Bil	Soalan	Jawapan
1	Terdapat beberapa persoalan berkaitan keselamatan data yang tersimpan dalam *Google Workspace* (GWS), khususnya penggunaan *Google Drive*, memandangkan ia turut melibatkan pelbagai inovasi serta interaksi dengan pelanggan umum. Apakah penjelasan khusus berkenaan perkara ini?	Penggunaan mana-mana perkhidmatan pengkomputeran awan (*cloud computing*) dalam Sektor Awam adalah tertakluk kepada arahan dan garis panduan keselamatan siber yang telah ditetapkan oleh Kerajaan. **A. Garis Panduan Tadbir Urus Perkhidmatan Komunikasi dan Kolaboratif Bersepadu Kerajaan (MyGovUC)** Selaras dengan **Garis Panduan Tadbir Urus Perkhidmatan MyGovUC**, tanggungjawab untuk menguruskan maklumat diletakkan kepada setiap pengguna. Para **1.4.1 (k)** garis panduan tersebut secara spesifik menyatakan: i. Penyimpanan maklumat klasifikasi **Terbuka** adalah dibenarkan; ii. Penyimpanan sementara maklumat rahsia rasmi yang diklasifikasikan sebagai **TERHAD** dan **SULIT** adalah dibenarkan melalui penggunaan fungsi keselamatan yang disediakan **(perkhidmatan e-mel sahaja)**; iii. Penghantaran, penerimaan, dan penyimpanan sementara maklumat rahsia rasmi yang diklasifikasikan sebagai **RAHSIA** dan **RAHSIA BESAR** adalah **TIDAK DIBENARKAN**; dan iv. Rakaman maklumat rahsia rasmi juga adalah **TIDAK DIBENARKAN**.

		Ketetapan ini menegaskan bahawa setiap penjawat awam yang menggunakan GWS bertanggungjawab sepenuhnya untuk memastikan data yang disimpan adalah maklumat klasifikasi **Terbuka sahaja**. Pihak tuan/puan boleh merujuk Garis Panduan Tadbir Urus Perkhidmatan MyGovUC melalui https://mygovuc.gov.my/uploads/content-downloads/file_20250826113205.pdf. B. **Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (*Cloud Computing*)** Penjelasan lanjut mengenai klasifikasi data yang dibenarkan untuk disimpan dalam perkhidmatan awan diperincikan dalam **Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (*Cloud Computing*) Dalam Perkhidmatan Awam Versi 2.0**. GWS dikategorikan sebagai perkhidmatan **Awan Awam (*Public Cloud*)**. Berdasarkan garis panduan ini, hanya maklumat dengan klasifikasi **Terbuka** sahaja yang dibenarkan untuk diuruskan menggunakan platform *Public Cloud*. Berikut adalah **Matrik Klasifikasi Maklumat Dalam Pelaksanaan Pengkomputeran Awan Dalam Perkhidmatan Awam** yang menerangkan model perkhidmatan Cloud dan residensi data:

Klasifikasi Maklumat	Peringkat Keselamatan	Tradisional (Pusat Data Jabatan)	MODEL CLOUD YANG DIBENARKAN			RESIDENSI DATA			
			Public	Private	Hybrid	*Onshore* (Dalam Negara) Bagi Fasiliti / Infrastruktur Utama			*Offshore* (Luar Negara) Bagi Tujuan Sandaran Data
						On-Premise (Premis Kerajaan)		Off-Premise	Premis CSP
						CSP Tempatan (termasuk MyGovCloud@PDSA)	CSP Asing (dibangunkan untuk Kerajaan	CSP Tempatan / CSP Asing	
RASMI	Data Terbuka	/	/	/	/	/	/	/	/
	Data Terkawal (Kewangan, Rekod Perubatan, Data Peribadi atau PII)	/	/	/	/	/	/	/	/**
RAHSIA RASMI	TERHAD	/	/	/	/	/	/	/*	/**
	SULIT	/	/	/	/	/	/	/*	/**
	RAHSIA	Isolate	x	X	x	x	x	x	x
	RAHSIA BESAR	Isolate	x	X	x	x	x	x	x

Berdasarkan matriks di atas, adalah jelas bahawa platform Public Cloud seperti GWS **hanya dibenarkan** untuk menyimpan dan menguruskan maklumat yang diklasifikasikan **Terbuka** sahaja kerana residensi data GWS berada di luar negara.

