

## **PEMATUHAN KEPADA PERLINDUNGAN DATA PERIBADI PEKERJA DI INSTITUSI PENGAJIAN TINGGI**

**FARAH MOHD SHAHWAHID**

**NAWAL SHOLEHUDDIN**

**UMMI MUNIRAH SYUHADA MUHAMMAD ZAN**

Kolej Universiti Islam Antarabangsa Selangor

### **ABSTRAK**

Akta Perlindungan Data Peribadi 2010 mewajibkan pengguna data dari 13 sektor memberi perlindungan ke atas data peribadi data subjek, iaitu pihak-pihak yang berurusan dengan pengguna data untuk tujuan komersial. Kertas kerja ini membincangkan berkenaan perlindungan data peribadi di tempat kerja dalam sektor pendidikan. Dalam konteks pekerjaan, pekerja adalah subjek data dan majikan bertindak sebagai pengguna data. Perhubungan antara kedua pihak ini mewujudkan beberapa hak dan tanggungjawab yang perlu dipenuhi berkaitan pemrosesan data peribadi. Kertas kerja kualitatif ini, melalui analisis kepustakaan dan juga sesi temubual dengan pihak pengurusan sumber manusia di sebuah institusi pengajian tinggi akan membincangkan konteks data peribadi, jenis-jenis data peribadi dan perundangan yang berkaitan dengan perlindungan data peribadi pekerja. Selain itu, artikel ini juga mengenalpasti langkah-langkah pematuhan yang diambil oleh institusi pengajian tinggi dan juga cabaran-cabaran yang dihadapi dalam mematuhi Akta ini. Dapatan kajian menunjukkan bahawa pihak pengurusan institusi pengajian tinggi menyedari kewajipan untuk mematuhi perundangan ini dan pematuhan kepada Akta ini memerlukan komitmen daripada pihak pengurusan institusi sebagai pengguna data dan juga kerjasama daripada para pekerja dalam mengambil langkah melindungi data peribadi mereka.

**Kata Kunci** : perlindungan data peribadi, privasi, institusi pengajian tinggi, prinsip-prinsip perlindungan data peribadi)

### **1. Pengenalan**

Di bawah perundangan Malaysia, perlindungan data peribadi dikuatkuasakan di bawah Akta Perlindungan Data Peribadi 2010 (APDP). Akta ini, yang mula dikuatkuasakan secara berkala pada tahun 2013 merupakan perundangan pertama di Malaysia yang mempertanggungjawabkan pengguna data untuk mengambil langkah-langkah tertentu untuk melindungi data peribadi subjek data dengan mewajibkan pematuhan prinsip-prinsip perlindungan data terhadap pengguna data. Perintah Perlindungan Data Peribadi (Golongan Pengguna Data) 2013 menyenaraikan golongan pengguna data yang perlu mendaftar dengan Jabatan Perlindungan Data Peribadi seperti yang termaktub bawah Seksyen 14 APDP. Salah satu golongan pengguna data tersebut adalah sektor pendidikan termasuklah institusi pengajian tinggi swasta yang berdaftar di bawah Akta Institusi Pendidikan Tinggi Swasta 1996. (Akta 555)

Sebagai pengguna data, institusi pengajian tinggi swasta (IPTS) bertanggungjawab melindungi data peribadi dua kategori subjek data iaitu pelajar dan pekerja di institusi tersebut. Walaupun jenis data yang dilindungi mungkin berbeza, langkah-langkah pematuhan yang diambil untuk melindungi data peribadi tersebut adalah sama.

## **2. Data Peribadi**

Kamal (2012) menyatakan data peribadi merujuk kepada data mana-mana individu atau orang. Laman sesawang Jabatan Perlindungan Data Peribadi pula menerangkan data peribadi sebagai bermaksud apa-apa maklumat yang digunakan di dalam transaksi komersial yang berhubungan secara langsung atau tidak langsung dengan seseorang subjek data yang dikenalpasti daripada maklumat tersebut. Kedua-dua definisi yang diberikan adalah selari dengan apa yang dinyatakan dalam APDP.

