DATA PROTECTION POLICY

E-GOVERNMENT NATIONAL CENTRE

Table of Contents

Document Control

Organisation	E-Government National Centre
Title	Data Protection Policy
Author	Pg Dr Adrian Pg Hj Salleh AB Rahaman
Owner	Policy and Standards
Data Classification	Restricted

Revision History

Date	Version	Revised By	Description of Revision
29/01/2012	V.1.0	Pg Dr Adrian	-
29/09/2014	V.2.1	Pg Dr Adrian	Approved version
27/08/2015	V.2.2	Raini Manyansin	Revised version

1. Introduction

1.1. Data including personal data are national assets that the Government of Brunei has a responsibility and requirement to protect.

1.2. Protecting data assets is not simply limited to covering electronic data or paper records that the Government maintains. It also addresses the people that use them, the processes they follow and the physical equipment used to access them.

1.3. This Data Protection Policy addresses all these areas to ensure that high confidentiality, quality and availability standards of information are maintained.

1.4. The following policy details the basic requirements and responsibilities for the proper management of data assets in the Government. The policy also specifies the means of data handling and transfer.

2. Definition

2.1. The following definitions apply in this policy:

2.1.1. **Administrator —** refers to the E-Government National Centre;

2.1.2. **Advisory Committee —** refers to a committee with members appointed by the Authority to provide strategic advice to the Prime Minister and the Authority with regards to the performance of any of the required functions under this policy;

2.1.3. **Agency** — Any Government Ministry or Department including Educational Institutions and Statutory Body;

2.1.4. **Authority —** refers to the Minister at the Prime Minister's Office;

2.1.5. **Chairman** — refers to the Permanent Secretary or Deputy Permanent Secretary at the Prime Minister's Office;

2.1.6. **Committee Secretary** — refers to Director of E-Government National Centre as the Head of the Administrator;

2.1.7. **Computer systems** — Desktop or Personal computers, notebooks, network computers, pocket PCs, mobile devices and personal digital assistants that are used to store, process or access data;

2.1.8. **Collection** — the act of gathering, acquiring, or obtaining Personal Data from any source, including third parties and whether directly or indirectly by any means;

2.1.9. **Consent** — voluntary agreement by the Individual with the processing done or proposed on his/her data. Consent by the Individual can be either express or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the party seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the Individual;

2.1.10. **Control** — in relation to an agency, natural or legal person, public authority, organisation or any other body which alone or jointly with others has the power to determine the purposes and means of the processing of data, and the manner in which the data is processed;

2.1.11. **Data** — all data including personal data in electronic or manual form;

2.1.12. **Disclosure** — making data available to others outside the Agencies;

2.1.13. **Employee** - includes all paid and unpaid employees of a Government Agency including those working under an unpaid volunteer work relationship;

2.1.14. **Government** — The Government of His Majesty the Sultan and Yang Di-Pertuan of Brunei Darussalam;

2.1.15. **Government resources** — All Government data, hardware or software implemented for official use by the Government and its authorised personnel;

2.1.16. **Head of Agency** — refers to the Permanent Secretary of Government ministry, Head of Government Department, Head of Educational Institutions and Chief Executive Officer (CEO) of Statutory Body;

2.1.17. **Individual** — refers to a natural person to whom the data relates to, whether living or deceased;

2.1.18. **Investigation** — means an investigation relating to:

(a) a breach of this policy;

(b) a contravention of any written law or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or

(c) a circumstance or conduct that may result in a remedy or relief being available under any law;

2.1.19. **National Interest** — includes national security, defence, public security, the conduct of international affairs and the financial and economic interest of Brunei Darussalam;

2.1.20. **Official** — This means any business related to the Government and/or agency;

2.1.21. **Organisation** — includes any individual, company, association or body of persons, corporate or unincorporated;

2.1.22. **Personal Data** — means data, whether true or not, about an individual who can be identified
(a) from the data; or
(b) from the data and other information which is in the possession of, or is likely to come into the possession of, the Agencies

2.1.23. **Processing —** 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, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

2.1.24. **Third Party** — any party other than the Individual, the Agencies or any person who processes data on behalf of the Individual;

2.1.25. **Trans-border Data Transfers —** the movement of data across national and international borders; and

2.1.26. **Use** — refers to the treatment and handling of data.