Sebarang maklumat terperingkat (contohnya rekod perubatan pesakit, data sensitif jabatan, atau dokumen di bawah Akta Rahsia Rasmi 1972) yang diklasifikasikan sebagai **Terhad**, **Sulit, Rahsia, atau Rahsia Besar** adalah **TIDAK DIBENARKAN SAMA SEKALI** untuk disimpan, diproses, atau dikongsi menggunakan platform GWS.

		Pihak tuan/puan boleh merujuk Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (*Cloud Computing*) menerusi https://www.cgso.gov.my/wp-content/uploads/2021/11/GARIS-PANDUAN-PENGURUSAN-KESELAMATAN-MAKLUMAT-MELALUI-PENGKOMPUTERAN-AWAN-CLOUD-COMPUTING-DALAM-PERKHIDMATAN-AWAM-VERSI-2.0.pdf Walaupun GWS menyediakan pelbagai ciri keselamatan yang terkini dengan dilengkapi dengan teknologi AI, pematuhan kepada **Arahan Keselamatan Kerajaan** adalah **mandatori**. Setiap Ketua Jabatan dan kakitangan awam adalah bertanggungjawab untuk memastikan tiada pelanggaran dasar keselamatan berlaku.
2	Adakah model pelaksanaan ini selari dengan ketetapan semasa?	Model pelaksanaan ini mempunyai beberapa aspek positif, terutamanya amalan ***data minimisation*** di mana nombor kad pengenalan (*Identity Card* (IC)) hanya digunakan sebagai kunci carian dan tidak dipaparkan semula. Walau bagaimanapun, pengumpulan dan pemprosesan nombor IC di platform **Awan Awam (*Public Cloud*)** seperti *Google Sites* menimbulkan beberapa risiko ketidakpatuhan yang signifikan. i. **Garis Panduan Tadbir Urus MyGovUC:** a) Seperti yang telah dikemaskini, garis panduan ini membenarkan **penyimpanan sementara** maklumat rahsia rasmi yang diklasifikasikan sebagai **TERHAD** dan **SULIT** melalui penggunaan fungsi keselamatan yang

		disediakan. Namun, maklumat **RAHSIA** dan **RAHSIA BESAR** adalah dilarang sama sekali. b) Walaupun output sistem (status laporan) mungkin bersifat terhad, proses input yang mengumpul nombor IC (data peribadi sensitif) boleh ditafsirkan sebagai pengendalian data **Sulit**. Ini meletakkan tanggungjawab yang berat untuk memastikan "fungsi keselamatan yang disediakan" adalah kukuh dan boleh diaudit. ii. **Akta Perlindungan Data Peribadi 2010 (Akta 709) - Dikemaskini dengan Pindaan 2024:** a) Nombor IC adalah "data peribadi sensitif". **Pindaan 2024** kepada Akta ini telah memperketatkan lagi tanggungjawab pengendalian data. b) **Pengenalan Konsep "Pemproses Data":** Pindaan ini meletakkan tanggungjawab perundangan bukan sahaja kepada "pengguna data" (MOH) tetapi juga kepada "pemproses data" (*Google* sebagai penyedia platform). Ini bermakna sebarang pelanggaran keselamatan di pihak mereka boleh memberi kesan perundangan secara langsung kepada jabatan. c) **Kewajipan Notifikasi Pelanggaran Data:** Pindaan ini memperkenalkan **kewajipan mandatori untuk melaporkan pelanggaran data peribadi** kepada Pesuruhjaya dalam tempoh 72 jam. Sekiranya berlaku kebocoran nombor IC yang dikumpul, pihak puan bertanggungjawab di bawah