APDP mentafsirkan data peribadi sebagai apa-apa maklumat yang berkenaan transaksi komersial yang berhubungan secara langsung atau tidak langsung dengan subjek data, yang dikenal pasti atau boleh dikenal pasti daripada maklumat itu. Memandangkan APDP hanya melindungi data daripada transaksi komersial, data yang diproses untuk tujuan-tujuan peribadi adalah tidak dilindungi di bawah akta ini.

Dalam konteks perlindungan data peribadi di IPTS, pusat IPTS adalah pengguna data yang memproses data pelajar dan juga pekerja. Pekerja di IPTS adalah subjek data di mana pelbagai jenis data peribadi pekerja yang diproses oleh majikan mereka iaitu pihak IPTS. Jenis data peribadi yang dibenarkan oleh akta untuk diproses oleh pengguna data termasuklah tetapi tidak terhad kepada maklumat peribadi termasuk maklumat keagamaan, maklumat untuk menghubungi pekerja, maklumat perubatan, maklumat kewangan, dan juga maklumat penggajian dan prestasi di tempat kerja (Selvamalar & Siva Kumari, 2020).

## **3. Perlindungan Data Peribadi dan Tempat Kerja**

### **3.1 Perlindungan Data Peribadi Pekerja**

Menurut International Labour Organisation, terdapat banyak sebab mengapa majikan mengumpul data peribadi pekerja dan juga calon pekerja: sebagai langkah pematuhan undang-undang, untuk membantu pemilihan pekerja, untuk tujuan Latihan dan kenaikan pangkat, tujuan keselamatan, perkhidmatan pelanggan dan juga perlindungan harta majikan. Terdapat keperluan untuk mengawal selia proses-proses pengumpulan data kerana dengan setiap proses pengumpulan data wujud juga risiko kepada pekerja yang datanya dikumpul. (ILO, 1997)

Menurut Kamal (2012) tafsiran data peribadi dalam APDP menunjukkan bahawa perundangan ini hanya terpakai bagi data yang berkaitan dengan transaksi komersial. Transaksi komersial dalam konteks ini didefinisikan sebagai transaksi yang bersifat komersial, sama ada secara kontrak atau tidak, yang merangkumi hal-hal yang berkaitan dengan pembekalan atau pertukaran barang atau perkhidmatan, agensi, pelaburan, pembiayaan, perbankan dan insurans. Dalam hal ini, 'transaksi komersial' dengan mudah diperluas ke pekerjaan kerana kata 'perkhidmatan' di bahagian itu merujuk kepada pekerjaan. Perhubungan yang wujud antara majikan dan pekerja biasanya diikat melalui satu perjanjian atau kontrak, sama ada kontrak yang dimeterai antara kedua pihak adalah 'kontrak perkhidmatan' atau 'kontrak untuk perkhidmatan'. Di bawah kedua-dua kategori kontrak tersebut, terdapat banyak situasi di mana akan berlakunya pemprosesan data. Mengikut tafsiran APDP, majikan adalah pengguna data

manakala pekerja yang menyerahkan data peribadi kepada majikan adalah data subjek, Oleh itu, majikan wajib menguruskan data peribadi individu atau pekerja mengikut APDP.

Kontrak perkhidmatan mewujudkan tugas, kewajipan dan tanggungjawab yang mesti dilaksanakan oleh kedua-dua pihak. Majikan perlu menjalankan tanggungjawabnya terhadap pekerja dan pekerja perlu menjalankan tanggungjawabnya terhadap majikan (Kamal& Rozana, 2009). Salah satu tanggungjawab majikan adalah menyediakan tempat kerja yang selamat. Pematuhan terhadap APDP adalah salah satu cara memastikan tempat kerja adalah selamat kerana kebelakangan ini, banyak dilaporkan pelbagai kes kesalahan berkaitan kebocoran data peribadi, penipuan identiti dan frod yang semuanya melibatkan penyalahgunaan data peribadi. Tempat kerja merupakan salah satu sumber utama untuk pihak yang tidak bertanggungjawab memperolehi data peribadi individu yang ramai.

