Regulations on Personal Data Protection

May 24th 2019

State Bank of India
Japan

Regulations on Personal Data Protection

Regulations

Chapter 1 General Provisions

Article 1 Purpose

These Regulations set down the basic items on personal data protection that should contribute to the appropriate protection and use of personal information handled in the cause of business by the branches in Japan of the State Bank of India (ñ**Branch**ò).

Article 2 Definitions

Terms appearing in these Regulations are defined as follows:

(i) Personal information: Means information relating to a living individual which falls under any of each following item.

a. those containing a name, date of birth, or other descriptions etc. (ie, any and all matters, excluding an individual identification code, stated, recorded or otherwise expressed using voice, movement or other methods in a document, drawing or electromagnetic record (ie, a record kept in an electromagnetic form that cannot be recognized through the human senses)) whereby a specific individual can be identified, including those which can be readily collated with other information and thereby identify a specific individual

b. those containing an individual identification code

(ii) Individual identification code: Means those prescribed by cabinet order which are any character, letter, number, symbol or other codes falling under any of each following item.

a. those able to identify a specific individual that are a character, letter, number, symbol or other codes into which a bodily partial feature of the specific individual has been converted in order to be provided for use by computers

b. those character, letter, number, symbol or other codes which are assigned in regard to the use of services provided to an individual or to the purchase of goods sold to an individual, or which are stated or electromagnetically recorded in a card or other document issued to an individual so as to be able to identify a specific user or purchaser, or recipient of issuance by having made the said codes differently assigned or, stated or recoded for the said user or purchaser, or recipient of issuance

(iii) Personal information database, etc.: A collection of information including personal information, referring to the following:

a. A collection of information that is structurally organized so that specific personal information can be retrieved by computer.

b. Besides the database cited in a., a collection of information structurally organized so that specific personal information can be easily retrieved by organizing the personal information included therein according to a set of fixed rules, having a list of contents, an index, codes, and other means for simplifying retrieval.

(iv) Personal data: Refers to the personal information that constitutes personal information databases, etc. Note that it includes personal information downloaded from personal information databases, etc. to a recording media and personal information output on paper (or a copy).

(v) Retained personal data: Refers to personal data that the Bank has the authority to disclose, correct, add or delete the contents of, cease the utilization of, erase, and cease the third-party provision of, and other than <1> personal data where the public interest or other interest may be harmed when its existence is revealed or <2> personal data which is to be erased within 6 months (However, for the personal data that Branch received from within EU based on the Adequacy Decision, as long as it does not fall under <1> above, regardless of the period in which it is to be erased, it shall be treated as retained personal data)

(vi) Personal Information Protection Commission (ñPPCò): PPC was established on January 1st 2016, changed from the Specific Personal Information Protection Commission. The duties of the PPC are the protection of the rights and interests of individuals while taking into consideration proper and effective use of personal information including MY

