



GARISPANDUAN PERKONGSIAN DATA PERIBADI

GUIDELINES ON PERSONAL DATA SHARING

NO.	REKOD PENGEMASKINIAN <i>REVISION RECORD</i>	TARIKH BERKUATKUASA <i>EFFECTIVE DATE</i>
1	Keluaran Pertama <i>First Issue</i>	25 Mei 2023
2	Keluaran Kedua <i>Second Issue</i>	26 Julai 2023
3	Keluaran Ketiga <i>Third Issue</i>	15 Ogos 2023

Kandungan *(Contents)*

1. TUJUAN <i>(PURPOSE)</i>	3
2. LATAR BELAKANG <i>(BACKGROUND)</i>	3
3. SKOP DAN KEBOLEHGUNAAN <i>(SCOPE AND APPLICABILITY)</i>	4
4. DEFINISI UTAMA <i>(KEY DEFINITIONS)</i>	4
5. SENARIO BAGI PERKONGSIAN DATA PERIBADI <i>(SCENARIOS FOR PERSONAL DATA SHARING)</i>	7
6. TUJUAN YANG DIBENARKAN <i>(PERMITTED PURPOSES)</i>	7
7. LANTIKAN PEGAWAI PERLINDUNGAN DATA <i>(APPOINTMENT OF DATA PROTECTION OFFICER(S))</i>	9
8. PERMOHONAN PERKONGSIAN DATA <i>(DATA SHARING REQUEST)</i>	10
9. JADUAL BAGI PERKONGSIAN DATA PERIBADI <i>(SCHEDULE FOR PERSONAL DATA SHARING)</i>	11
10. FAIL FORMAT YANG DISARANKAN BAGI PERKONGSIAN DATA PERIBADI <i>(SUGGESTED FILE FORMATS FOR SHARING OF PERSONAL DATA)</i>	12
11. KESELAMATAN DAN KERAHSIAAN DATA PERIBADI <i>(SECURITY AND CONFIDENTIALITY OF PERSONAL DATA)</i>	13
12. DASAR PENYIMPANAN DAN PELUPUSAN <i>(RETENTION AND DISPOSAL POLICIES)</i>	15
13. PERJANJIAN PERKONGSIAN DATA PERIBADI <i>(PERSONAL DATA SHARING AGREEMENTS)</i>	17
14. PERKONGSIAN DATA PERIBADI DALAM SITUASI KECEMASAN <i>(PERSONAL DATA SHARING IN EMERGENCY SITUATIONS)</i>	18
15. CARTA ALIRAN BAGI PERKONGSIAN DATA PERIBADI <i>(FLOWCHART FOR PERSONAL DATA SHARING)</i>	18
JADUAL A BORANG PERMOHONAN PERKONGSIAN DATA <i>(SCHEDULE A DATA SHARING REQUEST FORM)</i>	19
JADUAL B CONTOH KLAUSA KONTRAK <i>(SCHEDULE B SAMPLE CONTRACTUAL CLAUSES)</i>	24
JADUAL C CARTA ALIRAN BAGI PERKONGSIAN DATA PERIBADI <i>(SCHEDULE C FLOWCHART FOR SHARING OF PERSONAL DATA)</i>	36
JADUAL D SENARAI SEMAK KEPERLUAN <i>(SCHEDULE D CHECKLIST OF REQUIREMENTS)</i>	38

1. Tujuan *Purpose*

- 1.1. Garispanduan ini menyediakan panduan praktikal dan Prosedur Operasi Standard (SOP) mengenai perkongsian data peribadi oleh agensi-agensi Kerajaan.
These Guidelines provide practical guidance and Standard Operating Procedures (SOPs) regarding the sharing of personal data by Government agencies.

2. Latar Belakang *Background*

- 2.1 Garispanduan ini bertujuan untuk menjelaskan beberapa salah faham dan halangan berkaitan perkongsian data peribadi.
These Guidelines aim to clear up some misconceptions and barriers to sharing of personal data.

2.1.1. Salah Faham 1

Perlindungan data peribadi menghalang perkongsian data peribadi.

(Misconception 1)

Personal data protection prevents the sharing of personal data.

Kenyataan

Perlindungan data peribadi tidak menghalang perkongsian data peribadi asalkan agensi-agensi Kerajaan dan organisasi-organisasi mengambil pendekatan dengan cara wajar, selamat dan berpatutan. Garispanduan ini boleh membantu agensi-agensi Kerajaan dan organisasi-organisasi untuk mengimbangi risiko dan faedah, serta melaksanakan perkongsian data peribadi jika ianya untuk kepentingan awam. Amalan terbaik dalam perlindungan data peribadi adalah penting bagi memastikan kepercayaan, penglibatan dan sokongan dari orang awam dalam penggunaan data peribadi secara inovatif dalam sektor awam dan swasta.

Reality

Personal data protection does not prevent sharing of personal data, as long as Government agencies and organisations approach it in a sensible, safe and proportionate way. These Guidelines help Government agencies and organisations balance the risks and benefits, and implement personal data sharing if it is in the public interest. Good practice in personal data protection is vital to ensure public trust in, engagement with and support for innovative uses of personal data in both the public and private sectors.

2.1.2. Salah Faham 2

Tidak banyak manfaat yang diperolehi daripada perkongsian data peribadi.

(Misconception 2)

There is little benefit to be gained from personal data sharing.

Kenyataan

Perkongsian data peribadi boleh memberikan manfaat kepada agensi-agensi Kerajaan, organisasi-organisasi, individu-individu dan masyarakat secara amnya. Sekiranya ianya dilaksanakan dengan baik, ianya boleh membantu agensi-agensi Kerajaan dan organisasi-organisasi untuk menyampaikan perkhidmatan-perkhidmatan yang moden, cekap dan lebih memenuhi keperluan orang ramai dan

menjadikan kehidupan orang ramai lebih mudah. Ianya juga boleh membantu mengenalpasti orang ramai yang berisiko dan membantu menangani masalah yang dihadapi orang ramai sebelum ianya menyebabkan kesan buruk yang ketara.

Reality

Personal data sharing can bring benefits to Government agencies, organisations, individuals and society at large. If it is done well, it can help Government agencies and organisations to deliver modern, efficient services which better meet people's needs and make their lives easier. It can also identify people at risk and address problems before they have a significant adverse impact.

2.1.3. Salah Faham 3

Data peribadi hanya boleh dikongsikan dengan persetujuan individu berkenaan.

(Misconception 3)

Personal data can only be shared with an individual's consent.

Kenyataan

Agensi-agensi Kerajaan dan organisasi-organisasi boleh mengongsikan data peribadi tanpa persetujuan dengan syarat ianya memenuhi tujuan-tujuan yang dibenarkan sepertimana di perenggan 6.1.

Reality

Government agencies and organisations can share personal data without consent if any of the permitted purposes are met under Paragraph 6.1.

3. Skop dan Kebolehgunaan

Scope and Applicability

- 3.1. Garispanduan ini hanya digunakan oleh agensi-agensi Kerajaan yang terlibat dalam perkongsian data peribadi dengan:

These Guidelines only apply to Government agencies that are involved in the sharing of personal data with:

- 3.1.1. Agensi-agensi Kerajaan yang lain;
other Government agencies;

- 3.1.2. Organisasi-organisasi; dan
organisations; and

- 3.1.3. Pemproses data.
data processors.

- 3.2. Perkongsian data peribadi oleh organisasi-organisasi akan dikawalselia di bawah mana-mana perundangan kebangsaan berkaitan dengan perlindungan data peribadi yang sedang berjalan.
The sharing of personal data by organisations will be regulated by any applicable national legislation on personal data protection.

4. Definisi Utama

Key Definitions

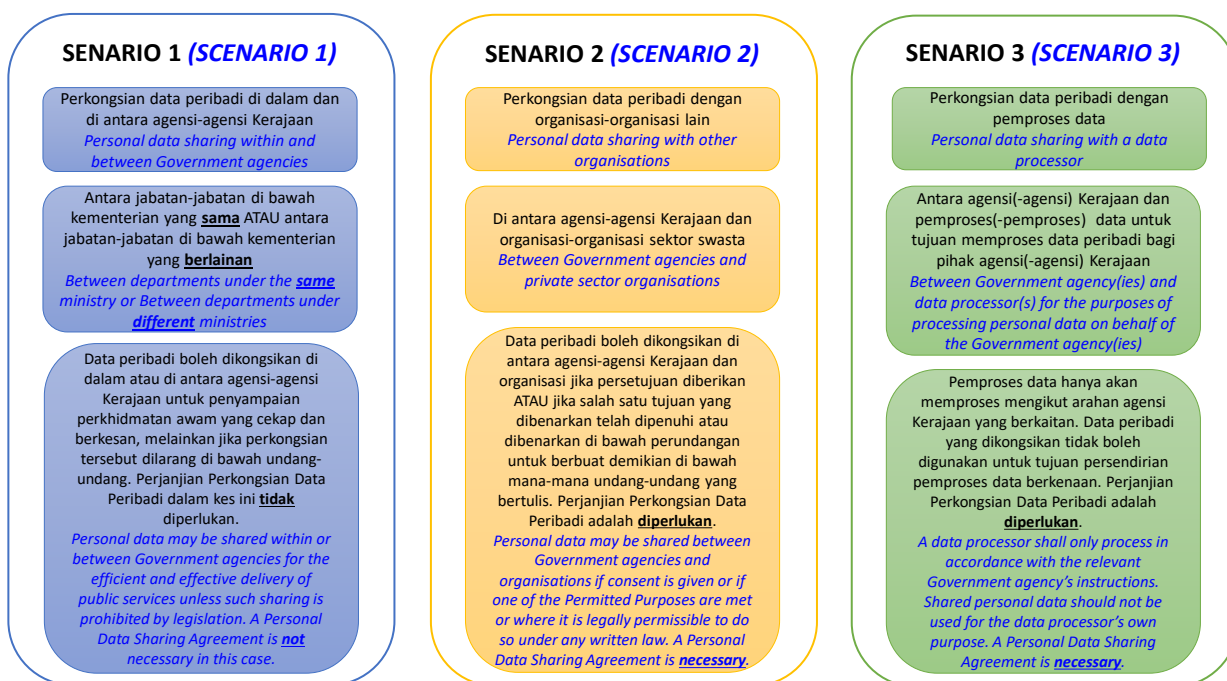
- 4.1. Dalam garispanduan ini, melainkan ianya memerlukan konteks berlainan –
In these Guidelines, unless the context otherwise requires –

- 4.1.1. “pengumpulan” bermakna mengumpul, memperolehi, atau mendapatkan data peribadi daripada mana-mana sumber sama ada secara langsung atau tidak langsung dengan apa cara sekalipun;
“collection” means gathering, acquiring, or obtaining personal data from any source whether directly or indirectly by any means;
- 4.1.2. “pengawal data” bermakna agensi Kerajaan atau organisasi secara persendirian atau secara bersama dengan pengawal-pengawal data yang lain bagi menentukan tujuan-tujuan dan cara-cara pemprosesan data peribadi;
“data controller” means the Government agency or organisation who alone or jointly with other data controllers determines the purposes and means of the processing of personal data;
- 4.1.3. “pemproses data” bermakna agensi Kerajaan atau organisasi yang memproses data peribadi bagi pihak pengawal data;
“data processor” means the Government agency or organisation who processes personal data on behalf of the data controller;
- 4.1.4. “mendedahkan atau mengongsikan” bermakna untuk memindahkan, mendedahkan, menyebarkan, mengongsikan atau menyediakan data peribadi dalam simpanannya kepada Pihak Penerima;
“disclose or share” means to transfer, disclose, disseminate, share or otherwise make available personal data in its possession to the Receiving Party;
- 4.1.5. “Pihak Yang Mendedahkan” bermakna agensi Kerajaan atau organisasi yang menghantar, memindahkan, menyebarkan, mendedahkan, mengongsikan atau menyediakan data peribadi dalam simpanannya kepada Pihak Penerima;
“Disclosing Party” means the Government agency or organisation who transmits, transfers, disseminates, discloses, shares or otherwise makes available personal data in its possession to the Receiving Party;
- 4.1.6. “Kerajaan” bermakna Kerajaan Kebawah Duli Yang Maha Mulia Paduka Seri Baginda Sultan dan Yang Di-Pertuan Negara Brunei Darussalam;
“Government” means the Government of His Majesty the Sultan and Yang Di-Pertuan of Brunei Darussalam;
- 4.1.7. “agensi Kerajaan” termasuk mana-mana kementerian atau jabatan Kerajaan, termasuk institusi-institusi pendidikan dan badan-badan berkanun;
“Government agency” includes any Government ministry or department, including educational institutions and statutory bodies;
- 4.1.8. “Ketua agensi” merujuk kepada Setiausaha Tetap dari Kementerian Kerajaan, Ketua Jabatan Kerajaan, Ketua institusi pendidikan, Ketua Eksekutif atau Pengarah Urusan badan-badan berkanun;
“Head of Agency” refers to the Permanent Secretary of the Government Ministry, Head of Government Department, Head of educational institutions, Chief Executive or Managing Director of statutory bodies;

