DATA PROTECTION COMPLIANCE POLICY
DUOPHARMA BIOTECH BERHAD
AND GROUP OF COMPANIES

1. Duopharma Biotech Berhad and its group of companies ("**Duopharma Biotech**") is committed to ensuring compliance with the requirements of the Personal Data Protection Act 2010 **("the PDPA**") and Personal Data Protection Standards 2015 (the "**PDPA Standards**"). Duopharma Biotech recognizes the importance of Personal Data to its business and the importance of respecting the privacy rights of individuals.

2. This Personal Data Protection Compliance Policy ("**this Policy**") sets out the principles which we will apply to our processing of Personal Data in accordance with the law.

3. Please read the following carefully to understand our practices regarding the processing of personal data and how we will treat it.

4. All Duopharma Biotech employees must familiarise themselves with this policy and are responsible for ensuring that he or she:

- Has knowledge of the fundamental principles of the PDPA and the PDPA Standards;
- Is aware of the consequences of non-compliance with the PDPA; and
- Is fully committed to achieving compliance with this Policy.

5. It is the responsibility of all our employees to assist Duopharma Biotech to comply with this Policy. The consequences of non-compliance are serious. Failure to do so could amount to misconduct, which is a disciplinary matter and could ultimately lead to dismissal. Serious breaches could also result in personal criminal liability.

6. In addition, a failure to comply with this Policy could expose the business to enforcement action by the Personal Data Protection Commissioner or to complaints or claims for compensation from affected individuals. There may also be negative publicity as a result of any breach that is made public.

7. If any employee is in doubt as to whether a particular course of conduct may be in conflict with the PDPA, the employee should notify his/her superiorimmediately to be escalated to Group Legal and Secretarial.

What is processing of Personal Data?

8. "**Personal Data**" means any information in respect of commercial transactions that relate to an identified or identifiable person which data is being processed wholly or partly by means of equipment (e.g. computer), is recorded (e.g. on paper) with the intention of being processed by means of such equipment (either wholly or in part), or is recorded as part of a filing system. The data is personal data if the person is identified or identifiable from that information / other information he /she can be identified (for example: email, telephone number, home address, identification number, position within organisation and distinguishing characteristics). This Policy applies to all Personal Data processed by Duopharma Biotech, including Duopharma Biotech's employees, contract workers, independent contractors, site visitors, shareholders, customers, suppliers, or business partners.

9. "**Sensitive Personal Data**"- means any personal data consisting of information as to the physical or mental health or condition of an individual, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence.

10. "**Processing**" has a wide meaning and covers virtually anything that can be done in relation to Personal Data, such a obtaining, collecting, recording, holding, storing, organizing, adapting, altering, retrieving, consulting, using, disclosing, aligning, combining, correcting, blocking, erasing, or destroying Personal Data.

11. "**Data Subject**" means an individual who is the subject of the personal data.

12. Duopharma Biotech will comply withthe following Seven Principles in respect of any personal data which it processes as a data user.

1st Principle

General Principle

Personal Data and Sensitive Personal Data must not be processed unless one of the conditions set out below is met.

13. You must justify your processing of **all** personal data under one of the conditions set out below. If you cannot find a condition that justifies your processing then that processing may **not** take place.

- ✓ The data subject has given his consent to the processing;
- ✓ The processing is necessary to perform a contract with the data subject;
- ✓ The processing is necessary for the taking of steps at the request of the data subject with a view to entering into a contract;
- ✓ The processing is necessary for compliance with legal obligations to which the data subject is the subject,
- ✓ The processing is necessary to protect the vital interests of the data subject;
- ✓ The processing is necessary for the administration of justice;
- ✓ The processing is necessary for the exercise of any functions conferred on any person by or under any law.

14. When considering the above conditions, remember the broad definition of processing. For example, obtaining consent to process means obtaining consent for the disclosure, collection, use, destruction etc. of Personal Data. You must ensure that if the form in which such consent is to be given also concerns another matter, the requirement to obtain consent shall be presented, distinguishable in its appearance from such other matter.

15. In addition, where you are processing sensitive Personal Data, you must also justify that processing under one of the conditions set out below. This is a safeguard which recognizes the sensitive and sometimes confidential nature of this category of Personal Data. The conditions are set out below:

- ✓ The Data Subject has given his explicit consent to the processingof the Personal Data; this will require a written consent signed by the Data Subject;
- ✓ The processing is necessary for the purpose of exercising orperforming any right or obligation which is conferred or imposed by law on Duopharma Biotech in connection with employment;
- ✓ The processing is necessary in

order to protect the vital interestsof the data subject or another person, in a case where (a) consent cannot be given by or on behalf of the data subject; (b) Duopharma Biotech cannotreasonably be expected to obtainthe consent of the data subject; This will include providing particulars of the mental health of an employee to the relevant authorities for medical benefits;

- ✓ The processing is necessary in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;
- ✓ The processing is necessary for medical purposes and is undertaken by (a) a healthcare professional or (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional;
- ✓ The processing is necessary for the purpose of, or in connection with, any legal proceedings;
- ✓ The processing is necessary for the purpose of obtaining legal advice;
- ✓ The processing is necessary for the purpose of establishing, exercising and defending legalrights;
- ✓ The processing is necessary for the administration of justice;
- ✓ The processing is necessary for the exercise of any functions conferred on any person by or under any written law; or
- ✓ The processing is necessary for any other purpose as the Ministerthinks fit.