		undang-undang untuk membuat laporan, di mana pengendalian data sensitif di *public cloud* meningkatkan profil risiko insiden sebegini. iii. **Akta Keselamatan Siber 2024 (Akta 854):** a) Akta ini diwujudkan untuk mengawal selia keselamatan **Infrastruktur Maklumat Kritikal Nasional (CNII)**, di mana sektor kesihatan adalah salah satu daripadanya. b) Sistem yang menguruskan data perubatan, walaupun hanya status, berpotensi dianggap sebagai sebahagian daripada aset CNII. Jika ditetapkan sedemikian, ia akan tertakluk kepada obligasi perundangan yang amat ketat di bawah seliaan **Agensi Keselamatan Siber Negara (NACSA)**. Pembangunan di platform *public cloud* mungkin tidak selari dengan kehendak akta ini yang menuntut tahap kawalan dan jaminan yang lebih tinggi. iv. **Akta Pendaftaran Negara 1959 (Akta 384):** a) Seperti yang dibincangkan sebelum ini, **Peraturan 8A, Peraturan-peraturan Pendaftaran Negara 1990**, melarang mana-mana pihak selain pegawai berkuasa untuk **meminta dan merekodkan** butiran kad pengenalan. Walaupun untuk tujuan pengesahan, tindakan mengumpul nombor IC melalui borang dalam talian di platform *public cloud* adalah berisiko tinggi dari sudut perundangan ini.

		Walaupun inovasi ini mempunyai kawalan dalaman, model pelaksanaannya di *public cloud* **tidak sepenuhnya selari** dengan ketetapan semasa kerana ia menimbulkan risiko pematuhan yang signifikan terhadap pelbagai akta dan garis panduan keselamatan.
3	Adakah perlu proses migrasi aplikasi ini ke *Private Cloud* (contoh: MyGovCloud atau *server* hospital)?	Ya, proses migrasi ke persekitaran Awan Persendirian (*Private Cloud*) seperti MyGovCloud atau pelayan hospital adalah sangat disyorkan. Migrasi akan menyelesaikan sebahagian besar isu pematuhan yang dibangkitkan seperti berikut: i. **Pematuhan dan Kawalan:** Meletakkan sistem dalam persekitaran yang dikawal sepenuhnya oleh Kerajaan, menangani risiko kedaulatan data dan memudahkan pematuhan kepada Akta 854, Akta 384, dan PDPA; ii. **Selari dengan Amalan Terbaik:** Menyeragamkan tahap keselamatan aplikasi ini dengan sistem-sistem Kerajaan kritikal lain yang memproses data sensitif; dan iii. **Mengurangkan Risiko Audit:** Mengelakkan sebarang isu audit mengenai pemprosesan data peribadi sensitif di persekitaran *public cloud*.
4	Apakah senarai kawalan minimum yang perlu dipenuhi sekiranya aplikasi ini hendak terus digunapakai?	Sekiranya aplikasi ini perlu diteruskan buat **sementara waktu sebelum migrasi penuh**, berikut adalah senarai kawalan minimum tambahan yang **wajib** dilaksanakan untuk mengurangkan risiko:

		i. **Penilaian Risiko Keselamatan Maklumat:** Menjalankan **Penilaian Risiko Keselamatan Maklumat** untuk mendokumenkan semua potensi risiko dan langkah mitigasi yang telah dan akan diambil; ii. **Kawalan Kriptografi (Penyulitan):** Pastikan nombor IC di dalam pangkalan data (contoh: *Google Sheets*) **disulitkan (*encrypted*)** sepenuhnya dan tidak disimpan dalam format teks biasa; iii. **Pengukuhan Kawalan Akses:** Pertimbangkan untuk menambah satu lapisan pengesahan kedua (cth: OTP ke nombor telefon berdaftar) untuk mengelakkan pertanyaan secara pukal (*brute-force queries*) dan memastikan hanya pemohon yang sah membuat semakan; iv. **Pemantauan Aktif:** Wujudkan mekanisme pemantauan aktif ke atas *audit trail* untuk mengesan sebarang aktiviti anomali atau mencurigakan dalam masa nyata; dan v. **Notis Privasi:** Memaparkan notis privasi yang jelas di laman carian, memaklumkan pengguna bagaimana data IC mereka akan diproses, selaras dengan kehendak PDPA. Inovasi ini amat bermanfaat untuk perkhidmatan awam, namun ia perlu dioperasikan dalam persekitaran teknologi yang betul untuk memastikan ianya kalis audit dan mematuhi sepenuhnya undang-undang perlindungan data dan keselamatan siber negara. Untuk penjelasan lanjut mengenai penggunaan *public cloud* untuk perkhidmatan awam, pihak tuan/puan boleh merujuk terus dengan Bahagian Keselamatan ICT dan Rahsia Rasmi, Pejabat

		Ketua Pegawai Keselamatan Kerajaan Malaysia dan maklumat pegawai CGSO boleh didapati melalu url https://www.cgso.gov.my/ms/hubungi-kami/direktori-pegawai-cgso/.