Di pihak pekerja, adalah menjadi tanggungjawab pekerja untuk mematuhi arahan majikan dan juga untuk menjalankan tugas yang diberikan dengan cekap, amanah dan suci hati. Dalam kajian Deakin & Morris (1998) kerangka teori perlindungan data peribadi dapat dikembangkan dari tugas pihak-pihak di bawah kontrak pekerjaan. Kontrak pekerjaan mengandungi terma dan syarat, dan kewajipan yang mesti dilaksanakan oleh pihak berdasarkan prinsip niat baik, kesetiaan dan kesetiaan.

Sebagai perantara antara institusi dan pihak ketiga, mana-mana pekerja yang berurusan dengan data peribadi subjek data, sama ada data pelajar ataupun data pekerja institusi, perlulah memproses data tersebut dengan cara-cara yang mematuhi peruntukan-peruntukan dalam APDP. Kegagalan pekerja menjalankan kewajipan tersebut, boleh dianggap sebagai pemecahan kontrak ataupun menimbulkan tuntutan di bawah tort atau pelanggaran terma kontrak (Kamal & Rozana, 2009). Sebagai pekerja juga, dari aspek subjek data, mereka berhak untuk memastikan majikan telah mengambil semua langkah-langkah yang sepatutnya untuk melindungi dan menjaga kerahsiaan data peribadi mereka.

Menurut Chia Swee Yik (2017), pada 2017 terdapat satu kes di mana seorang majikan telah didakwa di bawah APDP 2010 kerana memproses data atau maklumat peribadi bekas pekerjanya tanpa perakuan pendaftaran yang dikeluarkan oleh Pesuruhjaya Perlindungan Data Peribadi. Ini adalah pendakwaan pertama di bawah Akta walaupun hakikatnya 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.

Memandangkan kepentingan pihak pekerja dan majikan mengenai isu-isu berkaitan privasi kadang kalanya bertentangan, di mana majikan merasakan keperluan untuk menyimpan data pekerja manakala pekerja mempunyai kehendak untuk mengawal data peribadi mereka, wujud keperluan untuk merujuk kepada perundangan yang berkaitan. Perundangan digunakan untuk menentukan hak-hak pihak yang terlibat, walaupun kadang kala timbul perbezaan pentafsiran mengenai hak privasi data peribadi. (Bhave, Teo et al, 2020)

### **3.2 Hak Subjek Data**

Berkaitan dengan pemprosesan data peribadi individu, hak berkanun tertentu diberikan di bawah APDP. Kajian Farah dan Surianom (2014) menyenaraikan hak-hak subjek data, keenam-enam hak tersebut adalah hak untuk diberitahu, hak untuk mengakses data peribadi,

hak untuk membetulkan data peribadi, hak untuk menarik persetujuan, hak untuk mencegah pemrosesan yang mungkin menyebabkan kerosakan atau kesusahan dan hak untuk mencegah pemrosesan untuk tujuan langsung pemasaran.

Seksyen 30 ke 33 APDP menerangkan hak untuk mengakses data peribadi. Seseorang berhak diberitahu jika data peribadinya sedang diproses oleh atau atas nama pengguna data. Seksyen 30 (2) mengatakan bahwa setelah pembayaran biaya yang ditentukan, pemohon dapat membuat permintaan akses data secara tertulis kepada pengguna data untuk mendapatkan informasi mengenai data peribadi subjek data yang sedang diproses oleh pengguna data dan agar informasi tersebut disampaikan kepadanya dalam bentuk yang difahami. Walau bagaimanapun, seksyen 32 menetapkan beberapa keadaan di mana pengguna data boleh menolak untuk memenuhi permintaan tersebut.

Hak untuk membetulkan data peribadi juga diperuntukkan dalam Akta di bawah seksyen 34. Seksyen 34 (1) menyatakan bahwa di mana pemohon permintaan akses data atau subjek data sendiri menganggap bahawa data pribadi yang dipegang oleh pengguna data tidak tepat, pemohon atau subjek data, dapat membuat permintaan pembetulan data secara tertulis kepada pengguna data untuk pindaan yang perlu dibuat terhadap data peribadi. Walau bagaimanapun, seksyen 36 menyatakan bahawa dalam keadaan tertentu, pengguna data mungkin menolak untuk mematuhi permintaan pembetulan data.

