TIM PERIKSA DATA

Urgensi Perlindungan Data Pribadi di Indonesia

Prepared by Tim Periksa Data

Belajar 'lagi' dari Kasus Kebocoran Data BPJS Kesehatan

KRONOLOGI

RABU, 12 MEI 2021

Sejumlah 279 juta data pribadi penduduk Indonesia diperjualbelikan di RaidForums oleh akun bernama Kotz, 20 juta diantaranya memiliki foto profil. Data pribadi tersebut berupa NIK, nomor ponsel, e-mail, alamat, dan gaji, serta termasuk data penduduk Indonesia yang telah meninggal dunia. Kotz juga memberikan sampel sebanyak 1 juta data yang dapat diakses secara bebas dan gratis, yang disebar dalam tiga tautan yaitu bayfiles.com, mega.nz, dan anonfiles.com;

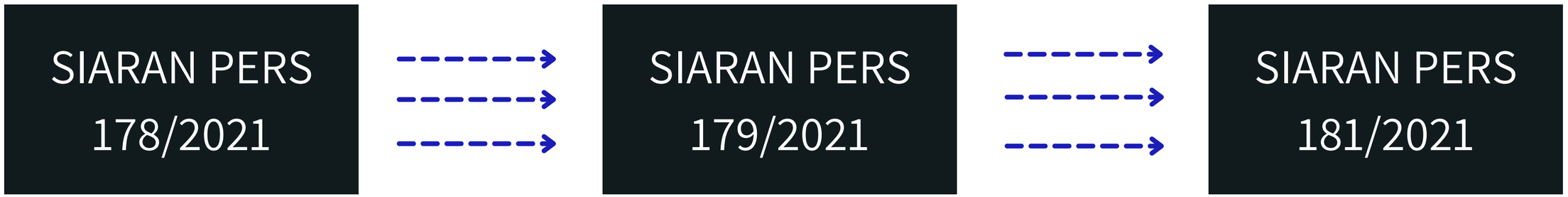
KAMIS, 20 MEI 2021

Sebuah akun twitter bernama @ndagels mencuitkan informasi pertama kalinya mengenai kebocoran data yang diperdagangkan oleh Kotz pada RaidForums

KAMIS-JUMAT, 20-21 MEI 2021

Merespon keriuhan publik, Kementerian Komunikasi dan Informatika (“Kemenkominfo”) menerbitkan beberapa Siaran Pers, antara lain: [i] Siaran Pers No. 178/HM/KOMINFO/05/2021 tertanggal 20 Mei 2021; [ii] Siaran Pers No. 179/HM/KOMINFO/05/2021 tertanggal 21 Mei 2021; dan [iii] Siaran Pers No. 181/HM/KOMINFO/05/2021 tertanggal 20 Mei 2021.

Temuan 1

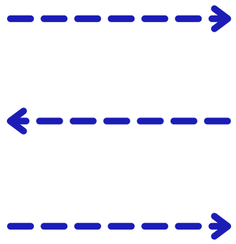


Catatan:

Akibat eufemisme bahasa birokrasi sebagaimana dimaksud pada diagram di atas, publik in casu peserta BPJS terganggu haknya atas informasi (rights of information) dikarenakan tidak mendapatkan kejelasan informasi kuantitafif jumlah data yang bocor a quo.

Temuan 2

SIARAN PERS
BPJS KESEHATAN
25 MEI 2021



PERNYATAAN
BARESKRIM POLRI
04 JUNI 2021

"data yang ditawarkan di forum online yang diberitakan menyerupai data BPJS Kesehatan."

"data yang bocor diduga keras merupakan data BPJS Kesehatan."

Catatan:

Eufemisme bahasa birokrasi kembali terjadi. Lagi-lagi, publik dibuat bingung dengan istilah-istilah yang digunakan dalam mengualifikasikan data yang bocor.

Temuan 3

Hingga detik ini, BSSN belum menerbitkan rilis apapun atas kejadian kebocoran data ini. Meski demikian, bukan berarti BSSN tidak memberikan pernyataan. Melalui Sekretaris Utama-nya, BSSN menyampaikan setidaknya dua poin penting:

[i] Penelusuran kasus kebocoran data, dengan jenis kasus yang sama dengan kebocoran data a quo, di sejumlah negara, memerlukan waktu 3-4 bulan; dan

[ii] BSSN tidak pasang target untuk penyelesaian kasus a quo karena sifat kerjanya hanya menunjang keinginan BPJS.

Tanggapan:

Pernyataan BSSN ini jauh dari solutif, baik ditinjau dari segi kewenangan dan fungsi yang BSSN miliki, maupun dari segi rasionalisasi atas apa yang dimaksud dengan ‘penelusuran kasus’.

