

# LEGAL BUZZ

PEJABAT PENASIHAT UNDANG-UNDANG, UNIVERSITI MALAYSIA TERENGGANU



**TANGGUNGJAWAB  
KERAHSIAAN DAN  
PERLINDUNGAN DATA  
PERIBADI**

# SIDANG REDAKSI

## PENAUNG

Prof. Dato' Dr. Mazlan Abd Ghaffar, FAsc.  
vc@umt.edu.my

## PENASIHAT

Dr. Fahirah Syaliza Mokhtar  
fahirah.mokhtar@umt.edu.my

## KETUA PENGARANG

Roslina Ghazali  
rosrina.ghazali@umt.edu.my

## PENGARANG

Muhammad Hafizuddin Zakaria  
m.hafizuddin@umt.edu.my

Amirah Nabilah Ismail  
a.nabilah@umt.edu.my

## PENYELARAS BAHAN

Azmi Che Pa  
ainzaminya@umt.edu.my

Laila Mamat  
achik@umt.edu.my

Noor Akmal Mamat@Aziz  
noor.akmal@umt.edu.my

# KANDUNGAN

- 3 Dari Meja Penasihat Undang-Undang
- 4 Perutusan Naib Canselor
- 5 Dokumen Rasmi UMT: Tergugat? Selamat? Dilindungi?
- 9 Kepentingan "Non-Disclosure Agreement" dalam Pengurusan Penyelidikan dan Pengkomersialan Universiti
- 14 Tanggungjawab Bekas Pekerja terhadap Perjanjian Kerahsiaan
- 17 Perlindungan Data Peribadi: Kenapa Anda Perlu Cakna?
- 21 Sisipan Kes Undang-Undang

Penulisan artikel di dalam Legal Buzz ini hanyalah sebagai panduan umum sahaja dan bukan suatu penasihatan undang-undang yang muktamad. Pandangan atau pendapat yang dinyatakan oleh pengarang adalah milik pengarang sahaja, dan tidak menggambarkan pandangan atau pendapat UMT atau PPUU. Buletin ini diedarkan tanpa menjelaskan hak harta intelek milik UMT. Sebarang pengeluaran semula, penduaan atau pengubahan buletin ini, dalam apa jua bentuk atau cara, sama ada sebahagian atau keseluruhannya, adalah tidak dibenarkan dan dilarang sama sekali. UMT juga melarang penggunaan buletin ini dan semua atau mana-mana kandungannya di sini, untuk penjualan, keuntungan komersial dan/atau peribadi.



# DARI MEJA PENASIHAT UNDANG-UNDANG

Assalamualaikum w.b.t. dan salam sejahtera.

Pertama sekali, segala puji dan syukur saya rafakkan ke hadrat llahi atas kurniaan ilham dan kesempatan masa sehingga Legal Buzz untuk edisi ke-8 ini berjaya diterbitkan.

Sabtu tahun, kita sering mendengar mengenai kes kebocoran maklumat di agensi-agensi Kerajaan yang boleh menjelaskan reputasi dan imej jabatan yang berkaitan. Antara kes terkini adalah kebocoran maklumat berkaitan tender projek Air Kelantan, kawasan pembalakan, lot tanah dan sebagainya oleh Kerajaan Negeri Kelantan, yang didedahkan melalui platform media sosial kepada masyarakat umum. Kesemua maklumat ini adalah maklumat rasmi Kerajaan dan penyiarannya kepada umum tanpa kebenaran Ketua Jabatan adalah suatu kesalahan di bawah Akta Rahsia Rasmi 1972.

Pada tahun ini juga, kita dikejutkan dengan berita mengenai dakwaan penjualan 22 juta data peribadi rakyat Malaysia yang berusia 18 hingga 82 tahun yang berada dalam kawalan Jabatan Pendaftaran Negara (JPN) di forum pasaran pangkalan data. Walaupun berita ini telah dinafikan oleh Pengarah JPN dan Menteri Dalam Negeri Malaysia, ianya tetap menimbulkan kegusaran masyarakat mengenai keberkesanan sistem keselamatan data di Malaysia. Sekiranya benar terdapat kebocoran data peribadi daripada pangkalan data jabatan dan badan awam, ia adalah suatu pelanggaran keselamatan (*security breach*) yang serius dan mendedahkan orang ramai kepada pelbagai risiko termasuk penipuan, kecurian identiti dan juga menjelaskan keselamatan negara.

Di UMT sendiri, masalah kebocoran maklumat bukan suatu perkara yang asing. Adakalanya sebelum sesuatu keputusan mesyuarat dikeluarkan secara rasmi oleh pihak yang bertanggungjawab, maklumat keputusan tersebut telahpun tersebar di kalangan warga. Walaupun mungkin tiada kerosakan atau kesan serius berlaku akibat daripada kebocoran maklumat tersebut, ianya tetap melanggar etika dan integriti seorang penjawat badan berkanun.

Justeru, melalui kupasan Legal Buzz kali ini, kami cuba memberikan pencerahan kepada para pembaca, khususnya warga UMT mengenai tanggungjawab dan kepentingan untuk menjaga kerahsiaan dalam perkhidmatan dan isu-isu undang-undang yang berkaitan dengannya serta bagaimana undang-undang sedia ada boleh melindungi data peribadi seseorang individu.

Semoga kupasan kali dapat dijadikan panduan dan memberi manfaat kepada semua warga UMT.

Selamat membaca!

**"Profesional, Berwibawa, Berintegriti"**

#UMTsohor  
#ppuumesrawarga

**Salam hormat,**

*Dr. Fahirah Syaliza Mokhtar*



# PERUTUSAN NAIB CANSELOR

Bismilahirrahmanirrahim.

Assalamualaikum w.b.t dan salam sejahtera.

Warga UMT yang dikasihi, menjaga kerahsiaan dokumen dan maklumat rahsia rasmi Kerajaan dan UMT bukan sahaja menjadi kewajipan utama Ketua Jabatan bahkan ianya amanah yang perlu dipikul oleh semua penjawat UMT. Tanggungjawab ini adalah sejajar dengan perakuan yang ditandatangani oleh semua penjawat UMT apabila diterima berkhidmat untuk mematuhi semua peruntukan berkaitan Akta Rahsia Rasmi 1972. Namun dukacita, di era globalisasi yang membolehkan maklumat dicapai di hujung jari, berlaku penyebaran maklumat-maklumat rahsia dan sensitif yang boleh menjelaskan kredibiliti, integriti dan imej Universiti.

Justeru, UMT melalui Pejabat Pendaftar telah mengeluarkan Garis Panduan Pengurusan Rahsia Rasmi UMT pada tahun 2021. Objektif utama penyediaan Garis Panduan ini adalah untuk memastikan keselamatan dan tahap kerahsiaan dokumen rahsia rasmi di premis UMT sentiasa dilindungi dan selamat dari sebarang penyalahgunaan oleh pihak yang tidak bertanggungjawab dan sentiasa mematuhi Arahan Keselamatan (Semakan dan Pindaan 2017).

Selain daripada penjagaan dokumen rahsia rasmi, saya juga merasakan perlu ada mekanisme lanjut untuk mengekang kecurian atau kebocoran maklumat Universiti seperti keputusan tender, temuduga, idea penyelidikan dan sebagainya. Kita semua maklum, maklumat seperti ini selalunya disebarluaskan melalui telefon bimbit menggunakan aplikasi WhatsApp, Telegram dan lain-lain.

Bagi tujuan kawalan, saya berpandangan perlu ada satu garis panduan untuk menentukan zon larangan penggunaan telefon bimbit atau peralatan komunikasi lain yang mampu merakam maklumat seperti yang diamalkan oleh agensi-agensi Kerajaan yang lain. Ianya juga selaras dengan Surat Pekeliling Am Bilangan 1 Tahun 2021 yang dikeluarkan oleh Jabatan Perdana Menteri yang melarang penggunaan telefon bimbit dan peralatan komunikasi yang boleh merakam dalam mesyuarat penting Kerajaan.

Keskes kebocoran maklumat berkait rapat dengan integriti. Saya amat berharap warga UMT cemerlang sekelian dapat sama-sama bermuhasabah, adakah kita semua benar-benar berintegriti dalam menjalankan tanggungjawab kita kepada Universiti ini. Akhir sekali, saya mengucapkan tahniah kepada Pejabat Penasihat Undang-Undang UMT di atas penerbitan Legal Buzz pada kali ini. Semoga ianya memberikan ilmu yang bermanfaat kepada semua warga UMT.

Sekian, terima kasih.

**"Terokaan Seluas Lautan Demi Kelestarian Sejagat"**

#UMTsohor

#wargaUMTcemerlang

**Prof. Dato' Dr. Mazlan Abd Ghaffar, FASc**

Naib Canselor

Universiti Malaysia Terengganu

# DOKUMEN RASMI UMT: TERGUGAT? SELAMAT? DILINDUNGI?



MUHAMMAD HAFIZUDDIN ZAKARIA

Penolong Penasihat Undang-Undang Kanan UMT



## PENGENALAN

Urusan pentadbiran dan pengoperasian Universiti Malaysia Terengganu (UMT) tidak boleh lari daripada pengurusan berkenaan dengan dokumen rahsia rasmi. Pengurusan berkenaan dengan dokumen rahsia rasmi ini antara lainnya adalah dari sudut pendaftaran, pengelasan, penyimpanan, pengelasan semula serta pelupusan dokumen rahsia rasmi. Pengurusan dokumen rahsia rasmi yang cekap dapat mengelakkan berlakunya akses yang tidak dibenarkan serta dapat membantu memudahkan penyiasatan terhadap sebarang kebocoran maklumat rahsia rasmi (jika berlaku) [1]. Kegagalan menguruskan dokumen rahsia rasmi boleh menyebabkan penyalahgunaan maklumat yang boleh membawa mudarat dan menggangu gugat keamanan serta kesentosaan UMT khususnya dan negara amnya.

## DEFINISI

Rasmi boleh ditakrifkan sebagai apa juu perkara berhubungan dengan perkhidmatan awam di mana UMT merupakan sebuah badan berkanun yang ditubuhkan di bawah suatu akta persekutuan iaitu Akta Universiti dan Kolej Universiti 1971 [2]. Oleh yang demikian, segala perkara berkenaan dengan pengoperasian dan pentadbiran di UMT merupakan suatu perkara rasmi.