Hak untuk menarik persetujuan untuk memproses data dijamin di bawah seksyen 38 yang menyatakan bahawa pengguna data akan menghentikan pemrosesan data peribadi setelah menerima notis secara bertulis untuk dia melakukannya.

Selanjutnya, seksyen 42 menjelaskan hak subjek data untuk mencegah pemrosesan data peribadi yang mungkin menyebabkan kerosakan atau kesusahan kepada subjek data atau orang lain. Peruntukan ini juga memberikan hak kepada subjek data untuk mencegah pengguna data mengumpulkan, memegang, memproses atau menggunakan data peribadinya. Untuk menggunakan peruntukan ini, subjek data mesti membuktikan bahawa pengumpulan, pemegangan, pemrosesan atau penggunaan data peribadi tersebut menyebabkan atau mungkin menyebabkan kerosakan atau kesusahan yang substantial, dan kerosakan atau kesusahan yang disebabkan adalah tidak wajar. Oleh kerana perkataan 'substansial' tidak didefinisikan dalam akta, maka perkataan itu perlulah ditafsirkan mengikut kesesuaian dengan jenis data peribadi atau industri tertentu dalam situasi tertentu.

Hak lain termasuklah hak untuk memutuskan sama ada subjek data ingin maklumat peribadi mereka digunakan untuk tujuan pemasaran langsung. Seksyen 43(1) menyatakan bahwa subjek data, dapat mengirimkan pemberitahuan secara tertulis kepada pengguna data, mengharuskan pengguna data berhenti atau tidak meneruskan dengan pemrosesan data peribadinya untuk tujuan pemasaran langsung. Pemasaran langsung didefinisikan dalam APDP yang bermaksud komunikasi dengan cara apa pun dari setiap iklan atau bahan pemasaran yang ditujukan kepada individu tertentu. Hak ini dapat dilaksanakan oleh subjek data pada bila-bila masa, walaupun pada awalnya mereka telah menyetujui penggunaan data peribadinya, persetujuan ini dapat dibatalkan kemudian.

### **3.3 Prinsip-prinsip Perlindungan Data Peribadi.**

Satu aspek utama dalam APDP adalah memastikan pematuhan pengguna data terhadap prinsip-prinsip perlindungan data peribadi selari dengan objektif Akta ini iaitu untuk mengawal selia pemprosesan data peribadi seseorang individu oleh pengguna data agar ia digunakan dengan cara yang penuh berintegriti, selamat dan tidak disalahgunakan.

Seksyen 5 APDP menyenaraikan tujuh (7) prinsip perlindungan peribadi yang perlu dipatuhi oleh institusi pengajian tinggi sebagai pengguna data iaitu:

Pertama - Prinsip Am di mana pengguna data tidak dibenarkan memproses data peribadi seseorang lain tanpa kebenarannya.

Kedua - Prinsip Notis dan Pilihan di mana maklumat dan tujuan pemprosesan data dimaklumkan kepada subjek data berkenaan.

Ketiga - Prinsip Penzahiran iaitu kepada siapa data peribadi seseorang subjek data itu dizahirkan perlu dikenalpasti dan dimaklumkan kepada subjek data

Keempat - Prinsip Keselamatan apabila memproses data peribadi mana-mana subjek, pengguna data perlu mengambil langkah supaya data tersebut selamat, tidak diubahsuai, disalahguna atau diberikan kepada pihak-pihak yang tidak berkenaan.

Kelima - Prinsip Penyimpanan mengatakan sesuatu data peribadi itu tidak dibenarkan disimpan di dalam sesuatu pemprosesan lebih daripada had masa yang diperlukan

Keenam - Prinsip Integriti Data bahawa setiap data peribadi dipastikan supaya tepat, lengkap, tidak mengelirukan dan terkini menepati maksud sesuatu data itu disimpan dan diproses.

Ketujuh - Prinsip Akses di mana seseorang hendaklah diberi hak akses kepada data peribadinya yang dipegang oleh seseorang pengguna data dan juga berhak membetulkan datanya..

