



## Kod Tata Amalan Perlindungan Data Peribadi

### 1.0 Pengenalan

Kami di Perbadanan Kemajuan Negeri Selangor (selepas ini dirujuk sebagai PKNS) bertanggungjawab mengurus, melindungi, memproses serta memindahkan maklumat atau data peribadi pelanggan kami dan pihak ketiga dalam urusan rasmi PKNS (Istilah 'maklumat peribadi' dan 'data peribadi' digunakan secara silih berganti di dalam seksyen-seksyen seterusnya). Dalam hal itu, Akta Perlindungan Data Peribadi (Akta PDP) 2010 memperuntukkan beberapa tanggungjawab ke atas PKNS dan perundangan subsidiarinya menetapkan kaedah-kaedah serta peraturan-peraturan yang harus dipatuhi.

### 2.0 Tafsiran

Melainkan jika konteksnya menghendaki makna yang berbeza, istilah-istilah yang digunakan dalam Kod Tata Amalan (KTA) ini hendaklah memberi makna yang berikut:

a.	"Anonimisasi" atau perlindungan identiti	:	data yang <i>anonimisasikan</i> iaitu apabila seseorang tidak lagi dapat dihubungkan dengannya, atau apabila hubungan kepada seseorang hanya boleh dibuat dengan perbelanjaan besar yang tidak seimbang dari segi masa, kos dan tenaga kerja.
b.	"Subjek data"	:	seseorang individu yang menjadi subjek atau empunya data peribadi yang diproses itu.
c.	"Pihak ketiga"	:	mana-mana orang selain: a. Seorang subjek data; b. Seorang yang berkaitan yang berhubung dengan seorang subjek data;

			<p>c. Seorang pengguna data;</p> <p>d. Seorang pemproses data;</p> <p>e. Seorang yang diberi kuasa secara bertulis oleh pengguna data untuk memproses data peribadi di bawah kawalan langsung pengguna data itu;</p> <p><i>*Berdasarkan definisi PDP.</i></p>
d.	“Persetujuan”	:	kebenaran yang diberi secara suka rela, di mana subjek data bersetuju dengan pemrosesan data berkenaan
e.	“Pengguna data”	:	seseorang sama ada berseorangan atau bersama dengan mana-mana orang lain memproses apa-apa data peribadi atau mempunyai kawalan terhadap atau membenarkan pemrosesan apa-apa data peribadi. (PKNS adalah pengguna data).
f.	“Data peribadi”	:	apa-apa maklumat yang berkaitan dengan transaksi komersial, yang sedang diproses, sama ada berhubung secara langsung atau tidak langsung dengan subjek data, yang dikenal pasti atau boleh dikenal pasti dari maklumat berkenaan dan maklumat lain dalam milikan PKNS sebagai pengguna data.
g.	“Data peribadi sensitif”	:	apa-apa data peribadi yang mengandungi maklumat tentang kesihatan atau keadaan fizikal atau mental seorang subjek data, pendapat politiknya, kepercayaan agamanya atau kepercayaan lain seumpamanya, pelakuan atau pengataan pelakuan apa-apa kesalahan olehnya.
h.	“Pemrosesan data peribadi”	:	<p>mengumpul, merekod atau menyimpan data peribadi itu atau menjalankan apa-apa pengendalian atau set pengendalian terhadap data peribadi itu termasuk:</p> <p>a. Penyusunan, penyesuaian atau pengubahan data peribadi;</p> <p>b. Mendapatkan kembali, merujuk kepada atau menggunakan data peribadi;</p>

		<p>c. Penzahiran data peribadi melalui penghantaran, pemindahan, penyebaran atau selainnya menjadikannya tersedia;</p> <p>d. Penjajaran, penggabungan, pembetulan, pemadaman atau pemusnahan data peribadi dengan / tanpa penggunaan proses berautomatik, untuk menyimpan, menyusun, menyesuaikan, mengubah, mendapatkan kembali, menggunakan, menyampaikan, menghantar, mengedarkan, menggabungkan atau mendamaikan (<i>reconcile</i>) data. Ini termasuk pemusnahan, pemotongan, pembetulan atau pemadaman data peribadi.</p>
--	--	---