Rahsia rasmi pula boleh ditakrifkan sebagai apa-apa suratan yang dinyatakan dalam Jadual dalam Akta Rahsia Rasmi 1972 dan apa-apa maklumat dan bahan yang berhubungan dengannya dan termasuklah apa-apa suratan rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai "Rahsia Besar", "Rahsia", "Sulit" atau "Terhad" [3]. Dalam konteks UMT, Menteri Pengajian Tinggi telah melantik beberapa orang pegawai UMT sebagai pegawai pengelas [4] dalam menentukan dan mengelaskan peringkat keselamatan sesuatu dokumen rahsia rasmi di UMT [5].

## PERINGKAT DOKUMEN RAHSIA RASMI

Dokumen rahsia rasmi boleh dikelaskan kepada empat (4) kategori iaitu Rahsia Besar, Rahsia, Sulit dan Terhad.

**Rahsia besar** ertiinya dokumen/maklumat/bahan rasmi yang berada dalam jagaan UMT jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada kepentingan Malaysia [6]. Antara contoh dokumen rahsia rasmi yang diperingkatkan sebagai Rahsia Besar adalah seperti kertas Jemaah Menteri yang mengandungi maklumat yang sangat penting berkenaan perkara politik atau ekonomi negara. Selain itu, maklumat berkenaan dengan perdagangan dan pertahanan negara Malaysia juga diperingkat sebagai Rahsia Besar.

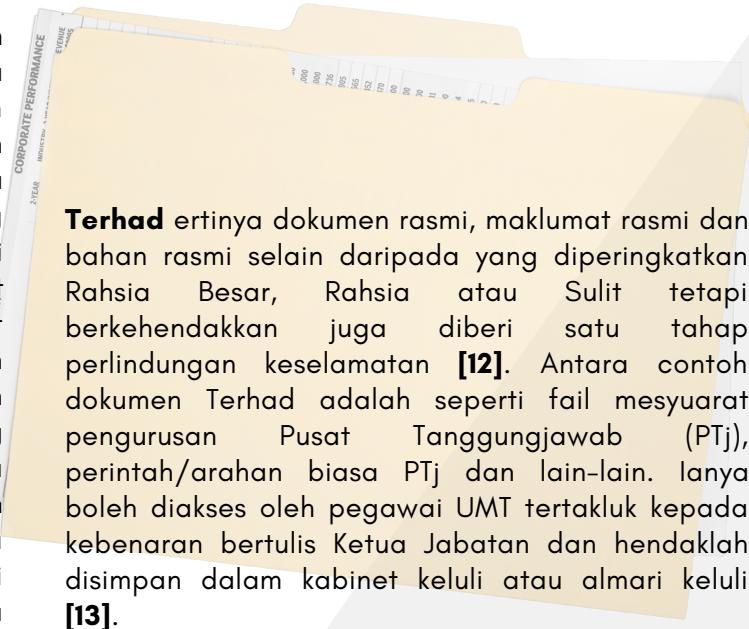
Rahsia Besar di UMT hanya boleh diakses oleh Naib Canselor dan mana-mana pegawai lain yang ingin mendapatkan akses kepada dokumen Rahsia Besar tersebut hendaklah mendapat kebenaran bertulis daripada Naib Canselor terlebih dahulu [7]. Dokumen Rahsia Besar hendaklah disimpan untuk sementara waktu di dalam almari keluli berkunci dan hendaklah dikembalikan semula ke dalam bilik kebal/peti besi setelah selesai urusan terhadap dokumen Rahsia Besar tersebut.

**Rahsia** pula ertiinya dokumen/maklumat/bahan rasmi yang berada dalam jagaan UMT jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan UMT dan/atau Malaysia [8]. Antara contoh dokumen rahsia rasmi yang diperangkatkan sebagai Rahsia adalah seperti kertas berkaitan Jemaah Menteri, maklumat berkenaan pertubuhan subversif atau maklumat berkenaan perundingan UMT/Malaysia dengan negara asing. Dokumen Rahsia boleh diakses oleh Ketua Jabatan di UMT manakala pegawai UMT yang lain dibenarkan untuk mendapatkan akses kepada dokumen Rahsia setelah mendapat kebenaran bertulis daripada Ketua Jabatan. Dokumen Rahsia hendaklah disimpan di dalam bilik kebal/peti besi setelah selesai urusan terhadap dokumen Rahsia tersebut [9].

## **Rahsia rasmi pula boleh ditakrifkan sebagai apa-apa suratan yang dinyatakan dalam Jadual dalam Akta Rahsia Rasmi 1972 dan apa-apa maklumat dan bahan yang berhubungan dengannya dan termasuklah apa-apa suratan rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”, “Sulit” atau “Terhad”**

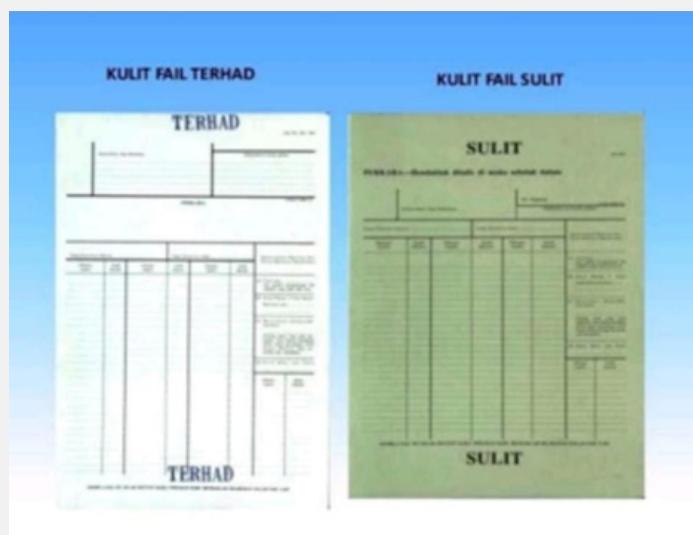
**Sulit** ertiinya dokumen/maklumat/bahan rasmi yang berada dalam jagaan UMT jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan Malaysia, kegiatan Kerajaan atau UMT tetapi memudaratkan kepentingan Malaysia, kegiatan Kerajaan, UMT, orang perseorangan atau akan menyebabkan keadaan memalukan, kesusahan kepada pentadbiran atau akan menguntungkan sesebuah pihak luar atau kuasa asing [10].

Dalam konteks UMT, antara contoh dokumen Sulit adalah seperti laporan siasatan salahlaku, kertas mesyuarat Lembaga Pengarah/Pengurusan UMT, maklumat berhubung kewangan UMT, soalan peperiksaan dan fail kes perundangan. Pegawai UMT boleh mengakses dokumen Sulit tertakluk kepada kebenaran bertulis daripada Ketua Jabatan bagi tujuan urusan kerja rasmi. Dokumen Sulit hendaklah disimpan dalam kabinet keluli atau dalam bilik berkunci di pejabat masing-masing [11].



**Terhad** ertiinya dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperangkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan [12]. Antara contoh dokumen Terhad adalah seperti fail mesyuarat pengurusan Pusat Tanggungjawab (PTj), perintah/arahan biasa PTj dan lain-lain. Ianya boleh diakses oleh pegawai UMT tertakluk kepada kebenaran bertulis Ketua Jabatan dan hendaklah disimpan dalam kabinet keluli atau almari keluli [13].

Walau apa pun, Pegawai Pengelas [14] berhak untuk menentukan klasifikasi sesuatu dokumen rahsia rasmi samada ada Rahsia Besar, Rahsia, Sulit atau Terhad yang berada di luar Jadual Akta Rahsia Rasmi 1972. Fail dokumen rahsia rasmi ini hendaklah ditandakan seperti mana contoh-contoh berikut:



## **TATACARA PENGHANTARAN/MEMBAWA KELUAR DOKUMEN RAHSIA RASMI**



Penghantaran dokumen rahsia rasmi boleh dibuat melalui sampul surat mahupun beg berkunci dengan menggunakan Borang Jadual Penghantaran Dokumen Rasmi ("Borang Penghantaran Dokumen Rasmi") sepetimana di Lampiran B Garis Panduan Pengurusan Rahsia Rasmi UMT 2021.

Penghantaran dokumen rahsia rasmi melalui pos hendaklah dibuat melalui sistem dua sampul surat. Sampul surat sebelah dalam hendaklah ditandakan dengan peringkat keselamatan dan nombor rujukan dokumen rahsia rasmi berkenaan serta nama dan alamat penerimanya dan dimeterikan dengan meteri atau pelekat keselamatan PTj yang menghantar. Sampul surat tersebut kemudiannya hendaklah dimasukkan ke dalam sampul surat lain yang bertulis nama dan alamat penerimanya sahaja dan dilekatkan dengan gam [15].

Penghantaran dokumen rahsia rasmi melalui sistem Beg Berkunci pula hanyalah menggunakan satu sampul surat sahaja. Sampul tersebut hendaklah ditandakan dengan peringkat keselamatan dan nombor rujukan dokumen berkenaan serta nama dan alamat penerimanya dan dimeterikan dengan meteri atau pelekat keselamatan PTj yang menghantar [16].

Borang Penghantaran Dokumen Rasmi hendaklah digunakan bagi setiap penerima dokumen rahsia rasmi yang dihantar. Ianya hendaklah diisi dalam dua salinan di mana salinan asal hendaklah dihantar bersekali kepada penerima dokumen rahsia rasmi. Pengesahan resit akuan penerimaan dokumen rahsia rasmi daripada penerima hendaklah diperoleh dan sekiranya tidak diperoleh dalam masa 7 hari, penyiasatan berkenaan keberadaan dokumen rahsia rasmi tersebut hendaklah dibuat. Penghantar dokumen rahsia rasmi juga hendaklah memberi peringatan kepada penerima untuk mengembalikan semula resit akuan penerimaan dokumen rahsia rasmi sebagai rekod.

Dokumen rahsia rasmi hanya boleh dibawa keluar daripada pejabat atas urusan rasmi sahaja. Dokumen rahsia rasmi yang diperingkatkan sebagai Rahsia Besar atau Rahsia hanya boleh dibawa keluar daripada premis UMT setelah mendapat kebenaran bertulis daripada Naib Canselor manakala bagi dokumen rahsia rasmi yang diperingkatkan sebagai Sulit dan Terhad, kebenaran bertulis daripada Ketua Jabatan adalah memadai. Suatu daftar rekod pengeluaran dokumen rahsia rasmi hendaklah diwujudkan bagi memastikan dokumen rahsia rasmi yang dibawa keluar daripada PTj/UMT adalah direkodkan.

**"Borang Penghantaran Dokumen Rasmi hendaklah digunakan bagi setiap penerima dokumen rahsia rasmi yang dihantar. Ianya hendaklah diisi dalam dua salinan di mana salinan asal hendaklah dihantar bersekali kepada penerima dokumen rahsia rasmi. Pengesahan resit akuan penerimaan dokumen rahsia rasmi daripada penerima hendaklah diperoleh"**

## **PERANAN PEGAWAI PENGELAS DAN PENDAFTAR RAHSIA KECIL/BESAR**

Pegawai Pengelas dan Pendaftar Rahsia Kecil/Besar yang dilantik dalam kalangan staf UMT adalah bertujuan bagi memastikan proses pengurusan rahsia rasmi UMT dapat dilaksanakan selaras dengan peruntukan yang dinyatakan dalam Garis Panduan Pengurusan Rahsia Rasmi UMT 2021 dan Arahan Keselamatan (Semakan dan Pindaan) 2017. Pegawai Pengelas dan Pendaftar Rahsia Kecil/Besar hendaklah saling bekerjasama dalam proses pengelasan dokumen. Secara asasnya, dokumen-dokumen yang dimulakan (pembuat dokumen) di PTj masing-masing hendaklah disemak, dinilai, ditandakan peringkat keselamatan, didaftarkan dan ditandatangan oleh Pegawai Pengelas di dalam Buku Daftar Am 492, Buku Daftar Am 492A dan Buku Daftar Am 492B. Bagi dokumen rasmi, maklumat rasmi dan bahan rasmi yang diterima daripada agensi luar, ianya hendaklah didaftarkan di dalam Buku Daftar Am 10 (Dokumen Terperingkat).

Kegagalan mematuhi proses ini boleh menyebabkan sesuatu dokumen rahsia rasmi itu secara teknikalnya bukan suatu rahsia rasmi dan jika didedahkan/dibocorkan tindakan pendakwaan di bawah Akta Rahsia Rasmi 1972 tidak dapat dilaksanakan.

Ianya telah dinyatakan oleh hakim dalam kes **Prem Kumar a/l Pandel Rangam v Pendakwa Raya [17]** di mana sesuatu dokumen rahsia rasmi hendaklah didaftarkan dalam Buku 492A dan dikelaskan oleh Pegawai Pengelas yang dilantik oleh Menteri di bawah Seksyen 2B Akta Rahsia Rasmi 1972.

## KESAN PELANGGARAN

Objektif utama pengurusan dokumen rahsia rasmi adalah untuk mengelakkan kehilangan dan kebocoran maklumat. Seandainya berlaku kehilangan dokumen rahsia rasmi, ianya hendaklah dilaporkan dengan segera kepada Pegawai Keselamatan UMT atau Naib Canselor [18]. Suatu siasatan berkenaan kehilangan dokumen rahsia rasmi tersebut hendaklah dibuat dan laporan siasatan tersebut diserahkan kepada Naib Canselor. Naib Canselor pula hendaklah melaporkan kehilangan dokumen rahsia rasmi tersebut kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia Negeri Terengganu dalam tempoh 24 jam [19].

Pegawai UMT yang didapati cuai atau tidak mematuhi prosedur pengurusan dokumen rahsia rasmi atau dengan sengaja menyebabkan kehilangan atau pembocoran maklumat rahsia rasmi boleh dikenakan tindakan tatatertib di bawah Akta Badan-Badan Berkanun (Tatatertib & Surcaj) 2000 sehingga boleh dikenakan hukuman buang kerja. Dalam keadaan yang lebih serius, pegawai UMT tersebut boleh didakwa di mahkamah di bawah Seksyen 8 Akta Rahsia Rasmi 1972 dan boleh dikenakan hukuman tidak kurang dari setahun dan tidak lebih dari 7 tahun.

Berdasarkan kes **Prem Kumar a/l Pandel Rangam v Pendakwa Raya [20]** tertuduh telah didakwa di mahkamah di bawah Seksyen 8(1) (c) (iii) Akta Rahsia Rasmi kerana telah membocorkan maklumat rahsia rasmi berkenaan dengan soalan peperiksaan Ujian Penilaian Sekolah Rendah (UPSR) tahun 2014 bagi mata pelajar Matematik, Sains dan Tamil melalui perkongsian di aplikasi WhatsApps. Mahkamah mendapati tertuduh adalah bersalah di bawah Akta Rahsia Rasmi 1972 dan dijatuhkan hukuman penjarा selama 3 tahun.

## KESIMPULAN

Teknologi masa kini memudahkan pembocoran dan penyalahgunaan dokumen rahsia rasmi berlaku. Namun, setiap pegawai UMT yang diamanahkan atau mempunyai akses kepada dokumen rahsia rasmi UMT hendaklah menjaga dan mematuhi peraturan berkenaan dengan pengurusan dokumen rahsia rasmi UMT sepetimana yang termaktub di dalam Garis Panduan Pengurusan Rahsia Rasmi UMT. Prinsip [21] "Perlu Mengetahui", "Perlu Menyimpan" dan "Lihat serta Kembalikan" hendaklah diterapkan dalam pengurusan dokumen rahsia rasmi di UMT. Pengurusan dokumen rahsia rasmi yang sistematik dapat melindungi dokumen rahsia rasmi daripada disalahguna, dimanipulasi atau disebarluaskan kepada pihak-pihak yang tidak bertanggungjawab sekaligus kepentingan UMT dan kerajaan sentiasa dapat dipelihara.

## Nota Hujung:

1. Perenggan 76, Bab 4, Keselamatan Rahsia Rasmi, Arahan Keselamatan (Semakan dan Pindaan) 2017
2. Dr Che Wan Fadhil Che Wan Putra & Yang Lain v Universiti Teknologi Malaysia [2010] 8 CLJ 845
3. Seksyen 2, Akta Rahsia Rasmi 1972
4. Pegawai Pengelas dilantik oleh Menteri Pengajian Tinggi di bawah Seksyen 2B Akta Rahsia Rasmi 1972
5. Seksyen 2B, Akta Rahsia Rasmi 1972
6. Bab 1, Tafsiran, Arahan Keselamatan (Semakan dan Pindaan) 2017
7. Perenggan 5.3.1 (c), Garis Panduan Pengurusan Rahsia Rasmi UMT 2021
8. Bab 1, Tafsiran, Arahan Keselamatan (Semakan dan Pindaan) 2017
9. Perenggan 5.3.2 (e), Garis Panduan Pengurusan Rahsia Rasmi UMT 2021
10. Rahsia Rasmi UMT 2021
11. Bab 1, Tafsiran, Arahan Keselamatan (Semakan dan Pindaan) 2017
12. Bab 1, Tafsiran, Arahan Keselamatan (Semakan dan Pindaan) 2017
13. Perenggan 5.3.4 (g), Garis Panduan Pengurusan Rahsia Rasmi UMT 2021
14. Pegawai Pengelas di UMT dilantik oleh Menteri Pengajian Tinggi di bawah Seksyen 2B Akta Rahsia Rasmi 1972
15. Perenggan 5.4 (d), Garis Panduan Pengurusan Rahsia Rasmi UMT 2021
16. Perenggan 5.4 (c), Garis Panduan Pengurusan Rahsia Rasmi UMT 2021
17. [2019] MLJU 2167
18. Perenggan 5.6 (a), Garis Panduan Pengurusan Rahsia Rasmi UMT 2021
19. Perenggan 5.6 (b), Garis Panduan Pengurusan Rahsia Rasmi UMT 2021
20. [2019] MLJU 2167
21. Perenggan 18, 19 dan 20 Arahan Keselamatan (Semakan dan Pindaan) 2017



# KEPENTINGAN "NON-DISCLOSURE AGREEMENT" DALAM PENGURUSAN PENYELIDIKAN DAN PENGKOMERSIALAN UNIVERSITI



**ROSLINA GHAZALI**

Timbalan Penasihat Undang-Undang UMT

## APA ITU NON-DISCLOSURE AGREEMENT?

Non-Disclosure Agreement (NDA) atau perjanjian kerahsiaan bolehlah didefinisikan sebagai suatu perjanjian atau kontrak antara sekurang-kurangnya dua pihak mengenai penggunaan atau pendedahan maklumat bukan umum (*non-public information*) tertentu yang dimiliki oleh pihak-pihak yang berkaitan. Maklumat yang didedahkan melalui NDA ini biasanya dirujuk sebagai "Maklumat Sulit" (*Confidential Information*).

Tidak ada definisi atau senarai khusus mengenai apa yang boleh terkandung sebagai Maklumat Sulit. Setiap pihak mungkin mempunyai definisi yang berbeza mengenai dokumen atau maklumat yang diklasifikasikan sebagai sulit. Justeru, apa yang termasuk dalam kategori Maklumat Sulit hendaklah ditentukan oleh pihak-pihak. Pihak yang mendedahkan Maklumat Sulit biasanya menafsirkan Maklumat Sulit seluas mungkin untuk memastikan tidak ada penyalahgunaan maklumat oleh pihak yang satu lagi atau pihak ketiga yang lain. Maklumat Sulit adalah sejenis harta intelek atau kebiasaan juga dirujuk sebagai Rahsia Perdagangan (*Trade Secret*).

Tujuan utama NDA adalah untuk menghalang pihak-pihak menggunakan Maklumat Sulit yang dikongsi tersebut untuk tujuan yang tidak berkaitan dengan maksud perjanjian atau mendedahkannya kepada mana-mana pihak lain yang mana pendedahan tersebut boleh menjelaskan hak dan kepentingan pemilik Maklumat Sulit yang berkaitan.

Secara ringkasnya tujuan NDA boleh dijelaskan seperti Rajah di bawah:

## TUJUAN NDA?

01

### KLASIFIKASI MAKLUMAT SULIT

NDA secara jelas menggariskan maklumat apa diklasifikasi sebagai Maklumat Sulit. Ia juga menjelaskan kenapa Maklumat Sulit tersebut dipersetujui untuk didedahkan kepada pihak-pihak.

02

### MELINDUNGİ MAKLUMAT SULIT

NDA menghalang pihak-pihak menggunakan Maklumat Sulit yang didedahkan untuk tujuan selain daripada yang dipersetujui. Pihak-pihak juga dihalang dari mendedahkan Maklumat Sulit tersebut kepada pihak lain.

03

### REMEDI JIKA BERLAKU PELANGGARAN PERJANJIAN

Jika berlaku sebarang pelanggaran syarat-syarat NDA, pihak yang terjejas boleh menuntut remedii atau gantirugi daripada pihak yang melakukan pelanggaran tersebut.

NDA boleh bersifat "unilateral" atau "bilateral" bergantung kepada persetujuan pihak-pihak. Unilateral NDA adalah suatu kontrak yang melibatkan dua pihak. Satu pihak mendedahkan Maklumat Sulit itu, sementara pihak penerima mempunyai kewajiban untuk melindungi Maklumat Sulit tersebut. Bilateral NDA pula ialah apabila kedua-dua pihak saling mendedahkan Maklumat Sulit masing-masing dengan tujuan untuk melindungi maklumat tersebut daripada pihak luar.

## BILAKAH NDA PERLU DITANDATANGANI?

Dalam konteks penyelidikan atau pengkomersialan di UMT, NDA biasanya merupakan dokumen perjanjian pertama yang perlu ditandatangani sebelum rundingan lebih serius dibuat dengan pihak pemberi dana atau entiti perniagaan yang berminat untuk mengkomersialkan harta intelek UMT.

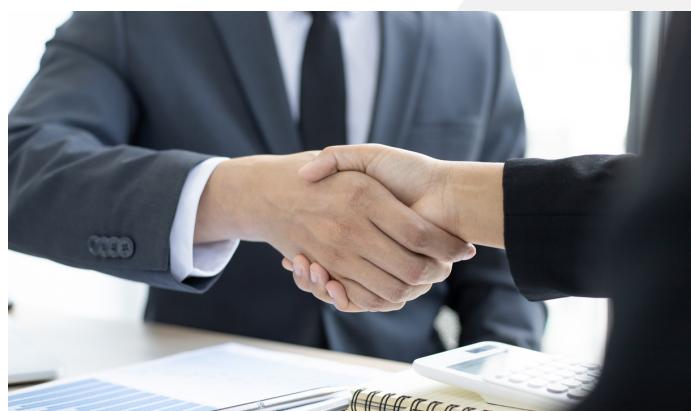
Walau bagaimanapun keperluan untuk melindungi Maklumat Sulit melalui NDA ini boleh mempunyai tujuan yang pelbagai dan tidak terhad kepada aktiviti penyelidikan dan pengkomersialan sahaja. NDA kebiasaannya perlu juga ditandatangani dalam situasi-situasi berikut:



- (1) Semasa mendapatkan perkhidmatan dari syarikat atau individu di mana syarikat atau individu tersebut akan diberikan Maklumat Sulit institusi anda. Contohnya ketika berurusan dengan pihak Bank berkaitan apa-apa pinjaman, pelaburan dan sebagainya.
- (2) Apabila pekerja diberi akses kepada Maklumat Sulit semasa menjalankan tugas. Kebiasaannya klausa kerahsiaan ini telah dimasukkan dalam kontrak pekerjaan.
- (3) Semasa membentangkan idea perniagaan atau pengkomersialan kepada bakal rakan kongsi atau pelabur yang berpotensi. Dalam hal ini, NDA sangat penting untuk melindungi idea anda daripada dicuri.
- (4) Semasa berkongsi maklumat kewangan, undang-undang, dapatan penyelidikan, produk baharu, harta intelek dan sebagainya dengan bakal pelabur, pembeli, pelesen atau rakan kongsi.

## TERMA-TERMA PENTING YANG PERLU ADA DALAM NDA

Walaupun NDA pada kebiasaannya bukan suatu dokumen yang sarat dan rumit, namun terma-terma penting yang diperlukan dalam NDA tersebut perlu difahami sewajarnya bagi mengelakkan pelanggaran kontrak hingga menyebabkan kebocoran Maklumat Sulit.



### (1) Pihak-Pihak

Pihak-pihak kepada NDA perlu diperincikan dengan tepat. Namun, dalam sesetengah keadaan, oleh kerana organisasi telahpun menyediakan template NDA, maklumat pihak yang satu lagi dibiarkan kosong dan tidak dilengkapkan sewajarnya. Pihak ini juga mestilah mempunyai "locus standi" atau kuasa untuk memasuki NDA.

### (2) Tujuan NDA

Tujuan NDA perlu dinyatakan dengan jelas bagi memastikan Maklumat Sulit yang dikongsi hanya digunakan untuk tujuan tersebut. Sebagai contoh, NDA yang ditandangani antara UMT dan Agensi XYZ adalah untuk membuat kajian berkaitan kebolehpasaran graduan perikanan UMT di Malaysia. Maka, apa-apa Maklumat Sulit yang dikongsikan oleh UMT dengan Agensi XYZ tidak boleh digunakan untuk maksud selain yang dinyatakan dalam NDA.

### (3) Definisi Maklumat Sulit

Takrifan Maklumat Sulit hendaklah jelas dan dipersetujui bersama oleh pihak-pihak. Walaupun, takrifan yang umum dan luas biasa digunakan dalam NDA, dalam sesetengah keadaan, Maklumat Sulit disenaraikan mengikut tujuan perjanjian. Sebagai contoh, dalam NDA yang dimeterai bagi tujuan penyelidikan, pihak-pihak menyenaraikan jenis-jenis Maklumat Sulit yang akan dikongsikan berkaitan penyelidikan tersebut.

#### (4) Obligasi Pihak-Pihak

NDA yang baik hendaklah menyenaraikan tanggungjawab pihak-pihak berkaitan dengan pengurusan/penjagaan Maklumat Sulit yang didedahkan. Salah satu contoh obligasi yang penting ada penegasan bahawa pihak yang menerima Maklumat Sulit tidak boleh menggunakan maklumat yang diperolehi tersebut untuk tujuan selain daripada yang telah dipersetujui. Tanggungjawab lain pula, adalah menjaga keselamatan Maklumat Sulit daripada kecurian, kebocoran dan sebagainya.

#### (5) Pengecualian

Peruntukan pengecualian ini menyenaraikan keadaan-keadaan di mana Maklumat Sulit tersebut tidak lagi boleh diklasifikasikan sebagai sulit sebagaimana takrifan dalam NDA. Pengecualian yang biasa ada dalam sesbuah NDA adalah seperti berikut:

- (1) Maklumat Sulit telah menjadi maklumat awam;
- (2) Maklumat Sulit telah diketahui terlebih dahulu oleh pihak yang menerimanya daripada sumber yang lain; atau
- (3) Maklumat Sulit tersebut telah diarahkan untuk didedahkan oleh pihak berkuasa dalam suatu prosiding Mahkamah.

#### (6) Tempoh NDA

Tarikh kuat kuasa dan tempoh kesahan NDA hendaklah dinyatakan secara jelas. Tempoh NDA ini boleh bersifat kekal (*perpetual*) bergantung kepada kepentingan sesuatu Maklumat Sulit itu. Jika perjanjian yang dimasuki oleh pihak-pihak melibatkan pendedahan "rahsia perdagangan" atau "trade secrets" adalah wajar tanggungjawab menjaga kerahsiaan tersebut adalah bersifat kekal dan tidak bertempoh. Manakala bagi Maklumat Sulit yang mungkin akan didedahkan kepada umum kemudian, tiada keperluan untuk NDA bersifat kekal.



#### (7) Hak Milik Maklumat Sulit

Hak pemilikan terhadap Maklumat Sulit yang dikongsi hendaklah dijelaskan dalam NDA. Ini bagi mengelakkan pihak yang menerima Maklumat Sulit tersebut beranggapan ia turut mempunyai hak dan kepentingan ke atas Maklumat Sulit tersebut.

#### (8) Kesan Pelanggaran NDA dan Remedies

Pihak-pihak kepada NDA perlu dijelaskan tentang kesan perlenggaran mana-mana peruntukan atau obligasi NDA yang ditandatangani. Tiga jenis tindakan yang boleh diambil jika berlaku perlenggaran NDA iaitu tuntutan ganti rugi, injunksi dan *equitable relief* sebagaimana yang diterangkan dalam Rajah di bawah.



##### TUNTUTAN GANTI RUGI

Permohonan kepada Mahkamah tuntutan berdasarkan kerugian yang dialami sama ada yang boleh dikira ataupun tidak.



##### PERINTAH INJUNKSI

Permohonan kepada Mahkamah menghalang pihak yang berkaitan daripada terus mengguna atau mendedahkan Maklumat Sulit.



##### EQUITABLE RELIEF

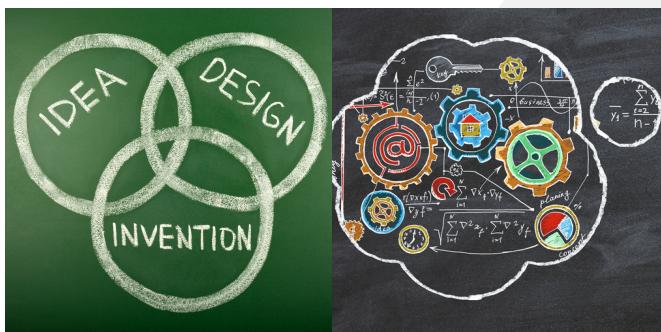
Permohonan kepada Mahkamah mengenai lain-lain bentuk pampasan yang bersesuaian.

Dalam kes **Svenson Hair Center Sdn Bhd v Irene Chin Zee Ling [2008] 7 MLJ 903**, Mahkamah telah membenarkan permohonan injunksi interim oleh Plaintiff untuk menyekat Defendan daripada menghubungi semua atau mana-mana pelanggan Plaintiff yang dikenali oleh Defendan semasa Defendan berkhidmat dengan Plaintiff. Permohonan injunksi ini dipohon oleh Plaintiff selaras dengan perjanjian pekerjaan yang ditandatangani oleh Defendan yang mengandungi larangan khusus berkaitan dengan maklumat sulit mengenai butir-butir pelanggan Plaintiff. Mahkamah dalam kes ini mengatakan bahawa maklumat pelanggan tidak boleh menjadi sebahagian daripada "*own skill, knowledge and business experience*" Defendan. Walaupun persaingan dalam perniagaan adalah dibenarkan, namun menggunakan maklumat sulit secara salah seperti yang dilakukan oleh Defendan adalah melanggar peruntukan kerahsiaan yang ditandatangani.