### **3.4 Pematuhan IPTS sebagai pengguna data**

Kajian kualitatif ini menggunakan temubual untuk mendapatkan dapatan berkaitan tahap pematuhan perlindungan data peribadi di sebuah IPTS. Melalui temubual yang dijalankan bersama pengurus bahagian sumber manusia institusi tersebut, telah dimaklumkan bahawa IPTS tersebut telah berjaya mendaftar sebagai pengguna data beberapa tahun yang lalu dan telah pun diberikan perakuan pendaftaran pengguna data (seiring dengan Seksyen 16 APDP). IPTS ini kini sedang dalam proses penyediaan dasar privasi sebagai satu lagi langkah pematuhan kepada APDP. Walau bagaimanapun, langkah-langkah pematuhan masih sedang dan telahpun diambil sementara menunggu penyempunaan dasar privasi tersebut.

#### **3.4.1 Prinsip Am**

Untuk memenuhi syarat-syarat yang terkandung dalam Seksyen 6 berkaitan prinsip am perlindungan data, pihak IPT sedang dalam proses menyemak dan mengemaskini semua borang-borang yang melibatkan pemprosesan data pengguna subjek yang berurusan dengan IPY, termasuklah data pekerja dan juga data pelajar. Proses ini mengambil masa yang panjang kerana ia melibatkan Kerjasama banyak bahagian dan jabatan memandangkan terdapat banyak jenis data yang diproses oleh IPT.

Antara jenis data yang diproses oleh IPT apabila melibatkan pekerja termasuklah data yang dikumpul dari peringkat permohonan bekerja di institusi tersebut, data penjawatan (termasuklah data berkaitan kenaikan pangkat, penukaran jawatan dan rekod disiplin) data penggajian, dan juga data maklumat peribadi pekerja dan tanggungan (termasuk kelayakan manfaat pekerjaan seperti kelayakan cuti bersalin, cuti ehsan dan juga manfaat rawatan perubatan).

Menurut peruntukan ini, pengguna data yang ingin memproses data peribadi mengenai seorang subjek data perlu memastikan subjek data itu telah memberikan persetujuannya bagi pemprosesan data peribadi itu. Terdapat syarat yang lebih ketat berkaitan pemprosesan data sensitif, di mana pengguna data tidak boleh memproses data peribadi sensitif mengenai seorang subjek data kecuali mengikut peruntukan seksyen 40 APDP.

Amalan di IPT ini telah lama memerlukan pekerja untuk berkongsi pelbagai jenis data peribadi dengan pihak majikan. Pekerja juga diminta untuk menghubungi bahagian sumber manusia yang bertindak sebagai wakil pihak majikan untuk mengemaskini secara berkala data peribadi yang sedia ada. Belum ada sebarang dokumentasi spesifik yang memohon kebenaran daripada pekerja sebagai subjek data untuk pihak majikan memproses data peribadi pekerja. Selama ini, pihak majikan menggunakan kebenaran pekerja secara tersirat melalui andaian bahawa kebersediaan pekerja menyerahkan data peribadi mereka kepada majikan merupakan tanda persetujuan untuk majikan memproses data mereka. Setelah melengkapkan proses pendaftaran sebagai pengguna data, pihak majikan sedang mengenalpasti mekanisma terbaik untuk mendapatkan kebenaran secara tersurat (*expressed consent*) daripada pekerja.

Pemprosesan data di IPT ini meliputi pengendalian data melalui cara atau kaedah automatik dan juga manual. Terdapat data yang dipohon dan disimpan melalui kaedah automatik seperti pengisian borang dalam talian menggunakan google form dan borang-borang yang yang dihantar melalui emel dan terdapat juga data yang dikongsi dan disimpan secara manual contohnya pengisian borang dan serahan dokumen lampiran secara bersemuka kepada pegawai di Bahagian sumber manusia.