### 3.0 Tujuan Kod Tata Amalan

Kod Tata Amalan ini perlu dibaca selaras dengan Dasar Perlindungan Data untuk mendapatkan gambaran menyeluruh mengenai Polisi Perlindungan Data PKNS. Dokumen ini memberikan pengenalan kepada amalan dalam mengendalikan pemrosesan data peribadi di PKNS. Kod Tata Amalan ini adalah berlandaskan Dasar Perlindungan Data PKNS, yang berkaitan dengan pengumpulan, pemrosesan serta pendedahan data-data individu. Ia menyediakan amalan terbaik dan garis panduan korporat kepada anggota PKNS semasa pemrosesan data peribadi pelanggan dan pihak ketiga.

### 4.0 Status dan Skop Kod Tata Amalan

Kod Tata Amalan ini terpakai kepada pemrosesan data peribadi subjek data yang merangkumi pelanggan, kontraktor, pembekal atau perunding atau rakan niaga yang lain. Ia tidak dirangkumkan dalam kontrak pekerjaan rasmi, namun ia merupakan keperluan pekerjaan di mana anggota PKNS harus mematuhi Kod semasa pemrosesan data peribadi pelanggan dan pihak ketiga.

Kod Tata Amalan ini adalah sebahagian daripada kontrak kerja rasmi anggota serta perjanjian rasmi di antara anggota dengan PKNS. Semua anggota PKNS wajib mematuhi Kod ini dan sekiranya berlaku ketidakpatuhan, anggota tersebut boleh dikenakan tindakan tatatertib.

Adalah menjadi tanggungjawab PKNS dan seluruh anggota PKNS mematuhi Akta PDP 2010. Tindakan tatatertib boleh diambil terhadap mana-mana anggota PKNS atau penarikan balik akses pada kemudahan maklumat PKNS sekiranya berlaku pelanggaran Kod Tata Amalan. Sebarang persoalan ataupun kebimbangan berkaitan dengan tafsiran atau operasi Kod ini serta dasar-dasar perlindungan data hendaklah disalurkan kepada Pegawai Perlindungan Data, yang kemudiannya boleh mendapatkan khidmat nasihat daripada Pegawai Undang-undang.

## **5.0 Prinsip-Prinsip Pemprosesan Data Peribadi**

Akta PDP 2010 mengenakan obligasi terhadap PKNS, selaku pengguna data, untuk memproses data peribadi secara bertanggungjawab. PKNS bertekad untuk memastikan semua anggota PKNS sedia ada atau di masa hadapan mematuhi Akta ini supaya data peribadi yang disimpan dan diproses oleh PKNS sentiasa dilindungi pada setiap masa.

PKNS bertanggungjawab untuk memastikan pematuhan kepada Akta PDP 2010 dan pemprosesan data peribadi dengan mematuhi tujuh prinsip perlindungan data yang telah ditetapkan seperti berikut:

- Data hanya akan diproses dengan kebenaran subjek data bagi tujuan yang sah di sisi undang-undang serta data peribadi berkenaan memadai dan tidak berlebih-lebihan untuk tujuan tersebut.
- Subjek data mesti dimaklumkan mengenai dasar perlindungan data.
- Data peribadi mestilah tepat, lengkap dan terkini.
- Data hanya disimpan selama yang diperlukan bagi memenuhi tujuan pemrosesannya.
- Data perlu diproses selaras dengan hak subjek data.
- Data perlu disimpan secara selamat daripada akses yang tidak dibenarkan, kerugian yang tidak disengajakan atau kemusnahan.
- Data hanya didedahkan untuk tujuan lain atau kepada pihak ketiga dengan persetujuan subjek data.