## KEPENTINGAN NDA DALAM PENGURUSAN PENYELIDIKAN DAN PENGKOMERSIALAN

Sesuatu "idea" tidak dilindungi di bawah undang-undang. Seksyen 7 (2A), Akta Hak Cipta 1987 memperuntukkan bahawa, "perlindungan hak cipta tidaklah terpakai kepada apa-apa idea, prosedur, kaedah pengendalian atau konsep matematik". Sementara dalam pengurusan projek penyelidikan dan pengkomersialan, maklumat penting yang biasa akan dikongsikan semasa perundingan adalah "idea" dan cadangan yang boleh menyelesaikan sesuatu masalah atau menghasilkan keuntungan kewangan. Oleh kerana tiada undang-undang yang melindungi "idea", sering berlaku "idea" ini dicuri atau diciplak tanpa pengiktirafan (*recognition*) yang sewajarnya kepada penyelidik dan universiti.

Selain "idea", penyelidik juga mungkin akan mendedahkan maklumat berkaitan dapatan hasil penyelidikan, penemuan atau rekacipta (*invention*) yang berpotensi untuk dilindungi di bawah undang-undang harta intelek yang merangkumi paten, hak cipta, reka bentuk industri, trade secret, cap dagangan, petunjuk geografi dan perlindungan varieti baru tumbuhan. Sekiranya maklumat berkaitan penemuan, hasil penyelidikan atau rekacipta ini dikongsikan dengan pihak industri atau mana-mana institusi lain tanpa NDA, ianya boleh dianggap sebagai pendedahan awam (public disclosure). Pendedahan awam boleh menyebabkan hilangnya keupayaan universiti untuk mematenkan sesuatu rekacipta atau sesuatu formula atau proses yang sepatutnya menjadi rahsia perdagangan tidak lagi dilindungi kerahsiaannya di bawah undang-undang.



Rundingan mengenai pengkomersialan pula biasanya melibatkan pendedahan mengenai harta intelek universiti. Walaupun harta intelek yang telah didaftarkan dilindungi di bawah undang-undang, namun maklumat-maklumat lain berkaitan harta intelek tersebut mungkin tidak dilindungi seperti maklumat teknikal, "*know-how*", spesifikasi bahan dan sebagainya. Maklumat-maklumat ini juga, jika didedahkan tanpa kawalan boleh disalahgunakan ataupun di"*reverse engineer*" oleh pihak yang tidak bertanggungjawab.

Selanjutnya, sesuatu perundingan juga melibatkan pendedahan maklumat kewangan sama ada berkaitan kos penyelidikan, jumlah tajaan, cadangan harga jualan dan sebagainya. Maklumat kewangan ini sangat penting dalam mana-mana proses perundingan penyelidikan dan pengkomersialan. Kegagalan untuk melindungi maklumat-maklumat ini dari disebarluaskan kepada pihak ketiga yang tiada kaitan dalam perundingan boleh menyebabkan kerugian kepada universiti atau menimbulkan persaingan yang tidak wajar.

Dalam kes, **Electro CAD Australia Pty Ltd & Ors v. Mejati RCS Sdn. Bhd. & Ors [1998] 3 MLJ 422**, perlanggaran terhadap peruntukan kerahsiaan yang ditandangani melalui NDA menjadi kausa utama tuntutan plaintif. Dalam kes ini, plaintif pertama dan ketiga adalah syarikat yang diperbadankan di Australia, merupakan pemilik hak harta intelek dalam *Stopcard Auto Theft Device* ("Stopcard"). Plaintiff kedua diperbadankan di Malaysia untuk memasarkan Stopcard di Malaysia. Plaintiff ketiga telah mengikat perjanjian pelesenan dengan sebuah syarikat di mana defendant kedua adalah pengarah. Defendant kedua kemudiannya menjadi pengarah plaintif kedua dan telah menandatangani NDA bagi melindungi maklumat berkaitan Stopcard. Selepas itu, defendant kedua berhenti bekerja dengan plaintif kedua. Maklumat sulit berkaitan dengan Stopcard telah diberikan kepada defendant pertama oleh defendant kedua. Pada 30 November 1995, "Stopcar" dilancarkan oleh defendant pertama. Plaintiff-plaintif mendakwa bahawa barang keluaran defendant-defendant yang dinamakan "Stopcar" adalah berasal daripada Stopcard.

Mahkamah Tinggi Kuala Lumpur bersetuju dengan hujahan plaintiff-plaintif dan memutuskan bahawa defendant pertama, melalui pekerjanya, telah melanggar perjanjian kerahsiaan yang ditandatangani. Adalah juga jelas bahawa defendant kedua telah mendedahkan kepada defendant-defendant untuk kegunaan dan manfaat mereka maklumat sulit dan rahsia perniagaan berkaitan dengan barang keluaran plaintiff-plaintif. Seorang pengarah, seperti defendant kedua, adalah dihalang daripada menggunakan apa-apa manfaat yang diperolehi oleh sebab kedudukannya sebagai pengarah, terutamanya berkaitan dengan maklumat sulit yang diperolehi, selepas beliau berhenti kerja lebih-lebih lagi apabila pemberhentiannya dilihat sebagai didorong oleh hasrat untuk memperolehi keuntungan bagi dirinya sendiri. Oleh itu, plaintiff-plaintif adalah berhak untuk mendapat perintah injunksi terhadap defendant-defendant beserta dengan ganti rugi seperti yang dituntut.

## PERLINDUNGAN MAKLUMAT DALAM PENYELIDIKAN DAN PENGKOMERSIALAN

### IDEA / PROPOSAL

Melindungi idea, cadangan, kertas kerja dan sebagainya

### HARTA INTELEK

Memastikan maklumat berkaitan harta intelek universiti tidak disalahgunakan atau didedahkan kepada pihak ketiga.

### DAPATAN HASIL PENYELIDIKAN

Melindungi dapatan hasil penyelidikan daripada digunakan oleh pihak lain tanpa memberi apa-apa keuntungan kepada universiti.

### PRODUK BAHRU

Memastikan tiada imitasi produk-produk yang dihasilkan oleh universiti.

### PERINCIAN KEWANGAN

Melindungi maklumat berkaitan kewangan, hak milik atau harta universiti.

## KESIMPULAN

Aktiviti penyelidikan dan pengkomersialan harta intelek universiti merupakan salah satu agenda penting negara. Pelbagai inisiatif telah disediakan oleh Kementerian Pengajian Tinggi Malaysia (KPTM) dan Kementerian Sains, Teknologi dan Inovasi (MOSTI) bagi merancakkan pembangunan harta intelek dan teknologi, seterusnya mempercepat pengkomersialan. Namun dalam keterujaan para penyelidik universiti menyahut seruan Kerajaan ini, kadang-kala perkara-perkara asas dalam perundingan tidak dititik-beratkan sehingga akhirnya merugikan penyelidik dan universiti.

Pemeteraian NDA adalah perkara asas sebelum memulakan apa-apa proses perundingan. Seperti yang dibincangkan sebelum ini, NDA adalah penting bagi melindungi Maklumat Sulit universiti serta idea dan penemuan penyelidikan yang belum dilindungi atau tidak layak mendapat perlindungan harta intelek. Tuntasnya, NDA bukan suatu dokumen yang boleh dianggap remeh, bahkan kewujudannya sangat penting dalam membantu melancarkan proses perundingan penyelidikan atau pengkomersialan harta intelek universiti.

## KESAN JIKA NDA TIDAK DITANDATANGANI

Setelah kita mengetahui kepentingan dan keperluan untuk menandatangani NDA sebelum memulakan suatu rundingan bagi apa-apa projek penyelidikan dan pengkomersialan, maka selanjutnya diperincikan implikasi yang mungkin ditanggung oleh penyelidik atau universiti jika NDA tidak ditandatangani.

### (1) Tiada Perlindungan

Maklumat Sulit universiti tidak akan dilindungi dan boleh digunakan oleh pihak lain tanpa apa-apa sekatan.

### (2) Tiada Remedii

Tiada tindakan dapat diambil terhadap pihak yang mendedahkan atau menggunakan Maklumat Sulit.

### (3) Terdedah kepada Plagiat

Idea, kertas cadangan, rangka kerja dan sebagainya akan terdedah kepada plagiat.

### (4) Pendaftaran Harta Intelek

Mengganggu proses pendaftaran harta intelek.

### Rujukan:

1. <https://malaysianlitigator.com/2020/06/22/non-disclosure-agreement-when-to-use-it/>
2. <https://www.kass.com.my/confidentiality-agreement/>
3. The role of a non-disclosure agreement on the protection of intellectual property rights, Chinara Gasimova, LL. B., Baku State University, 2020
4. <https://harperjames.co.uk/article/non-disclosure-agreements-ndas-and-confidentiality-agreements-faqs/>
5. Ke Arah Pengkomersialan: Pengurusan Harta Intelek
6. Harta Intelek yang Optimum, Memperkasa Pendapatan Institusi, Kamal Kormin, MyIPO, 2015
7. <https://www.copperharbor.org/nda-agreement-malaysia/>
8. <https://dnh.com.my/latest-federal-court-case-employees-obligations-of-confidentiality/>
9. <https://asklegal.my/p/private-and-confidential-malaysia-breach-of-confidence>
10. Restraint of Trade: Emerging Trends 2016 2 MLJ xlvii



# TANGGUNGJAWAB BEKAS PEKERJA TERHADAP PERJANJIAN KERAHSIAAN



**AMIRAH NABILAH ISMAIL**

Penolong Penasihat Undang-Undang UMT

## PENDAHULUAN

Obligasi atau arahan untuk menjaga kerahsiaan dalam pekerjaan bukanlah suatu perkara yang asing. Seseorang yang diambil bekerja akan diminta untuk menandatangani akaun janji kerahsiaan sama ada secara khusus melalui perjanjian kerahsiaan (*Non-disclosure Agreement*) atau obligasi tersebut dimasukkan dalam kontrak pekerjaannya. Bagi sesetengah syarikat atau agensi, seseorang pekerja itu dikehendaki menandatangani perjanjian kerahsiaan semasa melapor diri di tempat kerja. Dalam konteks Universiti Malaysia Terengganu (UMT) pula, arahan menjaga kerahsiaan ini dimasukkan dalam kontrak perkhidmatan. Perjanjian atau obligasi ini adalah bertujuan untuk melindungi kerahsiaan maklumat syarikat atau agensi semasa berurusan dengan pihak luar. Maklumat-maklumat seperti data peribadi staf dan pelajar, kewangan, keputusan mesyuarat, harta intelek, inovasi dan idea penyelidikan adalah sangat penting bagi institusi pengajian tinggi seperti UMT. Jika maklumat-maklumat tersebut tidak dilindungi, dikhawatirkan akan menyebabkan penyalahgunaan oleh pihak yang tidak bertanggungjawab sekali gus memberikan kesan negatif kepada UMT.