Dasar Hukum Upaya Gugatan Perbuatan Melawan Hukum oleh Penguasa (PMH Penguasa)

- Pasal 75 Ayat (1) Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan;
- Pasal 48 Ayat (2) Undang-Undang Nomor 5 Tahun 1986 tentang Peradilan Tata Usaha Negara;
- Pasal 2 Ayat (2) Peraturan Mahkamah Agung Nomor 2 Tahun 2019 tentang Pedoman Penyelesaian Sengketa Tindakan Pemerintahan dan Kewenangan Mengadili Perbuatan Melanggar Hukum oleh Badan dan/atau Pejabat Pemerintahan (Onrechtmatige Overheidsdaad).

Perhatian-perhatian....

Surat Keberatan Administratif ini akan menguji bagaimana tata kelola data pribadi diimplementasikan, melalui dua bingkai dalil yakni pendekatan data governance dan pendekatan good governance.

Tata Kelola Data (Data Governance) yang Problematik

- Beberapa asas perlindungan data pribadi sebagaimana diamanatkan Pasal 2 Ayat (2) Permenkominfo No. 20/2016 dan persyaratan minimum terkait Penyelenggaraan Sistem Elektronik sebagaimana diwajibkan Pasal 4 PP No. 71/2019 terang terlanggar.
- Tidak terdapat satu pernyataan pun dari BPJS Kesehatan terkait pengakuan telah terjadinya kebocoran data pada sistemnya. Lebih lanjut, hingga detik ini, BPJS Kesehatan belum memberitahukan secara tertulis perihal alasan atau penyebab kebocoran data, potensi dampak kebocoran data, upaya yang sedang ditempuh BPJS Kesehatan, serta upaya yang dapat dilakukan masyarakat Indonesia dalam melindungi data pribadinya secara mandiri, sebagaimana diwajibkan pada Pasal 14 ayat (5) dan Pasal 28 ayat (3) dan (4) PP No. 71/2019.
- Hingga saat ini, tidak dapat ditemukan standar prosedur yang digunakan oleh BPJS Kesehatan yang disampaikan kepada publik, terkhususnya pemilik data yang bocor. Lebih lanjut, tidak ditemukan pemberitahuan atas digunakannya vendor-vendor oleh BPJS Kesehatan kepada publik. Artinya, publik tidak pernah mengetahui bahwa ada kemungkinan terjadinya perpindahan data-data mereka ke tangan lain selain BPJS Kesehatan.

TATA KELOLA DATA (DATA GOVERNANCE) YANG BAIK SEHARUSNYA....

Kepemilikan sertifikat ISO/IEC 27001 tidak sama dengan keberhasilan menegakkan standar yang tepat, berkesinambungan dan ketat tiap waktunya.

Berdasarkan ISO/IEC 27001:2013

a. Pelaporan Kejadian, Keamanan dan Kelemahan Keamanan Informasi (Lampiran ISO/IEC 27001:2013 Huruf A.16)

b. Pencatatan dan Pemantauan Huruf (Lampiran ISO/IEC 27001:2013 Huruf A.12.4)

c. Pelaksanaan Audit Internal Berkala dan Berkesinambungan (Angka 9.2 ISO/IEC 27001:2013)

d. Pengujian Sistem atau Penetration Testing (“Pentest”) (Angka 6 ISO/IEC 27001:2013)

Tata Kelola Pemerintahan (Good Governance) Terang Terabaikan

- Pasal 3 Peraturan Presiden Nomor 54 Tahun 2015 tentang Kementerian Komunikasi dan Informatika dan Pasal 35 Ayat (1) PP No. 71/2019 memberikan kewenangan pengawasan atas data pribadi masyarakat Indonesia kepada Kemenkominfo. Fungsi pengawasan tersebut juga dimiliki oleh BSSN sebagaimana tertulis dalam Pasal 12, 14, 16, 18 dan 21 Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara.
- Bahwa sudah sepatutnya Kemenkominfo dan BSSN mengindahkan fungsi dan kewenangan dimaksud dengan melakukan pengawasan dan tindakan pencegahan jauh sebelum data ini bocor. Pada poin ini, Kemenkominfo dan BSSN baru bertindak ketika hal ini ramai diperbincangkan di twitter oleh akun @ndagels (20 Mei 2020), bukan malah ketika hal ini tersiar di RaidForums, yang mana tanggal tersiarnya di RaidForums (12 Mei 2020).
- Terlebih lagi, bukan kali pertama RaidForums menjadi pasar daring untuk penjualan data pribadi penduduk Indonesia, yang mana oleh karenanya upaya preventif tentu saja tidak terlalu kompleks, dan dapat dilakukan dengan cara mengawasi pasar daring ini.

