Residensi Data

Perspektif Kebijakan AWS

Agustus 2020

Pemberitahuan

Pelanggan bertanggung jawab untuk melakukan penilaian independen mereka terhadap informasi dalam dokumen ini. Dokumen ini: (a) adalah untuk tujuan informasi saja, (b) merupakan praktik dan penawaran produk AWS saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak memberikan komitmen atau jaminan apa pun dari AWS dan afiliasi, pemasok, atau pemberi lisensinya. Produk atau layanan AWS disediakan “sebagaimana adanya” tanpa garansi, representasi, atau kondisi apa pun, baik secara tersurat maupun tersirat. Tanggung jawab dan kewajiban AWS kepada pelanggan dikendalikan oleh perjanjian AWS, dan dokumen ini bukan bagian dari, juga tidak mengubah, perjanjian apa pun antara AWS dan pelanggannya.

Daftar Isi

Pendahuluan

Dalam lingkungan komputasi yang kompleks saat ini, organisasi sektor publik terus memiliki kekhawatiran yang logis tentang keamanan data mereka. Akibatnya, beberapa pemerintah telah menetapkan bahwa dengan mewajibkan penyimpanan data, persyaratan bahwa semua konten pelanggan yang diproses dan disimpan dalam sistem TI tetap berada dalam batas negara tertentu – yang memberikan lapisan keamanan ekstra. Residensi data mencerminkan kombinasi masalah yang terutama terkait dengan risiko keamanan yang dialami (dan dalam beberapa kasus nyata) seputar akses pihak ketiga ke data, termasuk lembaga penegak hukum asing. Pelanggan sektor publik menginginkan jaminan bahwa data mereka dilindungi dari akses yang tidak diinginkan tidak hanya dari penyerang jahat, tetapi juga dari pemerintah lain.

Posisi residensi data yang ketat terkadang membatasi penggunaan penyedia layanan cloud (CSP) multinasional berskala besar, yang sering disebut CSP "skala hiper". Masalah keamanan cyber secara umum, serta kekhawatiran tentang potensi jangkauan yang berlebihan oleh entitas yang berdaulat, telah berkontribusi pada persepsi yang berkelanjutan bahwa kelas data tertentu harus disimpan di dalam negeri. Namun, persepsi tersebut kontraproduktif dengan tujuan mengamankan data sektor publik secara efektif. Seperti yang dibahas di bawah ini, CSP berskala hiper, yang mungkin memiliki aset infrastruktur yang berlokasi di negara yang berbeda dari tempat entitas sektor publik, memberikan basis pelanggan mereka dengan kemampuan untuk mencapai perlindungan data tingkat tinggi melalui perlindungan platform mereka dan dengan alat pengunci untuk pelanggan mereka. Arsitektur yang kuat dan praktik manajemen cloud, oleh karena itu, menghilangkan kekhawatiran yang membuat pelanggan mempertimbangkan pembatasan residensi data.

Layanan cloud berskala hiper menunjukkan gangguan transformasional dalam teknologi karena tingkat efisiensi, kelincahan, dan inovasi yang tinggi untuk memberikan keamanan kelas dunia guna mendukung pelanggan mereka. CSP berskala hiper merancang, mengoperasikan, dan memelihara penawaran guna memungkinkan pelanggan di berbagai sektor (komersial, publik, teregulasi) untuk mengatasi beberapa kerentanan dan risiko keamanan yang paling umum. Pelanggan mengandalkan penawaran CSP berskala hiper untuk mewujudkan praktik keamanan yang dinamis dan responsif terhadap ancaman waktu nyata, yang secara dramatis meningkatkan postur keamanan setiap pelanggan. CSP, terutama CSP yang beroperasi dengan basis bayar-saat-pakai, memiliki semua insentif yang tepat untuk mempertahankan keamanan cyber kelas dunia karena mereka akan menghadapi konsekuensi jangka panjang yang substansial - termasuk dampak yang terkait dengan gangguan sistem, hilangnya kepercayaan pelanggan, dan rusaknya citra merek. Dengan kata lain, keamanan terbaik bersifat wajib bagi CSP berskala hiper yang sukses dan keamanan harus diintegrasikan sepenuhnya ke dalam desain, pengembangan, dan operasi layanan cloud berskala hiper.

Makalah ini mencakup hal-hal berikut:

- Menurunkan risiko keamanan yang diekspresikan oleh pemerintah ketika mereka menuntut residensi data di dalam negeri.

- Dampak negatif terhadap komersial, sektor publik, dan industri teknologi secara keseluruhan yang timbul dari kebijakan residensi data dalam negeri dengan yang diterapkan pada data pemerintah.
- Pertimbangan bagi pemerintah untuk dievaluasi sebelum memberlakukan persyaratan yang secara tidak sengaja dapat membatasi tujuan transformasi digital sektor publik yang mengarah pada peningkatan risiko keamanan cyber.

Mengapa Residensi Data Tidak Menghasilkan Keamanan yang Lebih Baik

Kepemilikan dan penempatan geografis data telah menjadi topik utama keamanan cyber dan inisiatif kebijakan cloud di seluruh dunia. Secara historis, komando dan kontrol atas data perusahaan yang sensitif berarti menampung informasi secara lokal di lokasi atau di fasilitas milik kontraktor yang dapat diakses secara fisik dalam suatu negara.

Memiliki kepemilikan penuh atas "tumpukan", mulai dari lantai dan dinding gedung hingga perangkat lunak di server, membuat orang merasa nyaman bahwa data mereka sudah sangat aman. Alasan ini masih digunakan oleh banyak pemerintahan.

Seiring perkembangan teknologi, tiga realitas mendasar telah mengganggu model "kontrol tumpukan penuh" tradisional:

1. **Yang Paling Rentan adalah yang Dieksploitasi dari Jarak Jauh.** Lokasi fisik data memiliki sedikit atau tidak ada dampak terhadap ancaman yang disebarkan melalui Internet. Sistem yang terhubung ke Internet memaparkan organisasi ke ruang ancaman yang luas, yang semuanya disebarkan dari lokasi mana pun. Misalnya, ransomware Petya baru-baru ini memengaruhi layanan perawatan kesehatan, melemahkan operasi dan kemampuan mereka untuk melakukan perawatan pasien. Ini adalah dampak dari malware yang memengaruhi pusat data lokal yang tersebar melalui Internet. Meskipun ada banyak upaya untuk mengamankan sistem yang saling terhubung melalui firewall dan perangkat antiintrusi lainnya, pengalaman menunjukkan bahwa keamanan perimeter adalah bagian yang sangat kecil dari sistem yang dilindungi. Terlepas dari lokasi fisiknya, jika sistem TI terhubung dengan cara apa pun ke Internet (atau jaringan multipihak lainnya), bahkan secara tidak langsung, sistem tersebut berisiko dan rentan terhadap berbagai ancaman akses logis.

> Terlepas dari lokasi fisiknya, jika sistem TI terhubung dengan cara apa pun ke Internet (atau jaringan multipihak lainnya), bahkan secara tidak langsung, sistem tersebut memiliki risiko yang cukup besar.

2. **Proses Manual Menimbulkan Risiko Kesalahan Manusia.** Kegagalan proses manusia berperan dalam akar penyebab kegagalan (jika bukan seluruh penyebab) dari sebagian besar peristiwa keamanan cyber. Contoh umumnya adalah kegagalan untuk melakukan pacth pada sistem yang rentan dengan pembaruan perangkat lunak yang dipublikasikan selama beberapa bulan sebelum eksploitasi. Proses manual memperbarui sistem dengan patch terbaru akan sulit dan tidak dapat dilakukan secara teratur tanpa otomatisasi.
3. **Ancaman Orang Dalam Dianggap sebagai Risiko yang Signifikan.** Sebagian besar peretasan data besar telah terjadi baik melalui kesalahan yang tidak disengaja atau perilaku jahat yang disengaja oleh individu yang menggunakan akun resmi untuk melakukan eksploitasi data. Pembobolan tingkat tinggi dalam beberapa tahun terakhir sebagian besar dikaitkan dengan praktik kebersihan dunia maya yang buruk. Skenario ancaman akun resmi yang paling umum meliputi:

- Tidak disengaja: kredensial yang hilang atau salah kelola sehingga penyerang dapat bertindak di dalam sistem sebagai pengguna yang valid.
- Rekayasa sosial: serangan phishing dan serangan rekayasa sosial yang menipu pengguna atau administrator agar mengungkapkan kredensial kepada penyerang.
- Berbahaya: ancaman orang dalam yang klasik – aktor jahat dalam organisasi dengan niat jahat.

Lokasi fisik data tidak ada hubungannya dengan realitas-realitas yang tercantum di atas.

Dalam kondisi saat ini, manajemen risiko adalah tugas yang sangat berat ketika mempertimbangkan teknologi seluler dan keterkaitan antara entitas eksternal dan internal. Arsitektur sistem apa pun yang tidak memiliki perlindungan keamanan yang sesuai menimbulkan vektor serangan yang kredibel, tanpa memerhatikan lokasi fisik infrastruktur atau sistem. Karena teknologi terus berkembang serta mengubah kerentanan dan vektor ancaman pelanggan, pemerintah harus mengevaluasi ulang cara mereka memodelkan strategi dan toleransi risiko mereka. Contoh dunia nyata telah menunjukkan bahwa menyimpan data di server, pusat data, dan negara Anda sendiri, bukanlah dasar yang memadai untuk mengamankan data.

