The current issue and full text archive of this journal is available at
http://journal.kuis.edu.my/muwafaqat

Prinsip Penyimpanan Data Peribadi Pekerja: Satu Kajian Perundangan di Malaysia

A Legal Analysis on The Retention Principle of Employees' Personal Data Protection in Malaysia

NAWAL BINTI SHOLEHUDDIN
(Corresponding Author)
FARAH BINTI MOHD SHAHWAHID
Jabatan Undang-undang
Fakulti Syariah dan Undang-Undang
Kolej Universiti Islam Antarabangsa Selangor (KUIS)
Bangi Selangor
nawal@kuis.edu.my, farahms@kuis.edu.my

UMMI MUNIRAH SYUHADA MOHAMAD ZAN
Jabatan Ekonomi dan Pengurusan
Fakulti Pengurusan dan Muamalah
Kolej Universiti Islam Antarabangsa Selangor (KUIS)
Bangi Selangor
ummi@kuis.edu.my

Submitted: 1 October 2021
Revised: 30 October 2021
Accepted: 30 October 2021
E-Published: 31 October 2021

ABSTRAK

Akta Perlindungan Data Peribadi 2010 yang mula dikuatkuasakan pada tahun 2013 memberi kesan yang besar kepada pihak majikan dengan mewujudkan beberapa tanggungjawab berkaitan pemprosesan data peribadi pekerja. Sebagai majikan, terdapat keperluan untuk mengumpul dan memproses data peribadi pekerja. Penyimpanan data peribadi pekerja oleh majikan boleh menimbulkan isu sekiranya terdapat kebocoran atau penyalahgunakan data peribadi tersebut. Mengikut prinsip penyimpanan yang termaktub di dalam Akta Perlindungan Data Peribadi 2010, perlu ada tempoh had masa yang munasabah bagi majikan untuk menyimpan data peribadi pekerja. Kajian ini akan mengkaji undang-undang berkaitan penyimpanan data peribadi pekerja oleh majikan menurut Akta Perlindungan Data Peribadi 2010 dan Akta Kerja 1955. Kajian ini juga akan membincangkan tentang amalan majikan di Malaysia dalam mematuhi Prinsip Penyimpanan semasa memproses data peribadi pekerja. pematuhan prinsip peyimpanan data peribadi pekerja yang perlu dilaksanakan oleh majikan. Kaedah yang digunakan adalah kajian kepustakaan dan analisis dokumen. Kajian ini akan menjadi rujukan kepada organisasi dalam melaksanakan peruntukan-peruntukan APDP 2010 dan sekaligus memberi kesedaran kepada pekerja dalam mengetahui hak-hak mereka ketika berkongsi data peribadi dengan majikan.

Kata Kunci: Akta Perlindungan Data Peribadi 2010, data peribadi, tanggungjawab majikan, pekerja, prinsip penyimpanan

The current issue and full text archive of this journal is available at
http://journal.kuis.edu.my/muwafaqat

ABSTRACT

The Personal Data Protection Act 2010 which has been enforced since 2013 has a great impact on employers as it introduces some obligations concerning the processing of employees' personal data. As an employer, there is a need to collect and process personal data of the employees. The collection of these data could be an issue if there were data leakage or data misuse. According to the principle of retention which is embodied in the Personal Data Protection Act 2010, an employer may retain the personal data of employees only for a reasonable period. This article will study the relevant laws relating to the retention of employees' personal data particullarly the Personal Data Protection Act 2010 (PDPA 2010) and the Employment Act 1955. This article will also discuss the practice of employers in Malaysia in complying with the retention principle when processing employees' personal data. The methods used are library-based research and document analysis. This paper could be a reference to organisations in complying with the legal provisions of PDPA 2010 and in providing awareness to the employees as to their rights when they have to share their personal data with the employers.

Keywords: Personal Data Protection Act 2010, personal data, duty of employer, employee, retention principle

PENGENALAN

Di Malaysia, Akta Perlindungan Data Peribadi 2010 (APDP 2010) telah diperkenalkan untuk mencegah sebarang bentuk penyalahgunaan terhadap penyimpanan atau pemprosesan data peribadi untuk tujuan transaksi komersial. APDP mendefinisikan transaksi komersial sebagai apa-apa perkara yang berhubung dengan pembekalan dan pertukaran barangan atau perkhidmatan, agensi, pelaburan, pembiayaan, perbankan dan insurans, sama ada secara kontrak atau tidak. Akta ini terpakai kepada golongan pengguna data yang disenaraikan di dalam Akta Perlindungan Data Peribadi 2010 Perintah Perlindungan Data Peribadi (Golongan Pengguna Data) 2013 iaitu komunikasi, perbankan dan institusi kewangan, insurans, kesihatan, pelancongan dan hospitaliti, pengangkutan, pendidikan, jualan langsung, perkhidmatan, hartanah dan utiliti. Pengguna data merujuk kepada seseorang yang sama ada berseorangan atau bersama dengan orang lain memproses apa-apa data peribadi atau mempunyai kawalan terhadap atau membenarkan pemprosesan apa-apa data peribadi, tetapi tidak termasuk seorang yang memproses data (seksyen 4, APDP 2010). Pemproses data, berhubung dengan data peribadi, ertinya mana-mana orang, selain seorang pekerja pengguna data, yang memproses data peribadi itu semata-mata bagi pihak pengguna data itu, dan tidak memproses data peribadi itu bagi apa-apa maksud persendiriannya (seksyen 4, APDP 2010).

APDP 2010 merupakan sebahagian matlamat dasar ke-10 Akta Komunikasi dan Multimedia 1998, iaitu bagi menjamin keselamatan maklumat dan kebolehpercayaan serta keutuhan rangkaian dalam perlindungan data di Malaysia (Mohd Hamdan, 2015). APDP 2010 ini tidaklah digubal untuk tujuan melindungi hak privasi seseorang

sebaliknya Akta ini lebih memfokuskan kepada memberi perlindungan terhadap penggunaan maklumat diri seseorang bagi tujuan komersial (Marina Abdul Manap, 2020). Dalam erti kata lain, Akta ini melindungi kepentingan subjek data dengan memastikan pengguna data mematuhi APDP 2010 semasa memproses data peribadi yang berkaitan bagi tujuan komersial. Seksyen 5 APDP 2010 menyenaraikan tujuh (7) prinsip perlindungan peribadi yang perlu dipatuhi oleh pengguna data iaitu: Prinsip Am, Prinsip Notis dan Pilihan, Prinsip Penzahiran, Prinsip Keselamatan, Prinsip Penyimpanan, Prinsip Integriti Data dan Prinsip Akses. Prinsip-prinsip ini termaktub di dalam APDP 2010 bermula dari seksyen 6 hingga sekyen 12. Kajian ini memfokuskan kepada Prinsip Penyimpanan (10, APDP 2010) yang mengatakan bahawa sesuatu data peribadi itu tidak dibenarkan disimpan di dalam sesuatu pemprosesan lebih daripada had masa yang diperlukan dan menurut peruntukan ini pengguna data iaitu majikan mempunyai tanggungjawab berat dan besar bagi memastikan dan menjamin segala data peribadi pekerja serta pelanggan yang diproses selamat dan dilindungi. Oleh itu, adalah penting bagi majikan mematuhi tujuh prinsip dalam APDP 2010.

Dalam konteks majikan dan pekerja, majikan mengumpul dan memproses data peribadi pekerja dan orang yang memohon pekerjaan di tempat mereka atas beberapa sebab; antaranya keperluan undang-undang, pemilihan pekerja, kursus, latihan dan kenaikan pangkat, keselamatan dan pengawasan, kawalan mutu, perkhidmatan pelanggan dan perlindungan harta benda. Kemunculan pelbagai teknologi dalam mengumpul serta memproses maklumat membawa kepada beberapa risiko baru kepada pekerja. Justeru itu, artikel ini ingin mengkaji undang-undang berkaitan pemprosesan data peribadi pekerja dan khususnya undang-undang berkaitan penyimpanan data peribadi pekerja oleh majikan menurut Akta Perlindungan Data Peribadi 2010 dan Akta Kerja 1955.

SOROTAN LITERATUR

Lazimnya, majikan akan mengumpulkan dan mendapatkan maklumat peribadi daripada pekerja seperti maklumat kesihatan, maklumat percukaian dan pemeriksaan latar belakang peribadi, serta melakukan pemantauan dan pengawasan berterusan terhadap pekerja di tempat kerja dan ketika mereka bekerja (Butler, 2009). Tambahan lagi, segala data peribadi yang diperlukan hendaklah sentiasa dalam keadaan tepat, relevan dan terkini (Kusumoningtyas dan Nasional, 1997).

APDP 2010 hanya digunakan untuk perlindungan data yang berkaitan dengan transaksi komersial. Mengikut seksyen 4 APDP 2010, transaksi komersial dalam konteks ini didefinisikan sebagai apa-apa transaksi bersifat komersial, sama ada secara kontrak atau tidak, yang termasuk apa-apa perkara yang berhubungan dengan pembekalan atau pertukaran barang atau perkhidmatan, agensi, pelaburan, pembiayaan, perbankan dan insurans (APDP, 2010). Perkhidmatan yang terkandung dalam senarai makna transaksi komersial ini menjadikannya relevan untuk digunakan dalam sektor pekerjaan di mana subjek data merujuk kepada pekerja dan pengguna data merujuk kepada majikan atau orang yang memproses apa-apa data peribadi (Adlin et al., 2019).