Regulations
NUMBER. The PPC is one of the highly independent organs in the Japanese legal framework. Based on the Act on the Protection of Personal Information (ñActò), the Chairman and Commission members exercise their authorities independently. (vii) Personal Data Protection Manager: Appointed by the Branch Manager within the bank, refers to a person who has the responsibility and authority for implementing and operating the various regulations, etc. related to personal data protection (viii) Personal Data Protection Division Manager: Appointed by the Personal Data Protection Manager, refers to a person who has responsibility and authority for implementing and operating the various regulations, etc. (those in line with (iv) above) related to personal data protection in each division (ix) Chief Audit Officer: Appointed by the Branch Manager in the bank, refers to a person who has authority for implementing audits and for reporting from a fair and objective position (x) Recipient: Refers to a person who is provided with personal information (xi) Information subject: Refers to an individual who is identified or can be identified by a set of information (xii) Consent of information subject: Refers to an indication of intention to consent to the acquisition, use, or provision of personal information about him/herself by an information subject after he/she has been given information on the acquisition, use, or provision. Note, however, that it refers to the consent of the guardian if the information subject is a child. (xiii) Acquisition purpose: The acquisition purpose sets the scope of the use and provision of personal information and requires the consent of the information subject. (xiv) Use: Refers to the processing of personal information in the Branch for business purposes (xv) Provision: Refers to the Branch being able to use personal information that it holds itself for an entity outside the Branch (xvi) Temporarily entrustment to another party: Refers to the Branch entrusting the personal information that it holds itself when delegating data processing, etc. to an entity outside the Branch (xvii) Inquiries Officer: The Branchôs Inquiries Officer for personal information appointed by the Branch Manager. Also serves as the Information Desk for replying to ordinary inquiries. (xviii) EU: Refers the European Union, including Iceland, Liechtenstein and Norway under the European Union and the European Economic Area (ñEEAò) Agreement (xix) GDPR: General Data Protection Regulation refers REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. The regulation applies if the data controller (an organization that collects data from EU residents), or processor (an organization that processes data on behalf of a data controller like cloud service providers), or the data subject (person) is based in the EU. Under certain circumstances, the regulation also applies to organizations based outside the EU if they collect or process personal data of individuals located inside the EU. The regulation does not apply to the processing of data by a person for a ñpurely personal or household activity and thus with no connection to a professional or commercial activity. (xx) Adequacy Decision: Refers a decision that, under Article 45 of the GDPR, the European Commission considers countries, regions, etc. to have adequate protection levels for personal data (xxi) Anonymously processed information: Refers information relating to an individual that can be produced from processing personal information so as neither to be able to identify a specific individual nor to be able to restore the personal information. With respect to personal data provided from within EU, based on the Adequacy Decision, only when it is impossible for anyone to re-identify an anonymous individual by deleting processing method information etc., it is regarded as anonymous processed information. Currently, Branch does not use anonymous processed information, and when starting to use them,

Regulations
ñRegulation on Anonymous Processed Information Handlingò is to be established.
Article 3 Personal Information to be Targeted These Regulations are target to the personal information handled by the Branch regardless of whether or not such information is processed by computer systems or recorded on paper.
Article 4 Specification of Personal Information The personal information that the Branch holds is specified on the basis of the ñBylaws on the Operation of Personal Data Protection,ò which are separately provided for. The risks (unauthorized access to personal information, loss, destruction, tampering with, or leaking of personal information, etc.) associated with identified personal information shall be recognized, and efforts made to achieve thoroughness in its management.
Article 5 Scope of Application These Regulations apply to the executives and employees of the Branch. Furthermore, if handling of personal information is outsourced or if temporary personnel are accepted in accordance with the Labor Services Temporary Assignment Law, appropriate efforts shall be made to protect personal information in accordance with the purpose of these Regulations.
Chapter 2 Acquisition Purpose of Personal Information
Article 6 Principles of Acquisition For the acquisition of personal information, the purpose of use shall be clearly set down within the scope of operations conducted by the Branch, and this shall be done to the limit required for achieving that purpose.
Article 7 Restrictions on Acquisition Methods Personal information shall be acquired by legal and fair means. When having provided personal data to a third party, keep a record on the date of the personal data provision, the name or appellation of the third party, and other matters prescribed by rules of the PPC. When receiving the provision of personal data from a third party, confirm those matters set forth in the following pursuant to rules of the PPC. the name or appellation and address of the third party and, for a corporate body, the name of its representative circumstances under which the said personal data was acquired by the said third party When having confirmed pursuant to above, keep a record on the date when it received the provision of personal data, a matter concerning the said confirmation, and other matters prescribed by rules of the PPC. Above record shall be maintained for a period of time prescribed by rules of the PPC from the date when it kept the record.
Article 8 Ban of Acquisition of Specific Sensitive Personal Information ñSpecial care-required personal information 要配慮個人情報 (Article 2 Clause 3 of the Personal Information Protection Act)ò Personal information including the contents indicated below must not be acquired, used, or provided. Note, however, this limitation does not apply if there is the explicit consent of the information subject to the acquisition, use, or provision of such personal information, if there are special provisions in the law, or if it is indispensable from the viewpoint of judicial proceedings: (i) Race (*ethnicity*), (ii) Creed (*matters relating to thoughts, articles of faith, or religion*),