Berkenaan pemprosesan data oleh pengguna data tanpa mendapat kebenaran pihak subjek data, pihak majikan mengakui terdapat beberapa situasi di mana mereka dibenarkan memproses data milik subjek data tanpa kebenaran. Antara sebab-sebab yang dibenarkan pemprosesan data sebegini adalah apabila terdapat permohonan bertulis dari pihak berkuasa seperti urusan pembayaran cukai pekerja oleh Lembaga Hasil Dalam Negeri (LHDN) atau untuk membantu penyiasatan pihak Polis Di Raja Malaysia (PDRM).

### 3.4.2 Prinsip Notis dan Pilihan

Seksyen 7 APDP mewajibkan pihak majikan Prinsip Notis dan Pilihan di mana maklumat dan tujuan awalan perlu dimaklumkan kepada subjek data berkenaan pemprosesan data peribadi mereka. Seperti yang telah dinyatakan di atas, pihak IPTS masih dalam proses untuk pematuhan penuh peruntukan ini. Antara langkah terawal yang diambil oleh institusi setelah berjaya mendaftarkan institusi sebagai pengguna data (Seksyen 15 APDP) adalah mengambil keputusan mempamerkan sijil perakuan pendaftaran pengguna data di suatu tempat umum. Berkenaan pemprosesan data peribadi pekerja, institusi mula bertindak seperti langkah pemakluman melalui emel mengenai data yang dipohon daripada pekerja. Di masa ini, pihak

IPTS sedang merangka satu notis bertulis yang seragam yang akan digunakan oleh semua jabatan di institusi untuk mematuhi syarat berkenaan keperluan untuk notis pemakluman secara bertulis berkaitan kebenaran pekerja utk pemprosesan data, jenis data yang diproses dan juga tujuan serta limitasi dalam penggunaan data yang diproses.

### 3.4.3 Prinsip Penzahiran

Prinsip penzahiran dalam Seksyen 8 APDP mengatakan bahawa data peribadi tidak boleh dizahirkan bagi apa-apa maksud selain maksud pada masa pengumpulan data peribadi itu dan juga tidak boleh dizahirkan kepada mana-mana pihak selain pihak ketiga yang telah dinyatakan dalam dasar privasi.

Bagi pematuhan prinsip penzahiran, pihak IPTS telah lama mengamalkan merahsiakan data peribadi semua pihak yang berhubung dengan mereka, sama ada pihak pelajar, mahupun pekerja di institusi. Secara spesifik, dalam memproses data peribadi pekerja, kebanyakan data peribadi pekerja adalah diproses oleh Bahagian sumber manusia dan akses kepada data ini adalah terhad kepada staf tertentu yang menjaga unit tertentu sahaja. Pihak IPTS ada berkongsi maklumat peribadi tertentu pekerja di laman sesawang IPTS tetapi data tersebut terhad kepada gambar korporat pekerja, nama penuh, jawatan dan emel rasmi pekerja sahaja. Keperluan untuk berkongsi maklumat ini juga telah dimaklumkan kepada semua pekerja. Maklumat yang dipaparkan adalah untuk memudahkan pihak institusi dan juga pihak ketiga yang perlu berhubung dengan pekerja institusi. Sebarang komunikasi adalah untuk tujuan rasmi atau yang berkait secara langsung dengan tugas pekerja tersebut di institusi. Ini merangkumi tetapi tidak terhad kepada komunikasi yang melibatkan pengajaran dan pembelajaran, penyelidikan, urusan pentadbiran dan urusan-urusan lain yang berkaitan dengan skop tugas pekerja tersebut.

Diakui, terdapat kes-kes terpencil di mana pihak ketiga dari luar telah menggunakan maklumat di laman sesawang institusi untuk menghubungi pekerja institusi untuk tujuan selain dari urusan rasmi, tetapi ini berlaku tanpa pengetahuan atau kebenaran pihak institusi. Situasi ini adalah di luar kawalan institusi kerana mereka tidak mampu mengawal pihak mana yang melawat laman sesawang institusi. Apa yang boleh diberi jaminan adalah pihak institusi sendiri tidak dan tidak pernah berkongsi atau memberi kebenaran kepada mana-mana pihak ketiga untuk menggunakan data peribadi pekerja untuk tujuan-tujuan di luar skop tugas pekerja. Antara penzahiran data peribadi yang pernah ditolak termasuklah permohonan data dari pihak ketiga yang mahu memasarkan produk jualan, atau permohonan data untuk membolehkan pihak ketiga menghubungi pekerja untuk urusan peribadi.