Misalnya, pembobolan tingkat tinggi terhadap lembaga pemerintah AS yang memengaruhi lebih dari 20 juta karyawan federal terjadi di lingkungan lokal sebagai akibat dari kredensial pengguna yang disusupi. Kredensial ini disusupi dan digunakan melalui kabel dari berbagai lokasi - menerobos semua perlindungan yang ditawarkan lingkungan lokal. Pembobolan lembaga pemerintah AS adalah contoh bagus mengenai ancaman yang berasal dari Internet tanpa memerhatikan lokasi data atau batas geografis.

Masalah ini berlaku untuk lebih dari sekadar sistem yang terhubung ke Internet. Sistem yang tidak memiliki koneksi langsung ke Internet memberi pengguna akses melalui koneksi Jaringan Pribadi Virtual (VPN) dari laptop, komputer rumah, atau perangkat seluler. Pembobolan tidak memerlukan akses fisik ke server tetapi mengeksploitasi kurangnya kontrol keamanan logika yang diterapkan secara efektif. Hal ini menunjukkan bahwa persyaratan residensi data memiliki sedikit relevansi untuk melindungi

informasi dari ancaman yang paling umum saat ini. Oleh karena itu, persyaratan lokasi geografis memiliki sedikit relevansi untuk melindungi informasi dari ancaman yang ada saat ini. Sebaliknya, mekanisme terbaik untuk melindungi, mendeteksi, merespons, dan memulihkan adalah dengan menggunakan keamanan transformasional yang ditawarkan CSP berskala hiper melalui modernisasi dan otomatisasi. CSP berskala hiper, seperti AWS, berinvestasi dan mencerminkan praktik terbaik keamanan teknis dan operasional karena ini adalah inti dari operasi dan penawaran mereka. Pelanggan mendapatkan keuntungan saat mereka memanfaatkan CSP seperti penawaran cloud dan infrastruktur AWS.

Gartner[1] dan IDC[2], dua organisasi riset TI terkemuka, menyimpulkan bahwa postur keamanan CSP utama sama dengan atau lebih baik dari pusat data perusahaan terbaik dan bahwa keamanan tidak lagi dianggap sebagai penghambat utama dalam adopsi layanan cloud. Faktanya, perusahaan benar-benar mendapatkan manfaat dari keamanan bawaan di cloud.

Mengapa Cloud Tidak Memengaruhi Risiko Akses Paksa

Bagi beberapa pemerintah, persyaratan residensi data dimaksudkan untuk mengurangi risiko yang terkait dengan akses entitas lain ke datanya. Bagian ini bertujuan untuk mengatasi risiko yang timbul dari kemampuan entitas untuk "memaksa akses" ke data entitas berwenang ketika data tersebut disimpan dalam lingkungan CSP berskala hiper. Konsep “pengungkapan paksa” atau “akses paksa” mengacu pada hak akses data oleh pemerintah atau departemennya berdasarkan hukum dan peraturan di tingkat nasional, provinsi, dan daerah di negara apa pun. Kekhawatiran yang dirasakan adalah bahwa pengungkapan paksa itu berpotensi membuat pemilik data tidak memiliki kemampuan untuk mencegah akses ke datanya oleh entitas berwenang yang bermaksud menerapkan hukum yang berlaku. Namun, akses resmi ke data oleh negara yang berwenang bukanlah masalah spesifik cloud.

Memiliki sistem fisik, baik secara langsung atau melalui kontrak yang dialihdayakan, tidak mengurangi risiko akses paksa karena sudah ada mekanisme hukum lain yang memberi sarana kepada pemerintah di suatu wilayah hukum untuk meminta akses ke data yang disimpan di wilayah hukum lain. Misalnya, Perjanjian Bantuan Hukum Bersama (MLAT)[3] dan Letters Rogatory[4] telah ditetapkan untuk mengatur permintaan data negara yang berwenang jauh sebelum munculnya teknologi cloud.

Dibandingkan dengan lingkungan lokal tradisional, penegakan hukum umumnya harus mengatasi lebih banyak hambatan saat mencoba memaksa CSP untuk mengungkapkan data pelanggan lain. Penegak hukum tidak dapat mencari atau menyita data yang disimpan di server CSP tanpa mematuhi kerangka kerja hukum yang mendukung serangkaian tujuan penegakan hukum yang ditargetkan secara sempit. Lebih lanjut, CSP dapat menolak permintaan yang berlebihan, melebihi otoritas pemohon, atau tidak sepenuhnya mematuhi hukum yang berlaku.

Lebih penting lagi, CSP seperti AWS berkomitmen penuh untuk memberikan pemberitahuan permintaan data kepada pelanggan yang terkait, memungkinkan pelanggan untuk terlibat dengan otoritas dan/atau mengambil tindakan lebih lanjut yang sesuai untuk mencegah pengungkapan datanya yang tidak tepat. Penting untuk disadari bahwa tantangan kompleks ini tidak hanya terjadi pada pemerintah AS atau perusahaan yang berbasis di AS, karena setiap perusahaan multinasional tunduk pada undang-undang dan peraturan yang berlaku di tingkat nasional, provinsi, dan daerah di negara tertentu, terlepas dari lokasi datanya.

Akses Paksa Terbatas

Sejak abad ke-20, banyak negara telah memiliki mekanisme hukum untuk memungkinkan akses ke informasi yang disimpan di luar negeri sebagai tanggapan atas permintaan yang sah atas informasi yang berkaitan dengan penyelidikan dan tuntutan kriminal. Misalnya, perusahaan yang berbisnis di Negara X dapat tunduk pada permintaan hukum atas informasi meskipun konten tersebut disimpan di Negara Y di bawah kerangka kerja hukum bilateral dan multilateral yang telah ditetapkan. Dalam banyak kasus, mekanisme hukum yang diakui adalah Perjanjian Bantuan Hukum Bersama (MLAT).

Selain MLAT negara bilateral, ada juga MLAT regional utama seperti MLAT Antar-Amerika, MLAT UE-AS, dan MLAT ASEAN. Jika MLAT tidak ada, negara dapat memperoleh Letter Rogatory untuk meminta bantuan dari pemerintah asing. Setiap undang-undang wilayah hukum akan berisi kriteria yang harus dipenuhi agar badan penegak hukum yang relevan dapat membuat permintaan yang sah. Misalnya, lembaga pemerintah yang meminta akses mungkin perlu mendapatkan perintah pengadilan atau surat perintah yang menunjukkan bahwa ia memiliki alasan yang sah untuk meminta akses ke konten tersebut. Meskipun mekanismenya sah, instrumen hukum ini tidak dimaksudkan untuk menangani akses penegakan hukum ke data di dunia digital.

> Undang-undang yang mengatur akses ke data yang disimpan di luar negeri oleh lembaga penegak hukum untuk mendukung penyelidikan kejahatan berat, seperti terorisme, tidak dibuat dengan mempertimbangkan teknologi modern. Hal ini mengakibatkan kasus di mana perusahaan teknologi yang mematuhi perintah pengadilan berdasarkan undang-undang suatu negara juga menghadapi risiko melanggar undang-undang negara lain yang melarang pengungkapan.

> Undang-undang CLOUD memberikan kerangka kerja baru untuk menantang permintaan penegakan hukum ketika ada perjanjian eksekutif yang diberlakukan antara AS dan negara lain, dan juga menegaskan, berdasarkan prinsip saling menghormati antarnegara, hak penyedia layanan untuk menolak pengungkapan data apa pun jika pelaksanaan hal itu akan bertentangan dengan hukum negara lain, bahkan jika tidak ada perjanjian eksekutif. Ini juga memungkinkan penyedia layanan cloud untuk mengungkapkan data kepada pemerintah yang mengeluarkan perintah atau surat perintah permintaan informasi berdasarkan fakta yang cukup yang menunjukkan kemungkinan penyebab kejahatan serius telah terjadi dan bahwa informasi yang dicari terkait langsung dengan kejahatan tersebut.

Dalam upaya untuk menyelaraskan hukum asinkron dengan teknologi modern, AS mengeluarkan Undang-Undang Klarifikasi Penggunaan Data Luar Negeri yang Sah (CLOUD) pada bulan Maret 2018. UU CLOUD menyediakan mekanisme hukum internasional ketiga untuk memperoleh data yang disimpan di luar negeri melalui permintaan langsung yang dikeluarkan untuk penyedia layanan.[5] UU CLOUD menetapkan prosedur bagi AS untuk mengadakan Perjanjian Eksekutif dengan negara lain. Perjanjian Eksekutif ini berupaya menghapus batasan hukum atas kemampuan negara asing tertentu untuk mencari data langsung dari penyedia layanan di AS, asalkan AS telah menetapkan bahwa undang-undang negara asing tersebut secara memadai melindungi privasi dan kebebasan sipil. Di bawah UU CLOUD, CSP memiliki hak untuk menolak pengungkapan informasi jika hal itu bertentangan dengan hukum negara lain. MLAT, Letters Rogatory, dan Perjanjian Eksekutif di bawah UU CLOUD semuanya menyediakan mekanisme hukum internasional timbal balik untuk akses penegakan hukum ke data yang disimpan di luar negeri.

Undang-undang nasional suatu negara umumnya berlaku untuk semua perusahaan yang beroperasi di negara tersebut, terlepas dari di mana perusahaan tersebut didirikan atau apakah informasi tersebut disimpan di cloud, pusat data di tempat, atau dalam rekaman fisik. Ketika negara-negara terus mendigitalkan dan maju menuju masyarakat berbasis informasi modern, aturan akses yang diwajibkan secara hukum untuk mendukung penyelidikan atas kejahatan tinggi yang berdampak pada keamanan nasional, seperti terorisme, juga telah berkembang. Pemberlakuan UU CLOUD merupakan kerangka kerja lain yang bertujuan guna memperkuat proses hukum untuk permintaan penegakan hukum dalam konteks modern ini.