Regulations
(iii) Social status (*lineage*), (iv) Medical history (v) Criminal record, (vi) Fact of having suffered damage by a crime, (vii) or other descriptions etc. prescribed by cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal. (viii) *Domicile of origin (excluding information on prefecture of location), physical or mental disability, or other matters that could cause social discrimination* *(ix) Workers' right to organize, and bargain collectively, and other acts relating to group activities* *(x) Participation in acts of group demonstrations, exercise of right of petition, and other matters relating to the exercise of political rights* (xi) *Matters relating to health care and sex life* *Italic: Sensitive information 機微情報 under FSA's "Guidelines for Personal Information Protection in the Financial Field"* With respect to personal data provided from within EU, based on the Adequacy Decision, when information on sexual life, sexual orientation or labor union etc., as defined as "Special Categories of Personal Data" in GDPR, those information shall be treated as ñSpecial care-required personal informationò.
Article 9 Measures for Directly Acquiring Personal Information from Information Subject 1. If personal information is to be acquired directly from an information subject, the consent of the information subject shall be obtained by notifying the information subject in writing or by a substitute procedure of at least the matters in the Items shown below in a content equal to such matters or more: (i) The full name of the Personal Data Protection Manager or the full name or position title of his/her agent, the department to which he/she belongs, and contact details (ii) The purpose of the acquisition and/or use of the personal information (iii) If it is expected that the personal information will be provided, the purpose, the recipient of the information or the type of organization and attribute of the recipient, and the existence or non-existence of a contract on the handling of personal information (iv) If it is expected that the personal information will be temporarily entrusted to another party, such fact (v) If the personal information will be provided, the fact that it is the choice of the information subject, or, if the information was not provided, the affect on the information subject (vi) If personal information is incorrect as a result of the right to seek disclosure of personal information or, as a result of disclosure, the existence of the right to demand corrections or erasure, and the specific procedure and costs, etc. of exercising this right 2. If personal information is to be acquired directly from an information subject, the consent of the information subject shall be obtained prior to the acquisition on the basis of the ñBylaws on the Operation of Personal Data Protection.ò

Regulations

Article 10 Measures for Acquiring Indirectly from Other than Information Subject

1. If personal information is to be acquired indirectly from other than the information subject, the consent of the information subject shall be obtained by notifying the information subject in writing or by a substitute procedure of at least the matters in Article 9.1(i) through (iv) and (vi). This shall not apply if any of the Items below applies:

(i) When personal information is to be acquired from an information subject, if the acquisition is done by a provider who has obtained the consent of the information subject in advance that the information subject anticipates such information about itself will be provided in accordance with Article 9.1(iii).

(ii) If personal information is temporarily entrusted to another party for outsourcing data processing, etc.

(iii) If the acquisition falls within the scope of the proper activities of the Branch and the interests worthy of the protection of the information subject shall not be harmed

(iv) If it is evident that the information subject has received notification under the Items indicated in Article 9.1, and/or if this is acquired from information publicly announced to an unspecified large number of persons by the information subject

2. If personal information is acquired secondarily due to causes other than those listed in the Items of the previous Paragraph, consent shall be obtained for use by the Branch by notifying the information subject in writing about the following matters, upon prior consultation with the Personal Data Protection Management Administrator:

(i) The full name of the Personal Data Protection Manager of the enterprise that is the primary acquirer, his/her job title, the department to which he/she belongs, and contact details

(ii) The purpose of use of the personal information by the Branch

(iii) The purpose of the personal information being provided to a third party and the name of the recipient

(iv) The existence of rights to demand disclosure, correction, or erasure and the procedures for exercising such rights

3. If there are any reasons to doubt that the primary acquirer may have not acquired the personal information of the information subject by appropriate or legitimate means, the legitimacy and appropriateness of the acquisition of the information must be checked with the primary acquirer under the direction of the Personal Data Protection Management Administrator.