- 4.1.9. “Ketua organisasi” merujuk kepada tahap kuasa yang tertinggi dalam organisasi;
“Head of Organisation” refers to the highest level of authority in organisations;
- 4.1.10. “organisasi” termasuk mana-mana individu, syarikat, persatuan atau badan perseorangan, korporat atau bukan korporat, sama ada atau tidak –
“organisations” includes any individual, company, association or body of persons, corporate or unincorporated, whether or not –
- (a) ditubuhkan atau diiktiraf di bawah Undang-Undang Negara Brunei Darussalam; atau
formed or recognised under the law of Brunei Darussalam; or
 - (b) bermastautin atau mempunyai pejabat atau tempat perniagaan di Negara Brunei Darussalam;
resident or having an office or place of business in Brunei Darussalam;
- 4.1.11. “pihak” merujuk kepada Pihak Penerima dan Pihak Yang Mendedahkan secara kolektif;
“parties” refer to the Receiving Party and the Disclosing Party collectively;
- 4.1.12. “data peribadi” bermakna data, dalam apa jua bentuk sama ada dalam format *softcopy* atau *hardcopy*, yang mana secara amnya tidak disediakan bagi rujukan orang awam atau dalam domain awam, sama ada benar atau tidak, mengenai individu yang boleh dikenalpasti daripada data berkenaan, atau daripada data berkenaan dan maklumat lain yang ada dalam simpanan agensi Kerajaan atau organisasi;
“personal data” means data, in any form whether in softcopy or hardcopy format, which is generally not made available to the public or within the public domain, whether true or not, about an individual who can be identified from the data, or from the data and other information which is in the possession of the Government agency or organisation;
- 4.1.13. “perjanjian perkongsian data peribadi” bermakna perjanjian antara Pihak Penerima dan Pihak Yang Mendedahkan;
“personal data sharing agreement” means the agreement between the Receiving Party and the Disclosing Party;
- 4.1.14. “pemprosesan” bermakna sebarang operasi atau set operasi yang dilakukan ke atas data, sama ada menggunakan elektronik atau tidak, seperti pengumpulan, rakaman, organisasi, penyimpanan, penyesuaian atau mengubah, pengambilan semula, perundangan, penggunaan melalui penghantaran, penyebaran atau penyediaan, penjajaran atau gabungan, penyekatan, penghapusan atau pemusnahan;
“processing” means any operation or set of operations performed upon data, whether or not by electronic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
- 4.1.15. “Pihak Penerima” bermakna agensi Kerajaan atau organisasi yang membuat permohonan atau menerima data peribadi yang berkaitan daripada Pihak Yang Mendedahkan; dan
“Receiving Party” means the Government agency or organisation who requests for or receives the relevant personal data from the Disclosing Parties; and

5. Senario bagi Perkongsian Data Peribadi *Scenarios for Personal Data Sharing*

- 5.1 Perkongsian data peribadi merujuk kepada pendedahan data peribadi kepada sebuah atau lebih dari sebuah agensi Kerajaan atau organisasi dan penyimpanan data peribadi tersebut.
Personal data sharing refers to the disclosure of personal data to one or more Government agency(ies) or organisation(s) and the latter's collection of that personal data.
- 5.2 Rajah 1 di bawah menggambarkan senario-senario yang berbeza di mana perkongsian data peribadi boleh berlaku.
The diagram below illustrates the different scenarios in which personal data sharing can take place.



Rajah 1 : Senario-Senario Perkongsian Data Peribadi
 Diagram 1: Personal Data Sharing Scenarios

- 5.3 Senarai semak keperluan di bawah setiap senario yang berbeza boleh diperolehi di **Jadual D**.
*A checklist of requirements under each of the different scenarios can be found in **Schedule D**.*

6. Tujuan Yang Dibenarkan *Permitted Purposes*

- 6.1 Pihak penerima hendaklah mengenalpasti tujuan dan objektif yang ingin dicapai dari perkongsian data peribadi tersebut.
Receiving Parties should identify the purpose and objectives that personal data sharing is meant to achieve.
- 6.2 Perkongsian data peribadi antara agensi-agensi kerajaan adalah tertakluk kepada undang-undang, peraturan dan dasar pada masa ini termasuk Akta Rahsia Rasmi (Penggagal 153); Dasar

Perlindungan Data di bawah Pusat Kebangsaan E-Kerajaan (EGNC) dan arahan yang terkandung di dalam Manual Keselamatan Perlindungan di bawah Jabatan Keselamatan Dalam Negeri (JKDN).

The sharing of personal data between Government agencies are subject to laws, regulations, policies and directions, which includes the Official Secrets Act (Chapter 153); the Data Protection Policy by the E-Government National Centre (EGNC) and instructions contained in the Protective Security Manual by the Internal Security Department (ISD).

- 6.3 Agensi-agensi kerajaan hanya dibenarkan untuk mengongsi data peribadi antara agensi-agensi kerajaan dan organisasi-organisasi **tanpa mendapatkan persetujuan** jika salah satu daripada **tujuan yang dibenarkan** dipenuhi antara lain seperti berikut:

*Government agencies are permitted to share personal data between other Government agencies and organisations **without consent** as long as one of the following **permitted purposes** are met:*

- 6.3.1. **Kewajipan Undang-Undang:** Pendedahan adalah diperlukan bagi memenuhi kewajipan undang-undang di bawah mana-mana undang-undang yang bertulis;
***Legal obligation:** The disclosure is necessary to comply with a legal obligation under any written law;*
- 6.3.2. **Keselamatan Negara:** Pendedahan adalah diperlukan dalam keadaan yang melibatkan keselamatan negara;
***National security:** The disclosure is necessary in the event of a national security;*
- 6.3.3. **Kesihatan Awam:** Pendedahan adalah diperlukan bagi melaksanakan tugas untuk kepentingan awam yang melibatkan kesihatan awam;
***Public health:** The disclosure is necessary to perform a task in the public interest in the area of public health;*
- 6.3.4. **Ketenteraman Awam:** Pendedahan adalah diperlukan bagi membolehkan sebarang penyiasatan atau *proceedings* bagi mengekalkan keamanan dan ketenteraman awam di dalam Negara Brunei Darussalam;
***Public order:** The disclosure is necessary for any investigation or proceedings and to maintain peace and public order within Brunei Darussalam;*
- 6.3.5. **Keselamatan Awam:** Pendedahan diperlukan bagi melaksanakan tugas demi kepentingan keselamatan awam;
***Public safety:** The disclosure is necessary to perform a task in the interest of public safety;*
- 6.3.6. **Tugasan Awam:** Pendedahan diperlukan bagi melaksanakan tugas untuk kepentingan awam dan tugas tersebut mempunyai asas yang jelas dalam undang-undang atau semasa melaksanakan tanggungjawab rasmi;
***Public task:** The disclosure is necessary to perform a task in the public interest and the task has a clear basis in law or in the exercise of an official authority;*
- 6.3.7. **Tujuan Penyelidikan:** Pendedahan data peribadi mengenai individu bagi tujuan penyelidikan termasuk bagi penyelidikan sejarah dan statistik;

Research purposes: The disclosure of personal data about an individual is for research purposes, including historical or statistical research¹;

- 6.3.8. **Kepentingan Mustahak:** Pendedahan peribadi diperlukan bagi melindungi nyawa seseorang; atau

Vital interests: The disclosure is necessary to protect someone's life; or

- 6.3.9. Pendedahan adalah mematuhi dasar, manual, garispanduan yang telah dikeluarkan oleh Kerajaan dan sebagainya.

The disclosure is in compliance with any related government issued policies, manuals, guidelines, etc.

- 6.4. Persetujuan dari individu berkenaan bagi mengongsikan data peribadi adalah diperlukan bagi tujuan yang tidak berkaitan dengan mana-mana tujuan di atas dan **bagi tujuan di mana perkongsian data peribadi adalah tidak dibenarkan di bawah mana-mana perundangan yang bertulis.**

An individual's consent should be sought for the sharing of personal data that is not related to any of the purposes above and where it is not legally permissible to do so under any written law.

- 6.5. Agensi-agensi Kerajaan hanya boleh mengongsikan data peribadi yang berkaitan dan diperlukan bagi mencapai tujuan yang telah dikenalpasti. Sebagai contoh, agensi-agensi Kerajaan mungkin diperlukan untuk mengongsikan nama dan alamat terkini sahaja dan bukan maklumat peribadi lain di bawah simpanan agensi berkenaan.

Government agencies should only share the specific personal data needed to achieve the purpose(s) identified. For instance, Government agencies might need to share somebody's current name and address, but not other information they may have in their possession.

7. Lantikan Pegawai Perlindungan Data *Appointment of Data Protection Officer(s)*

- 7.1. Pegawai Perlindungan Data akan dilantik sebagai pegawai hubungan fokal bagi:
Data Protection Officer(s) shall be appointed as focal contact person(s) for:

- 7.1.1. Menerima atau mengumpulkan dan menyediakan data peribadi yang berkenaan;
Receiving or compiling and providing the relevant personal data;

¹ Perkongsian data peribadi untuk tujuan penyelidikan **hanya dibenarkan jika keadaan berikut dipenuhi:** (i) tujuan penyelidikan tidak dapat dicapai melainkan data peribadi dikongsikan dalam *individually identifiable form*; (ii) adalah tidak praktikal untuk mendapatkan persetujuan daripada individu bagi mengongsikan data peribadi; (iii) memberikan manfaat kepada awam apabila data peribadi dikongsikan; (iv) hasil penyelidikan tidak akan digunakan untuk membuat keputusan yang memberi kesan kepada individu; dan (v) hasil penyelidikan, jika diterbitkan, mestilah dalam bentuk yang tidak mengenal pasti mana-mana individu.

The disclosure of personal data for research purposes is **only permitted if all the following circumstances are met:** (i) the research purpose cannot reasonably be accomplished unless the personal data is disclosed in an individually identifiable form; (ii) it is impracticable to seek the consent of the individual for the disclosure; (iii) there is a clear public benefit to disclosing the personal data for research purpose; (iv) the results of the research will not be used to make a decision that affects the individual; and (v) the results of the research, if published, must be in a form that does not identify any individual.

- 7.1.2. Memastikan data peribadi dikumpulkan, digunakan, diproses dan dikongsi dengan mematuhi mana-mana garispanduan dan undang-undang berkaitan dengan perlindungan data peribadi.
Ensuring that personal data is collected, used, processed and disclosed in compliance with any applicable guidelines and laws on personal data protection.
- 7.2 Peranan dan tanggungjawab Pegawai Perlindungan Data adalah seperti berikut:
The roles and responsibilities of a Data Protection Officer includes the following:
- 7.2.1. Menyediakan, merebui dan mengemaskini prosedur untuk memastikan pematuhan dengan garispanduan tersebut;
Establish, review and update procedures to ensure compliance with these Guidelines;
- 7.2.2. Menjalankan pemeriksaan secara mengejut dan berkala serta melaksanakan tindakan untuk memperbetulkan bila diperlukan; dan
Conducting regular spot checks and taking corrective action where necessary; and
- 7.2.3. Mencadangkan dan melaksanakan program latihan yang bersesuaian dalam pengendalian dan pengurusan data peribadi bagi memberikan dan menanamkan kesedaran di dalam agensi atau organisasi berkenaan.
Proposing and implementing suitable training programmes in the handling and management of personal data to create and instil awareness within the agency or organisation.
- 7.3 Maklumat perniagaan iaitu nama, alamat, nombor telefon dan/atau alamat emel Pegawai Perlindungan Data hendaklah dimaklumkan kepada orang ramai melalui laman sesawang agensi Kerajaan atau melalui platform media sosial bila mana ianya dikehendaki.
The business contact information, i.e. the name, address, phone number and/or email address of the Data Protection Officer shall be made available to the public via the Government agency's website or social medial platforms and as and when requested.
- 8. Permohonan bagi Perkongsian Data**
Data Sharing Request
- 8.1. Sebarang permohonan bagi perkongsian data peribadi mestilah dipohonkan oleh Pihak Penerima melalui Borang Permohonan Perkongsian Data. Pihak Penerima iaitu Pegawai Perlindungan Data hendaklah mengisikan Bahagian A di dalam Borang Permohonan Perkongsian Data.
Any requests for personal data sharing must be raised by a Receiving Party via a Data Sharing Request Form. The Receiving Party's Data Protection Officer must fill in Part A of the Data Sharing Request Form.
- 8.2. Bahagian A di dalam Borang Permohonan Perkongsian Data hendaklah disahkan oleh Ketua agensi bagi agensi kerajaan yang berkaitan atau pegawai yang memangku jawatan tersebut. Ketua agensi dibenarkan untuk mewakili kuasa secara bertulis kepada pegawai yang bersesuaian dan salinan perwakilan kuasa tersebut hendaklah dilampirkan pada Borang Permohonan Perkongsian Data.
Part A of the Data Sharing Request Form shall be verified by the Head of Agency of the relevant Government agency or their acting officers. The Head of Agency may delegate this authority

to an authorised officer² in writing, and a copy of the delegation shall be attached to the Data Sharing Request Form.