Perbandingan terhadap Preseden Ideal: Uni Eropa (Komparasi terhadap General Data Protection Regulation)

Sebagaimana disampaikan Sekretaris Utama BSSN pada wawancara dengan media, bahwa penelusuran kasus kebocoran data sejenis di sejumlah negara bahkan memerlukan waktu 3-4 bulan. Pernyataan demikian **terang nir-perbandingan** dengan ke-27 negara anggota Uni Eropa.

- Recital 85 menyatakan bahwa pelanggaran data pribadi jika tidak segera diselesaikan akan memunculkan kerugian fisik, material, dan non-material yang ditanggung oleh pemilik data (Prinsip Kecepatan dalam Penanganan Kebocoran Data).
- Recital 86 mewajibkan data controller in casu BPJS Kesehatan untuk mengomunikasikan kepada pemilik data secepat mungkin tanpa penundaan yang tidak perlu mengenai pelanggaran data pribadi yang terjadi serta menerangkan risiko yang muncul terhadap hak dan kebebasan pemilik data.
- Terkait dua poin di atas, lahir hak integral yakni hak atas informasi secepat mungkin, yang tentu saja tidak mungkin menunggu hingga 3-4 bulan sebagaimana disampaikan oleh Sekretaris Utama BSSN.

Pengawasan adalah Kunci.

Lantas, bagaimana jika data controller, in casu BPJS Kesehatan, tidak kunjung mengindahkan pertanggung-jawaban yang harus segera BPJS Kesehatan sampaikan?

Prepared by Tim Periksa Data

Pasal 34 Ayat (4) GDPR menerakan kewajiban bagi lembaga pengawas (supervisory authority), in casu Kemenkominfo dan BSSN, untuk menginstruksikan BPJS Kesehatan agar menyampaikan pertanggung-jawaban ini.

Jika kewajiban penyampaian pertanggung-jawaban ini tidak dimintakan, maka BPJS Kesehatan selaku data controller terang akan mempreservasi kelalaiannya atas tanggung-jawab terhadap kegagalan perlindungan data pribadi pengguna layanannya.

Fungsi Pengawasan Berdasarkan ISO/IEC 27001:2013

- Konsep pengawasan dalam ISO/IEC 27001:2013 sebenarnya dilakukan oleh lembaga yang menghimpun data, bukan dialihkan kepada lembaga lain. Dalam hal ini, pengawasan tersebut tidak seperti relasi antara BPJS Kesehatan sebagai penghimpun data dengan Kemenkominfo dan BSSN.

- Secara singkat, fungsi pengawasan tersebut harus berupa:
  a. Evaluasi efektivitas tindakan;
  b. Penilaian risiko keamanan informasi;
  c. Penanganan risiko keamanan informasi; dan
  d. Penggunaan sumber daya manusia yang mumpuni.

Pelanggaran terhadap Asas-Asas Umum Pemerintahan yang Baik

1. Asas Kecermatan
2. Asas Keterbukaan
3. Asas Pelayanan yang Baik

Prepared by Tim Periksa Data

Total Kerugian

- Kerugian Materiil
  Dihimpun dari CSIRT.ID Press Release 24 Mei 2021, disebutkan bahwa total kerugian yang dialami Indonesia akibat kebocoran 279 juta data penduduk yakni lebih dari Rp 600 Triliun, yang di dalamnya juga termasuk kerugian masyarakat Indonesia.

- Kerugian Immateriil
  Masyarakat Indonesia mengalami kekhawatiran, ketakutan, dan rasa tidak aman mengingat data ini sangat berkaitan dengan setiap sendi kehidupan masyarakat Indonesia.

PETITUM

Berdasarkan alasan-alasan tersebut, Tim Periksa Data meminta kepada pihak pemerintah (BPJS Kesehatan, Kemenkominfo dan BSSN) untuk melakukan:

- Mengakui telah gagal melindungi data masyarakat Indonesia pengguna layanan BPJS Kesehatan.
- Meminta maaf kepada seluruh masyarakat Indonesia atas kegagalan kinerja pemerintah yang mengakibatkan terjadinya kebocoran data tersebut di media nasional sebanyak 3 (tiga) kali periode yang 1 (satu) kali periodenya adalah 10 hari kerja.
- Menyusun kertas Asesmen terhadap dampak kebocoran data a quo yang mana kertas Asesmen dimaksud dipublikasikan kepada publik selambat-lambatnya 10 (sepuluh) hari kerja terhitung sejak Upaya Administratif diterima.
- Meninjau ulang, memperbaiki, dan merapikan Sistem dan Fungsi Pengawasan antar Kementerian/Lembaga terutama Kemenkominfo-BSSN-BPJS Kesehatan.
- Mendorong disusunnya cetak biru Perlindungan Data Nasional untuk mencegah kejadian serupa terjadi berulang yang mana cetak biru ini bersifat partisipatif dan diinformasikan kepada publik.