JAWATANKUASA PENGKOMPUTERAN AWAN

SOALAN LAZIM MENGENAI KLASIFIKASI MAKLUMAT/DATA DALAM PENGGUNAAN PENGKOMPUTERAN AWAN

OGOS 2021

1. LATAR BELAKANG

1.1. Soalan Lazim Mengenai Klasifikasi Maklumat/Data Dalam Penggunaan Pengkomputeran Awan ini bertujuan untuk membantu Kementerian/Agensi Kerajaan mengenal pasti klasifikasi maklumat/data mengikut empat (4) peringkat keselamatan Rahsia Rasmi di bawah Akta Rahsia Rasmi 1972 iaitu Rahsia Besar, Rahsia, Sulit dan Terhad.

1.2. Selain daripada menerangkan definisi dan kaedah penentuan klasifikasi maklumat/data, soalan lazim ini turut menerangkan penggunaan kemudahan pengkomputeran awan dan langkah-langkah yang perlu dilaksanakan oleh Kementerian/Agensi Kerajaan dalam memastikan keselamatan maklumat/data yang ditempatkan di kemudahan tersebut.

1.3. Inisiatif ini adalah selaras dengan aspirasi Kerajaan untuk menggalak dan memperluaskan penggunaan kemudahan pengkomputeran awan di sektor awam. Dengan pemahaman yang jelas tentang proses penentuan klasifikasi maklumat/data, Kementerian/Agensi berupaya menggunakan kemudahan pengkomputeran awan ke tahap yang optimum.

1.4. Soalan lazim ini dibangunkan melalui hasil kerjasama Agensi Keselamatan Siber Negara (NACSA), Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO), Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perlindungan Data Peribadi (JPDP), Malaysia Digital Economy Corporation (MDEC) dan Cybersecurity Malaysia (CSM).

2. SEKSYEN A: KLASIFIKASI MAKLUMAT/DATA DAN PENGKOMPUTERAN AWAN

2.1. Apakah yang dimaksudkan dengan Maklumat Rasmi dan Rahsia Rasmi?

Jawapan:

Arahan Keselamatan (Semakan dan Pindaan 2017) dan Akta Rahsia Rasmi 1972 (Akta 88) mentakrifkan Maklumat Rasmi dan Rahsia Rasmi seperti berikut:

Maklumat Rasmi	:	Pengetahuan mengenai perkara rasmi, walau cara mana sekalipun diperoleh, termasuk: • Jenis atau kandungan apa-apa dokumen rasmi atau sebahagiannya; • Jenis, kegunaan dan komposisi bahan-bahan; • Kaedah dan cara menghasilkan serta teknik dan proses yang digunakan untuk pengeluaran;

- Proses saintifik terutama sekali berkenaan dengan pembuatan senjata dan kelengkapan; dan
- Butir-butir kegiatan rasmi yang diperoleh secara lisan.

Rahsia Rasmi : Apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 (Akta 88) dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”, “Sulit” atau “Terhad” mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu Negeri atau mana-mana pegawai awam yang dilantik bawah seksyen 2B Akta 88.

2.2. Apakah yang dimaksudkan dengan Rahsia Besar, Rahsia, Sulit dan Terhad dalam Rahsia Rasmi?

Jawapan:

Arahan Keselamatan (Semakan dan Pindaan 2017) mentakrifkan Rahsia Besar, Rahsia, Sulit dan Terhad seperti berikut:

Rahsia Besar : Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia.

Rahsia : Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing.

Sulit : Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing.

Terhad : Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan sebagai “Rahsia Besar”, “Rahsia” atau “Sulit” tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan.

2.3. Apakah yang dimaksudkan dengan data terbuka?

Jawapan:
Garis Panduan Pelaksanaan Data Terbuka Sektor Awam yang dikeluarkan oleh MAMPU mentakrifkan data terbuka sebagai data yang boleh digunakan secara bebas, boleh dikongsikan dan digunakan semula oleh rakyat, agensi kerajaan dan swasta untuk pelbagai tujuan. Penentuan data terbuka hendaklah merujuk kepada Pekeliling Am Bil. 1 Tahun 2015: Pelaksanaan Data Terbuka Sektor Awam.

Data Terbuka adalah maklumat rasmi yang telah dibuat saringan dan pengesahan di peringkat pemula data untuk bebas digunakan, dikongsi serta digunakan semula oleh orang awam, agensi Kerajaan dan organisasi swasta untuk pelbagai tujuan. Penentuan dan tafsiran data terbuka merujuk kepada Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (*Cloud Computing*) Dalam Perkhidmatan Awam yang dikeluarkan oleh CGSO.

2.4. Bagaimanakah kaedah penentuan klasifikasi maklumat/data ditentukan sama ada ianya Maklumat Rasmi atau Rahsia Rasmi?

Jawapan:
Secara ringkasnya, pemilik/pemula perlu membuat penilaian risiko ke atas suratan, maklumat dan bahan rasmi yang dikelaskan. Pemilik/pemula maklumat/data perlu menentukan sama ada maklumat/data tersebut boleh memberi implikasi kepada orang perseorangan, keselamatan, pertahanan, fungsi pentadbiran Kerajaan, atau kepentingan dan kedaulatan negara.