- 8.3. Pihak yang Mendedahkan mestilah mengakui penerimaan Borang Permohonan Perkongsian Data dengan melengkapkan maklumat yang terkandung di Bahagian B di dalam Borang Permohonan Perkongsian Data.
The Disclosing Party must acknowledge receipt of the Data Sharing Request Form by completing the information contained in Part B of the Data Sharing Request Form.

- 8.4. Bahagian B di dalam Borang Permohonan Perkongsian Data hendaklah disahkan oleh Ketua agensi di bawah agensi Kerajaan yang berkaitan atau ketua organisasi atau pegawai yang memangku jawatan tersebut. Ketua agensi atau Ketua organisasi boleh mewakilkan kuasa ini kepada pegawai yang diberi kuasa secara bertulis, dan salinan tersebut hendaklah dilampirkan pada Borang Permohonan Perkongsian Data.
Part B of the Data Sharing Request Form shall be verified by the Head of Agency of the relevant Government agency or the Head of Organisation or their acting officers. The Head of Agency or Head of Organisation may delegate this authority to an authorised officer in writing, and a copy of the delegation shall be attached to the Data Sharing Request Form.

- 8.5. Borang Permohonan Perkongsian Data boleh diisikan dan ditandatangani secara elektronik dan dihantar melalui e-mel kepada Pegawai Perlindungan Data pihak berkenaan bersama-sama dengan lampiran dokumen kebenaran yang diperlukan. Kandungan e-mel hendaklah dilindungi dengan kata laluan atau *encrypted*.
The Data Sharing Request Form can be filled in and signed electronically and e-mailed out to the relevant parties' Data Protection Officers along with the necessary authorisation documents attached to the e-mail. The contents of the e-mail must be password protected or encrypted.

- 8.6. *Templat Borang Permohonan Perkongsian Data adalah disediakan dalam Jadual A*
*A template of the Data Sharing Request Form is provided in **Schedule A**.*

9. Jadual bagi perkongsian maklumat peribadi ***Schedule for Personal Data Sharing***

- 9.1. Agensi-agensi kerajaan untuk menentukan sama ada perkongsian tersebut dilaksanakan sebagai proses yang berterusan atau sama ada ianya hanya perlu dilaksanakan sebagai tindak balas kepada acara atau tujuan yang tertentu.
Government agencies should determine whether the sharing should be an ongoing process or whether it should only take place in response to a particular event or purpose.

9.2. Perkongsian data secara *ad-hoc* atau *one-off*

² Pegawai berkuasa ialah mana-mana pegawai yang diberikan tanggungjawab oleh Ketua Agensi untuk memberi pengesahan, yang mana besar kemungkinan adalah pegawai yang memangku tugas beliau. Walau bagaimanapun, ianya tidak sepatutnya dijalankan oleh Pegawai Perlindungan Data (DPO) bagi mengelakkan sebarang *conflict of interest* kerana DPO bertanggungjawab terhadap pengumpulan data peribadi.

The authorised officer is any officer that the Head of Agency delegates the responsibility of verification to, most likely his or her acting officer. However, it should not be the Data Protection Officer (DPO) to avoid any conflict of interest as the DPO is responsible for compiling the personal data.

Perkongsian data peribadi berkemungkinan hanya diperlukan semasa situasi diluar perancangan berkala atau semasa situasi kecemasan.

Ad hoc or one-off sharing of personal data

The sharing of personal data may be required in situations outside a periodic arrangement or in an emergency situation.

9.3. Perkongsian data peribadi secara berterusan atau berkala

Perkongsian yang dilaksanakan dengan cara ini adalah secara rutin dan terancang. Secara amnya, ianya akan melibatkan perkongsian data peribadi untuk set data peribadi yang sama, secara kebiasaannya, dan secara berjadual pada selang waktu.

Continuous or periodic sharing of personal data

Sharing done in this way is routine and pre-planned. It will generally involve the sharing of personal data for the same sets of personal data, at regular, scheduled intervals.

9.4. Pihak berkenaan diperlukan untuk mendokumenkan mekanisme perkongsian yang dipersetujui bagi tujuan audit di dalam Borang Permohonan Perkongsian Data.

Parties should document the agreed sharing mechanisms for audit purposes in the Data Sharing Request Form.

9.5. Perkongsian data peribadi hendaklah dilaksanakan di dalam keadaan selamat dan terjamin, termasuk *encrypting* atau melindungi dokumen menggunakan kata laluan yang kukuh.

The sharing of personal data must be done in a safe and secured manner, including encrypting or protecting documents with strong passwords.

10. Fail Format yang disarankan bagi perkongsian data peribadi.

Suggested File Formats for Sharing of Personal Data

10.1. Pihak yang bertanggungjawab mendedahkan data hendaklah memastikan fail format yang dipilih adalah terpelihara dan data yang dikongsikan adalah selamat.

The Disclosing Party shall ensure that the file formats chosen ensure preservation and security of shared data.

10.2. Pihak yang bertanggungjawab mendedahkan data hendaklah memastikan bahawa data asal yang tidak diubah dan disimpan dalam format asalnya sebagai data sumber yang tidak boleh diubah atau ditukar.

Disclosing Party shall ensure that the original unedited raw data are kept in their native formats as source data which should not be altered or edited.

10.3. Pihak yang bertanggungjawab mendedahkan data hendaklah membuat salinan fail asal sebelum sebarang analisa atau perkongsian data peribadi dilaksanakan.

The Disclosing Party shall make copies of the original files prior to any analysis or personal data sharing.

10.4. Fail format yang disarankan:

Recommended file formats³:

Teks, Dokumentasi, Skrip <i>Text, Documentation, Scripts</i>	XML, XLS, PDF/A, HTML, ASCII, UTF-8, Plain Text
Imej tidak bergerak <i>Still Image</i>	TIFF, JPEG 2000, PNG, JPEG/JFIF, DNG (digital negative), BMP, GIF
Imej Grafik <i>Graphic Image</i>	raster formats: TIFF, JPEG2000, PNG, PDF, JPEG/JFIF, DNG, BMP, GIF vector formats: Scalable vector graphics, AutoCAD Drawing Interchange Format, Encapsulated Postscripts, Shape files cartographic: Most complete data, GeoTIFF, GeoPDF, GeoJPEG2000, Shapefile
Audio	WAVE, AIFF, MP3, MXF, FLAC
Video	MOV, MPEG-4, AVI, MXF
Pangkalan Data <i>Database</i>	XML, CSV, TAB
Arkib Web <i>Web archive</i>	WARC
Geospatial	Shapefile (SHP, DBF, SHX), GeoTIFF, NetCDF
Containers	TAR, GZIP, ZIP
Tabular	CSV
Statistik <i>Statistics</i>	ASCII, DTA, POR, SAS, SAV

11. Keselamatan dan Kerahsiaan Data Peribadi
Security and Confidentiality of Personal Data

- 11.1. Dalam mengambil langkah-langkah berpatutan bagi memastikan keselamatan dan kerahsiaan data peribadi, agensi-agensi Kerajaan dikehendaki untuk mematuhi Dasar Perlindungan Data di bawah EGNC, Manual Keselamatan Perlindungan di bawah JKDN, Akta Rahsia Rasmi (Penggali 153) dan peruntukan di bawah sebarang perundangan yang berkaitan. Organisasi diperlukan untuk mematuhi peruntukan bagi sebarang perundangan berkaitan keselamatan data peribadi.

In taking appropriate steps to ensure the security and confidentiality of personal data, Government agencies must abide by the Data Protection Policy by EGNC, the Protective Security Manual by ISD, the Official Secrets Act (Chapter 153) and the provisions of any relevant laws. Organisations must abide by the provisions of any relevant personal data protection laws.

- 11.2. Agensi-agensi Kerajaan hanya dibenarkan untuk mengongsikan data peribadi kepada individu berkenaan di bawah agensi-agensi dan organisasi Kerajaan. Akses dan perkongsian data peribadi adalah terhad kepada kakitangan yang diberi kuasa sahaja termasuk pegawai perlindungan data.

³ Senarai ini tidak bertujuan untuk menyeluruh, dan dalam beberapa kes, fail format boleh ditambah atau dikeluarkan tertakluk kepada teknologi yang digunakan pada masa tersebut.

This list is not intended to be exhaustive and, in some cases, the file formats can be added to or deleted depending on the technology used at the time.

Government agencies should only share personal data to relevant individuals within Government agencies and organisations. Access to and disclosure of personal data should be limited to authorised staff including the Data Protection Officer.

- 11.3. Agensi-agensi Kerajaan hendaklah menggunakan langkah-langkah organisasi dan langkah-langkah teknikal yang bersesuaian bagi melindungi data peribadi menurut standard keselamatan antarabangsa yang dipraktikkan.

Government agencies should utilise appropriate organisational measures and technical measures to safeguard personal data in accordance with recognised international security standards.⁴

- 11.4. **Langkah-langkah Organisasi** termasuk seperti berikut:

Organisational measures include the following:

- 11.4.1. Penilaian Risiko – Adalah dicadangkan untuk menyediakan penilaian risiko ke atas semua aktiviti yang diproses untuk mengenalpasti data peribadi yang berpotensi menimbulkan risiko yang lebih tinggi dan langkah-langkah yang diperlukan untuk memastikan data peribadi tersebut selamat dan dilindungi.

Risk Assessment – It is suggested to do a risk assessment on all processing activities to ascertain which pose higher risks to personal data and what measures are needed to ensure that personal data is secure and protected.

- 11.4.2. Dasar dan Prosedur – Mempunyai dasar dan prosedur yang menyeluruh boleh membantu kakitangan mengenalpasti kewajipan masing-masing dan langkah-langkah yang perlu dilaksanakan jika berlakunya sebarang situasi.

Policies and Procedures – Having robust policies and procedures helps employees know what their obligations are and what to do if certain situations occur.

- 11.4.3. Latihan dan Kesedaran – Memastikan kakitangan mengetahui perlindungan data peribadi, mengetahui apa yang diperlukan dari mereka, dan tatacara mengekalkan pematuhan.

Awareness and Training – Ensure that employees are aware of personal data protection, know what is expected of them and how they should maintain compliance.

- 11.4.4. Reviu dan Audit – Mengenalpasti jurang dan kelemahan dengan cara mereviu dan mengaudit fungsi, aktiviti dan sistem terhadap dasar dan prosedur.

Review and Audits – Identify gaps and weaknesses by reviewing and auditing functions, activities and systems against policies and procedures.

- 11.4.5. Ketelitian dan Ketepatan Data Peribadi – Memastikan data peribadi yang dimiliki adalah terkini dan tepat.

Due Diligence and Accuracy of Personal Data – Ensure that the personal data in possession is up-to-date and accurate.

⁴ ISO telah mengkhususkan siri piawai ISO 27000 bagi urusan keselamatan maklumat. Standard ISO 27001 menyediakan rangka kerja rujukan yang komprehensif bagi sistem pengurusan keselamatan maklumat. Secara khusus, ianya merangkumi keselamatan rangkaian, keselamatan fizikal dan elektronik, keselamatan bagi operasi persekitaran dan keselamatan kakitangan operasional. (The ISO 27000 series of standards have been specifically reserved by ISO for information security matters. The standard ISO 27001 provides a comprehensive reference framework for information security management systems. In particular, it covers network security, physical and electronic security, security of the operating environment and security of operational staff.)

11.5. **Langkah-langkah Teknikal** termasuk, tetapi tidak terhad kepada perkara-perkara berikut:

Technical measures include, but are not limited to, the following:

- 11.5.1. Keselamatan Fizikal – Mengambil langkah-langkah dan menyediakan protokol bagi memastikan akses keselamatan kepada sebarang pejabat atau bangunan dan memastikan semua kakitangan mengetahui tentang kawalan tersebut. Pelawat untuk diberikan kad ID dan dimestikan untuk daftar masuk/keluar dari bangunan berkenaan. Akses keselamatan yang terhad ke kawasan yang mempunyai data peribadi dengan kunci biometrik atau log akses.

Physical Security – Take measures and develop protocols for securing access to any office or building and ensure that all employees are aware of such controls. Visitors should be assigned ID badges and be mandated to sign in/out of the building. Secure access to areas processing personal data with biometric locks or access logs.

- 11.5.2. Pelupusan – Penghapusan (*shredding*) rekod dalam bentuk *hardcopy* adalah diwajibkan bagi data peribadi dalam format kertas. Pelupusan aset IT dengan betul adalah diwajibkan bagi menjamin pemadaman yang berkesan dan lengkap bagi sebarang data atau akses peribadi.

Disposal – Shredding of hardcopy records is essential where personal data is contained in paper formats. Proper disposal of IT assets is necessary to guarantee effective and complete erasure of any personal data or access.

- 11.5.3. Melindungi peranti, rangkaian dan *servers* harus dilaksanakan tanpa mengira saiz dan skop agensi Kerajaan. Imbasan *vulnerability* boleh dilakukan pada semua peranti, rangkaian dan *servers* untuk mengenal pasti sebarang jurang atau kelemahan.

Protecting devices, networks and servers should be implemented regardless of the size and scope of a Government agency. Vulnerability scans may be carried out on all devices, networks and servers to identify any gaps or areas of weakness.

- 11.5.4. Langkah-langkah lain termasuk menggunakan *Virtual Private Network (VPN)*, autentikasi dua-hala, *encryption*, kata laluan atau biometrik.

Other measures include Virtual Private Network (VPN), two-factor authentication, encryption, passwords or biometrics.

12. **Dasar Penyimpanan dan Pelupusan**

Retention and Disposal Policies

- 12.1. Agensi-agensi Kerajaan hendaklah menyediakan dan mengimplementasikan dasar penyimpanan dan pelupusan persendirian berdasarkan tujuan bagi memproses data peribadi.

Government agencies should develop and implement their own retention and disposal policies based on the purposes for processing personal data.

- 12.2. Dalam menyediakan dasar tersebut, agensi-agensi Kerajaan hendaklah mengambil langkah-langkah berpatutan berkaitan data peribadi dan mengimbangi keperluan agensi dengan impak penyimpanan terhadap privasi individu berkenaan.

In developing such policies, Government agencies should take a proportionate approach to personal data retention, balancing their needs with the impact of retention on an individual's privacy.

- 12.3. Jika tidak lagi ada keperluan untuk menyimpan data peribadi tersebut, agensi-agensi Kerajaan hendaklah memastikan bahawa data peribadi tersebut secara selamat dan secara kekal dipadamkan atau dirahsiakan (anonymous).

Where there is no need to retain personal data any longer, Government agencies ensure that the personal data is securely and permanently deleted or anonymised.

- 12.4. Data peribadi hendaklah dipadamkan atau dihapuskan menggunakan salah satu cara yang terjamin iaitu:

Personal data must be deleted or destroyed using one of the following secure methods:

- 12.4.1. Dokumen yang disimpan secara elektronik hendaklah dipadamkan menggunakan utiliti elektronik yang selamat bagi memastikan maklumat tersebut tidak dapat diambil semula. Utiliti pemadaman standard yang hanya mengeluarkan *file pointer* tidak boleh digunakan.

Documents retained electronically should be deleted with a secure deletion utility that ensures that the information cannot be retrieved. Standard deletion utilities that only remove the file pointer should not be used.

- 12.4.2. Data peribadi di dalam *hard drives*, media mudah-alih atau sebarang peralatan yang serupa mestilah dipadamkan dengan selamat sebelum dilupuskan atau peralatan tersebut dipindahmilik.

Personal data on hard drives, removable media and any similar items must be securely erased before any disposal or reassignment of the equipment.

- 12.4.3. Jika data peribadi tersebut tidak dapat dipadamkan dari peralatan, ianya mestilah dilupuskan secara fizikal oleh pegawai yang diberikuasa, syarikat pakar dalam penghapusan, dan sijil penghapusan mestilah diperolehi.

Where personal data cannot be erased from equipment, it must be physically destroyed by an authorised, specialist destruction company, and certificates of destruction must be obtained.

- 12.4.4. Salinan kertas mesti dilupuskan menggunakan mesin *shredder*.

Paper copies must be destroyed using shredders.

- 12.5. Ketua-ketua agensi mestilah memberi kuasa bagi penghapusan atau pemadaman data peribadi dan Pegawai Perlindungan Data hendaklah merekodkan sebarang pelupusan, termasuk Tarikh (dan jam, jika berkenaan), kandungan data peribadi dan tatacara penghapusan atau pemadaman.

Heads of agencies must authorise the destruction or deletion of the personal data and the Data Protection Officer must record such deletion, including the date (and time, if relevant), the content of the personal data and the method of destruction or deletion.

13. Perjanjian Perkongsian Data Peribadi *Personal Data Sharing Agreements*

- 13.1 Sepertimana yang digambarkan di Perenggan 5.2, Perjanjian Perkongsian Data Peribadi adalah **dimestikan** dalam situasi berkenaan:
*As illustrated in Paragraph 5.2, a Personal Data Sharing Agreement is **necessary** in the following scenarios:*
- 13.1.1. **Senario 2:** Di mana perkongsian data peribadi adalah antara agensi Kerajaan (atau lebih dari satu agensi Kerajaan) dan organisasi (atau lebih dari satu organisasi) sektor swasta; dan
Scenario 2: Where personal data sharing is between Government agency(ies) and private sector organisation(s); and
- 13.1.2. **Senario 3:** Di mana perkongsian data peribadi adalah antara agensi Kerajaan (atau lebih dari satu agensi Kerajaan) dan data processor(s).
Scenario 3: Where personal data sharing is between Government agency(ies) and data processor(s).
- 13.2 Perjanjian Perkongsian Data Peribadi adalah **tidak dimestikan** bagi **Senario 1**, yang mana data peribadi berkenaan dikongsi bersama dan antara agensi-agensi Kerajaan kerana perkongsian data peribadi adalah penting bagi perkhidmatan awam yang cekap dan berkesan.
*A Personal Data Sharing Agreement is **not necessary** for Scenario 1, where personal data is shared within and between Government agencies because the sharing of personal data is crucial for the efficient and effective delivery of public services.*
- 13.3 Perjanjian Perkongsian Data Peribadi atau klausa (atau lebih dari satu klausa) yang merupakan sebahagian daripada perjanjian, seperti klausa di dalam perjanjian konsultasi, hendaklah menyenaraikan tujuan bagi perkongsian data peribadi, yang merangkumi apa yang akan terjadi kepada data berkenaan di setiap peringkat, menetapkan standard dan menyediakan penjelasan mengenai tugas dan tanggungjawab semua pihak yang terlibat dalam perkongsian data peribadi.
A Personal Data Sharing Agreement or clause(s) being part of an agreement, e.g. clauses inside a consultancy agreement, should set out the purpose/s of personal data sharing, cover what is to happen to the data at each stage, set standards and provide clarity on the roles and responsibilities of all the parties involved in the sharing of personal data.
- 13.4 **Jadual B** menyediakan contoh klausa kontrak yang boleh dimasukkan ke dalam Perjanjian Perkongsian Data Peribadi. Penggunaan sampel klausa tersebut tidak bermakna pematuhan kepada sebarang perundangan yang berkaitan. Pihak berkenaan hendaklah mendapatkan khidmat perundangan yang profesional jika terdapat sebarang ketidakpastian terhadap kewajipan di bawah undang-undang atau di dalam Perjanjian Perkongsian Data Peribadi, atau jika memerlukan bantuan bagi menderaf perjanjian jika diperlukan.
Schedule B provides sample contractual clauses that may be included in a Personal Data Sharing Agreement. Use of the sample clauses does not mean compliance with any relevant laws. Parties should seek professional legal advice if there are uncertainties of obligations under the law or in the Personal Data Sharing Agreement, or if assistance with the drafting of an agreement is required.

14. Perkongsian Data Peribadi dalam Situasi Kecemasan
Personal Data Sharing in Emergency Situations

- 14.1. Agensi-agensi Kerajaan hendaklah mengongsikan data peribadi sepertimana yang diperlukan dan berpatutan semasa situasi kecemasan. Data peribadi yang dikongsikan tidak perlu menyeluruh dan hendaklah terhad kepada yang diperlukan sahaja bagi mencapai tujuan dalam sebarang situasi kecemasan.

Government agencies should share personal data as is necessary and proportionate in an emergency situation. The personal data shared must not be excessive and limited to what is necessary to achieve the purpose in any particular emergency situation.

- 14.2. Situasi kecemasan yang timbul kemungkinan tidak pernah dijangkakan dan perlu ditangani dengan segera tanpa melengahkan masa, dalam jangkamasa yang singkat. Sebagai contoh situasi kecemasan ialah pandemik baru-baru ini yang melibatkan seluruh dunia berkaitan penyakit koronavirus 2019 (COVID-19), iaitu penyakit berjangkit yang disebabkan oleh sindrom pernafasan akut koronavirus 2 (SARS-CoV-2), yang mana telah menunjukkan keperluan bagi perkhidmatan awam untuk bergabung di mana perkongsian data peribadi telah menunjukkan perubahan yang ketara kepada keselamatan awam.

Emergency situations can arise that may not have been foreseen and have to be dealt with immediately without undue delay, within the shortest possible time. An example of an emergency situation is the recent global pandemic concerning the coronavirus disease 2019 (COVID-19), an infectious disease caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), which has illustrated the need for joined-up public services where personal data sharing can make a real difference to public safety.

- 14.3. Ianya adalah tidak praktikal untuk membangkitkan Borang Permohonan Perkongsian Data dalam situasi kecemasan. Walau bagaimanapun, sebarang kerja-kerja pentadbiran hendaklah disusul sebaik sahaja situasi mengizinkan.

It may not be practical to raise a Data Sharing Request Form in an emergency situation, however, any relevant administrative work should be followed up with as soon as the situation allows for it.

- 14.4. Dalam situasi kecemasan, ianya lebih berbahaya jika data peribadi tidak dikongsikan berbanding jika ianya dikongsikan. Agensi-agensi dan organisasi Kerajaan untuk mengambilkira faktor risiko dalam tidak mengongsikan data.

In emergency situations, it would be more harmful not to share personal data than to share it. Government agencies and organisations should factor in the risks involved in not sharing data.

15. Carta Aliran bagi Perkongsian Data Peribadi
Flowchart for Personal Data Sharing

- 15.1. Sila rujuk **Jadual C**.
*Refer to **Schedule C**.*

[MUKA SURAT SELEBIHNYA ADALAH SENGHAJA DIKOSONGKAN]
[THE REMAINDER OF THIS PAGE IS LEFT INTENTIONALLY BLANK]

JADUAL A | BORANG PERMOHONAN PERKONGSIAN DATA
SCHEDULE A | DATA SHARING REQUEST FORM

BAHAGIAN A – Untuk disikan oleh Pihak Penerima PART A – To be completed by Receiving Party	
Nama agensi Kerajaan: <i>Name of Government agency:</i>	
Tujuan: Mengenal pasti tujuan yang dibenarkan dan sila nyatakan objektif bagi memohon data peribadi berkenaan. <i>Purpose:</i> Identify the permitted purpose(s) and state the objectives of the personal data requested.	Sila pilih mana-mana yang berkenaan (boleh memilih lebih dari satu): Select whichever is applicable (can be more than one): ☒ Kewajipan Undang-Undang: Pendedahan adalah diperlukan bagi memenuhi kewajipan undang-undang di bawah mana-mana undang-undang yang bertulis; <i>Legal obligation: The disclosure is necessary to comply with a legal obligation under any written law;</i> ☐ Keselamatan negara: Pendedahan adalah diperlukan dalam keadaan yang melibatkan keselamatan negara; <i>National security: The disclosure is necessary in the event of a national security;</i> ☐ Kesihatan awam: Pendedahan adalah diperlukan bagi melaksanakan tugas untuk kepentingan awam yang melibatkan bidang kesihatan awam; <i>Public health: The disclosure is necessary to perform a task in the public interest in the area of public health;</i> ☐ Ketenteraman Awam: Pendedahan adalah diperlukan bagi membolehkan sebarang penyiasatan atau <i>proceedings</i> bagi mengekalkan keamanan dan ketenteraman awam di dalam Negara Brunei Darussalam; <i>Public order: The disclosure is necessary for any investigation or proceedings and to maintain peace and public order within Brunei Darussalam;</i> ☐ Keselamatan Awam: Pendedahan diperlukan bagi melaksanakan tugas demi kepentingan keselamatan awam; <i>Public safety: The disclosure is necessary to perform a task in the interest of public safety;</i> ☐ Tugasan Awam: Pendedahan diperlukan bagi melaksanakan tugas untuk kepentingan awam dan tugas tersebut mempunyai asas yang jelas dalam undang-undang atau semasa melaksanakan tanggungjawab rasmi; <i>Public task: The disclosure is necessary to perform a task in the public interest and the task has a clear basis in law or in the exercise of an official authority;</i> ☐ Tujuan Penyelidikan: Pendedahan data peribadi mengenai individu bagi tujuan penyelidikan termasuk bagi penyelidikan sejarah dan statistik;