### 3.4.4 Prinsip Keselamatan

Prinsip Keselamatan data adalah satu tunjang utama dalam perundangan perlindungan data peribadi. Seksyen 9 mewajibkan pengguna data yang memproses data peribadi mana-mana data subjek untuk memastikan keselamatan data dengan mengambil langkah-langkah perlindungan yang praktikal. Penggunaan terma 'langkah-langkah praktikal' menunjukkan pihak berkuasa menyerahkan kepada pihak pengguna data untuk memutuskan apakah tahap dan langkah-langkah keselamatan yang bersesuaian dengan operasi pengguna data.

Pihak IPTS ada memproses data peribadi dalam bentuk automatik dan juga manual. Menyedari kepentingan mematuhi peruntukan berkaitan keselamatan data, pihak IPTS telahpun mengambil beberapa langkah-langkah keselamatan yang bersesuaian. Data automatik disimpan dengan selamat dan di bawah pemantauan pekerja berkepakaran khas dalam bidang teknologi maklumat manakala data berbentuk manual disimpan dalam beberapa bilik fail yang dihadkan akses hanya kepada pekerja di bahagian berkenaan sahaja. Kebanyakan data peribadi berkaitan pekerja adalah di bawah bidang kuasa Bahagian sumber manusia dan pekerja-pekerja di bahagian tersebut sering diberikan latihan dan peringatan mengenai kepentingan mengikuti langkah-langkah keselamatan data.

#### 3.4.5 Prinsip Penyimpanan

Menurut prinsip ini, data peribadi yang diproses bagi apa-apa maksud tidak boleh disimpan lebih lama daripada yang diperlukan bagi memenuhi maksud itu dan menjadi kewajipan seorang 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.

Sebagai institusi pendidikan yang telah beroperasi hampir 30 tahun, IPTS menyimpan jumlah data yang sangat besar, merangkumi data peribadi pelajar semasa, bekas pelajar, pekerja semasa dan juga bekas pekerja. Dari semasa ke semasa, pihak IPTS akan menerima permohonan untuk mendapatkan salinan rekod data peribadi daripada pihak-pihak di atas. Permohonan ini ada masanya untuk data baru dan ada kalanya terdapat permintaan untuk data yang telah lama diproses. Contohnya, IPTS pernah menerima permohonan daripada bekas pelajar yang mahukan salinan transkrip pengajian diplomasnya, yang sudah lebih daripada 10 tahun. Terdapat juga permohonan untuk rekod pekerjaan bagi tujuan kenaikan pangkat pekerja, atau rekod penggajian untuk urusan percukaian, antaranya. Di atas justifikasi ini, pihak IPTS mengambil keputusan untuk mengkategorikan data kepada data aktif (yang masih digunakan) dan data tidak aktif (yang hanya akan diekstrak mengikut keperluan). Data ini disimpan secara berasingan di dua bilik fail yang berbeza di lokasi yang berlainan. Sebagai langkah pemeliharaan data (*preservation*) dan juga untuk menjimatkan ruang, pihak IPTS juga sedang mengambil langkah *digitalisation*, iaitu menyimpan data dalam bentuk digital yang lebih selamat.

#### 3.3.6 Prinsip Integriti Data

Langkah munasabah yang diambil oleh IPTS untuk memastikan data peribadi adalah tepat, lengkap, tidak mengelirukan dan terkini adalah dengan menyediakan peluang kepada semua pekerja untuk mengemaskini data peribadi mereka pada bila-bila masa. Borang akan ditandatangani pekerja sendiri sebagai bukti pengesahan. Pekerja hanya perlu mengisi borang secara automatik (serahan melalui emel) atau manual (serahan fizikal kepada pejabat bahagian sumber manusia). Ini merupakan langkah baru yang diperkenalkan. Sebelum ini, pihak bahagian sumber manusia akan menghubungi pekerja setahun sekali untuk proses mengemaskini maklumat. Keanjalan waktu yang diberikan untuk proses kemaskini atau pembetulan maklumat ini masih selari dengan peruntukan APDP.