> Membatasi CSP ke satu wilayah hukum tidak lebih baik melindungi data dari akses pemerintah

> Suatu analisis hukum independen di seluruh pengguna cloud awal di pemerintahan menilai undang-undang khusus negara yang mengatur akses penegakan hukum ke data berbasis cloud yang disimpan di luar negeri. Studi ini mengevaluasi sepuluh wilayah hukum internasional- Australia, Kanada, Denmark, Prancis, Jerman, Irlandia, Jepang, Spanyol, Inggris, dan AS - dan menemukan bahwa membatasi CSP ke satu wilayah hukum tidak lebih baik melindungi data dari akses oleh pemerintah.

Kenyataannya adalah bahwa akses paksa tersebut terjadi dalam jumlah kasus yang sangat terbatas, dan umumnya hanya jika terdapat kebutuhan informasi yang ekstrem (misalnya, untuk mencegah peristiwa terkait teror). Untuk mengurangi risiko rendah ini, organisasi dapat mempraktikkan uji tuntas dan membuat perlindungannya sendiri dengan layanan cloud yang tersedia. Di AWS, mitigasi seperti enkripsi data saat diam dan saat transit, dekomposisi dan distribusi data, serta strategi tokenisasi dapat digunakan untuk sebagian kecil dari beban sumber daya dibandingkan solusi di lokasi.

AWS sangat waspada dalam melindungi konten pelanggan kami, terlepas dari asal permintaan konten atau pelanggannya. AWS tidak akan mengungkapkan konten pelanggan kecuali diharuskan melakukannya untuk mematuhi perintah yang sah dan mengikat secara hukum, seperti panggilan pengadilan atau perintah pengadilan. AWS dengan cermat memeriksa setiap permintaan untuk mengautentikasi keakuratannya dan memverifikasi bahwa permintaan tersebut sudah mematuhi hukum yang berlaku. AWS akan menolak permintaan yang berlebihan, melebihi otoritas pemohon, atau tidak sepenuhnya mematuhi hukum yang berlaku. Kecuali dilarang oleh hukum, AWS juga berupaya mengarahkan kembali permintaan secara langsung ke pelanggan, memberikan pelanggan kesempatan untuk mengambil tindakan terhadap permintaan tersebut. Informasi tambahan dapat ditemukan dalam laporan transparansi terbaru kami dan Pedoman Penegakan Hukum Amazon kami.[6]

Mengapa Risiko Akses yang Tidak Sah Ternyata Lebih Rendah di Cloud

Bagi beberapa pemerintah, persyaratan residensi data dimaksudkan untuk mengurangi risiko yang terkait dengan akses entitas lain ke datanya. Bagian ini bertujuan untuk mengatasi persepsi peningkatan risiko akses tidak sah saat menggunakan CSP berskala hiper. Akses tidak sah adalah ancaman yang lebih umum yang diupayakan oleh musuh yang mencoba mendapatkan akses ke data pelanggan dengan menggunakan berbagai cara. Akses tidak sah dapat mencakup masalah akses pihak ketiga, termasuk kemungkinan ancaman orang dalam atau aktor jahat dari luar.

Persyaratan residensi data gagal mengatasi jalan umum yang digunakan penyerang untuk mendapatkan akses. Memanfaatkan vektor ini hampir selalu merupakan hasil dari kegagalan dalam disiplin ilmu kebersihan cyber dasar, seperti manajemen inventaris sistem, manajemen konfigurasi, enkripsi data, dan manajemen akses hak istimewa.

Memitigasi Akses Tidak Sah

Mencegah akses tidak sah membutuhkan praktik kebersihan keamanan yang tepat serta menerapkan kemampuan pencegahan dan deteksi yang kuat. Misalnya, sistem harus dirancang untuk membatasi "radius ledakan" dari setiap intrusi sehingga satu node yang terganggu memiliki dampak minimal pada node lain di perusahaan. CSP berskala hiper, seperti AWS, menyediakan lingkungan sarana keamanan penuh untuk memungkinkan pelanggan mempertahankan komunikasi terenkripsi dan menerapkan perlindungan gangguan guna mengurangi risiko akses yang tidak sah. AWS tidak memiliki visibilitas ke, atau pengetahuan tentang, konten akun pelanggan, termasuk apakah konten tersebut menyertakan informasi pribadi atau tidak. Pelanggan AWS diberdayakan untuk menggunakan berbagai teknik seperti enkripsi,[7] tokenisasi, dekomposisi data, dan penipuan cyber untuk membuat konten tidak dapat dipahami oleh AWS atau pihak lain yang mengupayakan akses ke kontennya.

- Enkripsi - Mengenkripsi data secara benar dapat membuat data tidak dapat dibaca. Artinya, menyimpan data terenkripsi di cloud, terlepas dari lokasinya, dapat memberikan perlindungan yang memadai terhadap sebagian besar ancaman eksfiltrasi. Kunci enkripsi data harus dikelola dengan hati-hati untuk memastikan tetap ada perlindungan yang kuat terhadap pihak yang menyadap. AWS menyediakan layanan yang dapat memberikan kemampuan ini di tingkat perusahaan dengan AWS CloudHSM atau AWS Key Management Service (KMS).[8] Jumlah kontrol yang ingin dimiliki pelanggan atas metode enkripsi, penyimpanan kunci kriptografi, dan manajemen kunci kriptografi yang digunakan dengan data mereka ditentukan sesuai keinginan pelanggan.[9]

- Tokenisasi – Tokenisasi adalah proses yang memungkinkan Anda menentukan urutan data untuk mewakili bagian informasi sensitif (misalnya, token untuk mewakili nomor kartu kredit pelanggan). Token tidak ada artinya jika digunakan sendirian dan tidak dapat dipetakan kembali ke data yang diwakilinya tanpa menggunakan sistem tokenisasi. Penyimpanan token dapat dibangun di VPC untuk menyimpan informasi sensitif dalam bentuk terenkripsi sembari membagikan token ke layanan yang disetujui untuk mengirimkan data yang dikaburkan. Selain itu, AWS memiliki sejumlah mitra yang berspesialisasi dalam menyediakan layanan tokenisasi yang terintegrasi dengan database populer dan layanan penyimpanan lainnya.

- Dekomposisi Data – Ini adalah proses yang mengurangi kumpulan data menjadi elemen yang tidak dapat dikenali yang tidak memiliki makna tersendiri.[10] Elemen atau fragmen ini kemudian disimpan dalam mode terdistribusi sehingga setiap gangguan dalam satu node hanya akan menghasilkan fragmen data yang tidak signifikan. Keuntungan khusus dari teknik ini adalah mengharuskan pelaku ancaman untuk mengganggu semua node, mendapatkan semua fragmen, dan mengetahui algoritme (atau skema fragmentasi) guna mengumpulkan data dengan cara yang koheren.

- Pertahanan terhadap Penipuan Cyber – Arsitektur dan solusi penipuan cyber dapat menjadi komponen kunci untuk memitigasi musuh yang canggih. Solusi penipuan dapat menggunakan jebakan dan umpan yang sangat mutakhir untuk membuat penyerang mengira bahwa mereka telah menyusup ke sistem, padahal sesungguhnya, ia dialihkan ke lingkungan yang sangat terkontrol. Informasi tentang penyerang dikumpulkan untuk mengurangi ancaman di masa depan dan serangan itu dinetralkan.

Pelanggan juga khawatir tentang kelayakan langkah-langkah kontrol akses untuk mencegah akses yang tidak sah oleh personel CSP. Tugas dan bidang tanggung jawab (misalnya, permintaan dan persetujuan akses, permintaan dan persetujuan manajemen perubahan, dsb.) harus dipisahkan di antara berbagai individu untuk mengurangi peluang modifikasi yang tidak sah atau tidak disengaja maupun penyalahgunaan sistem AWS. Personel AWS dengan kebutuhan bisnis untuk mengakses bidang manajemen diharuskan untuk terlebih dahulu menggunakan autentikasi multifaktor, yang berbeda dari kredensial Amazon perusahaan normal, untuk mendapatkan akses ke host administratif yang dibuat khusus. Host administratif ini adalah sistem yang dirancang, dibangun, dikonfigurasi, dan diperkuat secara khusus untuk melindungi bidang manajemen. Semua akses tersebut dicatat dan diaudit. Ketika seorang karyawan tidak lagi memiliki kebutuhan bisnis untuk mengakses bidang manajemen, hak istimewa dan akses ke host ini dan sistem yang relevan akan dicabut. AWS telah menerapkan kebijakan penguncian sesi yang diberlakukan secara sistematis. Kunci sesi disimpan hingga prosedur identifikasi dan autentikasi yang ditetapkan telah dilakukan.

AWS juga memantau manajemen jarak jauh yang tidak sah dan dengan cepat memutuskan atau menonaktifkan akses jarak jauh yang tidak sah setelah terdeteksi. Semua upaya akses administratif jarak jauh dicatat, dan log ditinjau, tidak hanya oleh manusia untuk aktivitas yang mencurigakan, tetapi juga oleh sistem pembelajaran mesin otomatis yang dibuat oleh tim keamanan AWS untuk mendeteksi pola akses tidak biasa yang mungkin menunjukkan upaya tidak sah untuk mengakses data. Jika aktivitas mencurigakan terdeteksi, prosedur respons insiden dimulai. Selanjutnya, AWS telah menetapkan kebijakan dan prosedur formal untuk menggambarkan standar akses logis ke infrastruktur dan host AWS. Kebijakan juga mengidentifikasi tanggung jawab fungsional untuk administrasi keamanan dan akses logis. Kecuali dilarang oleh hukum, AWS mengharuskan semua karyawan menjalani penyelidikan latar belakang yang sesuai dengan posisi dan tingkat akses mereka.