	Research purposes: <i>The disclosure of personal data about an individual is for research purposes, including historical or statistical research⁵;</i> ☐ Kepentingan Mustahak: Pendedahan diperlukan bagi melindungi nyawa seseorang; atau Vital interests: <i>The disclosure is necessary to protect someone's life;</i> ☐ Pendedahan ini adalah mematuhi mana-mana dasar, manual, garis panduan dan sebagainya yang dikeluarkan oleh kerajaan. Jika ya, sila nyatakan: _____ <i>The disclosure is in compliance with any related government issued policies, manuals, guidelines, etc.</i> <i>If yes, please specify:</i> _____ Sila nyatakan objektif (dan sebarang faedah yang berkenaan) bagi permohonan mendapatkan data peribadi. <i>State the objectives (and any relevant benefits) of requesting for the personal data.</i> 1. 2. 3. 4. 5.																
Kekerapan penghantaran data: Frequency of data transmission:	☐ Sekali sahaja. Tarikh Mula: _____ Tarikh Tamat: _____ <i>One-off. Start Date: _____ End Date: _____</i> ☐ Perkongsian berterusan/berkala. Kekerapan Maklumat*: _____ <i>Continuous/periodic sharing.</i> <i>Details of frequency*: _____</i> <i>*Tertakluk kepada ketersediaan data peribadi dan hanya digunakan untuk penghantaran secara digital</i> <i>*Subject to availability of personal data and only applicable for digital transmission.</i>																
Spesifikasi data peribadi: Sila berikan butiran data peribadi yang diminta,	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 5%;">No.</th><th style="width: 25%;">Data Element</th><th style="width: 45%;">Keterangan (Description)</th><th style="width: 25%;">Format*</th></tr> </thead> <tbody> <tr> <td>1</td><td></td><td></td><td></td></tr> <tr> <td>2</td><td></td><td></td><td></td></tr> <tr> <td>3</td><td></td><td></td><td></td></tr> </tbody> </table>	No.	Data Element	Keterangan (Description)	Format*	1				2				3			
No.	Data Element	Keterangan (Description)	Format*														
1																	
2																	
3																	

⁵ Pendedahan data peribadi untuk tujuan penyelidikan hanya dibenarkan jika semua keadaan berikut dipenuhi: (i) tujuan penyelidikan tidak dapat dicapai secara munasabah melainkan data peribadi didedahkan dalam bentuk yang boleh dikenal pasti secara individu; (ii) adalah tidak praktikal untuk mendapatkan persetujuan individu untuk pendedahan itu; (iii) terdapat faedah awam yang jelas untuk mendedahkan data peribadi untuk tujuan penyelidikan; (iv) hasil penyelidikan tidak akan digunakan untuk membuat keputusan yang memberi kesan kepada individu; dan (v) hasil penyelidikan, jika diterbitkan, mestilah dalam bentuk yang tidak mengenali pasti mana-mana individu.

*The disclosure of personal data for research purposes is **only permitted if all the following circumstances are met:** (i) the research purpose cannot reasonably be accomplished unless the personal data is disclosed in an individually identifiable form; (ii) it is impracticable to seek the consent of the individual for the disclosure; (iii) there is a clear public benefit to disclosing the personal data for research purpose; (iv) the results of the research will not be used to make a decision that affects the individual; and (v) the results of the research, if published, must be in a form that does not identify any individual.*

termasuk elemen data yang diperlukan. Jika lebih banyak ruang diperlukan, sila lampirkan secara berasingan pada penghujung borang ini.	4 5 6 7 8 9 10			
Personal data specifications: <i>Please provide details of the personal data requested, including the data elements required. If more space is needed, please attach a separate list at the end of this form.</i>	<i>*Sila nyatakan salah satu daripada format berikut: salinan hardcopy, softcopy (sila nyatakan format fail yang diperlukan, sebagai contoh. MS Excel, PDF, dll), integrasi pangkalan data atau lain-lain (sila nyatakan).</i> <i>*Please state either one of the following formats: hardcopy, softcopy (please specify the file format required, e.g. MS Excel, PDF, etc), database integration or others (please specify).</i>			
Kenyataan: <i>Remarks:</i>				
Tarikh Diperlukan: <i>Date required by:</i>				
Pengisytiharan Saya, yang bertandatangan di bawah, mengakui bahawa saya telah membaca Garis Panduan Perkongsian Data Peribadi dan saya bersetuju: 1. Untuk mematuhi Akta Rahsia Rasmi (Penggali 153) berhubung dengan menjaga maklumat rasmi; 2. Untuk menggunakan data peribadi yang diterima bagi tujuan yang dinyatakan di atas dan tidak mendedahkan maklumat untuk tujuan lain; 3. Untuk mengambil semua langkah-langkah teknikal dan organisasi yang sesuai untuk melindungi data peribadi yang didedahkan; 4. Untuk mengekalkan maklumat tidak lebih daripada yang diperlukan untuk mencapai tujuan tersebut, selepas itu maklumat tersebut sama ada akan dikembalikan kepada Pihak Pendedahan dan/atau dipadamkan dengan cara yang selamat dan tertutup; dan 5. Untuk mematuhi semua undang-undang yang berkaitan di Negara Brunei Darussalam, jika berkenaan.				
Declaration <i>I, the undersigned, acknowledge that I have read the Guidelines on Personal Data Sharing and I agree:</i> 1. To comply to the Official Secrets Act (Chapter 153) in relation to safeguarding official information;				

2. *To use the personal data received for the purpose/s stated above and not to disclose the information for any other purpose;*
3. *To take all appropriate technical and organisational measures to safeguard the personal data disclosed;*
4. *To retain the information for no longer than necessary for achieving such purposes, after which the information will either be returned to the Disclosing Party and/or be deleted in a secure and confidential manner; and*
5. *To comply with all relevant laws of Brunei Darussalam, where applicable.*

Tandatangan oleh Pihak Penerima

Signed by Receiving Party

Nama Pegawai Perlindungan Data <i>Name of Data Protection Officer</i>	
Kad Pengenalan: <i>NRIC:</i>	
Tandatangan Pegawai Perlindungan Data: <i>Signature of Data Protection Officer:</i>	
Tarikh: <i>Date:</i>	
Disahkan oleh: Nama Ketua Agensi. * <i>Verified by:</i> <i>Name of Head of Agency.*</i>	
Jawatan yang mengesahkan: <i>Designation of verifier:</i>	
Kad Pengenalan: <i>NRIC:</i>	
Tandatangan yang mengesahkan: <i>Signature of verifier:</i>	
Tarikh: <i>Date:</i>	

* Sekiranya Ketua Agensi mewakilkan kepada pegawai yang diberi kuasa secara bertulis, salinan perwakilan tersebut mesti dilampirkan pada Borang Permohonan Perkongsian Data.

* *In the event that the Head of Agency delegates this authority to an authorised officer in writing, a copy of that delegation must be attached to the Data Sharing Request Form.*

BAHAGIAN B – Untuk diisikan oleh Pihak Pendedahan <i>PART B – To be completed by Disclosing Party</i>	
Data peribadi diminta untuk dikongsi dengan Pihak Penerima? <i>Personal data requested to be shared with Receiving Party?</i>	☐ Ya (<i>Yes</i>) ☐ Tidak. Sila nyatakan sebab: (<i>No. Please specify reasons:</i>)
Ditandatangani oleh Pihak Pendedahan <i>Signed by Disclosing Party</i>	
Nama Pegawai Perlindungan Data: <i>Name of Data Protection Officer:</i>	
Kad Pengenalan: <i>NRIC:</i>	
Tandatangan Pegawai Perlindungan Data: <i>Signature of Data Protection Officer:</i>	
Tarikh: <i>Date:</i>	
Disahkan oleh: Nama Ketua Agensi atau Ketua Organisasi. * <i>Verified by:</i> <i>Name of Head of Agency or Head of Organisation.*</i>	
Jawatan yang mensahkan: <i>Designation of verifier:</i>	
Kad Pengenalan: <i>NRIC:</i>	
Tandatangan yang mensahkan: <i>Signature of verifier:</i>	
Tarikh: <i>Date:</i>	

* Sekiranya Ketua Agensi mewakilkan kepada pegawai yang diberi kuasa secara bertulis, salinan perwakilan tersebut mesti dilampirkan pada Borang Permohonan Perkongsian Data.

* In the event that the Head of Agency or Head of Organisation delegates this authority to an authorised officer in writing, a copy of that delegation must be attached to the Data Sharing Request Form.

[MUKA SURAT SELEBIHNYA ADALAH SENGHAJA DIKOSONGKAN]
[THE REMAINDER OF THIS PAGE IS LEFT INTENTIONALLY BLANK]

JADUAL B | CONTOH KLAUSA KONTRAK
SCHEDULE B | SAMPLE CONTRACTUAL CLAUSES

CONTOH KLAUSA SAMPLE CLAUSES	NOTA PENERANGAN EXPLANATORY NOTES
1. DEFINISI DEFINITIONS Dalam Perjanjian ini, melainkan jika konteks menghendaki sebaliknya, terma-terma berkenaan untuk memberi makna seperti berikut: <i>In this Agreement, unless the context otherwise requires, the following terms shall have the meanings assigned to them below:</i> (a) “Mekanisme Perkongsian yang dipersetujui” bermaksud mekanisme teknikal dan bukan teknikal yang digariskan dalam Lampiran A sebagai panduan yang mana perkongsian data peribadi antara pihak-pihak berkenaan hendaklah dikongsikan bersama; <i>“Agreed Sharing Mechanisms” means the technical and non-technical mechanisms outlined in Annex A being the means by which the Parties shall transmit shared personal data between each other;</i> (b) “Pihak Penerima” bermaksud [nama Pihak Penerima]; <i>Receiving Party” means [name of Receiving Party];</i> (c) “Pihak Pendedahan” bermaksud [nama Pihak Pendedahan]; <i>“Disclosing Party” means [name of Disclosing Party];</i> (d) “Data Peribadi” bermaksud data, sama ada benar atau tidak, mengenai individu yang boleh dikenal pasti: <i>“Personal Data” means data, whether true or not, about an individual who can be identified:</i> (i) daripada data tersebut sahaja; atau <i>from that data alone; or</i> (ii) daripada data tersebut dan maklumat lain yang Pihak Pendedahan mempunyai atau mungkin mempunyai akses.	Klausa 1 menyediakan istilah definisi yang digunakan. Jika Perjanjian sudah mempunyai klausa yang menetapkan istilah definisi (contohnya, "Klausa Tafsiran"), mungkin ianya lebih sesuai untuk memasukkan definisi dalam Klausa Tafsiran tersebut. <i>Clause 1 provides definitions of terms used. If the Agreement already has a clause that sets out the definitions of terms (for example, an “Interpretation Clause”), it may be more appropriate to include the definitions in the Interpretations Clause.</i> Terma yang telah ditetapkan boleh digantikan dengan terma yang digunakan dalam Perjanjian yang lain (jika berkenaan). Dalam masa yang sama, klausa ini dan klausa berikutnya boleh disusun semula mengikut keperluan. <i>Defined terms may be replaced with terms used in the rest of the Agreement (where applicable). Similarly, this clause and the following clauses may be renumbered as required.</i> Mekanisme Perkongsian khusus yang dipersetujui hendaklah disenaraikan di bawah Lampiran yang berasingan, sebagai contoh: Lampiran A, dan hendaklah termasuk mekanisme yang bersifat teknikal dan bukan teknikal. <i>The specific Agreed Sharing Mechanisms are to be listed out under a separate Annex, e.g. Annex A, and shall include mechanisms that are technical and non-technical in nature.</i>