16. If the Data Subject is under eighteen (18) years old, the consent of his/her parent, guardian or person who has parental responsibility on the Data Subject shall be obtained.

17. The consent from a Data Subject whose affairs is managed by a person appointed by a court or by a person authorized in writing by the Data Subject to manage his/her affairs if he/she is unable to do so, shall be obtained from the said appointed or authorised person.

2nd Principle

Notice and Choice

18. The Data Subject shall be given a written notice which informs him/her of the following:

Contents of data protection notice

- ✓ That personal data is being processed by or on behalf of Duopharma Biotech, and a description of what the Personal Data is;
- ✓ The purposes of processing the Personal Data;
- ✓ The source of that personal data where available;
- ✓ The Data Subject's right to request access to / correction of Personal Data; or withdraw consent of Personal Data; how to contact Duopharma Biotech with inquiries or complaints in respect of the Personal Data;
- ✓ To whom Duopharma Biotech may disclose the Personal Data;
- ✓ The extent to which the data subject may limit the processing of Personal Data, including Personal Data relating to third parties identifiable from that Personal Data and how to withdraw consent on Personal Data processing;
- ✓ Whether the supply of the data to Duopharma Biotech is obligatory or voluntary; and
- ✓ Where it is obligatory to supply the Personal Data, the consequences of not supplying the Personal Data.
- ✓ The practical measures that will be taken to ensure that the Personal Data is secured;
- ✓ How long the Personal Data will be retained in such processing.

Timing of data protection notice

19. The notice shall be given as soon as practicable when:

- ✓ The data subject is first asked by Duopharma Biotech to provide his Personal Data;
- ✓ Duopharma Biotech first collects the personal data of the data subject;
- ✓ In any other case, before Duopharma Biotech (i) uses the Personal Data for a different purpose from which the Personal Data was collected; or (ii) discloses the Personal Data to a third party.

Language of data protection notice

20. The notice shall be in both Bahasa Melayu and English languages;

21. You may obtain copies of our standard and current data protection notices from the Chief Legal Officer, Group Legal and Secretarial. These notices have been drafted to take account of thekind of processing that we do. You should use the data protection notices whenever you

obtain Personal Data. If you think the notices do not cover your particular processing activities,you must discuss this in the first instance with the Chief Legal Officer, Group Legal and Secretarial.

list of disclosure to third-parties in relation to Personal Data of the Data Subject that has been or is being processed.

3rd Principle

Disclosure

22. Personal data **cannot** be disclosed to third parties without the consent of the data subject forpurposes other than the purposes for which the data was collected ora purpose directly related. Personal Data can only be disclosed in the following circumstances:

- ✓ When Data Subject has given consent to the disclosure to the third party for that specific purpose, and notice has been given to the Data Subject in respect of the third parties to whom Duopharma Biotech woul disclose Personal Data to.
- ✓ The disclosure is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations; or is required or authorised by or under any law or by the order of a court.
- ✓ If Personal Data is required to be disclosed for any other purposes, please refer to Chief Legal Officer, Group Legal and Secretarial for further advice.

23. You must keep and maintain a

4th Principle

Security principle

24. It is Duopharma Biotech's intent to maintain the integrity and confidentiality of the Personal Data and in particular, take reasonable precautions to protect it from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction. The following guidelines are to be followed:

✓ IT Department to ensure technical measures are takenand maintained such assoftware controls to restrict user access; up-to-date virus checking software; audit trail software;

✓ All employees to ensure organisational measures are taken and maintained such as restricting access to buildings and computer rooms and storage facilities for personal data and ensuring secure disposal of information;

✓ If a third-party data processor isused (for e.g. external payroll providers, insurance service providers, healthcare service providers), you must ensure:

- A Data Processing Contract Letter is put in place in writing with each of our data processors under which they are obliged to act in accordancewith the PDPA;

- The right to audit our data processors to ascertain compliance with the data protection requirements of the processing contract is included;and

- The data processor agrees to comply with obligations equivalent to those imposed onus by the 7 Principles.

✓ If you are responsible for the selection, appointment or use of data processors, you must ensure that you only select those processors that are able to provide us with sufficient guarantees in respect of the technical and organisational measures they will apply to the processing of our Personal Data. Further, if you areresponsible for the drafting or negotiation of contracts with data processors, you must ensure those contracts contain all applicable data protection provisions. Seek further advice

from the Chief Legal Officer, Group Legal and Secretarial who will advise you on how to comply with the requirements of the PDPA.