Terakhir, instans virtual pelanggan hanya dikontrol oleh pelanggan yang memiliki akses root penuh atau kontrol administratif atas akun, layanan, dan aplikasi. Personel AWS tidak memiliki kemampuan untuk masuk ke mesin virtual pelanggan.

Cloud Berskala Hiper: Suatu Pendekatan Transformasi terhadap Keamanan

CSP berskala hiper terkemuka, seperti AWS, menawarkan kepada pelanggan peluang untuk membangun keamanan adaptif dan sangat tangguh untuk beban kerja mereka. Membatasi operasi untuk persyaratan

di negara tertentu akan menghambat inovasi layanan dan kemampuan untuk mengimbangi ancaman, seperti yang menargetkan ketersediaan. Produk sampingan merugikan lainnya dari kendala geografis dalam negeri adalah bahwa pelaku ancaman dapat memperoleh keakuratan penargetan dengan mengetahui bahwa data harus berada dalam wilayah tertentu. CSP berskala hiper memiliki penawaran dan arsitektur pendukung yang tersedia untuk menawarkan kemampuan pertahanan mendalam[11] dan pertahanan secara luas[12]. Hal ini disebabkan mekanisme keamanan menjadi intrinsik dalam desain dan pengoperasian penawaran CSP berskala hiper.

> Produk sampingan yang tidak diinginkan dari persyaratan residensi data dalam negara adalah bahwa pelaku ancaman dapat memperoleh akurasi yang lebih baik dalam sistem penargetan dengan mengetahui data tersebut berada di lokasi tertentu.

Enam item berikut mencerminkan atribut keamanan inti yang merupakan bagian integral dari CSP berskala hiper seperti AWS:

1. Integrasi keamanan dan kepatuhan yang mendalam (jarang dicapai dalam sistem tradisional) berarti bahwa keamanan secara langsung mendapat manfaat dari kepatuhan karena kontrol keamanan terus dipantau dan diperbarui.
2. Skala ekonomi berlaku tidak hanya untuk teknologi, tetapi juga personel dan proses keamanan, yang menghasilkan laba atas investasi yang belum pernah terjadi sebelumnya dibandingkan dengan sistem tradisional.
3. CSP mengambil bagian utama dari "area permukaan" keamanan, yang dijalankan dengan fokus dan keterampilan profesional melebihi hampir semua pelanggan di bumi. Sehingga pelanggan dapat memfokuskan kembali sumber daya dan profesional keamanan mereka pada bagian tantangan yang jauh lebih kecil seperti keamanan aplikasi.
4. Cloud memberikan visibilitas, homogenitas, dan otomatisasi yang belum pernah ada sebelumnya dalam sistem tradisional, yang semuanya menguntungkan keamanan secara masif. Ini mencakup kemampuan audit dan pembuatan log yang sangat dalam yang, misalnya, dapat merekam panggilan API dengan membuat log aktivitas CSP yang dapat memengaruhi akun pelanggan.
5. CSP beroperasi sebagai semacam "kontainer sistem" yang memberikan lebih banyak wawasan tentang perilaku dan fungsi sistem, termasuk operasi keamanan, memberikan lapisan baru "pertahanan mendalam" kepada pelanggan.
6. Dengan akses yang mudah dan murah ke penyimpanan dan kapasitas pemrosesan dalam jumlah besar, pelanggan AWS "menggunakan cloud untuk mengamankan cloud", artinya, mereka menjalankan analisis mahadata pada data keamanan dan data log, yang memberikan lebih banyak wawasan tentang postur dan hasil keamanan dalam remediasi masalah yang jauh lebih cepat.

Dengan kecepatan inovasi dan peningkatan skala, kisah keamanan cloud akan menjadi lebih baik. Misalnya, hanya dalam setahun terakhir AWS menambahkan kemampuan keamanan yang kuat seperti Amazon GuardDuty[13], penawaran deteksi ancaman terkelola yang terus memantau perilaku jahat atau tidak sah; Amazon Macie[14], penawaran yang menggunakan pembelajaran mesin untuk melindungi data sensitif; dan AWS CloudHSM 2.0[15], penawaran terkelola sepenuhnya yang menggunakan perangkat keras tervalidasi FIPS 140-2 Tingkat 3[16] yang secara otomatis diterapkan dalam klaster zona multiketersediaan yang sangat tersedia dan redundan yang memungkinkan pelanggan untuk dengan mudah menghasilkan, mengelola, dan menggunakan kunci enkripsi sendiri di AWS Cloud sembari memberikan AWS nol akses ke kunci master atau operasi enkripsi inti.

Enkripsi harus dianggap sebagai layanan inti karena dapat bertindak sebagai sarana untuk melindungi data jika kemampuan lain gagal. Enkripsi menambahkan lapisan keamanan dan jaminan kerahasiaan dan integritas data tambahan saat transit dan saat tidak digunakan. Perpaduan AWS Key Management Service (KMS) dan AWS CloudHSM adalah inti dari solusi enkripsi yang ketat.[17] CSP berskala hiper seperti AWS menawarkan enkripsi di mana-mana yang mungkin tidak terjangkau oleh operasi di lokasi. Misalnya, AWS Key Management Service (KMS), validasi FIPS 140-2 Tingkat 2, menawarkan opsi Bawa Kunci Milik Anda (BYOK) yang memungkinkan pelanggan untuk menggunakan materi kunci yang dibuat dan disimpan secara lokal pada layanan AWS. Pelanggan dapat memenuhi persyaratan keamanan dan kepatuhan tertentu seputar beban kerja yang sangat sensitif dengan kemampuan ini karena mereka dapat menyimpan dan mengelola materi utama mereka di luar AWS.

Tanggung Jawab CSP: Keamanan Bawaan di Cloud

Infrastruktur AWS dibuat khusus untuk cloud, dengan semua elemen yang dirancang untuk berkomunikasi dengan baik dan menyajikan permukaan serangan sekecil mungkin. Selain itu, kontrol keamanan fisik yang ada di pusat data kami telah dirancang untuk menjadi yang paling ketat di dunia. Arsitektur AWS telah ditinjau dan divalidasi terhadap lusinan kerangka kerja kepatuhan internasional.[18] Kami menggunakan penilai dan auditor pihak ketiga independen untuk mengevaluasi dan membuktikan kepatuhan kami terhadap metode ini, serta memberi akses ke laporan yang dihasilkan dan bukti pendukung kepada pelanggan. Untuk memenuhi berbagai macam persyaratan keamanan, AWS membangun pusat data dan arsitekturnya guna menyesuaikan skala dan maju dengan laju inovasi. Pendekatan ini telah membuat AWS dipercaya oleh pemerintah, organisasi militer, bank global, lembaga perawatan kesehatan, dan organisasi dengan sensitivitas tinggi lainnya.

Di AWS, lingkungan unik kami telah menjadi pendorong untuk membangun banyak alat keamanan kami. Alat-alat ini mengotomatiskan banyak tugas rutin yang memungkinkan pakar keamanan kami untuk fokus kepada aspek penting yaitu pengamanan lingkungan. Alat-alat kami menghasilkan persyaratan keamanan yang tertanam dan dipatuhi selama siklus pengembangan sistem. Masalah keamanan yang umum diatasi dalam fase awal pengembangan sistem yang memungkinkan pakar keamanan kami berfokus pada mitigasi ancaman lanjutan dan kompleks di tingkat produksi.

Tim keamanan kami memantau infrastruktur sepanjang hari dan setiap hari, serta terhubung dengan baik ke semua tim pengawas keamanan utama dan vendor guna mengidentifikasi potensi ancaman dengan cepat. Mereka melakukan ini dalam skala besar, yang menjadi pembeda organisasi keamanan AWS. Dengan menggunakan algoritme kompleks untuk memindai jutaan akun pelanggan aktif yang menjalankan hampir semua jenis beban kerja yang dapat dibayangkan, kami dapat melihat masalah yang mungkin hanya terjadi sekali dalam satu miliar operasi beberapa kali sehari. Saat memulihkan masalah, kami melakukannya untuk seluruh platform. Visibilitas dan respons semacam itu tidak dapat dicapai oleh kebanyakan organisasi yang menjalankan pusat data di lokasi. Nilai-nilai yang berasal dari keahlian terfokus dan dalam skala masif menjelaskan alasan Gartner dan IDC menentukan bahwa beban kerja infrastruktur sebagai layanan (IaaS) cloud publik akan mengalami insiden keamanan yang lebih sedikit daripada yang ada di pusat data tradisional. Penelitian Gartner memperkirakan setidaknya terdapat 60% pengurangan insiden keamanan.[19]

Opsi lokal tambahan untuk kebutuhan pelokalan

Adopsi cloud adalah perjalanan multitahap yang terdiri dari migrasi bertahap, yang sering kali tercermin dalam pendekatan cloud hibrida (yaitu, beban kerja yang didistribusikan di lingkungan cloud lokal dan komersial). Untuk berbagai alasan, pelanggan mungkin menemukan bahwa beban kerja tertentu lebih sesuai untuk manajemen di lokasi - baik untuk latensi yang lebih rendah atau kebutuhan pemrosesan lokal lainnya.