<i>from that data and other information which the Disclosing Party has or is likely to have access.</i>	
2. PENGENDALIAN DAN PERLINDUNGAN DATA PERIBADI (HANDLING AND PROTECTION OF PERSONAL DATA) 2.1. <u>Pemprosesan, Penggunaan dan Pendedahan</u> <u><i>Processing, Use and Disclosure</i></u> 2.1.1. Kedua-dua Pihak hanya dibenarkan memproses, menggunakan atau mendedahkan Data Peribadi: <i>Both Parties shall only process, use or disclose Personal Data:</i> (a) hanya bagi tujuan berikut: <i>strictly for the following purposes:</i> (i) [Tujuan 1]; <i>[Purpose 1];</i> (ii) [Tujuan 2]; <i>[Purpose 2];</i> (iii) [DII]; <i>[Etc.];</i> (b) dengan kebenaran secara bertulis individu berkenaan terlebih dahulu; <i>with the individual's prior written consent;</i> (c) jika pendedahan itu diperlukan untuk mematuhi kewajipan undang-undang di bawah mana-mana undang-undang yang bertulis; <i>when the disclosure is necessary to comply with a legal obligation under any written law;</i> (d) jika pendedahan diperlukan dalam keadaan yang melibatkan keselamatan negara; <i>when disclosure is necessary in the event of a national security;</i> (e) jika pendedahan diperlukan bagi melaksanakan tugas demi kepentingan awam dalam bidang kesihatan awam; <i>when disclosure is necessary to perform a task in the public interest in the area of public health;</i> (f) jika pendedahan diperlukan bagi sebarang penyiasatan atau prosiding dan untuk mengekalkan keamanan dan ketenteraman awam di dalam Negara Brunei Darussalam; <i>when disclosure is necessary for any investigation or proceedings and to maintain peace and public order within Brunei Darussalam;</i>	Klausa 2.1 di bawah Klausa Contoh memastikan bahawa Pihak-pihak berkenaan memproses, menggunakan atau mengongsikan Data Peribadi hanya di bawah keadaan tertentu yang dibenarkan sahaja. <i>Clause 2.1 of the Sample Clauses ensures that the Parties process, use or share Personal Data only under certain permitted circumstances.</i> Jika boleh, klausa 2.1(a) hendaklah merujuk kepada tujuan khusus yang memerlukan pemprosesan, penggunaan atau pendedahan data peribadi. <i>Where possible, clause 2.1(a) should refer to the specific purposes that require the processing, use or disclosure of personal data.</i> Apabila Pihak berkenaan diperlukan untuk memproses, menggunakan atau mendedahkan Data Peribadi menurut undang-undang atau atas perintah mahkamah, Klausa 2.1.2. di bawah Klausa Contoh menghendaki Pihak berkenaan untuk memaklumkan Pihak lain yang berkenaan secara lazimnya secepat mungkin sebelum mematuhi undang-undang atau perintah mahkamah tersebut. <i>Where a Party has to process, use or disclose Personal Data in accordance with a law or an order of court, Clause 2.1.2. of the Sample Clauses requires that the Party notifies the other Party as soon as practicable before complying with such law or order of court.</i>

(g) jika pendedahan diperlukan untuk melaksanakan tugas demi kepentingan keselamatan awam; <i>when disclosure is necessary to perform a task in the interest of public safety;</i> (h) jika pendedahan diperlukan bagi melaksanakan sesuatu tugas demi kepentingan awam dan tugas itu mempunyai asas yang jelas dalam undang-undang atau dalam menjalankan kuasa secara rasmi; <i>when disclosure is necessary to perform a task in the public interest and the task has a clear basis in law or in the exercise of an official authority;</i> (i) jika pendedahan diperlukan bagi penyelidikan dan penggubalan dasar; <i>when disclosure is necessary for research and policy formulation;</i> (j) jika pendedahan diperlukan untuk melindungi nyawa seseorang; <i>when disclosure is necessary to protect someone's life;</i> (k) Jika Pihak Penerima secara khusus diberi kebenaran oleh Pihak Pendedahan untuk mengongsikan data peribadi dengan pihak lain yang berkenaan tanpa persetujuan Pihak Pendedahan; <i>where the Receiving Party is explicitly permitted by the Disclosing Party to share personal data with other parties without the consent of the Disclosing Party;</i> (l) Jika pendedahan itu mematuhi garis panduan yang berkaitan yang dikeluarkan oleh Kerajaan; atau <i>when the disclosure is in compliance with a related government issued guideline; or</i> (m) apabila dikehendaki oleh undang-undang atau atas perintah mahkamah. <i>when required by law or an order of court.</i> 2.1.2. Jika data peribadi tersebut diperlukan untuk didedahkan menurut 2.1.1.(m) di atas, Pihak yang dikehendaki untuk mendedahkan data peribadi tersebut melalui perintah mahkamah hendaklah memaklumkan Pihak lain yang berkenaan secepat mungkin sebelum undang-undang atau perintah mahkamah tersebut dilaksanakan. <i>If the personal data is required to be disclosed pursuant to 2.1.1.(m) above, the Party required to disclose such</i>	
---	--

<i>personal data by an order of court shall notify the other Party as soon as practicable before complying with such law or order of court.</i> 2.1.3. Bagi tujuan Perjanjian ini, Pihak Yang Mendedahkan hendaklah mengongsikan data peribadi yang dimilikinya kepada Pihak Penerima melalui Mekanisme Perkongsian yang Dipersetujui di bawah Lampiran A, dan Pihak Penerima hanya akan menerima data peribadi yang dikongsikan melalui Mekanisme Perkongsian yang Dipersetujui. <i>For the purposes of this Agreement, the Disclosing Party shall share the personal data in its possession to the Receiving Party solely via the Agreed Sharing Mechanisms under Annex A, and the Receiving Party shall only receive the personal data shared via the Agreed Sharing Mechanisms.</i>	
2.2. Pemindahan data peribadi ke luar negara selain dari Negara Brunei Darussalam. <u><i>Transfer of personal data outside Brunei Darussalam.</i></u> 2.2.1. Pihak Penerima tidak boleh memindahkan Data Peribadi ke luar negara selain dari Negara Brunei Darussalam tanpa kebenaran bertulis daripada Pihak Yang Mendedahkan terlebih dahulu. <i>The Receiving Party shall not transfer Personal Data to a place outside Brunei without the Disclosing Party's prior written consent.</i> 2.2.2. Sekiranya Pihak Yang Mendedahkan memberikan persetujuan, Pihak Penerima hendaklah memastikan bahawa Data Peribadi yang dipindahkan ke luar negara selain dari Negara Brunei Darussalam tersebut akan dilindungi mengikut piawaian yang setanding dengan piawaian di bawah undang-undang yang berkaitan di Negara Brunei Darussalam. <i>In the event that a Disclosing Party provides consent, the Receiving Party shall undertake that the Personal Data transferred outside Brunei Darussalam will be protected at a standard that is comparable to that under the relevant laws of Brunei Darussalam.</i>	Klausa 2.2 memastikan bahawa Pihak Penerima tidak memindahkan Data Peribadi ke luar negara selain dari Negara Brunei Darussalam tanpa kebenaran Pihak Yang Mendedahkan. Jika Perjanjian memerlukan pemindahan Data Peribadi ke luar negara selain dari Negara Brunei Darussalam semasa ianya dalam proses pemprosesan, klausa ini boleh dipinda untuk membenarkan secara khusus pemindahan tersebut. <i>Clause 2.2 ensures that the Receiving Party does not transfer Personal Data outside of Brunei Darussalam without the Disclosing Party's consent. If the Agreement requires the transfer of Personal Data outside Brunei Darussalam in the course of processing, this clause may be amended to specifically allow for such transfers.</i> Jika persetujuan diberikan untuk pemindahan Data Peribadi ke luar negara, Pihak Yang Mendedahkan mungkin ingin memerlukan Pihak Penerima untuk memberikan pengesahan secara bertulis bahawa Data Peribadi yang dipindahkan di luar selain dari Negara Brunei Darussalam akan dilindungi di bawah piawaian yang setanding dengan undang-undang yang berkaitan di Negara Brunei Darussalam.

	<i>If consent is provided for the transfer of Personal Data overseas, the Disclosing Party may wish to require that the Receiving Party provides a written undertaking that the Personal Data transferred outside Brunei Darussalam will be protected at a standard that is comparable to that under the relevant laws of Brunei Darussalam.</i>
2.3. Langkah-langkah Keselamatan <u><i>Security Measures</i></u> 2.3.1. Kedua-dua Pihak hendaklah melindungi Data Peribadi di bawah kawalan atau simpanan masing-masing dengan membuat langkah-langkah keselamatan yang munasabah (termasuk, jika sesuai, langkah-langkah fizikal, pentadbiran, prosedur dan teknologi maklumat dan komunikasi) untuk menghalang akses, pengumpulan, penggunaan, pendedahan, penyalinan, pengubahsuaian tanpa kebenaran atau secara tidak sengaja, pelupusan atau pemusnahan Data Peribadi, atau risiko lain yang serupa. <i>Both Parties shall protect Personal Data in their control or possession by making reasonable security arrangements (including, where appropriate, physical, administrative, procedural and information and communications technology measures) to prevent unauthorised or accidental access, collection, use, disclosure, copying, modification, disposal or destruction of Personal Data, or other similar risks.</i> 2.3.2. Setiap Pihak hendaklah memastikan bahawa: <i>Each Party warrants that:</i> (a) sistem atau mana-mana saluran yang digunakan untuk menghantar atau memindah data peribadi kepada Pihak lain yang berkenaan adalah selamat; <i>the system or any other channel through which the personal data is transmitted to the other Party is secure;</i> (b) ia mempunyai sistem sandaran bagi membolehkan kesinambungan perkhidmatan dan penyambungan semula aktiviti dalam keadaan kecemasan; <i>it has a back-up system to enable the continuity of the service and the resumption of activities in an emergency;</i>	Klausa ini memerlukan kedua-dua Pihak untuk melindungi Data Peribadi dalam kawalan atau simpanan masing-masing dengan membuat langkah-langkah keselamatan yang munasabah untuk menghalang akses, pengumpulan, penggunaan, pendedahan, penyalinan, pengubahsuaian, pelupusan atau pemusnahan Data Peribadi yang tidak dibenarkan atau tidak sengaja, atau risiko lain yang serupa. <i>This clause requires both Parties to protect Personal Data in their control or possession by making reasonable security arrangements to prevent unauthorised or accidental access, collection, use, disclosure, copying, modification, disposal or destruction of Personal Data, or other similar risks.</i> Ia juga membenarkan pihak-pihak berkenaan untuk menetapkan prosedur keselamatan khusus yang perlu dipatuhi. Prosedur keselamatan boleh dinyatakan dalam klausa itu sendiri atau dalam Lampiran berasingan, dan klausa itu perlu dipinda sewajarnya dengan rujukan yang betul. <i>It also allows the Parties to set out the specific security procedures that need to be adhered to. The security procedures may be stated in the clause itself or in a separate Annex, and the clause should be amended accordingly with the correct reference.</i>

(c) ia mengekalkan infrastrukturnya (perkakasan, perisian, rangkaian) yang diperlukan untuk pemprosesan dan penghantaran data peribadi, tidak kira sama ada infrastruktur ini dihoskan oleh Pemilik atau oleh pihak ketiga; dan <i>it maintains its infrastructure (hardware, software, network) required for the processing and transmission of personal data, regardless of whether this infrastructure is hosted by the Party or by a third party; and</i> (d) sekiranya berlakunya gangguan yang tidak dirancang, Pihak berkenaan untuk melaksanakan rancangan kecemasan. <i>in the event of an unplanned interruption, the Party concerned implements an emergency plan.</i> 2.3.3. Tujuan Perjanjian ini, "aturan keselamatan yang munasabah" termasuk pengaturan yang ditetapkan [di bawah / dalam Lampiran B yang dilampirkan]: <i>For the purposes of this Agreement, "reasonable security arrangements" include arrangements set out [below / in the attached Annex B]:</i> [Sila nyatakan dan senaraikan langkah-langkah keselamatan khusus yang diperlukan untuk Pihak Pendedahan sertakan di dalam Jadual yang berasingan.] <i>[State the specific security measures that you want the Disclosing Party to adopt or insert a separate Schedule listing the required measures.]</i>	
2.3.2 Kedua-dua Pihak hendaklah membenarkan hanya kakitangan yang diberi kuasa seperti yang dinyatakan dalam Lampiran C untuk mengakses Data Peribadi atas dasar keperluan untuk mengetahui. <i>Both Parties shall only permit the authorised personnel set out in Annex C to access Personal Data on a need to know basis.</i>	Klausa ini memerlukan kedua-dua Pihak untuk membenarkan hanya kakitangan yang diberi kuasa yang disenaraikan dalam Jadual yang dilampirkan pada Perjanjian untuk mengakses Data Peribadi atas dasar keperluan untuk mengetahui. Klausa ini adalah secara opsional dan boleh digunakan jika pihak-pihak berkenaan memerlukan kawalan yang lebih ketat mengambilkira data peribadi yang terlibat adalah sensitif. <i>This clause requires that both Parties permit only the authorised personnel listed in a Schedule attached to the Agreement to access Personal Data on a need to know basis. This clause is optional and may be used where the Parties wishes to have more stringent controls</i>

