasama antara program privasi dan keselamatan siber organisasi adalah penting. Jika seorang individu ditugaskan untuk berbilang peranan, mengurus potensi konflik kepentingan harus dipertimbangkan.
- **Strategi pengurusan risiko perusahaan (GV.RM-P)**

Strategi pengurusan risiko perusahaan membantu menyelaraskan misi dan nilai organisasi dengan toleransi risiko organisasi, andaian, kekangan dan keutamaan. Pengehadan sumber untuk mencapai misi atau objektif perniagaan dan untuk mengurus portfolio risiko yang luas mungkin memerlukan pertukaran. Membolehkan kakitangan yang terlibat dalam proses pengurusan risiko privasi untuk lebih memahami toleransi risiko organisasi seharusnya membantu untuk membimbing keputusan tentang cara memperuntukkan sumber dan menambah baik keputusan mengenai tindak balas risiko.
- **Pihak berkepentingan utama (GV.PO-P4, ID.DE-P)**

Pihak berkepentingan privasi ialah mereka yang mempunyai kepentingan atau kebimbangan

terhadap hasil privasi sistem, produk atau perkhidmatan. Sebagai contoh, kebimbangan undang-undang mungkin tertumpu pada sama ada sistem, produk atau perkhidmatan beroperasi dengan cara yang akan menyebabkan organisasi tidak mematuhi undang-undang atau peraturan privasi atau perjanjian perniagaannya. Pemilik perniagaan yang ingin memaksimumkan penggunaan mungkin bimbang tentang kehilangan kepercayaan pada sistem, produk atau perkhidmatan kerana privasi yang lemah. Individu yang datanya sedang diproses atau yang berinteraksi dengan sistem, produk atau perkhidmatan akan berminat untuk tidak mengalami masalah atau akibat buruk. Memahami pihak berkepentingan dan jenis hasil privasi yang mereka minati akan memudahkan reka bentuk sistem/produk/perkhidmatan yang sesuai dengan keperluan pihak berkepentingan.

- **Keperluan privasi peringkat organisasi (GV.PO-P)**

Keperluan privasi peringkat organisasi ialah cara untuk menyatakan kewajipan undang-undang, nilai privasi dan dasar yang ingin dipatuhi oleh organisasi. Memahami keperluan ini adalah kunci untuk memastikan reka bentuk sistem/produk/perkhidmatan mematuhi kewajipannya.

Keperluan privasi peringkat organisasi mungkin diperoleh daripada pelbagai sumber, termasuk:

- Persekutaran undang-undang (cth., undang-undang, peraturan, kontrak);
- Dasar organisasi atau nilai budaya;
- Piawaian yang berkaitan; dan
- Prinsip privasi.

- **Artifak reka bentuk sistem/produk/perkhidmatan (ID.BE-P3)**

Artifak reka bentuk mungkin mempunyai banyak bentuk seperti seni bina reka bentuk sistem atau gambar rajah aliran data. Artifak ini membantu organisasi menentukan cara sistem, produk dan perkhidmatannya akan beroperasi. Oleh itu, mereka boleh membantu program privasi memahami cara sistem, produk dan perkhidmatan perlu berfungsi supaya kawalan atau langkah yang membantu mengurangkan risiko privasi boleh dipilih dan dilaksanakan dengan cara yang mengekalkan fungsi sambil melindungi privasi.

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

Peta data menggambarkan pemprosesan data dan interaksi individu dengan sistem, produk dan perkhidmatan. Peta data menunjukkan persekitaran pemprosesan data dan termasuk komponen yang melalui data sedang diproses atau dengan mana individu berinteraksi, pemilik atau pengendali komponen, dan tindakan data diskret dan elemen data khusus yang sedang diproses. Peta data boleh digambarkan dalam cara yang berbeza, dan tahap perincian mungkin berbeza-beza berdasarkan keperluan organisasi. Peta data boleh ditindih pada artifak reka bentuk sistem/produk/perkhidmatan sedia ada untuk kemudahan dan kemudahan komunikasi antara komponen organisasi. Seperti yang dibincangkan di bawah, peta data ialah artifak penting dalam penilaian risiko privasi.