3. Policy Statement

3.1. To establish and define a policy for the proper management of data assets including personal data existing in the Government of Brunei

3.2. The purpose of this policy is to govern the collection, use and disclosure of data including personal data by the Government in a manner that recognises both the right of individuals to protect their personal data and the need of the Government to collect, use or disclose data for purposes that a reasonable person would consider appropriate in the circumstances.

3.3. This policy ensures that high standards of confidentiality, integrity and availability of data will be maintained at all times.

3.4. This policy sets out the minimum requirements for the protection of data whether in electronic or manual form.

4. Policy Scope and Exemptions

4.1. This policy sets out the minimum requirements for the protection of Data, whether in electronic or manual form, by all Government Ministries,

Departments, Educational Institutions, and Statutory Boards. This policy is subject to any existing applicable legislation.

4.2. Agencies are allowed develop internal policies, guidelines and procedures to meet their specific circumstances, as long as the requirements specified in this policy are met, provided that the further extension to this policy does not contravene with any other Government policy or any national legislation.

4.3. The following data processing activities are EXEMPTED from the requirements of this policy:

4.3.1. processing required by any law or by the order of a court;

4.3.2. processing by any agency directly relating to a prospective, current or former employment relationship between the agency and the Individual;

4.3.3. processing of data relating to any Individual or organisation that is not held or stored electronically by the Agencies;

4.3.4. Data that is available to the public;

4.3.5. any processing which is necessary for:
(a) national and public security;
(b) national defence or internal security;
(c) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics, rules for regulated professions;
(d) national economic or financial interest, including monetary, budgetary and taxation matters;
(e) monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority; and
(f) processing for research or statistical purposes provided the results of the research or any resulting statistics involve techniques to prevent the identification of any specific Individual by any reasonably foreseeable means.

4.4. This policy applies to all data including personal data already in existence whether or not by electronic means.

4.5. This policy applies to any data which is processed or controlled by the Agencies, regardless of whether the data is processed within or outside Brunei Darussalam.

4.6. The policy applies to all individuals, whether resident in Brunei Darussalam or not, whose data is or has been processed by the Agencies.

5. Policy Authority and Administrator

5.1. The policy is under the responsible authority and accountability of the Minister at the Prime Minister's Office (as the Authority) and the compliance to this policy in the Government shall be ensured by the E-Government National Centre (as the Administrator).

5.2. The Administrator will report and provide recommendations to the Authority and Advisory Committee on all matters pertaining to this policy.

5.3. The Authority may appoint a number of Government officer(s) or employee(s) of a Statutory Body as members of the Advisory Committee, for a fixed term as decided by the Authority, to provide strategic advice and consultation to the Authority with regards to the performance of any of the required functions under this policy.

5.4. The role of the Advisory Committee is to provide strategic advice; review requests for exemptions; review and recommend changes to this policy to the Authority and when required by the Authority at any time, act on behalf of the Authority on all matters pertaining to data protection and this policy.

5.5. The members of the Advisory Committee shall comprise of a Chairman, Committee Secretary and other members of not fewer than three (3) members.

5.6. The responsibilities of the Administrator, as required by this policy, include:

5.6.1. to promote awareness of data protection in the Government;

5.6.2. to perform investigations of any occurrences of non-compliance or breach of this policy within the Government and to provide recommendations to remedy or prevent such occurrences;

5.6.3. to provide consultancy, advisory, technical, managerial or other specialist services relating to data protection;

5.6.4. to advise the Government on all matters relating to data protection;

5.6.5. to represent the Government internationally on matters relating to data protection and data privacy;

5.6.6. to conduct research and studies, and promote educational activities relating to data protection, including organising and conducting seminars, workshops and symposia relating thereto, and supporting other organisations conducting such similar activities;

5.6.7. to manage technical co-operation and exchange in the area of data protection with other organisations, including foreign data

protection offices and international inter-governmental organisations, on behalf of the Government;

5.6.8. to administer and enforce this policy;

5.6.9. to provide regular reports, relating to this policy, to the Authority and the Advisory Committee;

5.6.10. to engage in such other activities and to perform such functions as the Authority may permit or assign to the Administrator.

6. Policy Compliance

6.1. If a specific data processing practice is not authorised under this policy (those not listed in clause 4.3), but is deemed by the Agency to be necessary in the national interest, the Head of Agency shall seek the authorisation of the Authority via the Chairman of the Advisory Committee, and the Authority must authorise such data processing to exempt that practice from the requirements of this policy.