Article 10-2 Confirmation and recording upon receiving third-party provision

1. Upon receiving personal data from a third-party, Branch shall make confirmation and record and preserve records based on Article 26 of the Act.

2. With respect to personal data provided from within EU, based on the Adequacy Decision, (inclusive of those provided through other ñpersonal information handling business operatorò), based on the provisions of Article 26 Paragraph 1 and 3 of the Act, Branch will confirm and record the circumstances of the acquisition including the purpose of use specified at the time of receiving the personal data.

3. With respect to personal data provided under the preceding paragraph, Branch shall specify the scope of the purpose of use within the range specified at the time of initially or secondary receiving the personal data and use them within the scope of the purpose Branch specified.

Regulations

Chapter 3 Purpose of Use of Personal Information

Article 11 Identifying Purpose of Use

The purpose of use of personal information in the Branch is to implement it for example for the sake of financial products and to perform services.

- To check that the person is the customer or the agent of the customer
- To check authority of various contracts
- To canvas or market the financial products and services of the Branch and to provide information related to this
- Besides this, to obtain the contact details of corporations for work related purposes
- Regarding the personal information of the Branchôs employees (including persons who will become employees, persons who intended to become employees, and persons who in the past were employees), for the purpose of personnel management such as decision on recruitment

Article 12 Restrictions on Range of Use

1. The use and provision of personal information shall be within the scope of the purpose of use. This shall not apply, however, if any of the following Items applies:

(i) If it is based on the provisions of the law

(ii) If it is necessary to protect an important interest such as the life, health, or property of the information subject or the general public, and is difficult to obtain the consent of the information subject

(iii) If the information subject has given consent or taken equivalent measures.

2. If the use or provision of personal information that falls within the scope of previous Paragraph 1(i) and (ii) is carried out, the approval of the Personal Data Protection Manager shall be obtained on a case-by-case basis in accordance with the ñBylaws on the Operation of Personal Data Protection,ò which are separately provided for.

Article 13 Measures to Take for Use or Provision is Outside the Scope of Purpose of Use

1. If personal information is used or provided without falling under the items of Paragraph 1. in the previous Article, the information subject shall be notified at least in writing or by a substitute procedure of the matters indicated in Article 9.1(i) to (iv) and (vi), and it shall be done with the prior consent of the information subject. The information subject shall also be given the opportunity to reject that use or provision.

2. If the consent of the information subject is to be sought for a use or provision outside the scope of the acquisition purpose, the approval of the Personal Data Protection Manager shall be obtained in accordance with the ñBylaws on the Operation of Personal Data Protection,ò which is separately provided for.

Chapter 4 Fair Management Obligation

Article 14 Ensuring Accuracy of Personal Information

Personal information shall be managed in an accurate and up-to-date state within the scope of the acquisition purpose. Regarding personal data become no longer needed, Branch shall endeavor to eliminate such personal data without delay.

Article 15 Ensuring Safeness of Use of Personal Information

Besides the matters set out in these Regulations, appropriate security measures shall be taken in accordance with the ñBylaws on the Operation of Personal Data Protectionò against the risks

Regulations

(unauthorized access, leaks, loss, and damage, etc.) associated with personal information.

Article 16 Obligations of Practitioners for Protection of Personal Information

Persons engaged in operations handling personal information such as acquiring, using, providing, or outsourcing of processing personal information shall perform those operations, paying sufficient attention to the protection of personal information in accordance with the provisions of the law, these Regulations, and other internal regulations or matters indicated by the Personal Data Protection Manager.