5th Principle

Retention Principle

25. You should review the Personal Data which you hold on a regular basis and delete any data which isno longer required for the original purpose. When carrying out this exercise you should consider legal or other requirements to retain data. You should also consider the type of relationship Duopharma Biotech haswith the Data Subject and expectationsthat data will be retained for any given period of time (for e.g. our employees may expect us to retain their data for aperiod of time after they have left).

6th Principle

Data integrity- data to be accurate, complete, not misleading and kept up-to-date

26. Personal Data will be inaccurate if it is incorrect or misleading as to any matter of fact (for e.g. incorrectname or address). If you are entering data into our system and are unsure as to the accuracy of the same (for e.g. because the handwriting is illegible or because it appears to be an obvious mistake or omission), you should try to get in touch with the Data Subject to clarify the issue.
27. You must take reasonable steps to keep data up to date to the extent necessary. The purpose for which data is held will determine the need to keep the same data up to date. For example, historical records of transactions should not,as a general rule, be updated.

7th Principle

Data Access

28. If you receive a request in writing from an individual requesting;

    a) access to Personal Data;
    b) correction of Personal Data;
    c) withdrawal of consent to Personal Data;
    d) prevention of processing of Personal Data likely to cause damage;
    e) prevention of processing of Personal Data likely to cause damage or distress; or
    f) prevention of processing of Personal Data for purposes of direct marketing,

    you must pass the request promptly to the Chief Legal Officer, Group Legal and Secretarial.

29. You may refuse to comply with the Data Subject to access Personal Data if;

    a) You are not provided with necessary information reasonably required to establish the identity of the Data Subject;
    b) you are not provided with sufficient information to locate the Personal Data to which the data access request relates;
    c) the access would cause disproportionate burden and expense;
    d) the access would cause disclosure of Personal Data of others;
    e) the access would constitute a violation of court's order;
    f) the access would cause disclosure of confidential commercial information; or
    g) the access to such access to Personal Data is regulated by another law.

30. You may refuse to comply with the request by Data Subject to correct Personal Data if;

    a) you are not provided with necessary information reasonably required to establish the identity of the Data Subject;
    b) you are not supplied with sufficient information reasonably required to determine how the Personal Data is inaccurate, incomplete, misleading or not up-to-date; or
    c) you are not satisfied that the correction requested is inaccurate, incomplete, misleading or not up-to-date.

31. Standard is defined as minimum requirement issued by the Personal Data Protection Commissioner that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.

32. The PDPA Standards includes the establishment of the Security Standard (4th Principle), the Retention Standard (5th Principle) and the Data Integrity Standard (6th Principle) for Personal Data processed electronically and non-electronically.

33. Setting these Standards will ensurethe security of user's Personal Data and the smoothness of commercial transactions involving international trade, foreign investment, electronic commerce activities, protection towards national interest, trade and business, subject data, and the adoption of personal data protection culture in Duopharma Biotech's governance.

34. For Security Standard, a Data User shall, take practical steps to protect the Personal Data from any loss, misuse, modifications, unauthorized or accidental access or disclosure, alteration or destruction for personal data processes electronically and non-electronically.

35. With regard to the Retention Principle,a Data User shall take all reasonable steps toensure that all Personal Data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed electronically and non-electronically.

36. A Data User, under Data Integrity Standard Principle, shall take reasonable steps to ensure that the Personal Data isaccurate, complete, not misleading and kept updated by having regard to the purpose, including any directly related purpose, for which the personal data was collected and processed further.

A 'STEP BY STEP' CHECKLIST

- Do I need this information about an individual?
- Do I know what I am going to use it for?
- Does the individual concerned know what I have got? Is he likely to understand what the information will be used for?
- Am I disclosing the information to third parties? Is the individual aware of such disclosure?
- Am I satisfied the information is being held securely?
- Do I take steps to ensure the data is accurate and kept up-to-date?
- How long am I going to keep this information? Do I delete the information when I don't require it further?
- Is access to the information controlled and limited to those with a strict need to know?
- If I want to monitor staff, for example by checking their use of email or via any surveillance device, have I told them about this and explained why?
- Are my staff well trained to be aware of their duties and responsibilities under the PDPA and are they putting them into practice?
- Does the individual have a right to access and correct his information?

Contacts and responsibilities

37. If you have any queries regarding the Policy or compliance with the PDPA in general, please refer to Chief Legal Officer, Group Legal and Secretarial for further advice.

38. Any incident involving either suspected or confirmed breach of security, theft, loss or misuse of Personal Data should be reported promptly to the Chief Legal Officer, Group Legal and Secretarial.

39. The Policy will be updated from time to time by the Chief Legal Officer, Group Legal and Secretarial to reflect any changes in legislation or in our methods or practices.

Date of issue: