Regulations for Management of Personal Data Protection
under the Personal Data Protection Act B.E. 2562 in Thailand

CHAPTER 1
GENERAL RULES

(Purpose)
Article 1

These Regulations for Management of Personal Data Protection (these "**Regulations**") aim to realize proper protection of Personal Data (as defined below) held by JSR Trading Bangkok Co., Ltd. (the "**Company**") to ensure compliance with the Personal Data Protection Act B.E. 2562 (the "**PDPA**")

(Definitions)
Article 2

The terms used herein shall be defined as set forth below:

(1) "**Personal Data**" means any information relating to a natural person (the "**Data Subject**") that enables the identification of such Data Subject, directly or indirectly, but not including information of deceased persons.
(2) "**Data Controller**" means a natural or juridical person having the power and responsibility to make decisions regarding the collection, use, or disclosure of Personal Data.
(3) "**Data Processor**" means a natural or juridical person that is not a Data Controller but that performs the collection, use, or disclosure of Personal Data pursuant to direction given by or on behalf of a Data Controller.
(4) "**Sensitive Personal Data**" means Personal Data comprising the Data Subject's race; ethnicity; political opinions; cult, religious, or philosophical beliefs; sexual behavior; criminal records; health data; disability; trade union information; genetic data; biometric data; or any other data that may affect the Data Subject in the same manner, as prescribed by the Committee.
(5) "**Committee**" means the Personal Data Protection Committee stipulated in the PDPA.
(6) "**Office**" means the Office of the Personal Data Protection Committee.
(7) "**Employee(s)"** means persons (including employees, directors, auditors, executive officers, temporary workers, etc.) engaged in the handling of Personal Data under the direction and supervision of the Company.
(8) "**Data Management Officer**" means a person responsible for securing the proper processing of Personal Data by the Company in accordance with the Regulations and the PDPA.

(Scope of Application)
Article 3

(i) The Regulations shall apply to all Employees of the Company in handling personal data.
(ii) In the event that the handling of Personal Data is outsourced, the proper protection of Personal Data shall be handled in accordance with these Regulations.

CHAPTER 2
PROTECTION OF PERSONAL DATA

(Personal Data Protection General Regulations)
Article 4

(i) The Company shall not collect, use, or disclose Personal Data unless the Data Subject has given consent prior to or at the time of such collection, use, or disclosure, except where permitted under the provisions of the PDPA or any other applicable law.
(ii) A request for consent shall be explicitly made in a written statement or via electronic means unless such request cannot be made in such a manner due to its nature.
(iii) When requesting the consent of Data Subjects, the Company shall also inform the Data Subjects of the purpose of the collection, use, or disclosure of the Personal Data. Such request for consent shall be presented in a manner that is clearly distinguishable from other matters, in an easily accessible and intelligible form, using clear and plain language that does not deceive

or mislead the Data Subject regarding such purpose.

(Personal Data Protection General Regulations for the Personal Data of Minors)
Article 5

In the event that the Data Subject is a minor who is not *sui juris* by marriage or has no capacity as a *sui juris* person under Article 27 of the Civil and Commercial Code, the request for the consent of such Data Subject shall be made as follows:

(1) Where the minor's consent is not an act that the minor is entitled to take alone under Articles 22, 23, or 24 of the Civil and Commercial Code, the consent of the holder of parental responsibility over the minor is required; or
(2) Where the minor is below the age of ten years, consent shall be obtained from the holder of parental responsibility over the minor.

CHAPTER 3
COLLECTION OF PERSONAL DATA

(Collection of Personal Data)
Article 6

The collection of Personal Data shall be limited to the extent necessary for the lawful purposes of the Company. No Personal Data shall be acquired by deceit or other improper means.

(Restrictions on the Collection of Personal Data)
Article 7

The Company shall not collect Personal Data without the consent of the Data Subject, unless such collection is:

(1) for the achievement of a purpose relating to the preparation of historical documents or archives for public interest or for purposes relating to research or statistics, in which suitable measures to safeguard the Data Subject's rights and freedoms are put in place and in accordance with notifications prescribed by the Committee;
(2) for preventing or suppressing a danger to a person's life, body, or health;
(3) necessary for the performance of a contract to which the Data Subject is a party or to take steps at the request of the Data Subject prior to entering into a contract;
(4) necessary for the performance of a task carried out by the Company for the public interest or to exercise official authority vested in the Company;
(5) necessary for the legitimate interests of the Company or any third party, except where such interests are overridden by the fundamental rights of the Data Subject; or
(6) necessary to comply with a law to which the Company is subject.

(Restriction of Collection of Sensitive Personal Data)
Article 8

The Data Controller shall not collect Sensitive Personal Data without the consent of the Data Subject, unless such collection is:

(1) to prevent or suppress a danger to a person's life, body, or health, where the Data Subject is incapable of giving consent for any reason;
(2) carried out in the course of legitimate activities with appropriate safeguards by foundations, associations, or any other non-profit bodies with political, religious, philosophical, or trade union purposes for their members, former members, or persons having regular contact with such foundations, associations, or non-profit bodies in connection with such purposes, without disclosure of the Personal Data outside of such foundations, associations, or non-profit bodies;
(3) information disclosed to the public with the explicit consent of the Data Subject;
(4) necessary for the establishment, compliance, exercise, or defense of legal claims; or
(5) necessary for compliance with a law enacted to achieve purposes with respect to:
    (a) preventive or occupational medicine;
    (b) public health;

(c) health or social care systems;
(d) scientific, or historical research; or
(e) a substantial public interest.

(Procedure for Collection)
Article 9

When collecting Personal Data, the Company shall inform the Data Subject of the following, prior to or at the time of such collection, except where the Data Subject already knows such information:

(1) the purpose of the collection of Personal Data for use or disclosure, including the purposes permitted under Article 7 of these Regulations for the collection of Personal Data without the Data Subject's consent;
(2) notification that the Data Subject must provide his or her Personal Data to comply with a law or contract or where it is necessary to provide Personal Data to enter into a contract, including notification of the possible effect of the Data Subject failing to provide such Personal Data;
(3) the Personal Data to be collected and the period for which the Personal Data will be retained (if it is not possible to specify the retention period, the expected data retention period according the data retention standards shall be specified);
(4) the categories of persons or entities to whom the collected Personal Data may be disclosed;
(5) information, address, and the contact method details of the Company; and
(6) the rights of the Data Subject provided in Chapter 6 of these Regulations.

(Restriction of Indirect Collection of Personal Data)
Article 10

The Company shall not collect Personal Data from any source other than the Data Subject directly, except where:

(1) the Company has informed the Data Subject of the collection of Personal Data from other sources without delay, not exceeding thirty (30) days after the date of such collection, and has obtained the consent of the Data Subject; or
(2) the collection of Personal Data falls under an exception to consent under Article 7 or Article 8 of these Regulations.

CHAPTER 4
USE AND DISCLOSURE OF PERSONAL DATA

(Restriction of Use and Disclosure of Personal Data)
Article 11

(i) The Company shall not use or disclose Personal Data to a third party without the consent of the Data Subject, unless it is Personal Data collected without the consent requirement in accordance with Article 7(1)-(6) or Article 8 (1)-(5) of these Regulations.
(ii) A person that obtains Personal Data as a result of disclosure pursuant to paragraph (i) shall not use or disclose such Personal Data for any purpose other than the purpose previously provided to the Company in the request for such Personal Data.
(iii) In the event that the Company uses or discloses Personal Data that is exempt from the consent requirement of paragraph (i), the Company shall maintain a record of such use or disclosure as prescribed in Article 16 of these Regulations.

(Restriction of Transfer of Personal Data to a Foreign Country)
Article 12

(i) Notwithstanding Article 11, where the Company provides Personal Data to a third party located in a country or an international organization outside Thailand (a "**Foreign Country**"), such Foreign Country shall have adequate data protection standards, and such transfer shall be carried out in accordance with the rules for the protection of Personal Data prescribed by the Committee, except in cases falling under any of the following items:

(1) where such transfer is for compliance with the law;
(2) where the consent of the Data Subject has been obtained, provided that the Data Subject has been informed of the potentially inadequate personal data protection standards of the destination country or international organization;
(3) where such transfer is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;
(4) where such transfer is for compliance with a contract between the Company and other persons for the interests of the Data Subject;
(5) where such transfer is necessary to prevent or suppress a danger to the life, body, or health of the Data Subject or other persons, where the Data Subject is incapable of providing consent at such time; or
(6) where such transfer is necessary for carrying out activities in relation to a substantial public interest.

(ii) The provisions of paragraph (i) shall not apply to those cases set forth in each item below:
(1) Personal Data is transferred to another Data Controller or Data Processor who is in a foreign country, and is in the same affiliated business, or is in the same group of undertakings, in order to jointly operate the business or group of undertakings in accordance with a personal data protection policy that has been reviewed and certified by the Office; or
(2) Other suitable protection measures enabling the enforcement of the Data Subject's rights, including effective legal remedial measures according to the rules and methods prescribed and announced by the Committee.

CHAPTER 5
ADMINISTRATION OF PERSONAL DATA

(Administration of Personal Data)
Article 13

The Company shall endeavor to administer Personal Data in such a way as to prevent unauthorized access, to maintain accuracy and timeliness within the scope necessary to achieve the purposes of use, and to delete Personal Data without delay when such use has become unnecessary.

(Security Control Measures for Personal Data)
Article 14

The Company shall have the following duties to secure Personal Data:
(1) The Company shall provide appropriate security measures to prevent the unauthorized or unlawful loss, access to, use, alteration, correction, or disclosure of Personal Data, and such measures shall be reviewed when necessary or when technology is changed in order to efficiently maintain appropriate security and safety. Such security measures shall be in accordance with the minimum standards specified and announced by the Committee.
(2) In the event that Personal Data is to be provided to third parties other than the Company, the Company shall take actions to prevent such third parties from using or disclosing such Personal Data unlawfully or without authorization.
(3) The Company shall put in place an review system for the erasure or destruction of Personal Data when the retention period ends, when the Personal Data is irrelevant or beyond the purpose for which it has been collected, when the Data Subject requests, or when the Data Subject withdraws consent, except where the retention of such Personal Data is for the purpose of freedom of expression, a purpose under Article 7(1) or (4) or Article 8(5)(a) or (b) of these Regulations, or the purpose of establishment, compliance, exercise, or defense of legal claims or of compliance with the law.
(4) The Company shall notify the Office of any Personal Data breach without delay and, where feasible, within 72 hours after having become aware of it, unless such Personal Data breach is unlikely to result in a risk to the rights and freedoms of the Data Subjects. If such Personal Data breach is likely to result in a high risk to the rights and freedoms

of the Data Subjects, the Company shall also notify the affected Data Subject(s) of the Personal Data breach and the remedial measures therefor without delay. The notification and exemptions to the notification shall be made in accordance with the rules and procedures set forth by the Committee. Any Personal Data Breach shall be handled in accordance with the Annex "Protocol Personal Data Breach" as attached.

(Retention Period of Personal Data)
Article 15

(i) Personal Data will be kept for no longer than required for the purpose for which it has been collected or processed, in accordance with applicable laws, or to allow the Company to protect the legitimate rights and interests of itself or of third parties.
(ii) In order to determine the appropriate retention period for Personal Data, the Company shall consider the amount, nature, and sensitivity of Personal Data; the potential risk of harm from unauthorized use or disclosure of the Personal Data; the purposes for which the Company processes the Personal Data and whether the Company can achieve those purposes through other means; and the applicable legal requirements.
(iii) Personal Data of employees will be kept for 10 years after the expiration of the employment contract with the employees. Provided, however, that the Company may keep the Personal Data of the employees more than 10 years if necessary.

(Records of Personal Data)
Article 16

The Company shall maintain the following records in a written or electronic form to enable the review of the Data Subject and the Office:

(1) the collected Personal Data;
(2) the purpose of the collection of the Personal Data in each category;
(3) details of the Data Controller;
(4) the retention period of the Personal Data;
(5) rights and access methods for the Personal Data, including the conditions necessary to exercise the right to access the Personal Data;
(6) the use or disclosure of Personal Data without the consent of Data Subjects;
(7) rejections of requests or objections; and
(8) explanation of the security measures.

(Data Processing Agreement)
Article 17

In the event that the Company uses any Data Processor to process Personal Data, the Company shall execute a data processing agreement with the Data Processor to control the activities carried out by the Data Processor, and such activities must be performed in accordance with the Data Processor's obligations under the PDPA.

.

CHAPTER 6
RIGHTS OF DATA SUBJECTS

(Right to Access)
Article 18

(i) The Data Subject is entitled to request access to and obtain copy of his or her Personal Data that is under the responsibility of the Company and to request the disclosure of the acquisition of the Personal Data obtained without the Data Subject.
(ii) A request made pursuant to paragraph (i) may be rejected only where permitted by law or pursuant to a court order and where such access to and/or obtaining a copy of the Personal Data would adversely affect the rights and freedoms of others.
(iii) In the event that the Company rejects a request made pursuant to paragraph (i), the Company shall record its rejection with supporting reasons in the records prescribed in Article 16 of these Regulations.
(iv) When a Data Subject makes a request pursuant to paragraph (i) and such request cannot be

rejected for the reasons provided in paragraph (ii), the Company shall fulfill the request without delay, but not exceeding thirty (30) days from the date of receiving such request.

(Right to Data Portability)
Article 19

(i) The Data Subject shall have the right to receive his or her Personal Data from the Company. The Company shall arrange such Personal Data in a readable or commonly used format by way of automated tools or equipment and that can be used or disclosed by automated means. The Data Subject is also entitled to:
    (1) request that the Company send or transfer the Personal Data in such format to other Data Controllers, if such transfer can be done by automated means; and
    (2) request to receive the Personal Data directly in the format the Company uses to send or transfer the Personal Data to other Data Controllers, unless it is impossible to do so due to technical circumstances.

(ii) The Personal Data requested pursuant to paragraph (i) must be Personal Data for which the Data Subject has given consent for the collection, use, or disclosure in accordance with PDPA, these Regulations, Personal Data exempt from the consent requirements under Article 7(3), or any other Personal Data referred to in Article 7 as prescribed by the Committee.

(iii) The exercise of rights of the Data Subject pursuant to paragraph (i) shall not apply to the Company's sending or transferring of Personal Data in the performance of a task carried out in the public interest, for compliance with the law, or where the exercise of such rights violates the rights and freedoms of others.

(iv) In the event that the Company rejects a request for such reason, the Company shall record such rejection with the reasons therefor in the record prescribed in Article 16 of these Regulations.

(Right to Object to Processing)
Article 20

(i) The Data Subject shall have the right to object to the collection, use, or disclosure of his or her Personal Data at any time in the following circumstances:
    (1) where Personal Data is collected under an exemption to the consent requirement under Article 7(4) or (5), unless the Company can prove that:
        (a) the Company can demonstrate that it has compelling legitimate grounds for the collection, use, or disclosure of such Personal Data; or
        (b) the collection, use, or disclosure of such Personal Data is carried out for the establishment, compliance, exercise, or defense of legal claims.
    (2) the collection, use, or disclosure of such Personal Data is for the purpose of direct marketing; or
    (3) the collection, use, or disclosure of Personal Data is for the purpose of scientific, historical, or statistical research, unless it is necessary for the Company to perform a task carried out for reasons of public interest.

(ii) In the event that the Data Subject exercises his or her right to object pursuant to paragraph (i), the Company shall no longer be able to collect, use, or disclose such Personal Data, and the Company shall immediately and clearly distinguish such Personal Data from other matters at the time the Data Subject gives notice of his or her objection to the Company.

(iii) In the event that the Data Controller rejects the objection for a reason pursuant to paragraph (i)(1)(a) or (b) or (3), the Company shall record such rejection with the reasons therefor in the record prescribed in Article 16.

(Right to Request Deletion)
Article 21

(i) The Data Subject shall have the right to request that the Company erase, destroy, or anonymize the Personal Data such that it cannot be used to identify the Data Subject on the following grounds:
    (1) the Personal Data is no longer necessary for the purposes for which it was collected, used, or disclosed;
    (2) the Data Subject withdraws the consent on which the collection, use, or disclosure is

based, and the Company has no other legal grounds for collection, use, or disclosure;

(3) the Data Subject objects to the collection, use, or disclosure of the Personal Data under Article 20(i)(1) and the Company cannot reject such request for a reason provided in Article 20 (i)(1)(a) or (b), or the Data Subject exercises his or her right to object pursuant to Article 20(ii);

(4) the Personal Data has been unlawfully collected, used, or disclosed.

(ii) Paragraph (i) shall not apply to the extent that Personal Data retention is necessary for the purpose of freedom of expression; a purpose under Article 7(1) or (4) or Article 8(5)(a) or (b); the purpose of establishment, compliance, exercise, or defense of legal claims; or for compliance with the law.