## IKATAN KERAHSIAAN

Adalah dimaklumi bahawa perjanjian kerahsiaan adalah bertujuan untuk mendapatkan jaminan kerahsiaan daripada seseorang pekerja sepanjang perkhidmatannya dengan syarikat atau agensi tersebut. Namun selepas seseorang pekerja itu berhenti atau tidak lagi berkhidmat di syarikat atau agensi terbabit, adakah perjanjian atau akujanji kerahsiaan tersebut masih mengikatnya?

Persoalan ini telah dirungkaikan dalam keputusan kes **Dynacast (Melaka) Sdn Bhd & Ors v Vision Cast Sdn Bhd & Another [2016] 3 MLJ 417** yang telah dibuat oleh Mahkamah Persekutuan pada 16 Mei 2016. Kes ini melibatkan Encik Cheok, seorang pekerja yang memegang pelbagai jawatan peringkat tinggi dalam kumpulan syarikat Dynacast. Beliau telah mula bekerja dari tahun 1980 sehingga 2002. 15 bulan selepas peletakan jawatan beliau daripada kumpulan Dynacast, beliau telah menubuhkan satu syarikat yang bersaing dengan Dynacast. Lanjutan daripada penubuhan syarikat tersebut, Dynacast telah menyaman Encik Cheok dan mendakwa bahawa beliau telah menyalahgunakan maklumat sulit kumpulan syarikat tersebut dengan tujuan untuk menganggu projek Dynacast yang sedang berjalan dan bersaing dengan kumpulan Dynacast. Dynacast seterusnya cuba untuk menguatkuasakan perjanjian kerahsiaan yang telah ditandatangani oleh Encik Cheok semasa beliau masih menjadi pekerja Dynacast.

Keputusan Mahkamah Persekutuan telah memihak kepada Encik Cheok. Dalam membuat keputusan ini, Mahkamah Persekutuan telah menjawab tiga persoalan penting yang dibangkitkan oleh pihak-pihak.

**Persoalan pertama:** Adakah tanggungjawab seseorang pekerja untuk menjaga kerahsiaan organisasi itu kekal untuk selama-lamanya?

Dalam kes ini, perjanjian kerahsiaan yang telah ditandatangani Encik Cheok tidak menetapkan sebarang had masa. Mahkamah memutuskan bahawa peruntukan sedemikian adalah sah kerana jika had masa ditetapkan, seseorang bekas pekerja itu boleh dengan sewenang-wenangnya mengeksplorasi maklumat sulit kerana apa yang perlu dibuat oleh pekerja tersebut hanyalah menunggu tempoh had masa bagi perlindungan maklumat sulit tersebut tamat, dan perkara ini bukanlah tujuan perjanjian perlindungan maklumat rahsia dibuat. Tujuan perjanjian kerahsiaan adalah untuk menjaga maklumat sulit syarikat daripada terlepas ke pihak ketiga dan seterusnya akan mendatangkan kesan buruk kepada syarikat, sebagai contoh, syarikat berkemungkinan terlepas tender sesuatu projek.

Mahkamah Persekutuan telah mengikuti keputusan mahkamah Australia yang mengiktiraf kewajipan melindungi maklumat rahsia kekal. Oleh yang demikian, boleh disimpulkan bahawa tiada halangan untuk perjanjian kerahsiaan mengikat pihak-pihak yang menandatangani perjanjian tersebut secara kekal, termasuklah sekiranya pekerja tersebut telah berhenti daripada syarikat atau institusi berkenaan.

**Persoalan kedua:** Adakah klausa kerahsiaan yang kekal menjadi tidak sah kerana menghalang perdagangan?

Mahkamah Persekutuan memutuskan bahawa meskipun perlindungan maklumat rahsia boleh menjadi kekal, namun demikian ianya masih tertakluk kepada prinsip undang-undang dan ekuiti lain yang mungkin terpakai seperti doktrin sekatan perdagangan. Seksyen 28, Akta Kontrak 1950 memperuntukkan bahawa mana-mana klausa yang menghalang perdagangan akan terbatal. Malangnya, Mahkamah Persekutuan enggan menjawab secara khusus persoalan sama ada perjanjian untuk tidak mendedahkan maklumat sulit "semasa bekerja atau pada bila-bila masa selepas itu" adalah terbatal oleh Seksyen 28 Akta Kontrak 1950 kerana menghalang perdagangan.

**Mahkamah Persekutuan memutuskan bahawa meskipun perlindungan maklumat rahsia boleh menjadi kekal, namun demikian ianya masih tertakluk kepada prinsip undang-undang dan ekuiti lain yang mungkin terpakai seperti doktrin sekatan perdagangan. Seksyen 28, Akta Kontrak 1950 memperuntukkan bahawa mana-mana klausa yang menghalang perdagangan akan terbatal.**

Walau bagaimanapun, Mahkamah tetap memberi amaran terhadap majikan yang menggunakan dakwaan samar-samar pelanggaran kerahsiaan untuk menyekat keupayaan bekerja bekas pekerja daripada bersaing.

Memetik penghakiman Scott J dalam kes **UK Balston Ltd v Headline Filters Ltd (1987) FRS 330**, "penggunaan sekatan terhadap maklumat sulit bertujuan untuk menyekat pekerja-pekerja daripada menggunakan kemahiran dan pengalaman mereka untuk bersaing dengan bekas majikan mereka, pada pandangan saya, berpotensi berbahaya. Ia mampu menjadikan satu bentuk perhambaan yang baru."

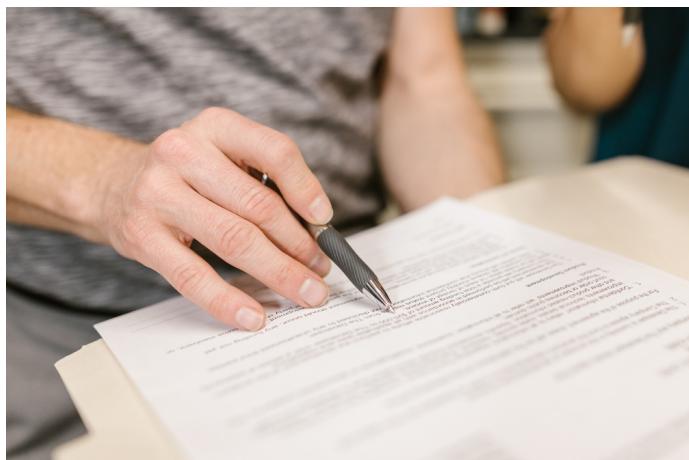
Tuntasnya, sama ada sesuatu klausa itu terbatal kerana berada dalam "sekatan perdagangan" masih perlu ditentukan berdasarkan kes demi kes dan majikan juga tidak boleh menyekat pekerja-pekerja daripada terus mengembangkan bakat dan kerjaya masing-masing di tempat baru hanya kerana beliau telah menimba ilmu dan pengalaman di syarikat sebelumnya.

**Persoalan ketiga:** Keperluan untuk menyatakan perlanggaran kerahsiaan secara khusus.

Tuntutan Dynacast dalam kes ini gagal kerana ia tidak menyatakan secara spesifik jenis maklumat sulit atau rahsia perdagangan yang didakwa disalahgunakan oleh Encik Cheok. Dalam tuntutan undang-undang, adalah tidak mencukupi bagi majikan untuk mendakwa bahawa bekas pekerja telah "menyalahgunakan maklumat peribadi dan sulit" tanpa memberikan butiran yang mencukupi dan terperinci. Seorang bekas pekerja berhak mengetahui apakah maklumat peribadi dan sulit yang dikatakan telah disalahgunakan olehnya supaya beliau boleh mempertahankan diri terhadap tuntutan yang dikenakan terhadapnya.

Berdasarkan keputusan kes ini, majikan harus mengambil kira beberapa perkara apabila berurusan dengan tanggungjawab kerahsiaan. Antaranya adalah, Mahkamah Persekutuan berpendapat bahawa tanggungjawab kerahsiaan pekerja adalah sangat bergantung kepada terma kontrak yang dipersetujui.

Pekerja yang mempunyai akses kepada maklumat sulit hendaklah dikehendaki menandatangani perjanjian kerahsiaan (NDA) dan draf Perjanjian Kerahsiaan perlulah digubal mengikut kehendak syarikat dan undang-undang yang berkuatkuasa. Memandangkan kebolehkuatkuasaan NDA mungkin berbeza dari satu bidang kuasa ke satu bidang kuasa, template NDA hendaklah sentiasa disemak dan mematuhi perspektif undang-undang tempatan.



Selain itu, sekiranya berlaku pelanggaran kerahsiaan, majikan perlulah mengenal pasti dan mengkhususkan maklumat sulit yang dikatakan telah disalahgunakan. Undang-undang membenarkan bekas pekerja menggunakan pengetahuan dan pengalaman mereka sendiri yang terkumpul selama bertahun-tahun dan ini termasuk bakal pelanggan, arah aliran harga dan maklumat pasaran yang berada dalam domain awam.

Penggunaan pengetahuan dan pengalaman peribadi ini bukanlah pelanggaran kerahsiaan. Perkara ini perlu diambil cakna oleh majikan supaya tidak membuat tuntutan melulu hanya kerana seseorang telah menggunakan ilmu dan pengalaman beliau semasa bekerja di syarikat atau organisasi terdahulu di tempat kerja baharu.

Jika bekas pekerja telah menujuhkan perniagaan yang bersaing dengan syarikat majikan, majikan mesti menilai sama ada terdapat penyalahgunaan maklumat sulit oleh bekas pekerja dan jika terdapat bukti yang jelas, baru tindakan boleh diambil.

Tindakan menujuhkan perniagaan yang bersaing semata-mata bukanlah satu kesalahan undang-undang, dan majikan tidak boleh menggunakan kewajipan kerahsiaan untuk menghalang persaingan.

## KESIMPULAN

Akhir sekali, adalah penting untuk seseorang majikan dan pekerja tahu hak dan tanggungjawab masing-masing semasa menandatangani sesuatu perjanjian kerahsiaan. Pekerja perlulah mempunyai integriti yang tinggi untuk tidak menggunakan maklumat sulit syarikat sebelumnya demi kepentingan syarikat baru dan mendatangkan kerugian besar buat syarikat sebelumnya. Majikan pula perlulah mengenalpasti maklumat sulit apa yang telah disalahgunakan oleh bekas pekerja dan bagaimana ia mempengaruhi kerugian yang dialami oleh syarikat sebelum membuat sebarang tuntutan supaya pihak majikan mempunyai bukti yang kukuh di mahkamah.