	<i>because sensitive personal data is involved.</i>
2.4. <u>Akses kepada Data Peribadi.</u> <u>Access to Personal Data.</u> Pihak Yang Mendedahkan dibolehkan untuk mengongsikan Data Peribadi dalam simpanan dengan Pihak Penerima secepat mungkin sepertimana lazimnya dipraktikkan setelah menerima permohonan secara bertulis. <i>The Disclosing Party shall share the Personal Data in its possession with the Receiving Party as soon as practicable upon receiving the written request.</i>	Ini memerlukan Pihak Yang Mendedahkan untuk memberikan akses Data Peribadi kepada Pihak Penerima. <i>This requires the Disclosing Party to provide the Receiving Party with access to the Personal Data.</i>
2.5. <u>Ketepatan dan Pembetulan Terhadap Data Peribadi.</u> <u>Accuracy and Correction of Personal Data.</u> Jika Pihak Pendedahan memberikan Data Peribadi kepada Pihak Penerima, Pihak Pendedahan hendaklah mengambil langkah-langkah yang munasabah untuk memastikan Data Peribadi tersebut adalah tepat dan lengkap sebelum mengongsikannya kepada Pihak Penerima. Pihak Pendedahan hendaklah melaksanakan langkah-langkah yang sesuai untuk memastikan bahawa Data Peribadi dalam simpanan atau dalam kawalannya atau sebaliknya adalah tepat dan lengkap. Dalam apa jua keadaan, Pihak Yang Mendedahkan hendaklah mengambil langkah-langkah untuk membetulkan sebarang kesilapan dalam Data Peribadi, secepat mungkin seperti lazimnya dipraktikkan setelah mendapat maklumat mengenainya. <i>Where the Disclosing Party provides Personal Data to the Receiving Party, the Disclosing Party shall take reasonable steps to ensure that the Personal Data is accurate and complete before providing the same to the Receiving Party. The Disclosing Party shall put in place adequate measures to ensure that the Personal Data in its possession or control remain or is otherwise accurate and complete. In any case, the Disclosing Party shall take steps to correct any errors in the Personal Data, as soon as practicable upon notification.</i>	Klausa ini memerlukan Pihak Pendedahan untuk memastikan bahawa Data Peribadi dalam simpanan atau dalam kawalannya adalah tepat dan lengkap dan mengambil langkah-langkah berkenaan untuk membetulkan sebarang kesilapan. <i>This clause requires the Disclosing Party to ensure that the Personal Data in its possession or control is accurate and complete and to take steps to correct any errors.</i>
2.6. <u>Pengekalan Data Peribadi</u> <u>Retention of Personal Data</u> 2.6.1. Pihak Penerima tidak boleh menyimpan Data Peribadi (atau sebarang dokumen atau rekod yang mengandungi Data Peribadi, secara elektronik atau sebaliknya) untuk sebarang tempoh masa yang	Klausa ini memastikan bahawa Pihak Penerima tidak menyimpan Data Peribadi untuk sebarang tempoh masa yang melebihi tempoh lama daripada yang diperlukan di bawah Perjanjian ini. <i>This clause ensures that the Receiving Party does not retain Personal Data for</i>

melebihi tempoh lama daripada yang ianya diperlukan di bawah Perjanjian ini.

The Receiving Party shall not retain Personal Data (or any documents or records containing Personal Data, electronic or otherwise) for any period of time longer than is necessary to serve the purposes of this Agreement.

2.6.2. Peraturan yang mengawal pengekalan Data Peribadi yang dikongsikan bagi tujuan yang telah dikenalpasti di bawah Perjanjian ini, adalah sepertimana di dalam Lampiran D. (Pilihan)

The rules governing the retention on shared Personal Data for the purposes identified under this Agreement is defined under Annex D. (Optional)

2.6.3. Pihak Penerima hendaklah, atas permintaan Pihak Yang Mendedahkan:

The Receiving Party shall, upon the request of the Disclosing Party:

(a) Mengembalikan kepada Pihak Pendedahan, semua Data Peribadi; dan
return to the Disclosing Party, all Personal Data; and

(b) memadam semua Data Peribadi dalam simpanan, dan, selepas memulangkan atau memadam semua Data Peribadi, memberikan kepada Pihak Pendedahan pengesahan secara bertulis bahawa ia tidak lagi memiliki sebarang Data Peribadi. Jika berkenaan, Pihak Penerima hendaklah juga mengarahkan semua pihak ketiga yang mana Data Peribadi tersebut telah beliau kongsi bagi tujuan Perjanjian ini, untuk mengembalikan kepada Pihak Pendedahan dan untuk memadamkan Data Peribadi tersebut.

delete all Personal Data in its possession, and, after returning or deleting all Personal Data, provide the Disclosing Party with written confirmation that it no longer possesses any Personal Data. Where applicable, the Receiving Party shall also instruct all third parties to whom it has disclosed Personal Data for the purposes of this Agreement to return to the Disclosing Party and delete such Personal Data.

any period of time longer than is necessary to serve the purposes of the Agreement.

Pihak-pihak berkenaan untuk menyenaraikan dalam lampiran berasingan, (jika ada) mengenai peraturan dan prosedur, yang mengawal pengekalan data peribadi yang dikongsikan. Jika ini tidak diperlukan, klausa ini boleh dipadamkan dan baki perjanjian ini untuk dinomborkan semula.

The Parties shall outline, in a separate Annex, the rules and procedures, if any, that govern the retention of the shared personal data. If this is not necessary, this clause can be deleted and the rest of the agreement renumbered.

Selanjutnya, perkara ini memerlukan Pihak Penerima untuk memulangkan atau memadamkan sebarang Data Peribadi dengan serta-merta atas permintaan Pihak yang Mendedahkan dan memberikan pengesahan secara bertulis kepada Pihak Pendedahan bahawa mereka tidak lagi memiliki sebarang Data Peribadi.

This further requires the Receiving Party to return or delete any Personal Data immediately upon the Disclosing Party's request and provide the Disclosing Party with written confirmation that it no longer possesses any Personal Data.

2.6.4. Data peribadi mestilah dipadamkan atau dimusnahkan menggunakan salah satu kaedah yang dijamin selamat, seperti berikut: <i>Personal data must be deleted or destroyed using one of the following secure methods:</i> (a) Dokumen yang disimpan secara elektronik hendaklah dipadamkan dengan utiliti pemadaman dengan selamat bagi memastikan maklumat itu tidak boleh diambil semula. Utiliti pemadaman standard yang hanya mengeluarkan <i>file pointer</i> tidak boleh digunakan; <i>Documents retained electronically should be deleted with a secure deletion utility that ensures that the information cannot be retrieved. Standard deletion utilities that only remove the file pointer should not be used;</i> (b) Data peribadi pada cakera, media mudah alih dan apa-apa peralatan yang serupa mesti dipadamkan dengan selamat sebelum sebarang pelupusan atau peralatan tersebut dipindahmilik; <i>Personal data on hard drives, removable media and any similar items must be securely erased before any disposal or reassignment of the equipment;</i> (c) Jika data peribadi tidak boleh dipadamkan daripada peralatan, ianya mesti dimusnahkan secara fizikal oleh pegawai yang diberikuasa, syarikat pakar dalam penghapusan, dan sijil penghapusan mestilah diperolehi; dan <i>Where personal data cannot be erased from equipment, it must be physically destroyed by an authorised, specialist destruction company, and certificates of destruction must be obtained; and</i> (d) Salinan kertas mesti dimusnahkan menggunakan mesin <i>shredders</i>. <i>Paper copies must be destroyed using shredders.</i>	
2.7. <u>Pemberitahuan Pelanggaran</u> <u><i>Breach Notification</i></u> 2.7.1. Setiap Pihak hendaklah memantau dan segera melaporkan sebarang pelanggaran atau insiden	Klausa ini mewajibkan Pihak Penerima untuk memaklumkan kepada Pihak Yang Mendedahkan jika berlaku sebarang pelanggaran data peribadi. <i>This clause makes it mandatory for the Receiving Party to notify the Disclosing</i>

keselamatan yang berkaitan dengan mana-mana data peribadi yang dikongsi. <i>Each Party shall monitor and immediately report any breach or security incident related to any shared personal data.</i> 2.7.2 Setiap Pihak hendaklah memaklumkan Pihak lain yang berkenaan tentang pelanggaran data peribadi secepat mungkin secara lazimnya dipraktikkan, tetapi dalam apa jua keadaan, tidak lewat daripada tiga (3) hari selepas hari Pihak berkenaan mengetahui tentang pelanggaran data peribadi tersebut. <i>Each Party shall notify the other Party of a personal data breach as soon as is practicable, but in any case no later than three (3) days after the day the Party becomes aware of a personal data breach.</i> 2.7.3. Bagi tujuan klausa ini, pelanggaran data peribadi termasuk: <i>For the purposes of this clause, a personal data breach includes:</i> (a) akses tanpa kebenaran, pengumpulan, penggunaan, pendedahan, penyalinan, pengubahsuaian atau pelupusan data peribadi; atau <i>the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or</i> (b) kehilangan mana-mana media atau peranti di mana data peribadi disimpan dalam keadaan di mana akses tanpa kebenaran, pengumpulan, penggunaan, pendedahan, penyalinan, pengubahsuaian atau pelupusan terhadap data peribadi itu berkemungkinan berlaku. <i>the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.</i>	<i>Party in the event of any breach of personal data.</i>
3. GANTI RUGI INDEMNITIES Salah satu Pihak perlu membayar ganti rugi bagi Pihak lain yang berkenaan dan pegawai, kakitangan dan ejen mereka, terhadap semua tindakan, tuntutan, kerugian, ganti rugi, hukuman berkanun, perbelanjaan dan kos (termasuk kos undang-undang atas dasar ganti rugi), berkenaan dengan:	Klausa ini menghendaki salah satu Pihak untuk menanggung kerugian pihak yang lain dan pegawai, kakitangan dan ejennya terhadap sebarang pelanggaran di bawah Perjanjian atau sebarang tindakan, peninggalan atau kecuaian satu Pihak yang menyebabkan atau mengakibatkan Pihak lain yang berkenaan untuk melanggar undang-undang perlindungan