## **6.0 Prinsip-Prinsip Amalan**

PKNS amat komited dalam pematuhan kepada Prinsip-prinsip Perlindungan Data semasa menjalankan tugas harian anggota apabila mengumpul dan memproses data peribadi dalam usaha menyediakan perkhidmatan kepada pelanggan dan berurusan dengan pihak ketiga.

## 6.1 Pengumpulan dan Pemrosesan

Data peribadi yang disimpan PKNS kebanyakannya diperolehi secara langsung daripada subjek data sendiri. Akta PDP menetapkan persetujuan mesti diperolehi bagi tujuan pengumpulan dan pemrosesan data. Anggota PKNS yang bertanggungjawab menguruskan pemrosesan data peribadi untuk aktiviti-aktiviti PKNS yang sah mesti memastikan persetujuan subjek data diperolehi. Hanya anggota yang diberi kuasa bertanggungjawab mengumpul, memproses atau menggunakan data peribadi yang ada. Penggunaan data untuk tujuan peribadi, pemberian atau penyebaran data kepada pihak yang tidak dibenarkan dengan apa-apa cara sekalipun adalah dilarang. "Pihak yang tidak dibenarkan" adalah termasuk rakan-rakan di tempat kerja, melainkan jika dibenarkan berdasarkan fungsi dan tanggungjawab serta tugas-tugas mereka.

PKNS bertanggungjawab untuk melindungi kerahsiaan dan kesahihan semua data peribadi yang disimpan atau dikumpulkan oleh anggota sama ada secara manual atau elektronik (dalam sistem fail atau komputer). Anggota PKNS yang bertanggungjawab dalam pemrosesan data peribadi perlu memastikan data selaras dengan Akta PDP 2010, Dasar Perlindungan Data serta Kod ini.

Semasa mengendalikan data peribadi, anggota PKNS hendaklah memastikan perkara-perkara berikut termasuk dalam skop bidang kuasa PKNS:

- (i) Jenis-jenis data peribadi yang disimpan;
- (ii) Tujuan ia digunakan;
- (iii) Pihak-pihak lain dimana data boleh didedahkan atau dikongsi.

Sekiranya tujuan pemrosesan data peribadi tidak difahami dengan jelas oleh subjek data (selain daripada tujuan pengumpulan yang jelas dan tujuan yang dikehendaki), anggota PKNS hendaklah memaklumkan kepada subjek data tujuan pengumpulan data tersebut semasa data dikumpulkan. Subjek data berhak untuk tidak memberikan data yang tidak diperlukan bagi tujuan pemrosesan data tersebut. Namun begitu, sekiranya tujuan pemrosesan data peribadi telah dinyatakan dengan jelas untuk tujuan perkhidmatan yang diperlukan oleh pelanggan, anggota PKNS tidak perlu memaklumkan kepadanya secara nyata.

## 6.2 Keselamatan Data Peribadi dan Tanggungjawab Anggota

Keselamatan data peribadi yang sedang dalam pemrosesan adalah sangat penting di dalam polisi perlindungan data. Adalah menjadi hak subjek data untuk memastikan segala data peribadinya disimpan dan diproses secara selamat serta tidak didedahkan kepada pihak yang tidak dibenarkan sama ada di dalam atau luar

daripada PKNS. Bagi menjamin keselamatan data peribadi di PKNS, semua anggota PKNS yang terlibat dalam pemprosesan data peribadi subjek data perlu mematuhi garis panduan am seperti yang dinyatakan di bawah.

Langkah-langkah teknikal serta garis panduan organisasi yang munasabah dilaksanakan bagi menjamin keselamatan data. Langkah-langkah ini bertujuan melindungi data peribadi dari diakses tanpa kebenaran, diproses atau didedahkan secara tidak sah di sisi undang-undang, diubahsuai, dimusnahkan serta dari kerugian yang tidak disengajakan. Langkah-langkah ini adalah berkaitan dengan keselamatan data yang mewajarkan perlindungan diberikan, samada diproses secara manual atau secara elektronik. Langkah-langkah teknikal dan garis panduan organisasi ini merupakan sebahagian daripada pelan pengurusan keselamatan maklumat bersepadu, dan akan disemak secara berkala selari dengan perkembangan teknologi dan perubahan organisasi.

Adalah menjadi tanggungjawab anggota PKNS untuk memastikan data peribadi yang disimpan oleh PKNS, sama ada secara manual atau secara elektronik sentiasa dalam keadaan selamat dan tidak didedahkan secara tidak sah disisi undang-undang sebagai pematuhan Dasar Perlindungan Data PKNS serta Kod Tata Amalan ini. Sekiranya berlaku pendedahan yang tidak dibenarkan, anggota tersebut boleh dikenakan tindakan tatatertib yang dianggap sebagai salah laku didalam kes-kes tertentu.

### **6.3 Penyimpanan data peribadi secara selamat**

- Setiap anggota PKNS yang bertanggungjawab ke atas penyimpanan data peribadi, sama ada secara manual atau elektronik, adalah bertanggungjawab untuk menyimpannya dengan selamat, selaras dengan Dasar Perlindungan Data PKNS. Data peribadi hendaklah disimpan di dalam kabinet yang berkunci, laci atau peti simpanan selamat; ataupun jika disimpan dalam sistem komputer, harus dikodkan, atau dilindungi dengan kata laluan pada pekakas cakera keras (hard drive) dan pada pemacu rangkaian (network drive) yang mempunyai simpanan sokongan (backup); dan jika salinan disimpan pada cakera atau media simpanan mudah-alih yang lain, media tersebut mesti disimpan dalam kabinet yang berkunci, laci atau peti simpanan selamat.
- Lazimnya, data peribadi tidak dibenarkan disimpan di luar pejabat sama ada dalam bentuk manual atau elektronik, di dalam komputer riba atau peranti mudah-alih peribadi atau laman kawalan jauh (remote sites).
- Setiap anggota PKNS perlu menyedari bahawa fail-fail log akan merekodkan butir-butir para pengguna yang mengakses, mengubah atau memadam atau

cuba untuk mengakses, mengubah atau memadam pangkalan data pusat dan fail-fail yang mengandungi data peribadi.

#### **6.4 Pemprosesan data peribadi secara selamat**

- Setiap anggota PKNS yang menggunakan data peribadi dalam tugas harian mereka, harus mengambil langkah-langkah pencegahan yang sewajarnya bagi memastikan keselamatan dan kerahsiaan data tersebut. Misalnya, di dalam pejabat terbuka, skrin komputer yang ada kemungkinan memaparkan data peribadi tidak harus diletakkan dalam kedudukan di mana anggota lain atau pihak ketiga yang tidak dibenarkan boleh melihat data tersebut secara mudah, harus menggunakan skrin yang dilindungi dengan kata laluan.
- Data peribadi dalam bentuk manual, seperti fail-fail kertas, surat-menyurat atau salinan cetakan-cetakan dari pangkalan data, dilarang dibiarkan terdedah di pejabat terbuka jika anggota berkenaan tidak berada di meja mereka. Sebaliknya ianya perlu disimpan di tempat berkunci atau sekurang-kurangnya ditutup.
- Dalam keadaan di mana rekod manual yang mengandungi data peribadi boleh diakses oleh beberapa orang anggota PKNS ketika menjalankan tugas-tugas mereka, buku log hendaklah digunakan bagi memantau penggunaan rekod tersebut.
- Lazimnya, data peribadi tidak digalakkan diproses di luar pejabat anggota, sama ada dalam bentuk manual atau elektronik, di dalam komputer riba atau peranti mudah alih peribadi atau laman kawalan jauh. Sekiranya pemprosesan *off-site* diperlukan, persetujuan Ketua Bahagian/Unit yang berkaitan mesti diperolehi, serta langkah-langkah praktikal yang munasabah perlu diambil bagi melindungi data.

#### **6.5 Pendedahan dan Pemindahan Data Peribadi**

- Ketua Bahagian atau anggota yang bertanggungjawab di bahagian berkaitan perlu memberi kesedaran dan sentiasa mengingatkan anggota yang menguruskan data peribadi mengenai tujuan sesuatu data diproses dan kepada siapa data tersebut sama ada secara keseluruhan atau sebahagian, boleh didedahkan atau dipindahkan secara sah, di dalam atau di luar PKNS.
- Data peribadi tidak dibenarkan didedahkan secara lisan atau bertulis atau melalui laman Web atau dengan apa cara sekalipun, sama ada secara manual atau elektronik, sama ada sengaja atau sebaliknya, kepada mana-mana pihak ketiga yang tidak dibenarkan.
- Sekiranya berlaku pendedahan yang tidak dibenarkan, anggota tersebut boleh dianggap sebagai telah melakukan salah laku dan dalam kes-kes tertentu boleh dikenakan tindakan tatatertib.

## 6.6 Keselamatan data semasa pemindahan

- Semasa menjalankan tugas rasmi, dalam keadaan dimana data peribadi yang dipindahkan diantara anggota PKNS, tahap keselamatan yang bersesuaian dengan jenis data hendaklah digunakan dengan mengambilkira risiko yang dikenal pasti. Sebagai contoh, data peribadi yang sensitif perlu dipindahkan mengikut tatacara Dokumen Terperingkat (surat dalaman yang diletakkan dalam sampul surat yang dilekatkan pelekat keselamatan, dimeterai atau dengan serahan tangan). Jika dipindahkan melalui e-mel, data tersebut harus dikategorikan sebagai sulit atau dihantar dengan lampiran yang dilindungi kata laluan dan kata laluan itu hendaklah diberi secara berasingan. (Nasihat lanjut mengenai keselamatan e-mel dan perlindungan kata laluan boleh diperolehi daripada Bahagian ICT.)

## 6.7 Pendedahan ke luar PKNS

- Secara amnya, tiada data yang boleh didedahkan atau dipinda melainkan dengan kuasa pihak yang berkuasa dan permohonan adalah yang sah sahaja. Sekiranya permohonan untuk pendedahan atau pindaan data peribadi pelanggan diterima dari mana-mana pihak yang mendakwa dirinya sebagai saudara-mara atau rakan-rakan, permohonan tersebut hendaklah ditolak melainkan dengan persetujuan subjek data, atau ia terjujlah dalam situasi di mana pendedahan tanpa kebenaran adalah dibenarkan oleh Akta PDP 2010 dan / atau undang-undang lain.
- Permohonan pendedahan dari pihak polis, Badan Kerajaan atau entiti atau agensi perundangan rasmi lain hendaklah disiasat secara menyeluruh bagi mengesahkan kesahihan permohonan tersebut dan tindakan boleh diambil sekiranya terdapat keperluan undang-undang untuk data berkenaan didedahkan, atau persetujuan subjek data telah diperolehi untuk penzahiran itu. Segala data peribadi sama ada secara manual atau elektronik, mesti disimpan dengan selamat dan tidak didedahkan secara bertentangan dengan undang-undang.