6.2. If any user is found to have breached this policy, an investigation will be carried out by the Administrator and they may be subject to Government disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist enforcement authorities in the prosecution of the offender(s).

6.3. The implementation of this policy at the Agency level will be monitored and managed by the designated Information Security Officer(s) or any other suitably nominated officer. This officer(s) will have the responsibility for carrying out scheduled and unscheduled compliance checks to ensure adherence to this policy.

6.3.1. The implementation of this policy at the Agency level will be monitored and managed by the designated officer(s) as nominated by the respective Agency. This officer(s) will have the responsibility for carrying out scheduled and unscheduled compliance checks to ensure adherence to this policy

6.4. The Agency is also advised to elect a team to support the designated officer(s) in carrying out the responsibilities in relation to this policy.

6.5. The designated officer(s) will report of any non-compliance or incidents of breach at the Agency to the Administrator at all times. If required by the Administrator, the designated officer(s) will assist in the investigation carried out by the Administrator. (Refer to clause 7.5)

6.6. After the investigation has been done, the Administrator will provide the Agency with recommendations to remedy the non-compliance or breach.

The designated officer(s) is required to implement the recommendations without delay and communicate any changes to affected users at the Agency

6.7. If any user is found to not understand the implications of this policy or how it may apply, do seek advice from the Administrator.

7. Risks of Non-compliance

7.1. This policy is aimed in its application at the processing of data, wholly or partly by electronic or manual means, or otherwise in a structured manner and carried out by the Government.

7.2. The following principles are interrelated. Agencies shall adhere to all principles as a whole.

7.3. This policy aims to mitigate the following risks:

7.3.1. Viruses, malware etc;

7.3.2. Increased risk of data loss;

7.3.3. Inappropriate access to and unacceptable use of the Government's network, software, facilities and documents;

7.3.4. Inadequate destruction of data;

7.3.5. The non-reporting of information security incidents;

7.3.6. Inconsistency in how users deal with 'secure' documents;

7.3.7. The sharing of passwords;

7.3.8. Incorrect or inappropriate classification of documents; and

7.3.9. Risk of reputation damage and further loss in public confidence

7.4. Non-compliance with this policy could have a significant effect on the efficient operation of the Government and may result in financial loss and an inability to provide necessary services to our customers.

8. Principle I – Accountability and Responsibility for Data Protection

8.1. Agencies are responsible for all data including personal data in its possession or custody. Head of Agency shall designate officer(s) who is to ensure that the Agency complies with the policy.

8.2. Where data is to be transferred to someone (other than the Individual or the Agencies, or its employees), the Agencies shall take reasonable measures to ensure that the data which is to be transferred will not be processed inconsistently with this policy.

8.3. Accountability for the Agencies compliance with the policy rests with the Head of Agency, even though other persons within the Agencies may be responsible for the operational day-to-day collection and processing of data. In addition the designated officer(s) within the Agencies may be delegated to act on behalf of the Head of Agency.

8.4. The Head of Agency has the responsibility to ensure that the Agency implements activities and provide resources in order to fully comply with this policy. These include:

8.4.1. implementing internal policies, guidelines and procedures to protect data;

8.4.2. ensuring sufficient and sustainable resources, including human and technology capacity and capability, are put in to place for the protection of data and the compliance of this policy;

8.4.3. providing training and communicating to employees and users with regards to data protection and this policy;

8.4.4. providing relevant and accessible information to explain this policy and internal policies, guidelines and procedures to the public; and

8.4.5. to designate officer(s) to monitor and manage the Agency's adherence to this policy (refer to clause 5.6).

8.5. The responsibilities of the designated officer(s), as required by this policy, include:

8.5.1. to establish and keep up-to-date internal policies, guidelines and procedures to protect data including personal data in the Agency;

8.5.2. to report of any non-compliance or incidents of breach at the Agency to the Head of Agency and the Administrator at all times;

8.5.3. to assist in any investigation carried out at the Agency when required by the Administrator including preparing impact assessments of incidents of non-compliance or breach;

8.5.4. to coordinate and facilitate any activities between the Agency, the Administrator and other Government Agencies including law enforcement relating to data protection;

8.5.5. to educate and instil awareness to Government employees and users on the importance of data protection, including this policy and the Agency's internal data protection policies, procedures and guidelines; and

8.5.6. to channel any employee or public queries or complaints in regards to the Agency's non-compliance with the policy to the Administrator.

9. Principle II - Specifying Purposes

9.1. Agencies shall specify the purposes for which data are collected.

9.2. Agencies shall document the purposes for which data is collected in order to comply with the Openness principle and the Individual Access principle.

9.3. The identified purposes should be specified to the Individual from whom the data is collected or to the Individual. Depending upon the way in which the data is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

9.4. Agencies shall specify these purposes at or before the time the data is collected or, in the event that this is not practicable, as soon thereafter as is reasonable.

9.5. When data that has been collected are to be used for a purpose not previously specified, the new purpose shall be specified to the relevant party prior to use, through suitable means, such as an online privacy policy. The uses of such data are still subject to the other principles in this policy.

9.6. The purposes must be specified in such a manner that the Individual can reasonably understand why the data is being collected and how the data will be used or disclosed.

10. Principle III – Consent

10.1. The knowledge and consent of the Individual are required for the collection, use, or disclosure of data to a third party, except where the following circumstances apply:

10.1.1. When ALL of the following apply:

(a) the collection, use, or disclosure is clearly in the interest of the Individual;

(b) it is impracticable to obtain the consent of the Individual to that collection, use, or disclosure; and

(c) if it were practicable to obtain such consent, the Individual would be likely to give it.

10.1.2. legal, medical, or security reasons make it impossible or impractical

to seek consent. For example, when data is being collected, used, or disclosed for the detection and prevention of fraud or for law enforcement, seeking the consent of the Individual might defeat the purpose of collecting the data.

10.1.3. seeking consent may be unnecessary if data collection, use, or disclosure assists the Individual to fulfil a statutory requirement.

10.1.4. seeking consent may be unnecessary when the data are collected, used or disclosed in an emergency that threatens the life, health or security of an Individual.

10.1.5. seeking consent may be unnecessary, if the data are generally available to the public.

10.1.6. collection, use or disclosure of data is necessary to render a service which the Individual has applied for.

10.1.7. disclosure is made to an institution whose purpose is the conservation of records of historic or archival importance and disclosure is for such purpose.

10.2. Consent shall be obtained by Agencies at or before the time of processing, except that where the Agencies wants to use data for a purpose not previously identified, consent with respect to use or collection may be obtained after the data are collected but before use.

10.3. Agencies may not, as a condition of the provision of a product or service, require an Individual to consent to the collection, use, or disclosure of data beyond that required to fulfil the specified and legitimate purposes.

10.4. The form of the consent sought by the Agencies may vary, depending upon the circumstances and the type of data. In determining the form of consent to use, the Agencies shall take into account the sensitivity of the data.

10.5. Whenever possible, the Agencies should obtain consent from the Individual in accordance to the guidelines in this policy. However, consent does not always have to be obtained directly from the Individual. Consent can be given by an authorised representative of the Individual (such as a legal guardian or a person having power of attorney).

10.6. Consent shall not be obtained through deception or by providing misleading or incomplete information.

10.7. The way in which the Agencies seek consent may vary, depending on the circumstances and the type of data collected. Agencies should generally seek express consent when the data are likely to be considered sensitive. Implied consent would generally be appropriate when the data are less sensitive.

10.8. An Individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The Individual may only be subjected to consequences where the information is required to fulfil the specified and legitimate purposes set out by the Agencies. The Agencies should inform the Individual of the implications of such withdrawal.

11. Principle IV – Collection of Data

11.1. The collection of data including personal data shall be limited to that which is necessary for the purposes specified by the Agencies.

11.2. Data is to be collected by fair and lawful means.

11.3. Collection beyond purposes specified is permitted in the following circumstances:

11.3.1. When all of the following apply:

(a) the collection is clearly in the interest of the Individual;
(b) it is impracticable to obtain the consent of the Individual to that collection; and
(c) if it were practicable to obtain such consent, the Individual would be likely to give it.

11.3.2. the Individual gives consent.

11.3.3. collection beyond purposes specified is for legal, medical, or security reasons. For example, when data is being collected for the detection and prevention of fraud or for law enforcement.

11.3.4. if data collection assists the Individual to fulfil a statutory requirement.

11.3.5. data is being collected in an emergency that threatens the life, health or security of an Individual.

11.3.6. collection of data which is generally available to the public.

11.3.7. collection of data is necessary to render a service for which the Individual has applied.

11.4. Agencies shall not collect data indiscriminately. Both the amount and the type of data collected shall be limited to that which is necessary to fulfil the purposes identified.

12. Principle V – Use, Disclosure and Retention of Data

12.1. Data shall not be used or disclosed to a third party for purposes other than those for which it was collected, except with the consent of the Individual or as required by law.

12.2. Data shall be retained only as long as necessary for the fulfilment of the purposes for which it was collected unless required by legislation to retain this data for archival purposes.

12.3. Use or disclosure beyond the purposes for which data were collected is permitted in circumstances such as the following:

12.3.1. When all of the following apply:
(a) The use or disclosure is clearly in the interest of the Individual;
(b) it is impracticable to obtain the consent of the Individual to that use or disclosure; and
(c) if it were practicable to obtain such consent, the Individual would be likely to give it.

12.3.2. use or disclosure of the data is for legal, medical, or security reasons, for example, when data is being used or disclosed for the detection and prevention of fraud or for law enforcement.

12.3.3. if data use or disclosure assists the Individual to fulfil a statutory requirement.

12.3.4. data is being used or disclosed in an emergency that threatens the life, health or security of an Individual.

12.3.5. use or disclosure of data which is generally available to the public.

12.3.6. use or disclosure of data is necessary to render a service which the Individual has applied for.

12.3.7. disclosure is made to an institution whose purpose is the conservation of records of historic or archival importance and disclosure is for such purpose.

12.4. If Agencies use the data for a new purpose it shall document this purpose in accordance with the Specifying Purposes principle (refer to clause 9.2).

12.5. The Agencies are allowed to develop internal policies, guidelines and procedures with respect to the retention and destruction of data. Data that has been used to make a decision about an Individual shall be retained long enough to allow the Individual access to the data after the decision has been made.

13. Principle VI – Accuracy of Data

13.1. Data shall be as accurate, complete, and up-to-date as is necessary for the purposes for which they are to be used.

13.2. Data should be collected directly from the Individual as far as it is practicable to do so. However, where the Individual consents, indirect collection can be used to increase convenience for the Individual so that the individual does not have to repeatedly provide the same information to the Agencies.

13.3. Agencies shall request updates of data from Individuals only where they are necessary to fulfil the purposes for which the data were collected.

13.4. Agencies, in complying with this principle, may take into consideration the extent to which compliance is reasonable.

14. Principle VII – Safeguards for Data

14.1. Agencies must ensure that all data shall be protected by appropriate security safeguards.

14.2. The security safeguards shall protect the data against accidental or unlawful loss, as well as unauthorised access, disclosure, copying, use, or modification. Agencies shall protect the data regardless of the format in which they are held.

14.3. The nature and extent of the safeguards will vary depending on:

14.3.1. the sensitivity of the data that have been collected;

14.3.2. the amount, distribution, and format of the data;

14.3.3. the method of storage;

14.3.4. the state of technological development; and

14.3.5. the cost and reasonableness of implementation of the safeguards.

14.4. The methods of protection should include one or more of the following:

14.4.1. physical measures, for example, secured filing cabinets and restricted access to offices;

14.4.2. organisational measures, for example, security clearances and limiting access on a "need-to-know" basis;

14.4.3. technological measures, for example, the use of passwords and encryption, as may be available, appropriate and reasonable from time to time.

14.5. Agencies shall make employees aware of the importance of maintaining the confidentiality of data.

14.6. Reasonable care shall be used in the disposal or destruction of Personal Data, to prevent unauthorised parties from gaining access to the data.

14.7. Safeguards for data protection shall be assessed by the Administrator from time to time, as and when required.

15. Principle VIII – Openness about Data Protection Policies and Procedures

15.1. Agencies shall make available information about its policies, guidelines and procedures for handling data including personal data.

15.2. Agencies shall be open about their policies, guidelines and procedures with respect to the management of data. Individuals should be able to acquire information about the Agencies policies, guidelines and procedures without unreasonable effort, for example through the Agencies website. Such information shall be made available in a form that is generally understandable.

15.3. The information made available shall include:

15.3.1. the contact details to whom complaints or inquiries can be forwarded;

15.3.2. the means of gaining access to data held by Agencies;

15.3.3. a description of the Agencies policies, guidelines or standards which make clear that data held by the Agencies or which are made available to other parties are necessary for the purposes of fulfilling a legal or regulatory requirement or for delivering a public service; and

15.3.4. procedures for an Individual to obtain more detailed information on data held by the Agencies or shared with other agencies for Individual cases, including any fees applicable for such a request.

16. Principle IX – Individual Access and Correction

16.1. Subject to the following exceptions, an Individual shall upon his/her request be informed of the existence, use, and disclosure of his/her Data that the Individual has earlier provided to the Agencies, and shall be given access to that data.

16.2. An Individual shall be able to challenge the accuracy and completeness of

his/her data and have them amended as appropriate. The reasons for denying access should be provided to the Individual upon request.

16.3. Agencies shall refuse the request of access where:

16.3.1. providing access would be likely to reveal data about another Individual, unless:

(a) the said person consents to the access;

(b) the Individual needs the information because a person's life, health or security are threatened, provided that where the data about the said person are severable from the record containing the data about the Individual, Agencies shall sever the data about the said person and shall provide access to the Individual; and

(c) an investigative body or government agency, upon notice being given to it of the Individual's request, objects to the agency's complying with the request in respect of its disclosures made to or by that investigative body or government agency.

16.3.2. data are protected by solicitor-client privilege;

16.3.3. it would reveal data that cannot be disclosed for public policy, legal, security, or commercial proprietary reasons;

16.3.4. it would threaten the life, health or security of a person;

16.3.5. data were collected under collection pertaining to an investigation of a breach of an agreement or the law (clause 11.3.3);

16.3.6. complying with the request would be prohibitively costly to the Agency; or

16.3.7. the request is deemed frivolous or vexatious by the Agencies .

16.4. Agencies shall verify the identity of the Individual concerned before granting access. Furthermore, the Individual may be required to provide sufficient data to permit an agency to provide an account of the existence, use and disclosure of data. The data provided shall only be used for this purpose.

16.5. In providing an account of recipients or categories of recipients to which it has disclosed data about an Individual, Agencies should attempt to be as specific as possible. When it is not possible to provide a list of the organisations to which it has actually disclosed data about an Individual, Agencies should provide a list of organisations to which it may have disclosed data about the Individual.

16.6. Agencies shall respond to an Individual's request within a reasonable time and may charge a reasonable fee for providing the information or data requested for. The requested data shall be provided or made available in a form that is generally understandable. For example, if Agencies use abbreviations or codes to record data, an explanation shall be provided.

16.7. When an Individual successfully demonstrates the inaccuracy or incompleteness of data, Agencies shall amend the data as required within a reasonable time. Depending upon the nature of the data challenged, amendment may involve the correction, deletion, or addition of data. Where appropriate, the amended data shall be transmitted to recipients having access to the data in question.

16.8. When a challenge is not resolved to the satisfaction of the Individual, the substance of the unresolved challenge shall be recorded by Agencies. When appropriate, the existence of the unresolved challenge shall be transmitted to recipients currently having access to the data in question.

17. Principle X – Challenge to Compliance

17.1. An Individual shall be able to address a challenge concerning compliance with the above principles to the Agencies.

17.2. Agencies shall put mechanisms and processes in place to receive and address complaints or inquiries about their policies and procedures relating to the handling of data including personal data. The complaint process should be simple and accessible.

17.3. Agencies shall inform persons who make inquiries or lodge complaints of the existence of relevant feedback mechanisms.

17.4. Agencies shall inform the Administrator of all complaints lodge in relation to the handling of data including personal data.

17.5. The Administrator shall record all complaints and shall investigate when necessary. If a complaint is found to be justified, the agency shall take appropriate measures, including, if necessary, amending its internal policies, guidelines and procedures.

18. Principle XI – Trans-border Data Transfers

18.1. Agencies may only transfer Personal Data to another party (other than the organisation or the Individual) outside of Brunei Darussalam only if:

18.1.1. the Agencies reasonably believes that the recipient of the data is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the data that are substantially

similar to the data protection principles in this Policy;

18.1.2. the Individual consents to the transfer;

18.1.3. the transfer is necessary for the performance of a contract between the Individual and the Agencies, or for the implementation of pre-contractual measures taken in response to the data subject's request;

18.1.4. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Individual between the Agencies and a third party; and

18.1.5. the Agencies or Individual has taken reasonable steps to ensure that the data which it has transferred will not be held, used or disclosed by the recipient of the data inconsistently with the data protection principles in this policy.

19. References

19.1. The following legislation, policy, standard and guideline documents are directly relevant to this policy, and are referenced within this document:

19.1.1. Official Secrets Act (Chap 153)

19.1.2. Protective Security Manual, JKDN

19.1.3. United Nations Guidelines concerning Computerized Personal Data Files