Menentukan Keupayaan Privasi

Keupayaan privasi boleh digunakan untuk menerangkan sistem, produk atau harta perkhidmatan atau ciri yang mencapai hasil privasi yang diingini (cth., "perkhidmatan membolehkan peminimuman data"). Objektif keselamatan ialitu kerahsiaan, integriti dan ketersediaan bersama-sama keperluan keselamatan digunakan untuk memaklumkan keupayaan keselamatan untuk sistem, produk atau perkhidmatan. Seperti yang dinyatakan dalam **Jadual 3**, satu set tambahan objektif kejuruteraan privasi boleh menyokong penentuan keupayaan privasi. Organisasi juga boleh menggunakan objektif kejuruteraan privasi sebagai alat keutamaan peringkat tinggi. Sistem, produk atau perkhidmatan yang rendah dalam kebolehramalan, kebolehurusan atau kebolehpisahan mungkin merupakan isyarat peningkatan risiko privasi, dan oleh itu memerlukan penilaian risiko privasi yang lebih komprehensif.

Dalam menentukan keupayaan privasi, organisasi boleh mempertimbangkan kejuruteraan privasi dan objektif keselamatan yang mana yang paling penting berkenaan dengan misi atau keperluan perniagaannya, toleransi risiko dan keperluan privasi peringkat organisasi (lihat Mengatur Sumber Persediaan di atas). Tidak semua objektif mungkin sama penting, atau pertukaran mungkin perlu di antara mereka. Walaupun keupayaan privasi memaklumkan penilaian risiko privasi dengan menyokong keputusan keutamaan risiko, keupayaan privasi juga mungkin dimaklumkan oleh penilaian risiko dan diselaraskan untuk menyokong pengurusan risiko privasi tertentu atau menangani perubahan dalam persekitaran, termasuk perubahan reka bentuk pada sistem, produk, atau perkhidmatan.

Jadual 3: Kejuruteraan Privasi dan Objektif Keselamatan¹⁸

	Objektif	Definisi	Fungsi Berkaitan Utama daripada Teras Rangka Kerja Privasi
Objektif Kejuruteraan Privasi	Kebolehramalan	Mendayakan andaian yang boleh dipercayai oleh individu, pemilik dan pengendali tentang data dan pemprosesannya oleh sistem	Kenal Pasti-P, Tadbir Urus-P, Kawal-P, Komunikasi-P, Lindung-P
	Keupayaan mengurus	Menyediakan keupayaan untuk pentadbiran data secara berbutir, termasuk pengumpulan, pengubahan, pemadaman, dan pendedahan terpilih	Kenal Pasti-P, Tadbir Urus-P, Kawal-P
	Kebolehpisahan	Mendayakan pemprosesan data atau peristiwa tanpa kaitan dengan individu atau peranti di luar keperluan operasi sistem	Kenal Pasti-P, Tadbir Urus-P, Kawal-P
Objektif Keselamatan	Kerahsiaan	Memelihara sekatan yang dibenarkan ke atas akses dan pendedahan maklumat, termasuk cara untuk melindungi privasi peribadi dan maklumat proprietari	Kenal Pasti-P, Tadbir Urus-P, Kawal-P
	Integriti	Menjaga daripada pengubahsuaian atau pemusnahan maklumat yang tidak betul; termasuk memastikan tanpa sangkalan (<i>non-repudiation</i>) dan kesahihah maklumat.	Kenal Pasti-P, Tadbir Urus-P, Kawal-P
	Ketersediaan	Memastikan akses dan penggunaan maklumat yang tepat pada masanya dan boleh dipercayai	Kenal Pasti-P, Tadbir Urus-P, Kawal-P

Menentukan Keperluan Privasi

Keperluan privasi menentukan cara sistem, produk atau perkhidmatan perlu berfungsi untuk memenuhi hasil privasi yang dikehendaki pihak berkepentingan (cth., "aplikasi dikonfigurasikan untuk membolehkan pengguna memilih elemen data tertentu"). Untuk menentukan keperluan privasi, pertimbangkan keperluan privasi peringkat organisasi (lihat Menyusun Sumber Persediaan di atas) dan output penilaian risiko privasi. Proses ini membantu organisasi menjawab dua soalan: 1) Apakah yang boleh dilakukan oleh sistem, produk atau perkhidmatan dengan pemprosesan data dan interaksi dengan individu? 2) Apakah yang perlu dilakukan? Kemudian organisasi boleh memperuntukkan sumber untuk mereka bentuk sistem, produk atau perkhidmatan dengan cara yang mencapai keperluan yang ditetapkan. Akhirnya, mentakrifkan keperluan privasi boleh membawa kepada pembangunan sistem,

¹⁸ Objektif kejuruteraan privasi diadaptasi daripada NIST IR 8062 [5]. Objektif keselamatan adalah daripada NIST SP 800-37, Rev. 2 [7].

produk dan perkhidmatan yang lebih mengambil berat tentang privasi individu, dan berdasarkan keputusan risiko termaklum.

Menjalankan Penilaian Risiko Privasi

Menjalankan penilaian risiko privasi membantu organisasi mengenal pasti risiko privasi yang ditimbulkan oleh sistem, produk atau perkhidmatan dan memberi keutamaan kepada mereka untuk dapat membuat keputusan termaklum tentang cara bertindak balas terhadap risiko tersebut (ID.RA-P, GV.RM-P). Metodologi untuk menjalankan penilaian risiko privasi mungkin berbeza-beza, tetapi organisasi harus mempertimbangkan ciri-ciri berikut:¹⁹

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

Model risiko mentakrifkan faktor risiko yang akan dinilai dan hubungan antara faktor tersebut.²⁰ Jika sesebuah organisasi tidak menggunakan model risiko yang telah ditetapkan, organisasi harus mentakrifkan dengan jelas faktor risiko yang akan dinilai dan hubungan antara faktor ini. Walaupun keselamatan siber mempunyai model risiko yang digunakan secara meluas berdasarkan faktor risiko ancaman, kerentanan, kemungkinan dan impak, tidak ada satu model risiko privasi yang diterima umum. NIST telah membangunkan sebuah model risiko privasi untuk mengira risiko berdasarkan kemungkinan tindakan data bermasalah didarab dengan kesan tindakan data bermasalah; setiap satu daripada tiga faktor risiko diterangkan di bawah.

Faktor Risiko Privasi:
Tindakan Data Bermasalah | Kemungkinan | Impak

- Tindakan data bermasalah ialah sebarang tindakan yang diambil oleh sistem untuk memproses data yang boleh mengakibatkan masalah kepada individu. Organisasi mempertimbangkan jenis masalah yang berkaitan dengan populasi individu. Masalah boleh berlaku dalam apa jua bentuk dan mungkin mempertimbangkan pengalaman individu.²¹
- Kebarangkalian ditakrifkan sebagai analisis kontekstual bahawa tindakan data berkemungkinan menimbulkan masalah bagi satu set individu yang mewakili. Konteks boleh merangkumi faktor organisasi (cth., lokasi geografi, persepsi awam tentang organisasi yang mengambil bahagian berkenaan dengan privasi), faktor sistem (cth., sifat dan sejarah interaksi individu dengan sistem, keterlihatan pemprosesan data kepada individu dan pihak ketiga), atau faktor individu (cth., demografi individu, minat atau persepsi privasi, kepekaan data).²² Peta data boleh membantu dengan analisis kontekstual ini (lihat Mengatur Sumber Persediaan).
- Kesan ialah analisis kos sekiranya masalah berlaku. Seperti yang dinyatakan dalam seksyen 1.2, organisasi tidak mengalami masalah ini secara langsung. Selain itu, pengalaman individu

¹⁹ NIST telah membangunkan Metodologi Penilaian Risiko Privasi (PRAM) yang boleh membantu organisasi mengenal pasti, menilai dan bertindak balas terhadap risiko privasi. Ia terdiri daripada satu set lembaran kerja yang terdapat di [3].

²⁰ Lihat NIST SP 800-30, Rev. 1, *Guide for Conducting Risk Assessments* [12] di m. 8.

²¹ Sebagai sebahagian daripada PRAM, NIST telah mencipta katalog ilustrasi tindakan data bermasalah dan masalah untuk dipertimbangkan [3]. Organisasi lain mungkin telah mencipta set masalah tambahan, atau mungkin merujuknya sebagai akibat buruk atau bahaya.

²² Lihat NIST PRAM untuk mendapatkan maklumat lanjut tentang faktor kontekstual. Id. di Lembaran Kerja 2.

mungkin subjektif. Oleh itu, kesan mungkin sukar untuk dinilai dengan tepat. Organisasi harus mempertimbangkan cara terbaik untuk memahami impak kepada individu untuk memberi keutamaan dan bertindak balas terhadap risiko privasi dengan sewajarnya.²³

- **Pendekatan penilaian**

Pendekatan penilaian ialah mekanisme di mana risiko yang dikenal pasti diutamakan. Pendekatan penilaian boleh dikategorikan sebagai kuantitatif, separa kuantitatif, atau kualitatif.^{24 25}

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

Had terpakai sumber organisasi yang diberikan, organisasi mengutamakan risiko untuk memudahkan komunikasi tentang cara bertindak balas..²⁶

- **Bertindak balas terhadap risiko (ID.RA-P5)**

Seperti yang diterangkan dalam seksyen 1.2.2, pendekatan tindak balas termasuk mitigasi, pemindahan/perkongsian, pengelakan atau penerimaan.²⁷

Mewujudkan Keperluan Privasi Kebolehkesanan

Sebaik sahaja organisasi telah menentukan risiko yang perlu dikurangkan, ia boleh memperhalusi keperluan privasi dan kemudian memilih dan melaksanakan kawalan (iaitu, perlindungan teknikal, fizikal dan/atau dasar) untuk memenuhi keperluan.²⁸ Organisasi boleh menggunakan pelbagai sumber untuk memilih kawalan, seperti NIST SP 800-53, *Kawalan Keselamatan dan Privasi untuk Sistem Maklumat dan Organisasi*.²⁹ Selepas pelaksanaan, organisasi menilai secara berulang kawalan untuk keberkesanannya dalam memenuhi keperluan privasi dan mengurus risiko privasi. Dengan cara ini, organisasi mewujudkan kebolehkesanan antara kawalan dan keperluan privasi, dan menunjukkan akauntabiliti antara sistem, produk dan perkhidmatannya serta matlamat privasi organisasinya.

Memantau Perubahan

Pengurusan risiko privasi bukanlah proses statik. Organisasi memantau bagaimana perubahan dalam persekitaran perniagaannya—termasuk undang-undang dan peraturan baharu serta teknologi baru muncul—and perubahan sepadan pada sistem, produk dan perkhidmatannya mungkin menjelaskan risiko privasi, dan secara berulang menggunakan amalan dalam lampiran ini untuk melaraskan sewajarnya. (GV.MT-P1)

²³ NIST PRAM menggunakan kos organisasi seperti kos ketidakpatuhan, kos perniagaan langsung, kos reputasi dan kos budaya dalaman sebagai pemacu untuk mempertimbangkan cara menilai impak individu. Id. di Lembaran Kerja 3, Tab Impak.

²⁴ Lihat NIST SP 800-30, Rev. 1, Panduan untuk Menjalankan Penilaian Risiko di [12] hlm. 14.

²⁵ NIST PRAM menggunakan pendekatan separa kuantitatif berdasarkan skala 1-10.

²⁶ NIST PRAM menyediakan pelbagai perwakilan keutamaan, termasuk peta haba. Lihat [3] Lembaran Kerja 3.

²⁷ NIST PRAM menyediakan proses untuk bertindak balas terhadap risiko privasi yang diutamakan. Id. di Lembaran Kerja 4.

²⁸ Lihat NIST SP 800-37, Rev. 2 [7].

²⁹ Lihat NIST SP 800-53 seperti yang dikemas kini [10].

Lampiran E: Definisi Peringkat Pelaksanaan

Empat Peringkat yang diringkaskan di bawah masing-masing ditakrifkan dengan empat elemen:

Peringkat 1: Separa

- **Proses Pengurusan Risiko Privasi** – Amalan pengurusan risiko privasi organisasi tidak diformalkan, dan risiko diurus secara ad hoc dan kadangkala reaktif. Pengutamaan aktiviti privasi mungkin tidak dimaklumkan secara langsung oleh keutamaan pengurusan risiko organisasi, penilaian risiko privasi, atau misi atau objektif perniagaan.
- **Program Pengurusan Risiko Privasi Bersepadu** – Terdapat kesedaran terhad tentang risiko privasi di peringkat organisasi. Organisasi melaksanakan pengurusan risiko privasi secara tidak teratur, kes demi kes disebabkan oleh pelbagai pengalaman atau maklumat yang diperoleh daripada sumber luar. Organisasi mungkin tidak mempunyai proses yang membolehkan perkongsian maklumat tentang pemprosesan data dan mengakibatkan risiko privasi dalam organisasi.
- **Hubungan Ekosistem Pemprosesan Data** – Terdapat pemahaman terhad tentang peranan organisasi dalam ekosistem yang lebih besar berkenaan dengan entiti lain (cth., pembeli, pembekal, penyedia perkhidmatan, rakan perniagaan, rakan kongsi). Organisasi tidak mempunyai proses untuk mengenal pasti bagaimana risiko privasi boleh berkembang di seluruh ekosistem atau untuk menyampaikan risiko atau keperluan privasi kepada entiti lain dalam ekosistem.
- **Tenaga kerja** – Sesetengah kakitangan mungkin mempunyai pemahaman terhad tentang risiko privasi atau proses pengurusan risiko privasi, tetapi tidak mempunyai tanggungjawab privasi khusus. Jika tersedia, latihan privasi adalah ad hoc dan kandungannya tidak disetarakan dengan amalan terbaik.

Peringkat 2: Risiko Termaklum

- **Proses Pengurusan Risiko Privasi** – Amalan pengurusan risiko diluluskan oleh pengurusan tetapi mungkin tidak ditetapkan sebagai dasar seluruh organisasi. Pengutamaan aktiviti privasi dimaklumkan secara langsung oleh keutamaan pengurusan risiko organisasi, penilaian risiko privasi, atau misi atau objektif perniagaan.
- **Program Pengurusan Risiko Privasi Bersepadu** – Terdapat kesedaran tentang risiko privasi di peringkat organisasi, tetapi pendekatan seluruh organisasi untuk mengurus risiko privasi belum diwujudkan. Maklumat tentang pemprosesan data dan risiko privasi yang terhasil dikongsi dalam organisasi secara tidak formal. Pertimbangan privasi dalam objektif dan program organisasi mungkin berlaku pada beberapa tetapi tidak semua peringkat organisasi. Penilaian risiko privasi berlaku, tetapi biasanya tidak boleh berulang atau berlaku lagi.
- **Hubungan Ekosistem Pemprosesan Data** – Terdapat beberapa pemahaman tentang peranan organisasi dalam ekosistem yang lebih besar berkenaan dengan entiti lain (cth., pembeli, pembekal, penyedia perkhidmatan, rakan perniagaan, rakan kongsi). Organisasi menyedari risiko ekosistem privasi yang dikaitkan dengan produk dan perkhidmatan yang disediakan dan digunakan, tetapi tidak bertindak secara konsisten atau formal terhadap risiko tersebut.
- **Tenaga kerja** – Terdapat kakitangan yang mempunyai tanggungjawab privasi khusus, tetapi mereka mungkin mempunyai tanggungjawab bukan privasi juga. Latihan privasi dijalankan secara kerap untuk kakitangan privasi, walaupun tiada proses yang konsisten untuk kemas kini

tentang amalan terbaik.