## 6.8 Penyimpanan Data Peribadi

- Bukan menjadi amalan PKNS untuk menyimpan data yang tidak lagi perlu atau membuat salinan data demi kepentingan pelanggan. Namun, PKNS masih perlu menyimpan data pelanggan di dalam melaksanakan obligasinya. PKNS menyimpan data bekas anggota – sebahagiannya bagi mematuhi keperluan undang-undang dan juga sebagai menyimpan rekod lampau yang lengkap. Walaubagaimanapun, PKNS tidak menggalakkan penyimpanan data peribadi dalam fail lebih dari tempoh yang diperlukan selaras dengan keperluan Akta PDP



2010. PKNS akan memastikan data peribadi yang telah memenuhi tujuannya dimusnahkan atau dipadamkan secara kekal atau *'anonymised'*.

- Sekiranya prinsip-prinsip Perlindungan Data Peribadi ini tidak dipatuhi, anggota berkenaan boleh dikenakan tindakan disiplin oleh PKNS. Di samping itu, sekiranya pelanggan mengalami kerugian besar atau kesulitan akibat itu, PKNS serta Ahli Pengurusan PKNS tertakluk kepada siasatan, boleh didakwa di bawah Akta PDP 2010.

## **7.0 Hak-hak Subjek Data**

7.1 Sekiranya terdapat sebarang persoalan atau aduan, subjek data boleh menghubungi Pegawai Perlindungan Data PKNS. Hak-hak subjek data di dalam Kod Tata Amalan PKNS adalah seperti berikut:

- Subjek data mempunyai akses kepada data peribadinya.
- Sebagai contoh, sekiranya semasa pelaksanaan hak akses subjek data, jelas didapati bahawa data peribadi subjek data tidak betul atau tidak lengkap, subjek data berhak untuk meminta PKNS membuat pembetulan terhadap maklumat berkaitan.
- Subjek data berhak untuk menyekat penggunaan datanya bagi tujuan pemasaran langsung.
- Subjek data berhak untuk menarik balik kebenaran bagi tujuan pemrosesan.
- Subjek data berhak untuk meminta supaya datanya tidak diproses sekiranya ia boleh mendatangkan kerugian atau kesulitan kepadanya.

7.2 PKNS mengiktiraf serta menghormati hak-hak yang diberikan kepada pelanggan serta pihak ketiga subjek data dan akan melaksanakan tanggungjawabnya bagi membolehkan subjek data menggunakan hak-hak tersebut sepanjang tempoh masa yang dinyatakan menurut Akta PDP 2010. Semua anggota yang berkenaan perlu mengambil tindakan terhadap permohonan pelanggan serta pihak ketiga di dalam melaksanakan hak-hak mereka. Pegawai Perlindungan Data akan memastikan setiap permohonan yang mematuhi Akta hendaklah diberi layanan yang sepatutnya.

## **8.0 Pemasaran Data/Pemrosesan Data bagi pihak/Penglibatan Pihak Ketiga**

8.1 PKNS akan mematuhi syarat-syarat berikut sekiranya PKNS melantik mana-mana pihak ketiga untuk memproses data peribadi bagi pihaknya:

- Hanya kontraktor, pembekal, perunding atau syarikat-syarikat yang boleh menjamin keperluan-keperluan teknikal dan organisasi serta peruntukan-peruntukan keselamatan yang diperlukan untuk pemprosesan akan dipilih bagi memproses data peribadi.
- Pemprosesan (bagi pihak PKNS) akan dimasukkan dalam kontrak bertulis atau dalam bentuk lain yang sesuai.
- PKNS bertanggungjawab dan merupakan rujukan pihak pelanggan, kontraktor, pembekal, perunding atau rakan kongsi kontrak-kontrak lain yang ingin melaksanakan hak-hak mereka.
- Pihak ketiga dari luar yang telah ditugaskan untuk menjalankan pemprosesan data atau tugas-tugas lain, sebagai contoh, dalam bidang pemasaran, penyelidikan pasaran dan tinjauan pendapat, adalah terikat dengan kontrak untuk memproses atau menggunakan data peribadi yang mereka terima dari PKNS menurut isi kandungan kontrak sahaja.
- Penggunaan data untuk tujuan mereka sendiri atau bagi tujuan pihak ketiga adalah dilarang oleh kontrak.
- Kerjasama dengan pihak ketiga lain di mana data peribadi boleh didedahkan atau disediakan kepada pihak ketiga itu, adalah juga tertakluk kepada tahap perlindungan serta keselamatan data yang sepadan dengan Akta PDP 2010 dan Kod Tata Amalan ini.