Sekiranya penilaian ke atas maklumat/data tersebut mendapati ia mempunyai implikasi kepada perkara-perkara di atas, maka ia perlu dikelaskan menjadi maklumat Rahsia Rasmi.

Penentuan peringkat keselamatan Rahsia Rasmi perlu dilaksanakan oleh Pegawai Pengelas[1] Kementerian/Agensi masing-masing melalui penilaian risiko dan semakan awal yang melibatkan proses menyemak, menilai, memberi tanda dan merekod, sepertimana yang digariskan dalam Garis Panduan Pengelasan dan Pengelasan Semula Mengikut Akta Rahsia Rasmi 1972 dan Surat Pekeliling Am Bilangan 2 Tahun 1987 yang dikeluarkan oleh CGSO.

[1] Pegawai yang dilantik di bawah peruntukan Seksyen 2B, Akta Rahsia Rasmi 1972 (Akta 88) untuk mengelaskan apa-apa suratan rasmi, maklumat atau bahan sebagai Rahsia Besar, Rahsia, Sulit atau Terhad.

2.5. Adakah agensi Kerajaan perlu menggunakan perkhidmatan pengkomputeran awan bagi menempatkan sistem aplikasi baharu Kerajaan yang ingin dibangunkan?

Jawapan:
Ya, berdasarkan Pekeliling Kemajuan Pentadbiran Awam Tahun 2020: Polisi Perkhidmatan Pengkomputeran Awan Sektor Awam, agensi Kerajaan hendaklah menggunakan kemudahan perkhidmatan pengkomputeran awan dalam pembangunan sistem aplikasi baharu[2]. Sebagai contoh, Kementerian/Agensi boleh menggunakan kemudahan pengkomputeran awan yang disediakan oleh MAMPU melalui Pusat Data Sektor Awam (PDSA).

Namun begitu, kaedah penggunaan kemudahan ini adalah berbeza mengikut klasifikasi maklumat/data yang terlibat dalam pembangunan sistem tersebut. Penerangan lanjut mengenai perkara ini adalah seperti di Seksyen B: Penentuan Model Pengkomputeran Awan Mengikut Klasifikasi Maklumat/Data.

2.6. Adakah agensi Kerajaan dibenarkan untuk menggunakan perkhidmatan pengkomputeran awan bagi tujuan menempatkan sistem aplikasi sedia ada yang ingin dinaik taraf?

Jawapan:
Ya, semua agensi Kerajaan dibenarkan untuk menggunakan perkhidmatan pengkomputeran awan bagi tujuan menempatkan sistem aplikasi sedia ada yang ingin dinaik taraf.

Walau bagaimanapun, pihak Kementerian/Agensi hendaklah melaksanakan penilaian risiko terhadap sistem aplikasi tersebut sebelum melakukan migrasi ke kemudahan pengkomputeran awan, khususnya yang berada di luar dari premis Kerajaan. Sebarang penentuan model pengkomputeran awan yang ingin digunakan hendaklah berdasarkan penilaian risiko yang dilaksanakan serta klasifikasi maklumat/data yang disimpan oleh sistem aplikasi berkenaan.

[2] Malaysia Cloud First Strategy

3. SEKSYEN B: PENENTUAN MODEL PENGKOMPUTERAN AWAN MENGIKUT KLASIFIKASI MAKLUMAT/DATA

3.1. Sistem yang akan dibangunkan oleh Kementerian/Agensi saya melibatkan maklumat/data Rahsia Rasmi. Apakah model pengkomputeran awan yang dibenarkan untuk menempatkan maklumat/data ini?

Jawapan:
Pada masa ini, perkhidmatan pengkomputeran awan tidak dibenarkan bagi tujuan menempatkan maklumat/data Rahsia Rasmi berperingkat Rahsia Besar dan Rahsia. Maklumat/data tersebut hendaklah disimpan di dalam premis Kementerian/Agensi.

Manakala, bagi maklumat/data Sulit dan Terhad atau Maklumat Rasmi, Kementerian/Agensi hanya boleh menggunakan perkhidmatan pengkomputeran awan Kerajaan yang disediakan oleh MAMPU melalui PDSA (MyGovCloud@PDSA) atau menggunakan perkhidmatan yang ditawarkan oleh *Cloud Service Provider* (CSP) tempatan atau asing secara Private Cloud yang dihoskan dalam negara. Kebenaran pengendalian oleh CSP bagi penyimpanan maklumat/data Sulit dan Terhad adalah tertakluk kepada pengesahan dengan merujuk kepada CGSO terlebih dahulu.

Penerangan lanjut mengenai penggunaan pengkomputeran awan yang melibatkan Rahsia Rasmi hendaklah dirujuk kepada Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (*Cloud Computing*) Dalam Perkhidmatan Awam yang dikeluarkan oleh CGSO.

3.2. Sistem yang akan dibangunkan oleh Kementerian/Agensi saya melibatkan data terbuka. Apakah model pengkomputeran awan yang dibenarkan untuk menempatkan maklumat/data ini?