(iii) In the event that the Company has publicly disclosed the Personal Data and receives a request to erase, destroy, or anonymize the Personal Data pursuant to paragraph (i), the Company shall be responsible for the implementation of the technology and expenses required to fulfill the request and shall notify other Data Controllers in order to obtain their responses regarding the actions to be taken to fulfill such request.

(Right to Request Limitation of Processing)
Article 22

(i) The Data Subject shall have the right to request that the Company restrict the use of the Personal Data where the following applies:

(1) when the Company's review in accordance with the Data Subject's request pursuant to Article 24(i) is pending;

(2) when Personal Data is scheduled to be erased or destroyed pursuant to Article 21(i)(4), but the Data Subject requests the restriction of the use of such Personal Data;

(3) when it is no longer necessary to retain such Personal Data for the purposes of the collection thereof, but the Data Subject requests retention for the purposes of the establishment, compliance, exercise, or defense of legal claims; or

(4) when the Company is awaiting verification in accordance with Article 20(i)(1) or examination in accordance with Article 20(i)(3) to reject an objection made by a Data Subject in accordance with Article 20(iii).

(ii) In the event that the Company does not take action pursuant to paragraph (i), the Data Subject shall have the right to complain to the Committee.

(Right to Withdraw Consent)
Article 23

(i) The Data Subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall be as easy as giving consent, unless there is a restriction of such withdrawal by law or a contract providing benefit to the Data Subject. The withdrawal of consent shall not affect the collection, use, or disclosure of the Personal Data for which the Data Subject has already given consent legally.

(ii) In the event that the withdrawal of consent will affect the Data Subject in any manner, the Company shall inform the Data Subject of such consequences of withdrawing consent.

(Right to Request Data Accuracy)
Article 24

(i) The Company shall ensure that the Personal Data remains accurate, up-to-date, complete, and not misleading.

(ii) In the event that the Data Subject requests the Company to comply with paragraph (i), if the Company does not take action in response to the request of the Data Subject, the Company shall record the request of the Data Subject with reasons for its failure to take action in response in the record prescribed in Article 16. The provisions of Article 23(ii) shall apply *mutatis mutandis*.

(Right to Lodge a Complaint with the Committee)
Article 25

The Data Subject shall have the right to file a complaint in the event that the Company violates or does not comply with the PDPA or notifications issued pursuant to the PDPA.

CHAPTER 7
ORGANIZATION AND SYSTEM

(Personal Data Protection Management)
Article 26

(i) The Data Management Officer shall be appointed as a person responsible for securing the proper processing of Personal Data in accordance with these Regulations and the PDPA with respect to the data processing of the Company.

(ii) The Company shall designate the Data Management Officer as Data Protection Officer under the PDPA under the following circumstances:
   (1) the activities of the Company in the collection, use, or disclosure of Personal Data require regular monitoring of Personal Data or the system due to a large amount of Personal Data, as prescribed and announced by the Committee; or
   (2) the core activity of the Company is the collection, use, or disclosure of Personal Data pertaining to race; ethnicity; political opinions; cult, religious, or philosophical beliefs; sexual behaviors; criminal records; health data; disabilities; trade union information; genetic data; biometric data; or any data that may affect the Data Subject(s) in the same manner.

(iii) Where the Company designates a Data Protection Officer, the Company shall have an obligation to provide the information, contact address, and contact methods of the Data Protection Officer to the Data Subjects and the Committee. Data Subjects shall be able to contact the Data Protection Officer regarding the collection, use, or disclosure of Personal Data and the exercise of the rights of Data Subjects under the PDPA.

(Education)
Article 27

The Data Management Officer shall be responsible for an education and training plan and shall conduct education and training continuously and regularly so that Employees understand the importance of compliance with Personal Data Protection.

(Audit)
Article 28

(i) The Data Management Officer shall implement an audit regarding whether the internal Personal Data Protection administration is implemented properly in accordance with these Regulations and the PDPA.

(ii) In the event that the Data Management Officer provides instructions for improvement, proper improvement measures shall be taken promptly, and the details thereof shall be reported to the Data Management Officer.

(Duty to Report and Penalties)
Article 29

(i) Any person who becomes aware that a leak of Personal Data or a contravention of these Regulations has occurred or is likely to occur shall immediately report to the Data Management Officer.

(ii) The Company shall investigate the details of a report made pursuant to paragraph (i).

Annex: Protocol Personal Data Breach