## Rujukan:

1. [https://rmc.upm.edu.my/upload/dokumen/20190405091417APA\\_ITU\\_NDA\\_\(050419\).pdf](https://rmc.upm.edu.my/upload/dokumen/20190405091417APA_ITU_NDA_(050419).pdf)
2. <https://malaysianlitigator.com/2020/06/22/non-disclosure-agreement-when-to-use-it/>
3. <https://www.mipa.org.my/pages.php?id=14>
4. <https://dnh.com.my/latest-federal-court-case-employees-obligations-of-confidentiality/>
5. <https://dnh.com.my/if-i-cant-have-you-nobody-can-applicability-of-non-compete-clauses-in-employment-contracts/>
6. <https://www.legal500.com/developments/thought-leadership/employment-non-disclosure-agreements-what-employers-need-to-know/>
7. <https://www.hg.org/legal-articles/law-on-breach-of-confidence-and-recourse-by-employers-against-employees-in-malaysia-49023>
8. <https://www.gannons.co.uk/insights/duty-confidentiality-employment/>

# PERLINDUNGAN DATA PERIBADI: KENAPA ANDA PERLU CAKNA?



**ROSLINA GHAZALI**

Timbalan Penasihat Undang-Undang UMT

## PENDAHULUAN

Dalam kepesatan teknologi hari ini, aliran maklumat juga semakin meningkatkan. Orang ramai tanpa teragak-agak berkongsi pelbagai data peribadi di media sosial dan lain-lain platform atas talian seperti *e-shopping*, *e-hailing*, *online games* dan sebagainya. Kita mungkin beranggapan perkongsian tersebut sebagai sesuatu yang perlu dan tidak merbahaya (*harmless*). Hakikatnya, data peribadi merupakan suatu komoditi berharga dan menjadi aset penting terutamanya kepada entiti perniagaan, parti politik, *scammer* dan pengodam siber.

Pada tahun 2018, dunia digemparkan dengan berita kebocoran data peribadi pengguna *facebook* yang telah dikutip secara tidak sah oleh firma analisis data, Cambridge Analytica, yang berpangkalan di London. Data peribadi ini dikatakan telah digunakan untuk mendapat maklumat pengundi sewaktu pilihan raya Amerika Syarikat, seterusnya membantu kemenangan presiden Donald Trump pada tahun 2016. Malaysia juga turut mendapat tempias dalam skandal ini apabila dikatakan parti UMNO juga telah menggunakan perkhidmatan Cambridge Analytica untuk membantu dalam proses pilihanraya umum 2013 yang dimenangi oleh Barisan Nasional. Skandal kebocoran data peribadi ini telah menyebabkan *facebook* didenda sebanyak £500,000 atau RM2.6 juta oleh Pesuruhjaya Maklumat Britain kerana gagal melindungi data penggunanya serta tidak telus mengenai bagaimana data tersebut boleh dituai melalui platformnya.



Pada Oktober 2019, sejumlah data peribadi staf akademik dan bukan akademik Universiti Malaya telah dibocorkan di internet selepas beberapa jam pautan pembayaran atas talian (*e-bayar*) milik universiti itu digodam. Hampir 24,000 emel ID login dan kata laluan dipercayai daripada pautan pembayaran *e-bayar* itu telah dibocorkan. Perbuatan tersebut menyebabkan maklumat gaji termasuk nama dan akaun bank individu, nombor cukai pekerja, nombor Kumpulan Wang Simpanan Pekerja, maklumat jabatan dan pangkat didedahkan kepada umum.

Manakala pada tahun 2020 pula, syarikat keselamatan siber India, Technisancet melaporkan lebih 300,000 butiran maklumat kad pembayaran seperti kad kredit dan debit, yang dipercayai milik beberapa bank terkemuka di enam negara Asia Tenggara iaitu Singapura, Malaysia, Indonesia, Thailand, Filipina dan Vietnam dijual di dalam pelbagai forum web gelap. Penemuan itu diperolehi ketika pasukan penganalisis ancaman Technisancet membuat penyelidikan untuk menganalisis ancaman terhadap sektor kewangan di Asia Tenggara. Pasukan Technisancet menganalisa 1136 nombor BIN bank dari enam negara itu, yang mana mereka menemui 319,669 maklumat kad termasuk nombor kad, nama pemegang kad, CVV, tarikh luput dan dalam beberapa kes membabitkan nombor PIN. Berdasarkan analisa, Filipina adalah negara yang mencatatkan jumlah tertinggi, sebanyak 172,828, diikuti Malaysia 37,145, Indonesia 35,354 dan Singapura 25,290.



## APA ITU DATA PERIBADI?

Pada 15 November 2013, Kerajaan Malaysia telah menguatkasakan Akta Perlindungan Data Peribadi 2010 ("PDPA 2010"). Tujuan PDPA 2010 dikanunkan adalah untuk mengawal selia pemprosesan data peribadi dalam transaksi komersial.

Data peribadi ditakrifkan dalam seksyen 4, PDPA 2010 sebagai apa-apa maklumat yang berkenaan apa-apa transaksi komersial, yang –

- (a) sedang diproses secara keseluruhannya atau sebahagiannya melalui kelengkapan yang dikendalikan secara automatik sebagai tindak balas kepada arahan yang diberikan bagi maksud itu;
- (b) direkodkan dengan niat bahawa ia sepatutnya diproses secara keseluruhannya atau sebahagiannya melalui kelengkapan itu; atau direkodkan sebagai sebahagian daripada sistem pemfailan yang berkaitan atau dengan niat bahawa ia sepatutnya menjadi sebahagian daripada sistem pemfailan yang berkaitan,

yang berhubungan **secara langsung atau tidak langsung dengan seorang subjek data, yang dikenalpasti atau boleh dikenalpasti** daripada maklumat itu dan maklumat lain dalam milikan seorang pengguna data, termasuk apa-apa **data peribadi sensitif** dan pernyataan pendapat tentang subjek data itu; tetapi tidak termasuk apa-apa maklumat yang diproses bagi maksud suatu perniagaan pelaporan kredit yang dijalankan oleh sesuatu agensi pelaporan kredit di bawah Akta Agensi Pelaporan Kredit 2010.

Secara ringkasnya data peribadi merujuk kepada apa-apa maklumat yang boleh menyebabkan seseorang individu itu (subjek data) dikenal pasti seperti nama, alamat, nombor kad pengenalan, gambar, tarikh lahir, nombor telefon, rakaman kamera litar tertutup, pekerjaan dan sebagainya.

PDPA 2010 juga memberikan takrifan khusus berkenaan data peribadi sensitif iaitu apa-apa maklumat berkaitan kesihatan atau keadaan fizikal dan mental seseorang subjek data, pendapat politiknya, kepercayaan agamanya termasuk pelakuan dan pernyataan pelakuan kesalahan oleh subjek data tersebut.

## PEMPROSESAN DATA PERIBADI

Pemprosesan data peribadi bermaksud apa-apa proses yang melibatkan aktiviti mengumpul, merekod, memegang atau menyimpan data termasuk apa-apa proses pengendalian lain seperti menyusun, mengubahsuai, mendapatkan kembali, menzahirkan, menggabung, membentulkan dan melupuskan data peribadi. Bagi melindungi keselamatan data peribadi, PDPA 2010 telah menggariskan bahawa pemprosesan data peribadi hendaklah mematuhi tujuh (7) prinsip perlindungan data peribadi seperti yang ditetapkan dalam seksyen 5 dan diringkaskan dalam Jadual di bawah:

Prinsip	Keterangan
<b>Am</b>	Pengguna data tidak boleh memproses data peribadi tanpa persetujuan subjek data. Data peribadi yang dikumpulkan hendaklah tidak berlebihan daripada yang diperlukan.
<b>Notis dan Pilihan</b>	Subjek data hendaklah dimaklumkan tentang tujuan data peribadinya diperlukan.
<b>Penzahiran</b>	Data peribadi tidak boleh didedahkan tanpa persetujuan subjek data dan data peribadi tidak boleh digunakan selain dari tujuan ianya dibenarkan.
<b>Keselamatan</b>	Pengguna data hendaklah mengambil langkah-langkah keselamatan bagi mengelakkan berlakunya kehilangan atau penyalahgunaan data peribadi.
<b>Penyimpanan</b>	Data peribadi tidak boleh disimpan melebihi tempoh ianya diperlukan. Pengguna data hendaklah memastikan data dilupuskan secara kekal apabila tidak lagi diperlukan.
<b>Integriti Data</b>	Pengguna data hendaklah memastikan data peribadi adalah tepat, terkini, tidak mengelirukan dan menepati tujuan data diproses.
<b>Akses</b>	Subjek data berhak untuk mengakses data peribadinya dan boleh membuat apa-apa pembetulan yang sewajarnya.

## PEMPROSESAN DATA PERIBADI SENSITIF

Selaras dengan prinsip am perlindungan data peribadi, pengguna data tidak boleh memproses data peribadi sensitif seseorang individu tanpa terlebih dahulu mendapat keizinan atau persetujuan individu berkenaan. Selanjutnya seksyen 40(2), PDPA 2010 memperuntukkan syarat-syarat tambahan yang perlu dipatuhi oleh pengguna data.

Pengguna data dibenarkan untuk memproses data peribadi sensitif jika data itu perlu –

- (a) bagi tujuan pelaksanaan undang-undang;
- (b) untuk melindungi kepentingan vital subjek data atau orang lain;
- (c) bagi maksud perubatan dan dilakukan oleh seorang profesional penjagaan perubatan;
- (d) bagi maksud berkaitan dengan apa-apa prosiding undang-undang;
- (e) bagi maksud mendapatkan nasihat undang-undang;
- (f) bagi maksud membuktikan atau mempertahankan hak di sisi undang-undang;
- (g) bagi pentadbiran keadilan;
- (h) bagi menjalankan fungsi yang diberikan kepada mana-mana orang di bawah undang-undang; dan
- (i) bagi apa-apa maksud lain yang difikirkan patut oleh Menteri.

**Secara ringkasnya data peribadi merujuk kepada apa-apa maklumat yang boleh menyebabkan seseorang individu itu dikenal pasti seperti nama, alamat, nombor kad pengenalan, gambar, tarikh lahir, nombor telefon, rakaman kamera litar tertutup, pekerjaan dan sebagainya**

## HAK SUBJEK DATA

Hak-hak subjek data dinyatakan secara jelas dalam Penggal 4, PDPA 2010. Kegagalan pengguna data untuk memberikan hak-hak yang terakru kepada subjek data seperti mana yang diperuntukkan dalam PDPA 2010 merupakan suatu kesalahan, dan jika sabit kesalahan, pengguna data boleh dikenakan denda tidak lebih RM100,000.00 atau penjara tidak lebih satu tahun atau kedua-duanya sekali.

