KEMENTERIAN DIGITAL

NOTIFIKASI INSIDEN KETIRISAN DATA

Templat pemberitahuan ini perlu digunakan apabila pengguna data ingin melaporkan ketirisan data peribadi yang telah berlaku atau mungkin telah berlaku dalam organisasi, dalam keadaan di mana ketirisan tersebut menimbulkan risiko kepada subjek data yang terlibat. Semasa melengkapkan borang ini, dilarang sertakan sebarang data peribadi yang terlibat dalam ketirisan tersebut. Sila ambil perhatian bahawa templat pemberitahuan ini tidaklah muktamad. Pesuruhjaya boleh meminta butiran lanjut mengenai insiden tersebut untuk memudahkan siasatan.

BUTIR-BUTIR PENGGUNA DATA DAN ORANG YANG MEMBERIKAN PEMBERITAHUAN INI

Organisasi : ----------

Alamat : ----------

Individu untuk dihubungi

Nama : ----------

Jawatan : ----------

Nombor Telefon : **Faks :** ----------

E-mel : ----------

Tarikh : ----------

Tandatangan : ----------

Berdasarkan maklumat yang anda berikan, kami akan menghubungi anda untuk memberitahu tentang langkah-langkah kami seterusnya. Semua data peribadi yang dihantar hanya akan digunakan bagi tujuan yang berkaitan secara langsung dengan pemberitahuan ini, pelaksanaan kuasa serta fungsi pengawalseliaan Pesuruhjaya.

Penyerahan pemberitahuan:

PESURUHJAYA PERLINDUNGAN DATA PERIBADI, MALAYSIA
Aras 8, Galeria PjH, Jalan P4W, Persiaran Perdana,
Presint 4, Pusat Pentadbiran Kerajaan Persekutuan
62100 Putrajaya, Malaysia
atau melalui e-mel: dbnpdp@pdp.gov.my

BUTIRAN TENTANG KETIRISAN DATA	
1.	**Ringkasan kejadian:** **a) Jenis ketirisan (cth: kehilangan, kebocoran, akses tanpa kebenaran, serangan siber, kelemahan teknologi, unsur jenayah, kehilangan peralatan dll.)** **b) Bila, di mana, dan bagaimana ketirisan itu berlaku? Adakah kompromi hanya berlaku pada pangkalan data atau termasuk ketirisan API?** **c) Bila ketirisan itu disedari?** **d) Siapa dan bagaimana ketirisan itu disedari?** **e) Apakah tempoh ketirisan data?** **f) Apakah punca ketirisan tersebut?** **g) Apakah sistem yang terjejas?** **h) Siapa yang membangunkan sistem yang terjejas? Adakah ia dibangunkan secara dalaman oleh syarikat atau pihak ketiga? Jika pihak ketiga, siapakah pembangunnya?** **i) Apakah kategori data organisasi yang dimiliki oleh pihak ketiga? Adakah pihak ketiga mempunyai akses langsung ke rangkaian organisasi?** **j) Bahagian sistem manakah yang telah terjejas? Sistem folder fail (NAS / SAN / Penyimpanan Awan) atau turut melibatkan pangkalan data dan sistem aplikasi?** **k) Adakah organisasi anda menggunapakai infrastruktur di premis atau infrastruktur awan?** **l) Siapakah penyedia perkhidmatan awan sebelum insiden ketirisan data berlaku? Apakah kekurangan pada langkah keselamatan yang diambil oleh pihak penyedia perkhidmatan awan tersebut?**
2.	**Data yang terjejas:** **a) Jumlah dan jenis data yang terjejas (kewangan, pekerjaan, data kesihatan dll.)** **b) Anggaran bilangan subjek data yang terjejas.** **c) Apakah data yang dikumpul, diproses, dan disimpan oleh organisasi? Di mana data disimpan, dan apa langkah keselamatan yang diambil untuk melindungi data tersebut?** **d) Siapakah yang mempunyai akses kepada data, dan bagaimanakah akses diberikan dan dipantau? Adakah terdapat pihak ketiga yang menerima atau memproses data, dan bagaimanakah akses dan penggunaan data pihak ketiga dipantau?**