8.2 Syarat-syarat yang dinyatakan di atas serta terma lain akan dimasukkan ke dalam kontrak perjanjian PKNS dengan kontraktor/organisasi sebelum pemprosesan dijalankan. PKNS akan memastikan bahawa kontrak tersebut boleh dikuatkuasakan di Malaysia dan di negara di mana organisasi itu berada. Di samping itu, PKNS akan menjalankan pengauditan ke atas organisasi berkenaan dan mengkehendaki mereka melaporkan mana-mana pelanggaran keselamatan atau masalah-masalah lain serta menyemak semula proses dan prosedur PKNS dari semasa ke semasa.

## **9.0 Tanggungjawab Anggota PKNS**

Semua anggota PKNS telah diperlengkapkan dengan pengetahuan mengenai Akta PDP 2010. Mereka dikehendaki mematuhi peruntukan-peruntukan Akta dan Dasar Perlindungan Data serta Kod Tata Amalan ini sepanjang menjalankan tugas dan fungsi masing-masing dalam pemprosesan data peribadi pelanggan dan pihak ketiga.

### **9.1 Tanggungjawab, Sekatan dan Pegawai PKNS**

Pihak yang ditetapkan/yang dibenarkan/yang dilantik bergantung pada tanggungjawab Bahagian masing-masing.

Pegawai/Anggota PKNS dikehendaki:

- Memastikan dan mengekalkan kerahsiaan yang ketat bagi semua data peribadi yang dikendalikan;
- Menjadi pusat rujukan pentadbiran bagi semua permintaan akses yang berkaitan dengan data peribadi yang disimpan oleh PKNS;
- Memberi nasihat kepada anggota PKNS yang lain dan pihak luar tentang penggunaan Dasar Perlindungan Data PKNS dan Kod Tata Amalan ini serta memastikan kepatuhan terhadapnya;
- Mengaudit aktiviti pemprosesan data peribadi yang dalam bidang kuasa PKNS setiap tahun bagi memastikan ianya selaras dengan Akta PDP 2010, Dasar Perlindungan Data dan Kod Amalan ini;
- Memastikan bahawa setiap anggota dilatih dan berpengetahuan dalam penggunaan dan pengendalian data peribadi PKNS.

Ahli Pengurusan PKNS / Ketua Bahagian yang bertanggungjawab dalam aktiviti pemprosesan data masing-masing bertanggungjawab untuk memastikan bahawa peruntukan undang-undang mengenai perlindungan data serta keperluan dalam dasar-dasar PKNS serta Kod ini sentiasa dipatuhi. Mereka juga bertanggungjawab memastikan langkah-langkah organisasi dan sumber manusia serta langkah-langkah teknikal dilaksanakan agar pemprosesan data yang dilaksanakan di jabatan mereka menepati peraturan serta mengambil kira kepentingan perlindungan data.

## **10.0 Penyelesaian serta Pegawai Perlindungan Data**

Pegawai Perlindungan Data bertanggungjawab memantau pematuhan Akta PDP 2010, Polisi Perlindungan Data, Polisi Perlindungan Data bagi Pengurusan Sumber Manusia serta Kod Tata Amalan ini. Beliau bertanggungjawab atas setiap polisi perlindungan data serta mengawasi dan memantau kepatuhan terhadapnya. Beliau dibenarkan menjalankan pemeriksaan dan pengauditan terhadap perlindungan data. Pegawai Perlindungan Data yang dilantik adalah bertanggungjawab untuk memastikan bahawa semua anggota PKNS mengetahui dan memahami Akta PDP 2010, Dasar-dasar Perlindungan Data serta Kod ini.