AWS terus berinovasi untuk memberi kontrol dan fleksibilitas tambahan saat pelanggan menerapkan pendekatan migrasi cloud. Misalnya, solusi hibrida seperti AWS Outposts[20], menyediakan opsi yang menghadirkan layanan cloud AWS ke pusat data pelanggan, meningkatkan fleksibilitas untuk memilih di mana aplikasi cloud, termasuk beban kerja sensitif, diterapkan.

Hingga AWS meluncurkan Outposts, pelanggan harus beroperasi di wilayah AWS terdekat untuk menyimpan data lebih dekat. Dengan memperluas infrastruktur dan layanan AWS ke lingkungan mereka, pelanggan dapat mendukung beban kerja yang perlu agar tetap berada di lokasi sambil memanfaatkan kemampuan keamanan dan operasional layanan cloud komersial.

Outposts akan terhubung ke infrastruktur AWS di wilayah pilihan pelanggan untuk bertukar data yang digunakan dalam menyediakan, meningkatkan, dan mengamankan layanan. Pelanggan dapat memilih untuk menyimpan konten di tempat di layanan penyimpanan penduduk Outpost, seperti EBS. Pelanggan juga dapat memilih untuk mengirim konten kembali ke wilayah tersebut demi ketersediaan dan daya tahan, biasanya dalam bentuk terenkripsi, misalnya snapshot EBS, cadangan RDS, dll.

AWS mendorong pelanggan untuk menilai pendekatan klasifikasi data mereka dan mempertajam data mana yang perlu tetap berada di dalam negara atau wilayah mereka, dan mengapa. Dengan demikian, pelanggan dapat menemukan bahwa data mereka, bahkan data yang berpotensi sensitif dan penting, dapat disimpan dan/atau direplikasi di tempat lain jika tidak ada persyaratan geografis hukum atau kebijakan tertentu. Hal ini nantinya dapat mengurangi risiko kerugian jika terjadi bencana dan memberikan akses pada teknologi dan kemampuan yang mungkin tidak tersedia di wilayah mereka.

Tanggung Jawab Pelanggan: Pendekatan Arsitektur yang Aman

Kemampuan keamanan yang asli dari penyedia cloud berskala hiper seperti AWS memberdayakan pelanggan untuk membuat arsitektur unik guna mengurangi risiko akses. Fasilitas on-premise dan fasilitas serupa tidak memiliki homogenitas, skala ekonomis, visibilitas, dan otomatisasi yang dapat membawa kemajuan keamanan yang besar. Kemajuan ini diperlukan untuk membangun sistem yang sangat aman yang dapat melawan ancaman yang berkembang baik secara eksternal maupun internal. Fasilitas on-premise kesulitan menerapkan konsep operasi baru ini karena kebutuhan sumber daya untuk memfaktor ulang jaringan dan pengadaan sistem baru, serta tenaga manusia yang diperlukan karena kurangnya infrastruktur yang ditentukan perangkat lunak. CSP berskala hiper membangun tingkat kecerdasan dan kemampuan beradaptasi ke dalam infrastruktur mereka untuk menerapkan kemajuan keamanan ini secara organik. Ini berarti bahwa pelanggan dapat menggunakan kemajuan baru dengan lebih mudah karena terintegrasi secara asli ke dalam penawaran CSP, yang memungkinkan pelanggan untuk membuat sistem menggunakan arsitektur unik seperti mikro-segmentasi, desain polimorfik[21], dan jaringan penipuan multitingkat.

Misalnya, dengan melihat lebih dekat desain berbasis segmentasi mikro di AWS, pelanggan dapat menggunakan beragam teknologi termasuk Amazon Virtual Private Cloud (Amazon VPC), AWS Identity and Access Management (IAM), Grup Keamanan, Daftar Kontrol Akses Jaringan, berbagai layanan enkripsi dan pembuatan log, serta AWS Certificate Manager untuk membentuk dasar guna membangun jaringan Zero Trust Model[22] (ZTM). Secara konsep, ZTM dapat memberikan keuntungan yang berbeda untuk mitigasi ancaman dan pemantauan performa. Organisasi memiliki kebutuhan yang jelas untuk menerapkan ZTM atau desain segmentasi keamanan serupa guna melawan ancaman saat ini, tetapi sangat sulit dan mahal untuk membangun jenis arsitektur ini di lingkungan perusahaan tradisional. Perpindahan ke penyedia cloud publik memberi organisasi kesempatan untuk menerapkan ZTM dan konsep serupa tanpa biaya yang signifikan dan beban sumber daya yang terkait dengan retrofit/build jaringan fisik.

Peran-peran untuk Perlindungan Data

Ada lima konsep dasar penting mengenai kepemilikan dan manajemen data dalam model tanggung jawab bersama:

1. Pelanggan tetap memiliki datanya.
2. Pelanggan memilih lokasi geografis untuk menyimpan data mereka — data tidak berpindah kecuali pelanggan memutuskan untuk memindahkannya.
3. Pelanggan dapat mengunduh atau menghapus datanya kapan pun mereka inginkan.

4. Pelanggan dapat "menghapus secara kripto" data mereka dengan menghapus kunci enkripsi utama yang diperlukan untuk mendekripsi kunci data, yang nantinya diperlukan untuk mendekripsi data.
5. Pelanggan harus mempertimbangkan sensitivitas data mereka dan memutuskan apakah dan bagaimana mengenkripsi data saat transit dan saat tidak digunakan.

Langkah perlindungan data paling efektif diterapkan setelah menentukan peran penanganan data untuk menentukan peran dan tanggung jawab pemangku kepentingan yang sesuai. Kebanyakan skema perlindungan data membedakan antara pengontrol data (juga disebut sebagai "pengguna") dan pemroses data serta kewajiban retribusi berdasarkan peran yang berbeda tersebut. Misalnya, di bawah Peraturan Perlindungan Data Umum UE, pengontrol data bertanggung jawab untuk menerapkan langkah-langkah teknis dan organisasi yang sesuai guna melindungi data dari kerusakan yang tidak disengaja atau melanggar hukum atau kehilangan yang tidak disengaja, perubahan, pengungkapan yang tidak sah, atau akses. Jika pemrosesan dilakukan oleh pemroses data atas nama pengontrol data, pengontrol data juga bertanggung jawab untuk memilih pemroses yang menyediakan langkah-langkah teknis dan organisasi yang memadai yang mengatur pemrosesan yang akan dilakukan. Perbedaan ini membantu menggambarkan tanggung jawab antara penyedia alih daya dan pelanggan mereka.

Sebagai penyedia infrastruktur layanan mandiri yang sepenuhnya berada di bawah kontrol pelanggan – termasuk yang terkait dengan bagaimana dan apakah data diproses – AWS menyediakan layanan infrastruktur bagi pelanggan yang ingin mengunggah dan memproses konten di AWS. AWS tidak memiliki visibilitas ke atau pengetahuan tentang unggahan pelanggan ke jaringannya, termasuk apakah konten tersebut menyertakan informasi pribadi atau tidak. Pelanggan AWS juga diberdayakan dan didorong untuk menggunakan enkripsi guna membuat konten tidak dapat dipahami oleh AWS dan pihak ketiga mana pun yang ingin mengakses data.

Aliran bebas data non-pribadi yang diusulkan sebagai de facto UE dan Wilayah Trans-Pasifik.

Komisi UE baru-baru ini menerbitkan rancangan Peraturan tentang aliran bebas data yang ***melarang aturan lokalisasi data nasional di Negara Anggota UE*** dan mengakui prinsip pergerakan bebas data nonpribadi di dalam UE. Proposal ini menetapkan aliran data lintas batas sebagai standar de facto, menempatkan tanggung jawab bagi Negara Anggota untuk memberikan justifikasi keamanan publik guna memberlakukan persyaratan lokalisasi data. Sedangkan pada tahap awal musyawarah, proposisi ini mengakui keuntungan ekonomi dan keamanan dari aliran data lintas batas, yang melebihi pertimbangan untuk menegakkan kebijakan residensi data.

Selanjutnya, pada awal 2018, **Perjanjian Kemitraan Trans-Pasifik yang Komprehensif dan Progresif** yang disusun oleh 11 negara juga mendukung ***aliran data lintas batas*** dan tidak mewajibkan perusahaan untuk membangun fasilitas komputasi dalam negeri sebagai syarat menjalankan bisnis di negara tersebut.

Layanan AWS adalah konten agnostik karena menawarkan tingkat keamanan tinggi yang sama bagi semua pelanggan, terlepas dari jenis atau wilayah geografis konten yang sedang diproses atau disimpan. Dengan kata lain, AWS mengadopsi batas keamanan tinggi yang sama di semua penawaran kami. Ini berarti bahwa kami mengambil tingkat klasifikasi data tertinggi yang melintasi dan disimpan di cloud komersial kami serta menerapkan tingkat perlindungan yang sama ke semua penawaran kami dan bagi semua pelanggan kami. Penawaran ini kemudian diantrekan untuk sertifikasi terhadap keamanan internasional dan kepatuhan standar tinggi, yang berarti pelanggan mendapatkan manfaat dari tingkat perlindungan yang tinggi untuk data pelanggan yang diproses dan disimpan di cloud. AWS Cloud telah disertifikasi terhadap berbagai industri yang diatur (perawatan kesehatan, keuangan, dll.), nasional (mis. FedRAMP AS, Germany C5, Australia IRAP), dan akreditasi global (mis. ISO 27001,[23] ISO 27018,[24] Payment Card Industry (PCI) Data Security Standard (DSS),[25] dan Service Organization Controls (SOC)[26], yang menguji dan memvalidasi keamanan sistem kami dengan standar yang paling ketat.