Jawapan:
Secara dasarnya, tiada halangan terhadap penempatan data terbuka di mana-mana model perkhidmatan pengkomputeran awan dalam dan luar negara. Walau bagaimanapun, Kementerian/Agensi perlu memastikan langkah-langkah keselamatan yang bersesuaian dilaksanakan berdasarkan keperluan atau syarat keselamatan asas (*baseline security requirement*) kemudahan pengkomputeran awan tersebut.

3.3. Apakah langkah-langkah yang perlu Kementerian/Agensi saya laksanakan untuk menggunakan kemudahan pengkomputeran awan, dan pada masa yang sama memastikan keselamatan maklumat/data yang terlibat?

Jawapan:
Kementerian/Agensi hendaklah melaksanakan penilaian risiko sebelum membangunkan sesuatu sistem aplikasi atau membuat keputusan untuk melaksanakan migrasi sistem aplikasi sedia ada ke sesuatu model pengkomputeran awan. Sebarang penentuan model pengkomputeran awan yang ingin digunakan hendaklah berdasarkan penilaian risiko yang dilaksanakan serta klasifikasi maklumat/data yang disimpan oleh sistem aplikasi berkenaan.

Kementerian/Agensi juga hendaklah melaksanakan langkah-langkah keselamatan yang bersesuaian, tertakluk kepada klasifikasi maklumat yang terlibat, antaranya seperti:

i) mengenalpasti perundangan dan polisi pemberi/penyedia perkhidmatan awan luar negara sebelum menempatkan maklumat/data terbuka;

ii) menggunakan produk kriptografi yang mematuhi Dasar Kriptografi Negara[3] bagi tujuan penyulitan (*encryption*) maklumat dan sistem yang mengandungi maklumat/data rahsia rasmi. Senarai produk kriptografi ini boleh diperolehi melalui pautan https://myseal.cybersecurity.my/index.html; dan

iii) menggunakan pendekatan keselamatan siber yang sesuai bagi tujuan melindungi *data-in-use*, *data-at-rest* dan *data-in-transit*. Sebagai contoh, Kementerian/Agensi boleh menggunakan produk keselamatan siber seperti *Next Generation Firewall* (NGFW), *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS), *Data Leakage Protection* (DLP) dan *Web Application Firewall* (WAF).

Kementerian/Agensi juga boleh merujuk Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (*Cloud Computing*) Dalam Perkhidmatan Awam dan Rangka Kerja Keselamatan Siber Sektor awam (RAKKSSA) bagi pelaksanaan langkah-langkah keselamatan yang bersesuaian.

[3] Rujukan kepada Dasar Kriptografi Negara

3.4. Apakah penilaian keselamatan yang perlu dipatuhi oleh produk keselamatan siber yang ingin digunakan?

Jawapan:
Kementerian/Agensi hendaklah memastikan supaya produk keselamatan siber yang ingin digunakan telah mendapat pensijilan keselamatan ICT dan diiktiraf oleh Kerajaan.

Kementerian/Agensi juga adalah digalakkan untuk menggunakan produk keselamatan siber yang mematuhi penilaian keselamatan berikut:

i) menjalani pengujian keselamatan seperti pengujian penembusan secara berkala (tahunan);

ii) menjalani audit konfigurasi produk dan sistem secara berkala (tahunan);

iii) mendapat pensijilan *Common Criteria* EAL2 yang tertakluk di bawah pengiktirafan *Common Criteria Recognition Authority* (CCRA) atau pensijilan lain yang setaraf dengannya daripada badan pensijilan yang diiktiraf Kerajaan; dan

iv) mendapat pensijilan skema *Technology Security Assurance* (TSA) atau pensijilan lain yang setaraf dengannya daripada badan pensijilan yang diiktiraf Kerajaan.

3.5. Apakah impak/kesan yang akan berlaku sekiranya Kementerian/ Agensi tidak melaksanakan langkah-langkah keselamatan sebelum menggunakan kemudahan pengkomputeran awan?

Jawapan:
Langkah-langkah keselamatan sepertimana yang dijelaskan dalam para 3.3. dan 3.4. perlu dilaksanakan bagi menjamin keselamatan maklumat/data yang akan menggunakan perkhidmatan pengkomputeran awan. Sekiranya Kementerian/Agensi tidak melaksanakan langkah-langkah keselamatan tersebut, pelepasan maklumat/data ini kepada pihak yang tidak dibenarkan dan boleh terdedah kepada risiko kebocoran, kecurian, kehilangan dan penyalahgunaan oleh pihak lain.

Perkara ini seterusnya boleh menggugat keselamatan dan kedaulatan negara, memberi impak yang negatif terhadap imej Kerajaan, menyebabkan kerugian hasil pendapatan kepada Kerajaan dan mengganggu ketersediaan perkhidmatan Kementerian/Agensi.

4. SEKSYEN C: CARTA ALIRAN KLASIFIKASI MAKLUMAT/DATA DAN PENGGUNAAN PERKHIDMATAN PENGKOMPUTERAN AWAN DI SEKTOR AWAM