#### 3.3.7. Prinsip Akses



Seksyen 12 mengatakan subjek data hendaklah diberi akses kepada data peribadinya yang dipegang oleh seorang pengguna data dan boleh membetulkan data peribadi itu jika ianya tidak tepat, tidak lengkap, mengelirukan atau tidak terkini. Selari dengan peruntukan di atas, pihak IPTS sentiasa memberi akses kepada pekerja untuk memeriksa dan mengemaskini data peribadi mereka. Selain daripada berhubung dengan pegawai yang berkenaan, banyak maklumat berkaitan data peribadi pekerja ada dikongsi di portal pekerja yang hanya boleh diakses menggunakan ID dan kata kunci yang hanya diketahui oleh subjek data tersebut.

#### **4 Kesimpulan**

Tidak dinafikan bahawa perlindungan data peribadi menjadi semakin penting di era digital ini. Di mana kebanyakan urusan dijalankan secara maya dan hanya memerlukan pengesahan melalui data peribadi individu tersebut. Akses kepada data peribadi seseorang individu perlu dikawal untuk mengelakkan penyalahgunaan yang boleh mendatangkan kerugian dan kerosakan yang besar. Walaupun, pada umumnya, dilihat sektor pendidikan tidaklah berisiko tinggi kerana tidak banyak melibatkan pemprosesan data sensitif seperti sektor kewangan atau komunikasi, masih ada keperluan untuk pengguna data menjaga keselamatan data yang disimpannya. Secara keseluruhannya, pihak IPTS ini telahpun bermula dengan langkah positif ke arah pematuhan APDP, namun masih ada beberapa aspek yang perlu dipertingkatkan pematuhannya. Memperkenalkan dasar privasi dan menjalankan aktiviti kesedaran berkaitan privasi dan data peribadi merupakan antara langkah seterusnya yang boleh diambil ke arah pematuhan penuh.

#### **5. Rujukan**

Akta Perlindungan Data Peribadi 2010

Chia Swee Yik. (2017). Asas Perlindungan Data Peribadi untuk Majikan. 27 September 2017. <https://chiale.com.my/knowledge-hub/basics-of-personal-data-protection-for-employers> extracted on 18 Februari 2021

Deakin, S & Morris, G (1998). Undang-undang Buruh, ke-2. Ed. London: Butterworths.

Devasheesh P. Bhave Laurel H. Teo, Reeshad S. Dalal ,(2019) Privacy at Work: A Review and a Research Agenda for a Contested Terrain, *Journal of Management, Article Information* Volume: 46 issue: 1, page(s) 127-164

Farah Mohd Shahwahid & Surianom Miskam, (2014) Personal Data Protection Act 2010: Taking The First Steps Towards Compliance, E-proceedings, Conference on Management and Muamalah (CoMM 2014), (E-ISBN: 978-983-3048-92-2)

Kamal Halili Hassan & Rozanah Ab Rahman, (2009). *Hubungan Undang-undang Majikan dengan Pekerja*, Kuala Lumpur: Dewan Bahasa dan Pustaka.

Kamal Halili Hassan et al. (2007). *Undang-Undang Pekerjaan*. Jilid. 7. Kuala Lumpur: Dewan Bahasa Pustaka.

Perintah 7 Perlindungan Data Peribadi bagi Golongan Pengguna Data 2013

Protection of workers' personal data [https://www.ilo.org/wcmsp5/groups/public/---ed\\_protect/---protrav/---safework/documents/normativeinstrument/wcms\\_107797.pdf](https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf)

extracted on 20/3/2021

Selvamalar Alagaratnam & Siva Kumar Kanagasabai, (2020) Protection of Employee's Personal Data in Malaysia - General Data Protection Regulation ("GDPR") and Personal Data Protection Act 2010 ("PDPA") <https://www.skrine.com/insights/alerts/november-2020/protection-of-employee%E2%80%99s-personal-data-in-malaysia>

extracted on 22/3/2021