APDP 2010 turut menyenaraikan hak-hak subjek data terhadap data peribadi mereka yang diproses oleh majikan adalah hak untuk dimaklumkan, hak akses kepada data peribadi, hak untuk membetulkan data peribadi, hak untuk menarik balik persetujuan dan hak untuk mencegah pemprosesan untuk tujuan pemasaran langsung. Sebarang jenis pemprosesan data peribadi perlu mematuhi semua prinsip data. Peruntukan seksyen 5(1) menetapkan semua prinsip data hendaklah dipatuhi apabila data peribadi tersebut dikumpul, dipegang, diproses atau digunakan oleh pengguna data. Tujuh (7) prinsip tersebut adalah Prinsip Am, Prinsip Notis dan Pilihan, Prinsip Penzahiran, Prinsip Keselamatan, Prinsip Penyimpanan, Prinsip Integriti dan Prinsip Akses sebagaimana yang dinyatakan dalam seksyen 6, 7, 8, 9, 10, 11 dan 12 (APDP, 2010).

Prinsip am memaklumkan seseorang pengguna data tidak dibenarkan memproses data peribadi seseorang subjek data tanpa kebenarannya. Kedua, prinsip notis dan pilihan di mana pengguna data perlulah memaklumkan tujuan awal pemprosesan data kepada subjek data. Prinsip penzahiran pula bermaksud tujuan data peribadi seseorang subjek itu demi mengenal pasti maksud yang baginya data peribadi itu hendaklah dizahirkan. Prinsip keempat adalah prinsip keselamatan di mana dalam memproses mana-mana data, perlu mengambil langkah supaya data tersebut selamat, tidak diubahsuai, disalahguna atau diberikan kepada pihak yang tidak berkenaan. Seterusnya, prinsip penyimpanan iaitu sesuatu data peribadi tidak dibenarkan disimpan di dalam sesuatu pemprosesan lebih daripada had masa yang diperlukan. Keenam pula adalah prinsip integriti data di mana setiap data peribadi yang diproses perlu dipastikan tepat, lengkap, tidak mengelirukan dan terkini. Prinsip ketujuh adalah prinsip akses di mana seseorang hendaklah diberi hak akses kepada data peribadinya yang dipegang oleh seseorang pengguna data dan juga boleh membetulkan datanya itu supaya terkini (Muhammad Adnan dan Siti Zobidah, 2019).

PERLINDUNGAN DATA PERIBADI DAN PERHUBUNGAN ANTARA MAJIKAN DAN PEKERJA

Perhubungan antara majikan dan pekerja adalah berasaskan perjanjian atau kontrak perkhidmatan yang mewujudkan taggungjawab *fiduciary*. Menurut Seksyen 2 Akta Kerja 1955, kontrak perkhidmatan adalah mana-mana perjanjian, sama ada lisan atau bertulis dan sama ada nyata atau tersirat, di mana seorang bersetuju untuk mengambil bekerja seorang yang lain, dan orang yang lain itu bersetuju untuk berkhidmat dengan majikannya. Perhubungan antara majikan dan pekerja adalah berteraskan tanggungjawab pekerja menurut perintah dan menunjukkan hormat sewajarnya kepada majikan, dengan syarat majikan menunjukkan tanggungjawabnya untuk memelihara kebajikan pekerja dan memberikan layanan yang baik kepada pekerja.

Dalam konteks perlindungan data peribadi yang wujud dalam perhubungan majikan dan pekerja, majikan adalah pengguna data dan pekerja adalah data subjek. Majikan adalah berhak dan berkeperluan untuk memproses beberapa jenis data peribadi pekerja di fasa sebelum perlantikan, dalam perkhidmatan sebagai pekerja dan juga selepas penamatan perkhidmatan. (Zulkiflee Daud & Isa Mansur,2019). Antara data peribadi yang diproses termasuklah nama penuh, alamat, gambar, rekod

perkhidmatan dan rekod kewangan pekerja. Data-data peribadi ini diperlukan untuk pelbagai tujuan termasuklah perlantikan, latihan, gaji dan penilaian prestasi. Data-data ini juga disimpan untuk tempoh masa berbeza-beza dan dalam cara penyimpanan yang berbeza-beza.

Pekerja perlu untuk memberikan kerjasama untuk membolehkan data peribadi mereka diproses sekiranya tujuan pemprosesan data dimaklumkan kepada mereka. Pekerja juga berhak untuk mendapat jaminan bahawa data peribadi mereka adalah diproses dan disimpan dengan selamat seperti disebut dalam APDP 2010.

Kesedaran Pekerja Berkaitan Perlindungan Data Peribadi

Elemen yang paling utama dalam kesedaran keselamatan adalah elemen manusia atau pekerja dalam organisasi tersebut (Desman, 2003). Keselamatan sumber teknologi di tempat kerja sangat bergantung pada tingkah laku pekerja dan sangat penting sekiranya organisasi tersebut mengambil langkah untuk meningkatkan persepsi pekerja untuk mempraktikkan amalan terbaik keselamatan (Rantos et al., 2012). Abawajy (2014) menyatakan bahawa banyak pelanggaran keselamatan adalah disebabkan daripada kejahilan pengguna dan tingkah laku yang cuai ketika berkongsi maklumat seperti kata laluan dan membuka hantaran emel dari sumber yang tidak diketahui. Pekerja biasanya tidak menyedari akibatnya terhadap diri mereka sendiri atau organisasi apabila berlaku pelanggaran keselamatan ini.

Ross (2017) mendapati lebih daripada 90 peratus insiden keselamatan siber adalah berkaitan kesalahan pengguna siber itu sendiri. Walaupun banyak organisasi menerapkan teknologi keselamatan terkini seperti penggunaan biometrik, *firewall*, kad pintar dan enkripsi, tingkah laku pengguna terhadap keselamatan maklumat masih amat membimbangkan. Tingkah laku pekerja itu sendiri seperti tidak mencipta kata laluan yang kuat, berkongsi kata laluan dengan medium lain, membiarkan peranti disambungkan ke internet tanpa sebarang perlindungan dalam talian dan log masuk ke sistem organisasi melalui rangkaian tidak selamat. Selain itu, kecuaian pekerja ketika mengendalikan data dan maklumat organisasi banyak menyumbang kepada risiko ancaman keselamatan maklumat dalam organisasi (Norshima, 2021). Hal ini jelas memerlukan tindakan pihak eksekutif organisasi memberi latihan kesedaran keselamatan maklumat kepada semua pekerja.

Pada 2019, sejumlah data peribadi kakitangan Universiti Malaya dibocorkan di internet selepas beberapa jam pautan pembayaran atas talian milik universiti tersebut digodam. Kes ini melibatkan 649 kakitangan pengurusan dan 2,877 kakitangan sokongan. Hampir 24,000 emel ID login dan kata laluan dipercayai daripada pautan pembayaran dalam talian tersebut dibocorkan. Tambahan lagi, maklumat gaji ahli akademik dan bukan akademik termasuk nama dan akaun bank individu, nombor cukai pekerja, nombor Kumpulan Wang Simpanan Pekerja, maklumat jabatan dan pangkat didedahkan kepada umum serta sejumlah besar maklumat peribadi milik staf UM dibuang daripada dalam talian (Sinar Harian, 2019). Kes di atas menunjukkan bahawa institusi pendidikan juga menjadi tarikan kepada penjenayah siber dalam

salah guna data peribadi. Roman (2015) mencadangkan staf fakulti dan pelajar perlu diberi kesedaran tentang keselamatan siber dalam menerapkan tindakan yang lebih selamat ketika berkongsi data peribadi. Ini disokong oleh Furnell dan Clarke (2012) yang menyatakan pada era teknologi yang semakin mencabar ini, adalah penting untuk menganalisis faktor-faktor yang menyumbang kepada kesedaran keselamatan pengguna gajet kerana teknologi sahaja tidak dapat memberikan penyelesaian keselamatan yang lengkap kepada sesebuah organisasi. Kesedaran yang tidak mencukupi dalam kalangan pengguna dalam cara mengendalikan gajet dengan selamat seringkali membuka pintu kepada penjenayah siber untuk menggodam gajet.

Kajian oleh Muhammad Faheem dan Hasnira (2014) ke atas 100 orang pelajar Kolej Poly-Tech MARA (KPTM) Bangi menunjukkan sebanyak 98 peratus daripada mereka menyatakan kebimbangan tentang privasi maklumat peribadi mereka. Matlamat utama kesedaran keselamatan dalam organisasi adalah untuk meningkatkan kepentingan amalan terbaik keselamatan dan memberi kesedaran kepada pekerja tentang akibat yang akan diterima daripada pelanggaran keselamatan ini (Hanshe, 2001). Sebagai contoh dokumen yang dilupuskan secara cuai akan mendedahkan organisasi kepada risiko kecurian data peribadi yang dicetak. Ini merupakan kaedah biasa mencuri data peribadi yang mungkin digunakan oleh pihak ketiga yang berniat dalam menyalahgunakan data untuk mendapatkan akses ke rangkaian organisasi (Mayvin Loo, 2015).

Prinsip Penyimpanan Data Pekerja

Menurut seksyen 7 APDP 2010, sewaktu meminta data peribadi daripada pekerja, majikan perlu memberi notis yang mengandungi tujuan bagi memperoleh data peribadi tersebut dan semua maklumat lain yang dinyatakan di bawah seksyen yang sama. Hal ini jelas menunjukkan persetujuan dari pihak pekerja adalah diperlukan bagi memproses data peribadi. Dalam seksyen 4 APDP 2010, pemprosesan berhubung dengan data peribadi bermaksud mengumpul, merekod, memegang atau menyimpan data peribadi itu atau menjalankan apa-apa pengendalian atau set pengendalian terhadap data peribadi itu.

Menurut Jabatan Perlindungan Data Peribadi (2019), antara langkah pematuhan prinsip penyimpanan yang boleh diambil oleh majikan adalah memastikan organisasi menyediakan polisi privasi yang terperinci yang secara jelasnya memberitahu apakah dasar yang digunapakai oleh organisasi berkaitan peyimpanan data peribadi. Polisi privasi perlulah mengandungi klausa berkaitan penyimpanan data yang menyebut amalan organisasi yang akan merujuk kepada polisi dalaman dalam sebarang penyimpanan data peribadi tidak boleh melebihi tempoh yang sepatutnya. Perlu ada senarai segala jenis data peribadi pekerja yang disimpan oleh organisasi, huraian jenis data yang disimpan, tempoh penyimpanan, sebarang perundangan atau dasar pentadbiran yang membenarkan penyimpanan jenis data peribadi, langkah pelupusan data yang akan diambil dan pihak yang berkuasa untuk mengarahkan pelupusan data.

Selain itu, klausa penyimpanan juga perlu menerangkan sama ada data disimpan secara elektronik atau manual dan juga menyenaraikan langkah-langkah pelupusan data peribadi. Bagi pelupusan data peribadi yang disimpan secara fizikal, perlu dipastikan langkah yang dipilih dapat melupuskan data secara kekal atau dijadikan tanpa nama (*anonymised*) (Tataamalan Perlindungan Data Peribadi Untuk Sektor Utiliti (Elektrik), 2020). Begitu juga dengan data peribadi yang disimpan dalam medium elektronik, ianya perlu dipadamkan secara kekal. Ini kerana kadangkala berlaku situasi di mana data peribadi yang disimpan secara manual telah dilupuskan tetapi terdapat data peribadi digital yang terlepas pandang untuk pelupusan kekal dan dapat diakses semula oleh pihak-pihak tertentu. Walau bagaimanapun, data peribadi pekerja boleh disimpan untuk tujuan statistik atau analisis dengan syarat bahawa data tersebut tidak diproses bagi apa-apa tujuan lain dan statistik yang dihasilkan tidak tersedia dalm bentuk yang boleh mengenalpasti pemilik data peribadi tersebut(Tataamalan Perlindungan Data Peribadi Untuk Sektor Utiliti (Elektrik), 2020).

Selain itu, majikan juga boleh menetapkan jadual pelupusan data peribadi sebagai contoh, sebarang data peribadi yang tidak aktif dalam tempoh 24 bulan akan dilupuskan (Jillian, 2021). Dan jadual pelupusan tersebut perlu diselenggara secara berkala (Tataamalan Perlindungan Data Peribadi Untuk Sektor Utiliti (Elektrik), 2020). Kenyataan ini disokong oleh Munir (2010) yang berpendapat tempoh penyimpanan sesuatu data peribadi itu bergantung kepada tujuan di mana ia dikumpul.

Michael dan Richard (2018) menyatakan Sistem Maklumat Pengurusan Sumber Manusia (HRMIS) adalah sistem yang menyediakan maklumat daripada pangkalan data Pengurusan Sumber Manusia (PSM) yang boleh dianalisis secara menyeluruh dan terperinci mengikut pelbagai dimensi. Apabila melibatkan HRMIS dalam pengurusan perubahan di tempat kerja, organisasi mesti melihat kepada perspektif data dan perspektif proses. Perspektif data memfokuskan kepada analisis data, data organisasi yang diambil dan digunakan iaitu semua yang berkaitan dengan data yang diambil, dengan menumpukan cara yang paling berkesan dan efektif untuk mengambil dan menyimpan data dengan memastikan ketepatan (Nurhaziemah et al., 2019).

Ball et al.(2013) berpendapat walaupun terdapat pelbagai konsep berkaitan dengan privasi, kajian yang sering dikaitkan dengan privasi di tempat kerja adalah tertumpu kepada privasi data peribadi. Hal ini merangkumi maklumat yang dikumpul semasa pengambilan pekerja berkaitan pendidikan, latar belakang keluarga, keperibadian dan sejarah perubatan atau kesihatan yang didapati dapat menjejaskan privasi pekerja (Stone-Romero et al., 2003).

Selain itu, jika pemprosesan data peribadi sensitif pekerja seperti data kesihatan yang berkaitan dengan COVID 19 tidak diperuntukkan dalam kontrak atau polisi yang ada, majikan perlu mengeluarkan notis baru atau polisi tambahan kepada pekerja dan persetujuan daripada pekerja diperlukan (Darren et al, 2020). Perkara ini dapat mengelakkan berlakunya ketidaktelusan ketika mengumpul data peribadi daripada pekerja. Selain itu, menjadi persoalan tentang berapa lamakah tempoh penyimpanan data-data tersebut sama ada secara fizikal atau di alam maya oleh majikan.

Pekerja sebagai subjek data sudah tentu tidak mahu data peribadi mereka disimpan dan diproses oleh majikan secara tidak sah atau tanpa keperluan yang munasabah. Pekerja seharusnya terhindar daripada mengalami kebocoran atau pendedahan data peribadi kepada pihak lain tanpa kebenaran subjek data atau pekerja itu sendiri. Jika ini berlaku, kemungkinan besar majikan tersebut telah melanggar undang-undang dan seterusnya boleh menimbulkan akibat yang serius kepada majikan itu sendiri terutamanya apabila pekerja atau bekas pekerja membuat aduan (Chia Swee Yik, 2017).

Menurut seksyen 10 APDP 2010 tentang prinsip penyimpanan, APDP 2010 mewajibkan pengguna data untuk mengambil segala langkah yang munasabah untuk memastikan bahawa segala data peribadi dimusnahkan atau dipadamkan secara kekal jika data peribadi itu tidak lagi dikehendaki bagi maksud yang baginya data peribadi itu hendak diproses. Melalui ayat di dalam seksyen 10 ini tiada ketetapan bagi seberapa lama tempoh penyimpanan data namun perkataan 'dikehendaki' itu menjadi panduan dalam menetapkan seberapa lama data peribadi itu dapat disimpan (Sonny dan Maryam, 2011). Hal ini turut menjadi tanggungjawab majikan dalam penyimpanan data peribadi pekerja selepas pemberhentian pekerja tersebut (Hassan, 2012).

Walau bagaimanapun, sekiranya data peribadi ini mempunyai kaitan dengan undang-undang lain, tempoh penyimpanan data peribadi dapat ditentukan dan perkara ini tidak melanggar prinsip penyimpanan. Dalam erti kata yang lain, majikan ~~syarikat~~ mempunyai keperluan yang munasabah untuk menyimpan data tersebut lebih lama dari yang perlu disebabkan oleh tuntutan undang-undang. Majikan ~~Syarikat~~ juga hendaklah memastikan data peribadi pekerja tidak dilupuskan sebelum tamat tempoh yang ditetapkan oleh undang-undang yang mungkin boleh mengakibatkan ketidakupayaan bagi mempertahankan tuntutan litigasi, masalah operasi dan kegagalan untuk mematuhi mana-mana undang-undang dan peraturan terpakai (Tataamalan Perlindungan Data Peribadi Untuk Sektor Utiliti (Elektrik), 2020).

Mengikut seksyen 61 Akta Pekerja 1955, majikan dibenarkan untuk menyimpan maklumat pekerja untuk tempoh tidak kurang daripada enam (6) tahun daripada tempoh akhir perkhidmatan. Perkara ini dibenarkan mengikut seksyen 6 Akta Had Masa 1953 untuk memperuntukkan sebarang tindakan tuntutan oleh bekas pekerja sekiranya mengalami sebarang kecederaan adalah dalam tempoh enam (6) tahun. Ini jelas menunjukkan penyimpanan data peribadi pekerja turut melibatkan antara prinsip perlindungan data dan keperluan perundangan (Adlin et al., 2019).

Adlin et al. (2019) juga menjelaskan bahawa adalah penting untuk memastikan tujuan sesebuah data peribadi itu dikumpul. Sebagai contoh, majikan boleh menyimpan rekod pekerja yang telah cedera selama mereka bekerja sebagai data peribadi sensitif untuk jangka masa sehingga enam (6) tahun kerana terdapat potensi untuk tuntutan kecederaan diri. Hal ini seperti yang dinyatakan dalam Akta Had Masa 1953 bahawa sebarang tindakan mestilah dilakukan dalam masa enam (6) tahun daripada tarikh penyebab tindakan tersebut berlaku.

Kesalahan dan Hukuman berkaitan APDP 2010

Mengikut APDP 2010, pengguna data atau majikan boleh dikenakan tindakan sekiranya berlaku perlanggaran undang-undang berkenaan prinsip perlindungan data peribadi yang tertakluk dalam subseksyen 5(2) iaitu berkenaan kesalahan pemprosesan data peribadi yang tidak mematuhi Prinsip Perlindungan Data Peribadi. Hukuman yang akan dijatuhkan adalah denda tidak melebihi RM 300,000 atau dipenjarakan selama tempoh tidak melebihi dua (2) atau kedua-duanya.

Salah satu hak subjek data ialah hak untuk menarik balik kebenaran memproses data peribadi melalui notis bertulis seperti yang tertakluk dalam subseksyen 38(1). Sekiranya majikan tidak memberhentikan pemprosesan data peribadi selepas menerima notis menarik balik persetujuan daripada subjek data, majikan tersebut boleh didenda tidak melebihi RM 100,000 atau dipenjarakan selama tempoh tidak melebihi 1 tahun atau kedua-duanya.

Meskipun terdapat waktu yang lama untuk menyimpan data peribadi bekas pekerja organisasi, majikan seharusnya hanya menggunakan data tersebut secara beretika dan tidak menyalahgunakan kebenaran/kelonggaran yang diberikan oleh undang-undang. Pada 3 Mei 2017, seorang majikan dari syarikat Khas Cergas Sdn Bhd telah didakwa di bawah Akta Perlindungan Data Peribadi Malaysia 2010 kerana memproses data atau maklumat peribadi bekas pekerja Kolej Antarabangsa Victoria tanpa perakuan pendaftaran yang dikeluarkan oleh Pesuruhjaya Perlindungan Data Peribadi. Ini adalah pendakwaan pertama di bawah APDP 2010 walaupun pada hakikatnya akta ini telah berkuat kuasa sejak 15 November 2013. Kesalahan tersebut, jika disabitkan, boleh dihukum di bawah Akta dengan denda maksimum RM500,000 atau penjara sehingga tiga tahun, atau kedua-duanya (Mageswari, 2017). Kes ini berkenaan majikan yang memproses data peribadi bekas pekerjanya tanpa lesen atau perakuan pendaftaran yang dikeluarkan oleh Pesuruhjaya Perlindungan Data Peribadi di bawah subseksyen 16(1)(a) APDP 2010.

KESIMPULAN

Kajian ini telah meneliti peruntukan perundangan yang berkaitan prinsip penyimpanan perlindungan data peribadi di Malaysia dan secara khususnya menumpukan pada pematuhan kepada prinsip penyimpanan data peribadi pekerja oleh pihak majikan. Prinsip penyimpanan menekankan bahawa sesuatu data peribadi itu tidak dibenarkan disimpan di dalam sesuatu pemprosesan lebih daripada had masa yang diperlukan. Majikan sebagai pengguna data yang menyimpan pelbagai jenis data peribadi pekerja, bertanggungjawab memastikan bahawa semua data peribadi ini disimpan dengan selamat dan tidak disimpan mengikut tempoh yang berlebihan.

Langkah awal yang boleh diambil adalah dengan memastikan organisasi telah berdaftar sebagai pengguna data dengan Jabatan Perlindungan Data Peribadi dan telahpun menyediakan polisi privasi yang komprehensif. Antara tindakan lain yang boleh diambil oleh majikan adalah dengan mengambil langkah meningkatkan

kesedaran pekerja mengenai kepentingan perlindungan data peribadi. Pekerja di semua lapisan organisasi perlu diberikan pendedahan mengenai prinsip-prinsip perlindungan data. Selain itu, organisasi perlu juga memulakan proses semakan terhadap semua polisi, dokuman dan gerak kerja yang melibatkan penyimpanan data peribadi. Langkah seterusnya adalah perancangan di peringkat organisasi untuk bagaimana melaksanakan pematuhan dan penambahbaikan kepada amalan sedia ada.

Terdapat beberapa golongan pengguna data seperti perbankan dan institusi kewangan, pengankutan dan utiliti yang telah memiliki tataamalan tersendiri. Ini memudahkan organisasi-organisasi yang terlibat untuk merangka tindakan yang perlu diambil kerana telah wujud panduan yang jelas. Bagi golongan pengguna data lain, mereka perlu membuat perancangan dan penilaian sendiri bergantung kepada jenis dan keperluan terhadap data peribadi pekerja yang mereka simpan. Jika tiada perundangan lain yang meletakkan syarat tertentu, Seksyen 10 APDP memberi kelonggaran kepada pengguna data untuk memutuskan sendiri tempoh waktu yang dianggap bersesuaian untuk data tersebut disimpan.

Kajian ini diharapkan dapat memberi manfaat literatur kepada pengkaji dan kajian seterusnya berkaitan pemprosesan dan penyimpanan data peribadi pekerja. Kajian seterusnya dicadangkan dapat dilakukan dengan menggunakan data daripada kajian kes dan temubual mendalam dengan organisasi yang bertindak sebagai majikan. Ini akan menberikan dapatan yang lebih terperinci. Selain itu, penelitian tentang prinsip penyimpanan data peribadi pekerja ini juga diharap dapat menjadi panduan kepada pelbagai organisasi dalam menguatkuasakan undang-undang berkaitan perlindungan data peribadi dan pekerja.

RUJUKAN

Adlin Abdul Majid, Shariffullah Majeed and Arissa Ahrom. (2019). *Managing Employee Data Under the Personal Data Protection Act 2010*. Legal Herald, December 2019. Diakses daripada https://www.lh-ag.com/wp-content/uploads/2019/12/4_Managing-Employee-Data.pdf

Ball, Kirstie; Daniel, Elizabeth and Stride, Chris (2013). Dimensions of employee privacy: an empirical study. Information Technology and People (In press).

Butler Smith, L. (2009). Workplace privacy: We'll be watching you. *Ohio NUL Rev*. 35, 53.

Chia Swee Yik. (2017). *Basics of Personal Data Protection for Employee*. Chia, Lee and Associates. Retrieved from https://chialee.com.my/basics-of-personal-data-protection-for- employers/

Furnell, S., Clarke, N. (2012). Power to People? The Evolving Recognition of Human Aspects of Security. Computer & Security 31(8): 983-988.

Hanshe, S. (2001). *Designing a security awareness plan: Part I*. Information Systems Security, 14-22.

Hassan, Kamal. (2012). Personal data protection in employment: New legal challenges for Malaysia. Computer Law & Security Review. 28. 696–703. 10.1016/j.clsr.2012.07.006.

Kusumoningtyas, A. A., & Nasional, P. K. K. (1997). DILEMA HAK PERLINDUNGAN DATA PRIBADI DAN PENGAWASAN SIBER: TANTANGAN DI MASA DEPAN. *Jurnal Legislasi Indonesia*. Vol 17, No 2 (2020): Jurnal Legislasi Indonesia - Juni 2020, Direktorat Jenderal Peraturan Perundang-undang, Kementerian Hukum dan Hak Asasi Manusia.

Portal Rasmi Jabatan Perlindungan Data Peribadi. (2020). *Tatacara Pengendalian Bagi Aktiviti Pengumpulan, Pemprosesan Dan Penyimpanan Data Peribadi Oleh Premis Perniagaan Semasa Perintah Kawalan Pergerakan Bersyarat (PKPB) 2020*.

Mageswari M. (2017). College Operator First to be Hauled to Court under PDP Act. *The Star*, 4 May 2017. Retrieved from https://www.thestar.com.my/news/nation/2017/05/04/college-operator-first-to-be-hauled-to-court-under-pdp-act/#UmM5brVGW1SryPhh.99

Marina Abdul Manap. (2020). Perkembangan Undang-Undang Privasi Di England Dan Malaysia: Satu Tinjauan. *Journal of Law & Governance,* Volume 3 (No. 1) 2020:1-17. e-ISSN: 2637-0743.

Mayvin Loo. (2015. Workplace Tips on Personal Data Protection. *DPO Connect*. Personal Data Protection Commission Singapore. August 2015.

Michael J Kavanagh & Richard D. Johnson (2018). Human Resource Information System, Basic Application & future Direction 4th edision. SAGA Publishing

Mohd Hamdan Haji Adnan. (2015). Peranan Media Massa Memartabatkan Integriti Nasional. *Jurnal Komunikasi Borneo 2015*. Vol 2.

Muhammad Adnan Pitchan & Siti Zobidah Omar. (2019). Dasar Keselamatan Siber Malaysia: Tinjauan Terhadap Kesedaran Netizen dan Undang-Undang (Cyber Security Policy: Review on Netizen Awareness and Laws). *Jurnal Komunikasi: Malaysian Journal of Communication*. 35. 103-119. 10.17576/JKMJC-2019-3501-08.

Muhammad Faheem & Hasnira Md Lazim. (2014). The Privacy Concerns Of Kptm Bangi's Students Regarding The Online Application In KPTM Website. Diakses daripada (PDF) THE PRIVACY CONCERNS OF KPTM BANGI'S STUDENTS REGARDING THE ONLINE APPLICATION IN KPTM WEBSITE (researchgate.net)

Norshima Humaidi (Mei 21, 2021). Kesedaran keselamatan maklumat masih rendah. *Berita Harian Online*. Diakses pada 14 September 2021 daripada https://www.bharian.com.my/rencana/komentar/2021/05/819081/kesedaran-keselamatan-maklumat-masih-rendah

Nurhaziemah Adevin dan Nurul Aiman Syazwani Muhd Nor (2019). Pengaruh Human Resource Imformation System (Hris) Dalam Pengurusan Perubahan Tempat Kerja. Diakses daripada https://www.researchgate.net/publication/337631906_PENGARUH_HUMAN_RESOURCE_IMFORMATION_SYSTEM_HRIS_DALAM_PENGURUSAN_PERUBAHAN_TEMPAT_KERJA

Pesuruhjaya Perlindungan Data Peribadi. (2020). Tataamalan Perlindungan Data Peribadi Untuk Sektor Utiliti (Elektrik). Diakses pada 30 September 2021 daripada https://www.pdp.gov.my/jpdpv2/tata_amalan/tataamalan-perlindungan-data-peribadi-untuk-sektor-utiliti-elektrik-versi-2-0-bahasa-melayu/

Rantos, K., Fysarakis, K., Manafavis, C. (2012). How effective is your security awareness program? An evaluation methodology, *Information Security Journal: A Global Perspective*, 21(6), 328-345.

Roman, J. (2015). Universities: prime breach targets. Retrieved from https://www.databreachtoday.asia/universities-prime-breach-targets-a-7865

Ross Kelly (2017). Almost 90% of Cyber Attcks are Caused by Human Error or Behavior. Chief Executive. Diakses daripada https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/

Sinar Harian (Oktober 20, 2019). Penggodam papar data dalam internet. *Astro Awani*. Diakses pada 15 September 2021 daripada https://www.astroawani.com/berita-malaysia/penggodam-papar-data-dalam-internet-220542

Sonny Zulhuda dan Maryam Delpisheh (2011). Personal Data "Up in the Air": A Tale of Two Malaysian Airlines in Dealing with Consumers Online Privacy. *International Conference on Social Science and Humanity*. IPEDR vol.5 (2011), IACSIT Press, Singapore.

Stone-Romero, E.F.; Stone, D.L. and Hyatt, D. (2003), "Personal selection procedures and invasion of privacy", Journal of Social Issues, Vol 59 No 2, pp. 343 – 368.

Suara Sinar (Ogos 27, 2020). Isu Rekod Data Peribadi ketika COVID-19. *Sinar Harian*. Diakses daripada https://www.sinarharian.com.my/article/98460/SUARA-SINAR/Lidah-Pengarang/Isu-rekod-data-peribadi-ketika-Covid-19