	e) Berapa lama data disimpan, dan bagaimana ia dilupuskan? **f) Adakah organisasi mendapatkan persetujuan dari individu untuk memproses data peribadi mereka?** **g) Adakah ketirisan data tersebut hanya melibatkan warganegara Malaysia sahaja? Jika tidak, sila nyatakan negara yang terlibat dan jumlah subjek data yang terlibat.** **h) Adakah organisasi telah menjalankan penilaian impak perlindungan data untuk aktiviti pemprosesan berisiko tinggi?**
3.	**Apakah kemungkinan kemudaratan yang disebabkan oleh insiden? Ia mungkin termasuk:** **a) Ancaman terhadap keselamatan diri (Ya/Tidak);** **b) Kecurian identiti (Ya/Tidak);** **c) Kerugian kewangan (Ya/Tidak);** **d) Kerosakan reputasi, kehinaan, dan keaiban (Ya/Tidak) ;** **e) Kehilangan peluang perniagaan dan pekerjaan (Ya/Tidak);** **f) Lain-lain (sila nyatakan);**
4.	**Langkah keselamatan/kawalan yang sedia ada di organisasi (sebelum kejadian ini):** **a) Sila nyatakan langkah / kawalan keselamatan yang sedia ada di organisasi anda (sebelum kejadian ini).** **b) Adakah organisasi anda mempunyai pensijilan:** **- ISO/IEC27002:2022 Keselamatan Maklumat, Keselamatan Siber, dan Perlindungan Privasi (Kawalan Keselamatan Maklumat)** **- ISO/IEC27001:2022 Keselamatan Maklumat, Keselamatan Siber, dan Perlindungan Privasi (Sistem Pengurusan Keselamatan Maklumat)** **- ISO/IEC27701:2019 Teknik Keselamatan (Sistem Pengurusan Maklumat Privasi)** **Jika organisasi anda belum mempunyai obligasi untuk mematuhi piawaian di atas, sila nyatakan dan jelaskan secara terperinci langkah dan jangka masa untuk mendapatkan pensijilan tersebut.** **c) Sebarang pematuhan keselamatan data & sistem lain yang organisasi anda perlu diperakui dan mematuhinya? (Contoh: PCI DSS)** **d) Adakah sistem organisasi anda mempunyai penyelarasan *Network Time Protocol (NTP)* antara semua pelayan & peralatan rangkaian termasuk penyelarasan masa & peralatan keselamatan?** **e) Adakah organisasi mempunyai pelan pengurusan insiden keselamatan siber?**

	f) Adakah organisasi telah menjalankan *vulnerability assessment* terhadap sistem dan infrastruktur? **g) Adakah organisasi mempunyai langkah-langkah keselamatan yang sesuai untuk melindungi sistem daripada perisian hasad, keselamatan *phishing*, dan ancaman keselamatan siber?** **h) Adakah pekerja dilatih secara berkala mengenai amalan terbaik keselamatan siber?** **i) Adakah pihak ketiga tertakluk kepada kawalan keselamatan siber dan terma kontrak yang sesuai?**
PEMBENDUNGAN DAN PEMULIHAN	
5.	**a) Tindakan yang diambil untuk membendung ketirisan (cth: Prosedur / arahan dalaman untuk mengurangkan risiko kepada keselamatan data)** **b) Tindakan yang diambil untuk memulihkan data yang hilang dan mengurangkan ketirisan lanjutan (cth: Pemulihan data melalui *back-up server*/pita/cakera optik)**
KOMUNIKASI & PEMBERITAHUAN	
6.	**a) Pernahkah anda cuba berkomunikasi / berunding secara langsung dengan Pelaku Ancaman? (Ya/Tidak);** **b) Pernahkah anda cuba berkomunikasi / berunding dengan Pelaku Ancaman melalui ejen / proksinya? (Ya/Tidak);** **c) Adakah anda telah melantik mana-mana ejen / proksi dalam percubaan untuk berkomunikasi / berunding secara langsung dengan Pelaku Ancaman? (Ya/Tidak);** **d) Adakah anda telah melantik mana-mana ejen / proksi dalam percubaan untuk berkomunikasi / berunding dengan Pelaku Ancaman melalui ejen / proksinya? (Ya/Tidak).** **Sila berikan semua bukti berkaitan termasuk komunikasi suara yang ditranskripsi dengan Pelaku Ancaman atau ejen / proksinya.**
7.	**Adakah anda telah melaporkan kepada pihak-pihak berikut? Apakah kaedah yang digunakan untuk pelaporan?** **a) Pihak pengawalselia dan agensi penguatkuasaan undang-undang** **b) Subjek data** **c) Pihak-pihak lain yang terjejas** **d) Pemproses data** **e) Pihak berkuasa perlindungan data lain (luar negara) (jika perlu)**