Article 17 Measures on Outsourcing of Processing of Personal Information

1. If the Branch temporarily entrusts personal information outside for outsourcing data processing, etc., it shall select an entrustee (outsourcee) that satisfies the standards that it sets for the protection of personal information. Further, the Branch shall guarantee the protection level by determining the entrustee and by setting the content below, by means of a contract, etc. The written document of the contract, etc. or the record of the substitute for this shall be retained for the period of retention of the personal information.

(i) Authority to supervise, audit, and collect reports from outsourcees

(ii) Bans on leaks, theft, and tampering with personal information at outsourcee and bans on uses other than intended uses

(iii) Conditions for re-outsourcing

(iv) Responsibilities of outsourcee when of leaks, etc. occur

2. In case of providing personal data to a third party in a foreign country, a principal's consent shall be obtained in advance to the effect that he or she approves the provision to a third party in a foreign country

In following cases, a principal's in advance consent is not required:

a. The foreign country is those prescribed by rules of the PPC as a foreign country establishing a personal information protection system recognized to have equivalent standards to that in Japan in regard to the protection of an individual's rights and interests

b. The third party in the foreign country establishing a system conforming to standards prescribed by rules of the PPC as necessary for continuously taking action equivalent to the one that a personal information handling business operator shall take concerning the handling of personal data

3. In case of providing ñpersonal data provided from within EU, based on the Adequacy Decisionò to foreign country, except for the cases match with a. or b. of the preceding paragraph, Bank will obtain consent of the principal to allow personal data to be provided to third parties in foreign countries in advance, by providing information on the situation of relocation destination necessary for the principal to make a judgment pertaining to the consent.

Joint Use of Personal Information

If personal information is to be jointly used with third parties, the coordinator shall notify the Personal Data Protection Manager. The joint use of personal information must take place with the approval of the Personal Data Protection Manager and after the Personal Data Protection Manager has implemented the measures required.

Chapter 5 Rights of Information Subject to Own Information

Regulations

Article 18 Rights to Own Information

1. If disclosure of its own information has been required by an information subject in relation to the personal data held by the Branch, in principle, the Branch shall comply with this by the judgment of the Personal Data Protection Manager within the range in which the person concerned has sought disclosure within a reasonable period under the procedure specified separately in the Bylaws. However, the check that the person is the person concerned in the information must be made rigorously through the presentation of at least two identification documents. In addition, if the following reasons apply, all or part of the disclosure request may be treated as non-disclosed, in which case, the reason shall be explained to the requestor:

(i) If there is a risk that the life, body, property, or other rights and interests of the information subject or a third party may be harmed

(ii) If there is a risk that the fair implementation of the Branchôs operations may be significantly hindered

(iii) If it results in a breach of another law

2. In addition, if the content of retained personal data is found to be untrue a result of the disclosure and if correction or erasure is sought, the necessary investigation shall be made, and, as a rule, this will be acceded to within a reasonable period of time.

Article 19 Right to Reject Use or Provision of Own Information

If the use or provision of its own information to a third party has been rejected by an information subject in relation to the personal information held by the Branch, the Branch shall comply with this. This, however, shall not apply if Article 12. 1 (i) or (ii) applies.

Chapter 6 Organization, Education, Audits, Etc.

Article 20 Appointment of Personal Data Protection Manager

1. The Branch Manager shall appoint one Personal Data Protection Manager to perform operations.

2. The Personal Data Protection Manager may appoint an assistant if necessary.

Article 21 Responsibilities of Personal Data Protection Manager

1. The Personal Data Protection Manager is responsible for implementing measures such as devising and publicizing an action plan for establishing internal regulations on personal data protection, implementing security measures, and promoting education and training, etc., in accordance with the directions of the Branch Manager and provisions in these Regulations.

2. As well as observing matters provided for in these Regulations, the Personal Data Protection Manager shall encourage those engaged in operations handling personal information such as the acquisition, use, provision, or outsourced processing of personal information to understand and observe them.