Menyelaraskan Kebijakan Keamanan, Transformasi Digital, dan Pertumbuhan Ekonomi

Kebijakan harus berkembang untuk memenuhi realitas teknologi yang terus berubah dan dunia yang dibantu diciptakan. Jika tidak, pemerintah akan terus tertinggal dalam meningkatkan operasi mereka, melayani warganya, dan mengadopsi solusi paling modern dan aman. Bagian ini menjelaskan bagaimana AWS menangani tujuan keamanan yang mendasari persyaratan residensi data untuk mengurangi kekhawatiran pembuat kebijakan. Bagian ini juga mengeksplorasi tantangan modernisasi ekonomi dan TI yang terkait dengan residensi data dan pertimbangan kebijakan untuk memajukan adopsi cloud sektor publik yang aman.

Tantangan Sektor Komersial dan Publik terkait Residensi Data

Pemerintah harus mempertimbangkan bagaimana kebijakan nasional mereka bekerja untuk memajukan atau menghalangi pertumbuhan ekonomi dan peluang pengembangan tenaga kerja yang diberdayakan oleh layanan cloud berskala hiper. Mungkin ada dampak negatif yang signifikan dalam menerapkan persyaratan residensi data, seperti:

- **Efek merugikan pada bisnis lokal usaha ekspansi komersial multinasional** - Ketika bisnis tumbuh dan berkembang di luar operasi regional, mereka harus memiliki akses ke sumber daya yang memiliki jangkauan global. Membatasi akses ke layanan CSP berskala hiper sangat membatasi tingkat pengalaman pengguna yang dapat diberikan bisnis kepada basis pelanggan globalnya.

- **Opsi geo-redundansi yang terbatas dibandingkan dengan kawasan CSP global** - Bagi pemerintah dan bisnis, memastikan redundansi jika terjadi kegagalan operasional karena bencana atau keadaan lain sangat penting untuk stabilitas. Memiliki operasi yang berkerumun di satu negara memaparkan organisasi terhadap tingkat risiko yang jauh lebih besar daripada masalah akses data.
- **Struktur biaya mahal yang diperlukan untuk mengakomodasi persyaratan yang ketat** - Penyewa tunggal atau lingkungan "cloud" yang dibangun komunitas memerlukan tingkat harga untuk keberlanjutan operasional yang sebenarnya dapat mengurangi pengadaan kemampuan tambahan yang diperlukan guna mencapai pertahanan mendalam.

Teknologi cloud adalah pendorong untuk kemajuan sektor komersial dan publik, dan sejauh mana pemerintah mempromosikan atau menentang prinsip aliran data lintas batas akan memengaruhi kekuatan ekonomi lokal mereka serta daya saing pasar global.

Dampak Komersial

Memungkinkan aliran bebas data lintas batas memiliki dampak positif bersih yang signifikan pada ekonomi global. Studi terbaru oleh berbagai organisasi penelitian menekankan dampak ini, dan melangkah lebih jauh untuk menyoroti biaya untuk menetapkan hambatan aliran data. Laporan bulan Februari 2016 oleh McKinsey Global Institute memperkirakan bahwa aliran data lintas batas menyumbang hampir $2,8 triliun kepada ekonomi global pada tahun 2014[27] melalui pemberdayaan aliran barang, jasa, dan sumber daya lainnya. Laporan tersebut memperkirakan bahwa angka ini dapat mencapai $11 triliun pada tahun 2025. Pemerintah yang membutuhkan lokalisasi data dan membatasi arus ekonomi lintas batas harus membayar mahal. Pusat Ekonomi Politik Internasional Eropa (ECIPE), sebuah lembaga pemikir kebijakan independen, mengeluarkan studi tentang dampak ekonomi dari persyaratan lokalisasi data yang mendiskriminasi pemasok asing di tujuh wilayah hukum: Brasil, Tiongkok, UE, India, Indonesia, Korea Selatan, dan Vietnam.[28] Penelitian mereka menyimpulkan bahwa pembatasan sepihak pada aliran data lintas batas dan akses ke pasar luar negeri berdampak negatif pada pertumbuhan dan pemulihan ekonomi karena membatasi akses ke harga yang kompetitif, pertumbuhan pekerjaan di banyak sektor jasa dan barang, serta peluang investasi. Studi tersebut mencatat bahwa persyaratan residensi data tidak hanya memengaruhi aliran data, tetapi juga serangkaian peluang ekspansi komersial yang lebih luas yang bergantung pada aliran data lintas batas.

Studi serupa oleh Bank Dunia mempelajari enam negara berkembang dan 28 Negara Anggota UE, dan menemukan bahwa persyaratan lokalisasi data dapat mengurangi PDB hingga 1,7 persen, investasi hingga 4,2 persen, dan ekspor sebesar 1,7 persen.[29] Dampak ini paling dirasakan oleh bisnis skala kecil dan perusahaan rintisan. Melalui penggunaan cloud, misalnya, individu dan usaha kecil hingga menengah (UKM) dapat mengakses sumber daya TI dengan biaya dan skala yang hanya dapat diakses oleh entitas dengan kapitalisasi yang jauh lebih besar. UKM adalah pendorong utama untuk penciptaan lapangan kerja baru. Komputasi cloud mengurangi hambatan untuk penciptaan bisnis dan akses pasar, memungkinkan lebih banyak perusahaan baru terbentuk, yang pada akhirnya menciptakan lebih banyak

pekerjaan. Namun, menurut Komisi Eropa, perusahaan teknologi seperti CSP dapat menghadapi biaya yang signifikan untuk beradaptasi dengan berbagai undang-undang nasional yang menyebabkan biaya penjualan online melebihi keuntungannya. Baru-baru ini, pada Mei 2017, Information Technology and Innovation Foundation, sebuah lembaga riset nonpartisan, secara independen mencapai temuan serupa.[30]

Kesimpulan utama yang konsisten di seluruh studi ini yaitu melarang aliran data lintas batas dalam bentuk persyaratan residensi data yang dapat berdampak pada pertumbuhan ekonomi lokal dan regional serta daya saing di pasar global, dengan dampak terbesar ditanggung oleh UKM. Sistem yang aman di UE tidak lebih atau kurang aman dibandingkan dengan sistem yang dirancang serupa di Amerika Latin. Pemerintah memiliki kesalahpahaman bahwa perlindungan data umumnya tidak bergantung pada lokasi penyimpanan informasi, melainkan langkah-langkah yang digunakan untuk mengamankan data. Lokasi fisik umumnya tidak memiliki relevansi karena pusat data hampir selalu terhubung ke jaringan yang dapat diakses secara luas, sehingga keamanan sesungguhnya bergantung pada praktik dan proses teknis, operasional, dan manajerial yang diterapkan oleh CSP dan pelanggan.[31]

Biaya Pusat Data Dalam Negeri yang Beroperasi secara Eksklusif

Sebuah studi tahun 2015 oleh sebuah perusahaan keamanan informasi mengevaluasi bagaimana model pusat data dalam negeri jauh lebih mahal dibandingkan dengan memanfaatkan CSP global. Studi tersebut menemukan bahwa biaya layanan cloud dapat meningkat secara substansial karena lokalisasi data, tergantung pada ketersediaan layanan alternatif. Studi tersebut menemukan bahwa:

Jika Brasil telah memberlakukan pelokalan data sebagai bagian dari "UU Hak Internet" pada tahun 2014, perusahaan harus membayar rata-rata 54 persen lebih banyak untuk menggunakan layanan cloud (dari semua kategori) dari penyedia cloud lokal dibandingkan dengan harga terendah di seluruh dunia .

Jika Uni Eropa memberlakukan lokalisasi data, perusahaan masih harus membayar hingga 36 persen lebih untuk menggunakan layanan serupa yang disediakan oleh CSP berskala hiper. Pada saat penelitian dilakukan, beberapa pusat data dengan biaya terendah berada di Uni Eropa.[32]

Dampak bagi Sektor Publik

Negara yang memberlakukan hambatan aliran data dapat membatasi kemampuan warganya untuk memanfaatkan layanan inovatif yang meningkatkan kualitas hidup dan pemberian layanan pemerintah. Misalnya, aplikasi kecerdasan buatan dan pembelajaran mesin (AI/ML) memerlukan infrastruktur yang disesuaikan untuk fungsi yang optimal,[33] dan sementara CSP global terus memperluas jejak pusat data mereka, asumsi bahwa pusat data akan didirikan di setiap negara adalah hal yang tidak realistis. Oleh karena itu, karena AI/ML semakin banyak digunakan untuk meningkatkan layanan, seperti prognosis perawatan kesehatan dan prakiraan cuaca untuk kesiapsiagaan darurat, warga negara di negara-negara

dengan persyaratan tempat tinggal data yang ketat akan tertinggal dalam mengakses terobosan teknologi untuk layanan terkait warga negara.

Ada juga biaya sosioekonomi yang menurun untuk membatasi aliran data, khususnya tentang daya saing perdagangan dan pengembangan tenaga kerja. Seiring teknologi cloud menjadi tersebar di mana-mana dan semakin terkait erat dengan kemajuan ekonomi, perdagangan digital (dan mengurangi hambatannya) akan menjadi prioritas yang lebih tinggi bagi pemerintah. Negara-negara yang mengizinkan aliran data gratis akan mendapatkan keuntungan dengan mengakses teknologi terdepan, yang pada gilirannya akan berdampak pada modernisasi layanan sektor komersial dan publik, meningkatkan produktivitas pekerja, serta mempercepat pertumbuhan pekerjaan dan keterampilan lokal di seluruh sektor. Negara-negara yang membatasi aliran data dan perdagangan digital, pada waktunya, akan melihat kerugian kompetitif. Misalnya, berbagai manfaat penuh terkait dengan IoT untuk mengaktifkan pertanian "cerdas", manufaktur, atau kota tidak dapat direalisasikan dengan kebijakan yang membatasi analitik mahadata, pembelajaran mesin, atau fitur lain yang dilayani oleh pergerakan data yang bebas tetapi aman.