<i>Either Party shall indemnify the other Party and their officers, employees and agents, against all actions, claims, demands, losses, damages, statutory penalties, expenses and cost (including legal costs on an indemnity basis), in respect of:</i> (a) pelanggaran bagi satu Pihak terhadap mana-mana klausa di bawah Perjanjian ini; atau <i>one Party's breach of any of the clauses under this Agreement; or</i> (b) sebarang tindakan, peninggalan atau kecuaihan satu Pihak yang menyebabkan atau mengakibatkan Pihak lain yang berkenaan untuk melanggar undang-undang berkaitan perlindungan data peribadi, jika berkenaan. <i>any act, omission or negligence of the one Party that causes or results in the other Party being in breach of the relevant personal data protection law, if applicable.</i>	data yang berkaitan dalam Negara Brunei Darussalam, jika berkenaan. <i>This clause requires that either Party indemnifies the other and its officers, employees and agents for any breach under the Agreement or any act, omission or negligence of one Party that causes or results in the other Party being in breach of the relevant data protection law in Brunei Darussalam, if applicable.</i>
4. PENYELESAIAN PERTIKAIAN <i>DISPUTE RESOLUTION</i> 4.1. Jika sebarang permasalahan timbul atau yang berkaitan dengan Perjanjian ini, Pihak-Pihak berkenaan hendaklah berusaha untuk menyelesaikan permasalahan tersebut secara baik dengan tujuan untuk menyelesaikan permasalahan tersebut secara damai. <i>If any dispute arises under or in connection with this Agreement, the concerned Parties shall attempt to resolve such disputes amicably with the aim of resolving the dispute.</i> 4.2. Sebarang permasalahan yang tidak dapat diselesaikan dalam tempoh tiga puluh (30) hari dari tarikh pertikaian bermula, ianya hendaklah dirujuk bagi penyelesaian melalui timbangtara mengikut peruntukan di bawah Perintah Timbangtara, 2009 atau Perintah Timbangtara Antarabangsa, 2009. <i>Any dispute which cannot be resolved within thirty (30) days from the date when such dispute arose, shall be referred for resolution by arbitration in accordance with the provisions of the Arbitration Order, 2009 or the International Arbitration Order, 2009.</i> 4.3. Bahagian II Perintah Timbangtara Antarabangsa, 2009, dan Undang-undang Model yang dirujuk kepada Kontrak ini adalah dengan ini dikecualikan.	Klausa tersebut menggariskan kaedah yang dipersetujui bersama oleh pihak-pihak berkenaan bagi menyelesaikan permasalahan. Kaedah penyelesaian bagi kontrak Kerajaan adalah dengan cara timbangtara. Kecuali jika ianya dipersetujui sebaliknya, tempat bagi timbangtara tersebut untuk diadakan di Negara Brunei Darussalam. <i>The clause outlines the Parties' agreed method of resolving disputes. The method of resolving disputes for Government contracts is by way of arbitration. Unless agreed otherwise, the seat and place for the arbitration shall be Brunei Darussalam.</i> Tertakluk jika pihak lain yang berkenaan, sama ada ianya melibatkan pihak tempatan atau asing, timbangtara akan ditadbir oleh Perintah Timbangtara, 2009 atau Perintah Timbangtara Antarabangsa, 2009. Bahagian II Perintah Timbang Tara Antarabangsa, 2009 adalah dikecualikan bagi pihak tempatan. <i>Depending on whether the other Party is a local or foreign Party, the arbitration will either be governed by the Arbitration Order, 2009 or the International Arbitration Order, 2009. Part II of the</i>

<i>The application of Part II of the International Arbitration Order, 2009, and the Model Law referred thereto, to this Contract is hereby excluded.</i>	<i>International Arbitration Order, 2009 is excluded for local Parties.</i>
--	---

5. SYARAT TAMBAHAN UNTUK DISERTAKAN
ADDITIONAL TERMS TO INCLUDE

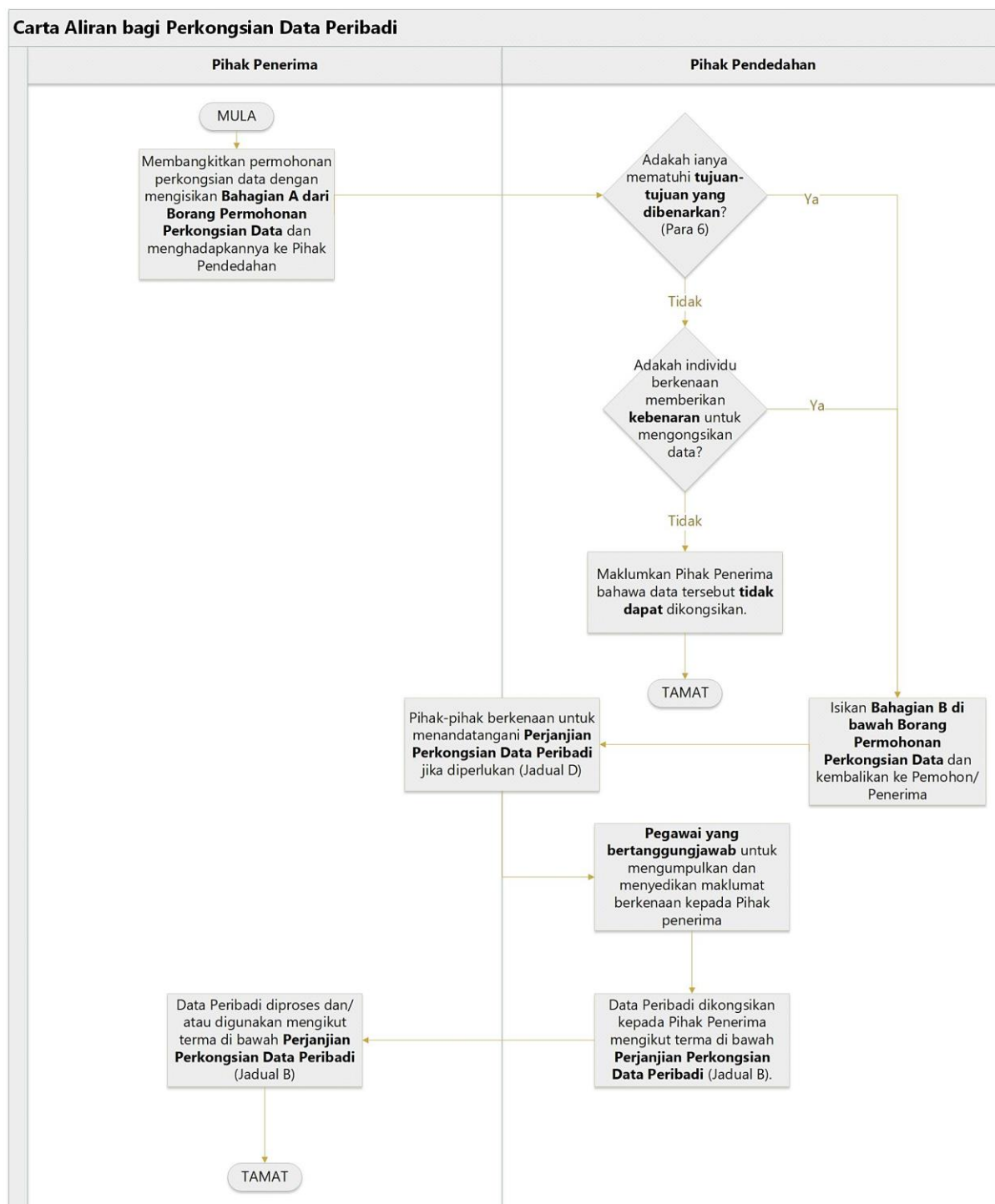
Pihak-pihak yang berkaitan dengan Perjanjian Perkongsian Data Peribadi hendaklah juga mempertimbangkan perkara-perkara berikut:

The parties to a Personal Data Sharing Agreement should also consider the following:

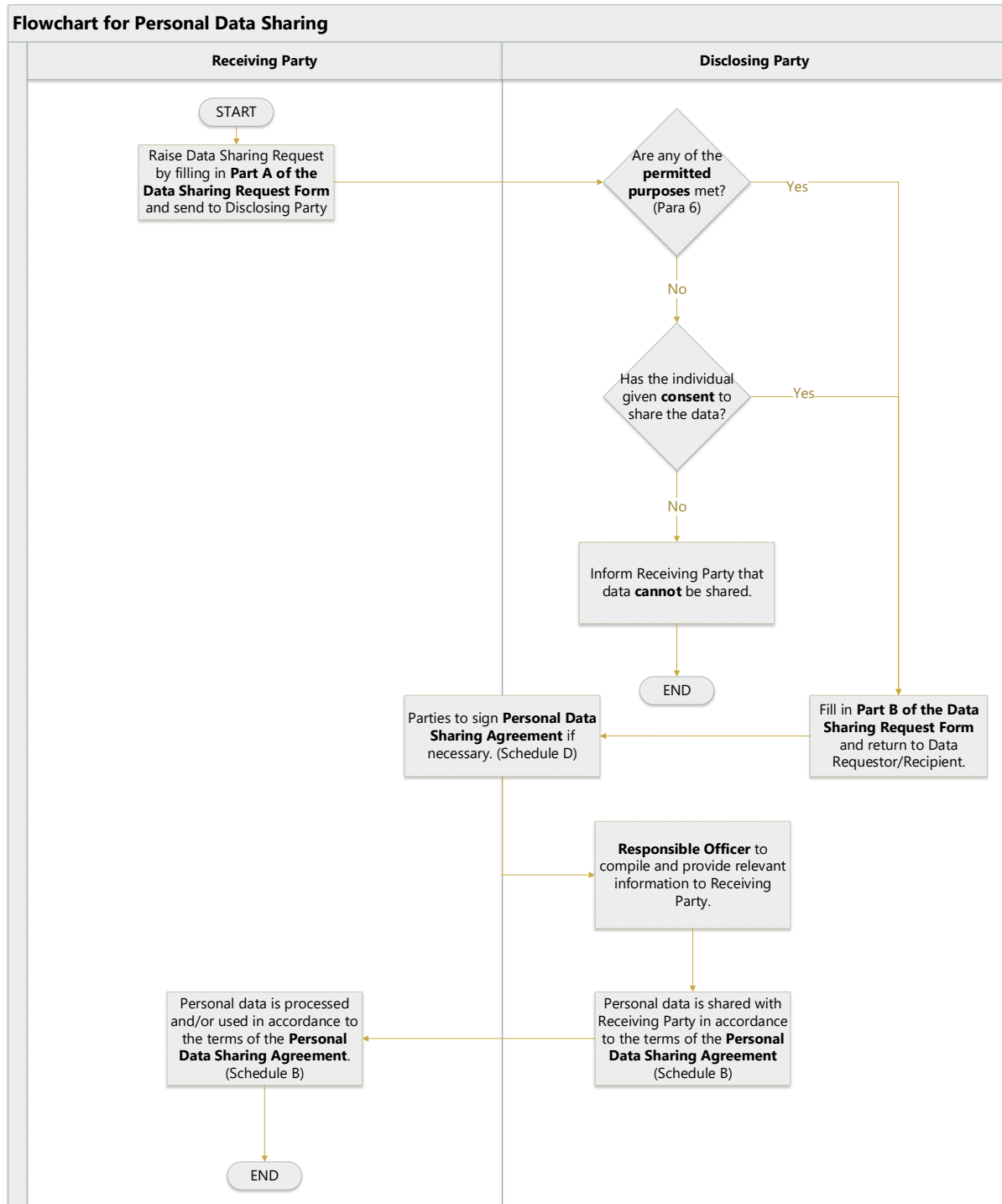
- (a) tarikh mula dan tempoh perjanjian;
the start date and duration of the agreement;
- (b) dalam keadaan apakah perjanjian itu akan berakhir, termasuk tamat tempoh dan penamatan awal;
in what circumstances the agreement comes to an end, including expiry and early termination;
- (c) proses bagi sebarang semakan, pengubahsuaian atau pindaan kepada perjanjian yang sedia ada;
the process for any revisions, modifications or amendments to the existing agreement;
- (d) pihak yang bertanggungjawab untuk mengemaskini atau membuat pembetulan terhadap data peribadi;
who is responsible for updating or making error corrections to personal data;
- (e) Perundangan dan bidang kuasa yang mengawal; dan
the governing law and jurisdiction; and
- (f) mana-mana peruntukan lain yang difikirkan perlu.
any other provision(s) deemed necessary by the Parties.

[MUKA SURAT SELEBIHNYA ADALAH SENGHAJA DIKOSONGKAN]
 [THE REMAINDER OF THIS PAGE IS LEFT INTENTIONALLY BLANK]

JADUAL C | CARTA ALIRAN BAGI PERKONGSIAN DATA PERIBADI



SCHEDULE C | FLOWCHART FOR SHARING OF PERSONAL DATA



JADUAL D | SENARAI SEMAK KEPERLUAN
SCHEDULE D | CHECKLIST OF REQUIREMENTS

	SENARIO 1 Antara agensi Kerajaan <i>SCENARIO 1</i> <i>Within and between Government agencies</i>	SENARIO 2 Antara agensi Kerajaan dan organisasi sektor swasta <i>SCENARIO 2</i> <i>Between Government agencies and private sector organisations</i>	SENARIO 3 Antara agensi Kerajaan dan pemproses data <i>SCENARIO 3</i> <i>Between Government agencies and data processors</i>
Borang Perkongsian Data Peribadi (Jadual A) Data Sharing Request Form (Schedule A)	Perlu <i>Necessary</i>	Perlu <i>Necessary</i>	Perlu <i>Necessary</i>
Perjanjian Perkongsian Data Peribadi (Jadual B) <i>Personal Data Sharing Agreement (Schedule B)</i>	Tidak Perlu <i>Not necessary</i>	Perlu <i>Necessary</i>	Perlu <i>Necessary</i>

*Jika perjanjian sudah wujud, adalah dicadangkan untuk meminta pengubahsuaian kepada perjanjian untuk memasukkan peruntukan berkaitan yang berkaitan dengan data peribadi.

**If an agreement already exists, it is suggested to request for a modification to the agreement to include the relevant provisions relating to personal data.*

[DOKUMEN BERAKHIR]
 [END OF DOCUMENT]