3. The Personal Data Protection Manager may appoint a coordinator to assist him/her (Assistant Personal Data Protection Manager) in the formulation of the compliance plan and its implementation.

Article 22 Education

1. The Personal Data Protection Manager conducts education and training on an ongoing and regular basis in accordance with the required education program and education materials

Regulations
in order to encourage employees to understand the importance of the various provisions, etc. in relation to personal data protection and to achieve reliable implementation. 2. The Personal Data Protection Manager shall be the officer responsible for the implementation of education and training, and the Assistant Personal Data Protection Manager shall perform the duties.
Article 23 Audits 1. The Branch Manager appoints a Chief Audit Officer and shall have such person to conduct audits regularly to audit the fact that the Branchôs internal personal data management is being implemented appropriately in accordance with the various provisions, etc. relating to personal data protection. However, an external person who has been separately appointed on the order of the Branch Manager may be added when it is necessary to do so for operational purposes. 2. The Chief Audit Officer shall prepare and implement an audit program in accordance with the internal audit regulations. 3. The Chief Audit Officer shall put together an audit report, and submit it to the Branch Manager. If there has been a breach of law, the Branch Manager shall provide directions for the required improvements to the Personal Data Protection Manager and other persons concerned. 4. In addition to promptly implementing measures for making the required improvements, the person who has received directions for improvement shall report the content to the Chief Audit Officer. 5. The Chief Audit Officer shall evaluate the improvement content, and shall report such evaluations to the Branch Manager and/or Personal Data Protection Manager.
Article 24 Duty to Report and Penalty Provisions 1. A person who has acquired knowledge of the breach of the various regulations, etc. on personal data protection or has discovered that a breach may have occurred shall report that fact to the Personal Data Protection Manager. 2. Without delay, the Personal Data Protection Manager shall investigate the content of the report, and, if he/she finds a breach, instructs the affected divisions within the bank and shall report the above to the Branch Manager. 3. As stated in Article 17 Paragraph 1 of the Financial Sector Guidelines, regardless of the Notice No. 1 in 2017 of the PPC, financial institutions should report leaks of personal information immediately to the Financial Services Agency (ñFSAò), not to the PPC. However, in case of leaks of employeesô or stockholdersô personal information, reporting to the PPC should be made and reporting to the FSA is recommended by the PPC. 4. With respect to "personal data", in the practical guideline 2-6-1, "when leakage occurs, etc. notification to the principal shall be implemented. (Obligation provision), and with respect of ñpersonal information (personal information other than personal data)", in Article 22, paragraph 3 of the guideline, leakage incident shall be promptly notified to the person who was the subject of the leakage case (obligation of effort). 5. Employees that have breached the various provisions, etc. on personal data protection intentionally or due to gross negligence shall be disciplined according to the Rules of

Regulations
Employment. 6. External outsourcees that have breached the various regulations, etc. on personal data protection shall be made to bear the responsibility as provided for in each contract.
Article 25 Review The Branch Manager shall instruct the Personal Data Protection Manager to routinely review the various regulations, etc. on personal data protection to maintain appropriate personal data protection in light of audit reports and other business environments, etc.
Article 26 Bylaws Bylaws shall be provided for separately on detailed regulation matters required for the operation of these Regulations.
Article 27 Inquiries Officer The Branch Manager shall set up a contact point for inquiries relating to personal information, and shall appoint one of the bank employees to be the person responsible. The Inquiries Officer shall record details of inquiries relating to personal information, and shall forward the inquiry to the appropriate division for replying together with the specified documents.
Chapter 7 Specific measure for the specific personal information
Article 28 Restriction of access **Access to the specific personal information shall be strictly restricted. to followings:** 1. Branchôs top management, ie, CH&CEO and COO, Compliance Department, Risk Management Department and IT system section, for the general management, risk control, auditing and IT system support. 2. Deposit and cross border remittance customersô specific personal information: Remittance section 3. Employeesô specific personal information: General Affaires section.