> Permintaan terus meninggi untuk keterampilan komputasi cloud di bidang-bidang utama seperti keamanan aplikasi, pengembangan aplikasi perusahaan cloud, migrasi cloud perusahaan, dan mahadata. Biro Statistik Tenaga Kerja AS melaporkan bahwa permintaan untuk pekerjaan di bidang keamanan informasi diperkirakan akan tumbuh pada tingkat 37% antara periode 2012-2022. Untuk memenuhi permintaan pekerjaan baru, pemerintah harus berinvestasi dalam memberikan kesempatan pendidikan dan pelatihan bagi individu dalam memperoleh keterampilan teknologi.

Batasan akses ke jenis layanan TI canggih yang disediakan oleh CSP berskala hiper juga akan menyebabkan kesenjangan terus-menerus dalam mengembangkan dan mempertahankan tenaga kerja yang sangat terampil dan menguasai teknologi. Ini karena bakat tenaga kerja berkorelasi dengan kecanggihan teknologi sebuah organisasi, yang pada gilirannya didasarkan pada kemampuan organisasi untuk mengakses teknologi mutakhir. Penggunaan teknologi modern secara efektif menuntut tenaga kerja dengan keterampilan yang sepadan untuk mengoperasikan teknologi tersebut. Mengingat luasnya dan kecepatan inovasi pada layanan cloud, ada kesenjangan keterampilan yang diketahui dan semakin lebar. Pemerintah, khususnya, telah tertinggal dalam perlombaan untuk mendapatkan pakar yang penting untuk memodernisasi aplikasi sementara pada saat yang sama melindungi informasi dan sistem sektor publik dari musuh dan pelanggaran yang sangat canggih yang meningkatkan frekuensi dan dampaknya.

Pertimbangan dalam Menetapkan Kebijakan Residensi Data

Seperti dibahas di atas, kedaulatan regulasi negara-bangsa terhadap data masih dapat dicapai sambil memanfaatkan biaya dan manfaat keamanan dari CSP berskala hiper seperti AWS. Langkah-langkah keamanan yang diterapkan di seluruh layanan AWS, dan diverifikasi melalui audit pihak ketiga kami, memberikan tingkat jaminan yang tinggi untuk mencegah dan mengatasi peristiwa risiko akses data yang melanggar hukum.

Kami mendorong pemerintah untuk mempertimbangkan kebijakan berikut dalam rangka memenuhi tujuan keamanan yang terkait dengan penyimpanan data.

1. Mengembangkan kebijakan dan persyaratan yang memungkinkan penggunaan fasilitas pemrosesan data luar negeri jika data diproses dan disimpan di lingkungan cloud yang modern, sangat aman, dan berskala hiper. Pelanggan juga dapat memilih lokasi yang konsisten dengan undang-undang perlindungan data yang konsisten mereka dan apabila perjanjian transfer data sudah ada.
2. Menyelaraskan kebijakan nasional dan persyaratan peraturan dengan prinsip pergerakan bebas data lintas batas untuk secara efektif menyeimbangkan tujuan keamanan, ekonomi, dan modernisasi TI.
3. Mengevaluasi model transfer data, seperti sistem Aturan Privasi Lintas Batas (CBPR) Kerjasama Ekonomi Asia-Pasifik (APEC), dan klausul kontrak standar, seperti Klausul Model UE, yang telah disetujui oleh otoritas perlindungan data UE dan mungkin digunakan dalam perjanjian antara penyedia layanan dan pelanggannya untuk memastikan bahwa data pribadi apa pun yang meninggalkan Wilayah Ekonomi Eropa akan ditransfer sesuai dengan Peraturan Perlindungan Data Umum (GDPR).[34] Jenis perjanjian transfer data ini memberikan jaminan bahwa CSP mengamankan data pribadi secara bertanggung jawab serta cara yang telah disetujui sebelumnya untuk melindungi dan mendukung aliran data internasional dengan cara yang aman dan sesuai.

> Peraturan Perlindungan Data Umum UE, yang mulai berlaku pada bulan Mei 2018, dimaksudkan untuk menyelaraskan undang-undang perlindungan data di seluruh Uni Eropa (UE) dengan menerapkan satu undang-undang perlindungan data yang mengikat di setiap negara anggota. GDPR tidak mensyaratkan undang-undang residensi data di dalam UE, tetapi mendukung kerangka kerja hukum dalam bentuk model transfer data dan klausul kontrak standar (yaitu, Klausul Model UE) untuk mendorong aliran data trans-regional.

Pasal 45 GDPR menetapkan prinsip bahwa transfer data pribadi ke negara ketiga atau organisasi internasional dapat terjadi jika negara ketiga, wilayah, atau satu atau beberapa sektor tertentu di negara tersebut, atau organisasi internasional yang bersangkutan memastikan tingkat perlindungan yang memadai. Untuk mencapai hal ini, pemerintah dapat:

- Mengubah undang-undang perlindungan data yang ada dan terlibat dalam diskusi yang memadai dengan negara lain. Misalnya, Selandia Baru sedang dalam proses mencapai keputusan kelayakan oleh Komisi Uni Eropa.
- Menetapkan kerangka kerja bilateral seperti Peraturan Privasi Lintas Batas APEC.

4. Memastikan CSP dan kontraktor pihak ketiga melaksanakan kontrol keamanan yang kuat untuk menangani akses pihak ketiga yang tidak sah ke data, sistem, dan aset melalui akreditasi pihak ketiga yang diakui secara internasional (misalnya ISO 27001, ISO 27018, SOC, PCI DSS, dsb.).
5. Mengklasifikasikan data dan menentukan peran dan tanggung jawab penanganan data untuk menentukan kewajiban perlindungan data yang sesuai bagi masing-masing pihak. Pemerintah harus memilih model penerapan cloud yang sesuai dengan kebutuhan spesifik mereka, jenis data yang mereka tangani, dan profil risiko. Untuk kumpulan data yang ditargetkan secara sempit dan diklasifikasikan pada tingkat sensitivitas tertinggi, pemerintah mungkin menganggap opsi hibrida lebih cocok.[1] Pemerintah juga harus mempertimbangkan untuk memanfaatkan ISO 27018 dalam menentukan peran pengontrol dan pemroses data. Pemerintah dapat bekerja dengan CSP untuk memahami dan menerapkan tanggung jawab perlindungan data secara memadai bagi pengontrol versus prosesor pada setiap model layanan cloud.
6. Memastikan pemahaman pelanggan dan penerapan layanan keamanan untuk mengenkripsi data. AWS telah memelopori layanan enkripsi yang memberi pelanggan kemampuan untuk mengontrol kunci enkripsi sepenuhnya. AWS memberi pelanggan opsi untuk mengenkripsi data menggunakan kunci mereka yang dapat disimpan di luar AWS atau secara aman dalam penawaran, memungkinkan mereka untuk mengontrol kunci dan akses ke data serta memenuhi kewajiban kepatuhan dan keamanan yang ketat.

[1][11] AWS Outposts menawarkan solusi cloud hibrida untuk beban kerja yang memerlukan manajemen data di lokasi.

7. Terlibat dalam upaya bilateral dan multilateral untuk memperbarui proses MLAT sehingga menyeimbangkan kebutuhan pemerintah untuk segera mendapatkan bukti yang diperlukan dalam penyelidikan dan penuntutan terhadap hak privasi individu atas konten elektronik yang mereka miliki. Kami mendukung undang-undang yang memperbarui privasi dan akses penegakan hukum ke komunikasi elektronik -- baik di dalam negeri maupun internasional. Kami juga mendorong pemerintah untuk meninjau dan memperbarui undang-undang nasional mereka guna menangani peran, tanggung jawab, dan mekanisme yang mengatur akses sah ke data yang sesuai dengan prinsip proses MLAT.

Kesimpulan

Pemerintah mungkin merasakan keamanan yang meningkat ketika memberlakukan persyaratan residensi data untuk data yang diproses dan disimpan di fasilitas TI lokal karena menawarkan kedekatan fisik dan kontrol, evaluasi yang lebih dalam menunjukkan bahwa membatasi layanan TI hanya untuk wilayah hukum lokal tidak memberikan keamanan data yang lebih baik secara keseluruhan. Dari perspektif manfaat-risiko, CSP berskala hiper, seperti AWS, dapat membantu mengelola risiko keamanan cyber dengan lebih baik sambil tetap meminimalkan risiko akses pemerintah asing ke data. Pemerintah juga perlu mempertimbangkan tarik-ulur yang signifikan terkait dengan persyaratan residensi data. Tidak hanya pemerintah yang menggunakan persyaratan residensi data ketat yang akan kehilangan akses ke beberapa lingkungan komputasi paling aman di dunia, tetapi, selain keamanan, mereka akan dipaksa untuk menghadapi kelambatan terus-menerus dalam akses ke layanan yang hemat biaya, teknologi mutakhir yang dibutuhkan untuk transformasi digital mereka. Kami mendorong pemerintah untuk mengevaluasi kembali tujuan keamanan yang sebenarnya mereka capai melalui pembatasan lokalisasi data yang terkait dengan ekonomi yang signifikan, modernisasi TI, dan biaya peluang keamanan. Kemampuan keamanan CSP berskala hiper tidak hanya menangani masalah yang diutamakan, tetapi juga memberikan keamanan di batas yang lebih tinggi daripada fasilitas lokal atau fasilitas yang dikontrak secara lokal. Solusi kebijakan, seperti perjanjian transfer data dan memanfaatkan akreditasi keamanan internasional yang terkenal, dapat berfungsi sebagai sarana yang memadai untuk menangani tujuan residensi data sembari mempromosikan tujuan transformasi digital sektor publik.

Revisi Dokumen

Tanggal	Keterangan
Agustus 2020	Pembaruan kecil pada teks untuk meningkatkan akurasi
November 2019	Publikasi pertama

Notes

[1] http://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

[2] Pete Lindstrom, "Assessing the Risk: Yes, the Cloud Can Be More Secure Than Your On-Premises Environment," International Data Corporation (Juli 2015).

[3] Perjanjian Bantuan Hukum Bersama (MLAT) umumnya memungkinkan pertukaran bukti dan informasi dalam masalah pidana dan yang terkait. https://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm

[4] Letters Rogatory adalah permintaan pengadilan di suatu negara kepada pengadilan negara lain yang meminta pelaksanaan suatu tindakan, yang jika dilakukan tanpa sanksi pengadilan luar negeri, dapat dianggap melanggar kedaulatan negara tersebut. Letters Rogatory dapat digunakan untuk memengaruhi layanan proses atau untuk mendapatkan bukti jika diizinkan oleh hukum negara asing. https://travel.state.gov/ content/ travel/en/legal/travel-legal-considerations/internl-judicial-asst/obtaining-evidence/Preparation-Letters-Rogatory.html

[5] UU CLOUD berlaku untuk perusahaan AS dan asing yang beroperasi di Amerika Serikat yang menyediakan "layanan komunikasi elektronik" dan/atau "layanan komputasi jarak jauh", seperti bisnis yang menawarkan email, olahpesan elektronik, atau layanan penyimpanan cloud kepada publik.

[6] http://d1.awsstatic.com/certifications/Amazon_LawEnforcement_Guidelines.pdf

[7] AWS memungkinkan pelanggan menggunakan mekanisme enkripsinya sendiri pada hampir semua layanan AWS, termasuk Amazon S3, Amazon EBS, Amazon DynamoDB, dan Amazon EC2. Tunnel IPSec ke VPC juga dienkripsi. Amazon S3 juga menawarkan Enkripsi Sisi Server sebagai suatu opsi bagi pelanggan. Pelanggan juga dapat menggunakan teknologi enkripsi pihak ketiga.

[8] Layanan AWS CloudHSM (Hardware Security Module) memungkinkan Anda melindungi kunci enkripsi dalam HSM yang dirancang dan divalidasi dengan standar pemerintah (FIPS 140-2 Level 3) untuk manajemen kunci yang aman termasuk perlindungan yang kuat. AWS KMS, divalidasi pada FIPS 140-2 Tingkat 2, menyediakan layanan serupa, tetapi lebih dapat diskalakan dan terintegrasi lebih dalam dengan berbagai layanan AWS, sehingga perlindungan diberikan secara otomatis berdasarkan perubahan sederhana dalam konfigurasi layanan. Menggunakan salah satu layanan tersebut, Anda dapat membuat, menyimpan, dan mengelola kunci kriptografi yang digunakan untuk enkripsi data dengan aman sehingga hanya dapat diakses oleh Anda. Untuk selengkapnya, lihat https://aws.amazon.com/cloudhsm/ dan https://aws.amazon.com/kms/.

[9] Opsi enkripsi AWS diperinci melalui tautan berikut: 1) Mengamankan Data yang Tidak Digunakan dengan Enkripsi, 2) Melindungi Data Menggunakan Enkripsi di Amazon S3, 3)Perincian Kriptografi AWS Key Management Service, dan 4) Ikhtisar Proses Keamanan AWS.

[10] Berbagai penelitian tersedia tentang teknik dekomposisi data. Salah satu laporan yang ditinjau untuk dokumen ini adalah Perlindungan data melalui fragmentasi di berbagai sistem penyimpanan terdistribusi yang berbeda - sebuah survei, Kapusta dan Memmi, 20 Juni 2017.

[11] Pertahanan mendalam adalah praktik penerapan beberapa lapis kontrol keamanan untuk memberikan independensi dan redundansi. Jika satu lapisan kontrol gagal, lapisan berikutnya tersedia untuk mengurangi serangan lebih lanjut terhadap aset.

[12] Pertahanan secara luas adalah pendekatan penggunaan aktivitas multidisiplin untuk menyediakan banyak mekanisme perlindungan pada setiap lapisan pertahanan yang diidentifikasi. Secara umum, ini berarti lebih banyak otomatisasi dan kontrol keamanan yang lebih bervariasi di masing-masing lapisan.

[13] https://aws.amazon.com/guardduty/

[14] https://aws.amazon.com/macie/

[15] https://aws.amazon.com/cloudhsm/

[16] FIPS 140-2, Persyaratan Keamanan untuk Modul Kriptografi mencakup 11 bidang yang terkait dengan desain dan penerapan suatu modul kriptografi.

[17] https://d1.awsstatic.com/whitepapers/compliance/AWS_Logical_Separation_Handbook.pdf

[18] https://aws.amazon.com/compliance

[19] https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

[20] AWS Outposts menghadirkan layanan, infrastruktur, dan model operasi AWS bawaan ke hampir semua pusat data, ruang lokasi bersama, atau fasilitas di lokasi. Untuk detail lebih lanjut, kunjungi https://aws.amazon.com/outposts/

[21] Sederhananya, desain polimorfik memungkinkan pembuatan target bergerak sehingga lebih sulit bagi musuh untuk melakukan serangan yang berhasil.

[22] Konsep tersebut pertama kali diciptakan oleh Forrester Research. Konsep ini mengusulkan bahwa tidak ada entitas di jaringan yang dipercaya. Tujuannya adalah melakukan akses aman ke semua sumber daya baik internal maupun eksternal. Ini berarti bahwa organisasi harus memahami dan mengklasifikasikan datanya serta memetakan bagaimana data tersebut, terutama data sensitif, mengalir antara penyimpanan, pemrosesan, transit, dan konsumen. Kemudian setelah data dipahami, organisasi dapat menerapkan mekanisme ZTM yang memberlakukan dan mengotomatiskan hak istimewa terkecil absolut, enkripsi ujung ke ujung, dan inspeksi lalu lintas penuh.

[23] ISO 27001/27002 adalah standar keamanan global yang diadopsi secara luas yang menetapkan persyaratan dan praktik terbaik untuk pendekatan sistematis dalam mengelola informasi perusahaan dan pelanggan berdasarkan penilaian risiko berkala yang sesuai dengan skenario ancaman yang selalu berubah.

[24] ISO 27018 adalah kode praktik yang berfokus pada perlindungan data pribadi di cloud. Ini didasarkan pada standar keamanan informasi ISO 27002 dan memberikan panduan penerapan pada kontrol ISO 27002 yang berlaku untuk Informasi Identifikasi Pribadi (PII) cloud publik. Ini juga menyediakan serangkaian kontrol tambahan dan panduan terkait yang dimaksudkan untuk memenuhi persyaratan perlindungan PII cloud publik yang tidak ditangani oleh rangkaian kontrol ISO 27002 yang ada.

[25] Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) adalah standar keamanan informasi eksklusif yang dikelola oleh Dewan Standar Keamanan PCI (https://www.pcisecuritystandards.org/), yang didirikan oleh American Express, Discover Financial Services, JCB Internasional, MasterCard Worldwide, dan Visa Inc. PCI DSS berlaku bagi semua entitas yang menyimpan, memproses atau mengirimkan data pemilik kartu (CHD) dan/atau data autentikasi sensitif (SAD) termasuk pedagang, pengolah, pengakuisisi, penerbit, dan penyedia layanan.

[26] Laporan Kontrol Organisasi Layanan (SOC 1, 2, 3) dimaksudkan untuk memenuhi berbagai persyaratan audit keuangan untuk lembaga audit AS dan internasional. Audit untuk laporan ini dilakukan sesuai Standar Internasional untuk Keterlibatan Jaminan No. 3402 (ISAE 3402) dan Institut Akuntan Publik Bersertifikat di Amerika (AICPA): AT 801 (sebelumnya SSAE 16).

[27] http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows

[28] European Centre for International Political Economy (ECIPE): "The Costs of Data Localization: A Friendly Fire on Economic Recovery,"

http://www2.itif.org/2015-cross-border-data-flows.pdf?_ga=1.8208626.1580578791.1473954628.

[29] http://documents.worldbank.org/curated/en/961621467994698644/pdf/102724-WDR-WDR2016Overview-ENGLISH-WebResBox-394840B-OUO-9.pdf

[30] Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" Information Technology and Innovation Foundation (May 2017) http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.243762501.1722557619.1508762047- 1611916082.1508762047.

[31] Ibid hal.4 Makalah ini menarik kesimpulan serupa secara independen.

[32] http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.51021357.566718019.1510350061-1611916082.1508762047

[33] Misalnya, sistem dengan kemampuan GPU untuk tujuan umum dan Field Programmable Gate Arrays (FPGA).

[34] Adendum Pemrosesan Data GDPR AWS, yang mencakup Klausul Model UE, sekarang menjadi bagian dari Persyaratan Layanan online kami. Ini berarti semua pelanggan AWS secara global dapat mengandalkan persyaratan DPA GDPR AWS kapan pun mereka menggunakan layanan AWS untuk memproses data pribadi berdasarkan GDPR. Informasi selengkapnya tentang pendekatan AWS untuk kepatuhan GDPR tersedia di sini: https://aws.amazon.com/ compliance/gdpr-center/.