Semua Ketua Bahagian hendaklah memaklumkan kepada Pegawai Perlindungan Data mengenai sebarang aktiviti baharu yang melibatkan pemprosesan data peribadi di Bahagian masing-masing. Pegawai Perlindungan Data pula akan menilai risiko kepada perlindungan data serta memastikan risiko berkenaan dapat dikurangkan dan aktiviti yang dijalankan mematuhi Akta PDP 2010, dasar-dasar dan Kod ini. Sekiranya aktiviti pemprosesan data yang dicadangkan boleh melibatkan risiko tertentu terhadap hak peribadi subjek data, Pegawai Perlindungan Data mesti

bertindak terlebih dahulu sebelum sebarang aktiviti pemprosesan data dijalankan terutamanya yang melibatkan data peribadi yang memerlukan perlindungan khas. Pegawai Perlindungan Data harus memastikan anggota PKNS yang mengendalikan data peribadi mempunyai ilmu pengetahuan mengenai perlindungan data.

Sekiranya terdapat sebarang aduan atau berlaku pelanggaran data, Ketua Bahagian mesti memaklumkan kepada Pegawai Perlindungan Data dengan segera. Di samping itu, mana-mana pelanggan atau pihak ketiga boleh menghubungi Pegawai Perlindungan Data pada bila-bila masa untuk menyuarakan kekusaran mereka, bertanyakan soalan, meminta maklumat, atau membuat aduan berkaitan dengan hal-hal perlindungan data. Kekusaran serta aduan pelanggan akan dikendalikan secara sulit atas permintaan pelanggan berkenaan. Keputusan yang dibuat oleh Pegawai Perlindungan Data bagi menyelesaikan pelanggaran terhadap perlindungan data mesti diiktiraf oleh anggota PKNS, Ketua Bahagian dan Ahli Pengurusan PKNS.

Butiran Pegawai Perlindungan Data PKNS adalah seperti berikut:

**Puan Hajah S. Normalis Binti Abd. Samad,  
Pegawai Perlindungan Data PKNS  
Perbadanan Kemajuan Negeri Selangor,  
Bahagian Integriti dan Pengurusan Risiko,  
Laman PKNS, Tingkat 1, Blok C  
No 20 Jalan Indah 14/8,  
Seksyen 14, 40000 Shah Alam  
Selangor Darul Ehsan  
Tel : 03-5525 0396 (talian terus) @ 03-5525 0300 ext 1308  
Tel. Bimbit : 013-340 1757  
Emel : malis @ pkns.gov.my**

## **11.0 Kesedaran**

Satu salinan Polisi Perlindungan Data, Polisi Perlindungan Data bagi Pengurusan Sumber Manusia serta Kod Tata Amalan ini akan diberikan kepada setiap anggota PKNS. Setiap anggota dikehendaki mengetahui dan mematuhi dasar-dasar dan Kod Tata Amalan ini pada setiap masa.

## **12.0 Pelaksanaan Polisi dan Penyemakan Semula**

Semua Polisi Perlindungan Data PKNS serta Kod Tata Amalan ini dikeluarkan oleh PKNS dan semakan semula secara tahunan akan dijalankan oleh Pegawai

Perlindungan Data dan Pegawai Undang-undang. Semua dokumen ini akan dikaji dan disemak semula untuk memastikan kesempurnaan, keberkesanan dan kebolegunaan di setiap Bahagian PKNS.

### **13.0 Pindaan kepada Kod Tata Amalan**

PKNS akan mengkaji dan menyemak semula Kod Tata Amalan ini setiap dua (2) tahun (sekiranya perlu) bagi memenuhi keperluan terkini dan akan mengemaskini Kod ini apabila diperlukan. Semua pihak yang terlibat akan dimaklumkan mengenai pengemaskinian tersebut.