Peringkat 3: Boleh Ulang

- **Proses Pengurusan Risiko Privasi** – Amalan pengurusan risiko organisasi diluluskan secara rasmi dan dinyatakan sebagai dasar. Amalan privasi organisasi sentiasa dikemas kini berdasarkan aplikasi proses pengurusan risiko kepada perubahan dalam misi atau objektif perniagaan dan risiko, dasar dan landskap teknologi yang berubah.
- **Program Pengurusan Risiko Privasi Bersepada** – Terdapat pendekatan seluruh organisasi untuk mengurus risiko privasi. Polisi, proses dan prosedur yang dimaklumkan tentang risiko ditakrifkan, dilaksanakan seperti yang dimaksudkan, dan dikaji semula. Kaedah yang konsisten disediakan untuk bertindak balas secara berkesan terhadap perubahan risiko. Organisasi memantau risiko privasi secara konsisten dan tepat. Eksekutif kanan privasi dan bukan privasi berkomunikasi secara kerap mengenai risiko privasi. Eksekutif kanan memastikan pertimbangan privasi melalui semua baris operasi dalam organisasi.
- **Hubungan Ekosistem Pemprosesan Data** – Organisasi memahami peranannya, kebergantungan dan tanggungannya dalam ekosistem yang lebih besar dan mungkin menyumbang kepada pemahaman masyarakat yang lebih luas tentang risiko. Organisasi menyedari risiko ekosistem privasi yang berkaitan dengan produk dan perkhidmatan yang disediakan dan digunakannya. Selain itu, ia biasanya bertindak secara formal ke atas risiko tersebut, termasuk mekanisme seperti perjanjian bertulis untuk menyampaikan keperluan privasi, struktur tadbir urus dan pelaksanaan dan pemantauan dasar.
- **Tenaga kerja** – Kakitangan privasi yang berdedikasi memiliki pengetahuan dan kemahiran untuk melaksanakan peranan dan tanggungjawab yang dilantik. Terdapat latihan privasi yang tetap dan terkini untuk semua kakitangan.

Peringkat 4: Mudah Suai

- **Proses Pengurusan Risiko Privasi** – Organisasi menyesuaikan amalan privasinya berdasarkan pengajaran yang dipelajari daripada peristiwa privasi dan pengenalpastian risiko privasi baharu. Melalui proses penambahbaikan berterusan yang menggabungkan teknologi dan amalan privasi termaju, organisasi secara aktif menyesuaikan diri dengan dasar dan landskap teknologi yang berubah dan bertindak balas tepat pada masanya dan berkesan terhadap risiko privasi yang berkembang.
- **Program Pengurusan Risiko Privasi Bersepada** – Terdapat pendekatan seluruh organisasi untuk mengurus risiko privasi yang menggunakan dasar, proses dan prosedur bermaklumat risiko untuk menangani tindakan data yang bermasalah. Hubungan antara risiko privasi dan objektif organisasi difahami dengan jelas dan dipertimbangkan semasa membuat keputusan. Eksekutif kanan memantau risiko privasi dalam konteks yang sama seperti risiko keselamatan siber, risiko kewangan dan risiko lain organisasi. Belanjawan organisasi adalah berdasarkan pemahaman tentang persekitaran risiko semasa dan diramalkan serta toleransi risiko. Unit perniagaan melaksanakan visi eksekutif dan menganalisis risiko peringkat sistem dalam konteks toleransi risiko organisasi. Pengurusan risiko privasi adalah sebahagian daripada budaya organisasi dan berkembang daripada pengajaran yang dipelajari dan kesedaran berterusan tentang pemprosesan data dan risiko privasi yang berhasil. Organisasi boleh dengan cepat dan cekap mengambil kira perubahan kepada objektif perniagaan/misi dalam cara risiko didekati dan disampaikan.
- **Hubungan Ekosistem Pemprosesan Data** – Organisasi memahami peranan, kebergantungan

dan tanggungannya dalam ekosistem yang lebih besar dan menyumbang kepada pemahaman masyarakat yang lebih luas tentang risiko. Organisasi menggunakan maklumat masa nyata atau hampir masa nyata untuk memahami dan bertindak secara konsisten terhadap risiko ekosistem privasi yang berkaitan dengan produk dan perkhidmatan yang disediakan dan digunakannya. Selain itu, ia berkomunikasi secara proaktif, menggunakan mekanisme formal (cth., perjanjian) dan tidak formal untuk membangun dan mengekalkan hubungan ekosistem yang kukuh.

- **Tenaga kerja** – Organisasi mempunyai kemahiran privasi khusus di seluruh struktur organisasi; kakitangan dengan pelbagai perspektif menyumbang kepada pengurusan risiko privasi. Terdapat latihan privasi yang tetap, terkini dan khusus untuk semua kakitangan. Kakitangan di semua peringkat memahami nilai privasi organisasi dan peranan mereka dalam mengekalkannya.