Rangkuman hak-hak subjek data dijelaskan melalui Rajah berikut:

- Hak untuk diberitahu sama ada data peribadinya diproses oleh pengguna data
- Hak untuk mengakses data peribadinya
- Hak untuk membetulkan data peribadinya
- Hak untuk menarik balik kebenaran memproses data peribadinya
- Hak untuk menghalang pemrosesan data peribadi yang boleh menyebabkan kerosakan atau distres
- Hak untuk menghalang pemrosesan data peribadi bagi maksud pemasaran langsung

Mana-mana individu yang merasakan bahawa data peribadinya telah diproses secara tidak benar atau telah melanggar mana-mana peruntukan PDPA 2010, boleh membuat aduan kepada Pesuruhjaya Data Perlindungan Data Peribadi. PDPA 2010 walau bagaimanapun tidak memperuntukkan secara spesifik hak subjek data untuk menuntut gantirugi daripada pengguna atau pemroses data.

## LIMITASI PDPA 2010

PDPA 2010 hanya melindungi data peribadi yang digunakan dalam transaksi komersial. PDPA 2010 adalah berguna dalam pengurusan data peribadi yang melibatkan urusan perbankan, e-dagang, jualan langsung dan lain-lain platform perniagaan. Namun data peribadi juga diproses untuk transaksi bukan komersial seperti media sosial, soal selidik, cookies dan sebagainya. Dalam transaksi bukan komersial seperti ini, data peribadi yang diproses tidak akan dilindungi sewajarnya.

PDPA 2010 juga tidak terpakai kepada Kerajaan Persekutuan dan Kerajaan Negeri. Oleh itu apa-apa data peribadi yang diproses oleh mana-mana agensi Kerajaan Persekutuan atau Kerajaan Negeri tidak akan tertakluk kepada obligasi untuk mematuhi prinsip perlindungan data peribadi seperti yang dibincangkan di atas. Walaupun Kerajaan sentiasa memberi jaminan bahawa data peribadi yang diproses oleh Kerajaan berada dalam keadaan baik dan selamat, namun beberapa cubaan menggodam sistem maklumat Kerajaan serta berita kebocoran data peribadi yang tular telah menimbulkan kegusaran umum.



## KESAN PENCEROBOHAN DATA PERIBADI

Pencerobohan atau kebocoran data peribadi boleh memberi kesan bukan sahaja kepada subjek data tetapi juga kepada pengguna data atau organisasi yang menguruskan pemprosesan data peribadi. Dalam era teknologi ini, walaupun terdapat kawalan keselamatan yang ketat, aktiviti menggodam dan menceroboh data juga semakin berleluasa.

### KESAN KEPADA INDIVIDU/ORGANISASI

**Kecurian Identiti.** Identiti individu yang dicuri digunakan untuk tujuan jenayah atau apa-apa tujuan yang tidak bermoral.

**Kerugian Kewangan.** Data peribadi yang diperolehi digunakan untuk tujuan fraud atau scam bagi mendapatkan wang daripada individu/organisasi

**Buli Siber.** Penceroboh menggunakan data peribadi individu untuk melakukan buli siber dengan mengganggu privasi individu.

**Imej dan Reputasi.** Data peribadi terutamanya data sensitif digunakan untuk menjelaskan imej atau reputasi seseorang individu atau organisasi.

**Gangguan Pemasaran.** Individu menerima promosi pemasaran yang tidak dikehendaki sama ada melalui telefon atau emel.

## KESIMPULAN

Walaupun PDPA 2010 mempunyai kelemahan, namun penggubalan akta ini menunjukkan komitmen Kerajaan untuk menjaga keselamatan data peribadi rakyat Malaysia agar tidak dimanipulasi atau digunakan oleh pihak-pihak berkepentingan dalam transaksi komersial tanpa kawalan atau sekatan yang sewajarnya.

Dalam kes, **Genting Malaysia Bhd v. Pesuruhjaya Perlindungan Data Peribadi & Ors. 2022 [2022] 11 MLJ**, pihak Lembaga Hasil Dalam Negeri (LHDN) telah mengarahkan pihak Genting Malaysia (pemohon) untuk menyerahkan semua maklumat berkaitan pelanggan pemohon, terutamanya mereka yang telah memperoleh kad keahlian di bawah Genting Rewards Loyalty Programme dan meminta butiran individu yang telah menang atau kalah di kasino pemohon. Tujuan arahan tersebut adalah supaya LHDN dapat menilai semula jumlah cukai yang patut dikenakan ke atas pemohon. Pemohon enggan menyerahkan maklumat yang dipohon oleh LHDN kerana ianya bercanggah dengan peruntukan PDPA 2010. Y.A Hakim Noorin Badarudin dalam keputusannya menyatakan bahawa Pesuruhjaya Perlindungan Data Peribadi dan LHDN telah mengabaikan kewajipan berkanun yang diamanahkan kepada mereka oleh Parlimen untuk melindungi data peribadi pelanggan pemohon dan dalam menangani isu sebenar dalam kes ini. Responden telah bertindak *ultra vires* dan tidak rasional dengan cara yang tidak akan dilakukan oleh pihak berkuasa lain.

Berdasarkan keputusan kes di atas, bolehlah disimpulkan bahawa undang-undang sedia ada mampu untuk melindungi data peribadi dalam transaksi komersial. Walaupun ada cubaan daripada agensi yang berkepentingan untuk mendapat faedah daripada kelompongan perundangan sedia ada, keputusan Mahkamah masih memihak kepada keperluan pematuhan kepada PDPA 2010.

## Rujukan:

1. Akta Perlindungan Data Peribadi: Satu Tinjauan, Fadhilah Abdul Ghani *et al*, 2021, Jurnal Dunia Pengurusan
2. Tinjauan Awal terhadap Konsep Data Peribadi kesihatan, Nazura Abdul Manap *et al*, 2020, JUUM Personal Data Protection Act 2010: Taking the First
3. Steps towards Compliance, 2015, Journal of Management & Muamalah;
4. Perlindungan Data Peribadi Malaysia, Nor Fadzlina Nawi, Buletin ACIS
5. <https://www.azmilaw.com/insights/six-6-things-your-business-need-to-know-on-personal-data-protection-in-malaysia/>
6. <https://www.dataguidance.com/notes/malaysia-data-protection-overview>
7. <https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches>



# SISIPAN KES UNDANG-UNDANG

**PUBLIC PROSECUTOR V. SUBBARAU & KAMALANATHAN  
[2017] 6 MLJ 434**

## **FAKTA KES**

Responden dan seorang yang bernama Prem Kumar telah ditangkap dan dua telefon bimbit, setiap satu telah didaftarkan di bawah nama Responden dan Prem Kumar telah dirampas. Beberapa imej telah dijumpai dalam telefon bimbit Prem Kumar dan imej-imej tersebut amat sama dengan kertas soalan UPSR sebenar untuk subjek Bahasa Tamil Penulisan 037, Sains 018/1, Matematik 035/2, Matematik 015/1 dan Bahasa Tamil Pemahaman 036. Imej-imej tersebut telah dikongsi melalui grup WhatsApp termasuk komunikasi dari telefon Responden. PW12 telah dilantik oleh Menteri Pendidikan Malaysia sebagai pegawai pengkelas dan mengarahkan agar kertas-kertas soalan UPSR 2014 diklasifikasikan sebagai "SULIT". Responden telah dituduh dengan lima (5) pertuduhan di bawah seksyen 8(1)(c)(iii) Akta Rahsia Rasmi 1972.

Mahkamah Sesyen memutuskan bahawa pendakwaan telah gagal untuk membuktikan kes *prima facie* dan akhirnya, Responden telah dilepas dan dibebaskan di penutup kes pendakwaan. Mahkamah Tinggi juga telah menolak rayuan perayu, justeru perayu sekali lagi merayu ke Mahkamah Rayuan. Isu yang perlu ditentukan oleh Mahkamah Rayuan adalah sama ada kertas peperiksaan UPSR 2014 yang terakhir menurut lima pertuduhan tersebut adalah rahsia rasmi.

## **KEPUTUSAN**

Mahkamah Rayuan membenarkan rayuan dan mengetepikan perintah-perintah Mahkamah Sesyen dan Mahkamah Tinggi; dan memerintahkan Responden memasuki pembelaannya lima (5) pertuduhan tersebut.

## **ALASAN PENGHAKIMAN**

YAA HMR Vernon Ong (majoriti) dalam penghakiman bertulisnya memutuskan seperti berikut:

Suatu dokumen yang telah diklasifikasikan termasuklah apa-apa maklumat dan bahan yang terkandung dalam draf awal dokumen tersebut, yang mana kandungannya adalah rahsia rasmi selepas dokumen tersebut diklasifikasikan, dan rahsia rasmi yang berkait dengan apa-apa maklumat dan bahan semua draf seterusnya termasuklah versi terakhir dokumen tersebut. Untuk memutuskan sebaliknya akan memerlukan pegawai awam yang mengesahkan untuk mengklasifikasikan setiap draf dokumen termasuk versi akhir dokumen itu. Ini merupakan suatu yang mustahil selanjutnya jika draf dan versi akhir tidak diklasifikasikan secara berasingan, maka maklumat dan bahan dalam draf berikutnya dan akhir tidak akan dilindungi sebagai rahsia rasmi.

Oleh itu, ia tidak perlu untuk diklasifikasikan setiap versi kertas peperiksaan UPSR. Adalah jelas bahawa kertas peperiksaan UPSR bertujuan untuk diklasifikasikan dan bahawa pengklasifikasian tersebut termasuklah maklumat dan bahan dalam draf awal dan berikutnya dan versi terakhir kertas peperiksaan UPSR. Oleh itu, kertas UPSR yang terakhir adalah rahsia rasmi.

Oleh itu, hakim perbicaraan dan hakim Mahkamah Tinggi telah salah arah dari segi undang-undang dan fakta. Berdasarkan keseluruhan keterangan, terdapat keterangan yang mencukupi untuk membuktikan kes *prima facie* ke atas semua lima pertuduhan tersebut.



**Pejabat Penasihat Undang-Undang**

Aras 2, Bangunan Canselori,  
Universiti Malaysia Terengganu,  
21030 Kuala Nerus, Terengganu