Personal Data Protection Policy

Contents

1 Purpose

The purpose of this Personal Data Protection Policy ("Policy") is to lay down personal data protection principles, requirements and objectives of personal data protection in Bank of China Limited, Luxembourg Branch and Bank of China (Luxembourg) S.A. and its branches (together or individually "Bank") so that it complies with the applicable regulatory requirements as well as that of Bank of China Limited. The applicable regulatory requirements are namely that of EU Regulation 2016/679 "General Data Protection Regulations" ("GDPR"). The supervisory Portuguese authority in personal data protection is "Commissão Nacional de Protecção de Dados'' (CNPD)

2 Definitions

For the purpose of this Policy the following definitions which are aligned to the one used in GDPR apply

a) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
b) processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
c) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
d) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
e) 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

3 Principles relating to processing of personal data

In the course of the Bank's business, the Bank is required to process personal data such as personal data of customers, employees, suppliers etc. The Bank is required to have rules in place in relation to the data processing, data transfer and the rights of persons concerned to the protection of their personal data. The Bank shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR. These measures shall be reviewed and updated where necessary.

I. With this in mind the Bank shall follow the following principles on relation to the processing of personal data

Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

II. Each department of the Bank shall have procedures in place to ensure that the data processing is in compliance of the principles contained in paragraph 1 above. Each head of department of the Bank shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability') and this Policy in general.

III. In line with the above principles, specifically (b) to (e), all staff should follow the Bank's data retention policy ("BoC - Data Retention Policy").

3.1 Lawfulness of processing

Article 6 of GDPR provides basis for lawfulness of processing. Below are those which are applicable to the Bank having taken account of the nature of business operations of the Bank. Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is party e.g. entering into a business relationship with the Bank, or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which the Bank is subject such as to fulfill the obligation of prevention of money laundering;

d) processing is necessary for the purposes of the legitimate interests pursued by the Bank or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require

3.2 Conditions for consent

a) Where processing is based on consent, the Bank shall be able to demonstrate that the data subject has consented to processing of his or her personal data. In relation to the processing of the personal data of a child, it shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child

b) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent for a specific matter shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

c) Consent can be by a written statement, including by electronic means, or an oral statement (where having positively identified the data subject, a record of which should be kept by the Bank). Silence, pre-ticked boxes or inactivity will not constitute consent.

d) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof.

e) Consent should be freely given by the data subject. Utmost care should be taken of whether, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

3.3 Processing of "special categories of personal data" (SCPD)

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited, except if any of the following is met.

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, unless Portuguese laws do not allow such prohibitions be lifted by the data subject. Compliance and/or Legal functions of the Bank should be consulted if processing of SCPD is based on explicit consent;

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Bank or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Portuguese law or a collective agreement

c) processing relates to personal data which are manifestly made public by the data subject;

d) processing is necessary for the Bank exercise or defence of legal claims

4 Providing transparent information for the exercise of data subject rights

I. The Bank shall take appropriate measures to provide any information referred to in sections 5.1 and 5.2 and any communication under section 5.3 (right of access) to section 5.9 (automated decision making) and section11.2 (notification of data breach to data subject) relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. The relevant staff shall keep relevant records including that such information has been provided orally at the request of the data subject.

II. The Bank shall facilitate the exercise of data subject rights under section 5.3 to section 5.9. In the cases that processing does not require the Bank to identify the data subject, the Bank shall not refuse to act on the request of the data subject for exercising his or her rights as above, unless the Bank demonstrates that it is not in a position to identify the data subject.

III. The Bank shall provide information on action taken on a request under section 5.3 to section 5.9 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account

the complexity and number of the requests. The Bank shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

IV. If the Bank does not take action on the request of the data subject, the Bank shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with CNPD and seeking a judicial remedy.

V. Information provided under section 5.1 and 5.2 and any communication and any actions taken under section 5.3 to section 5.9 and section11.2 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Bank may either:

a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

b) refuse to act on the request.

The Bank shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

VI. Where the Bank has reasonable doubts concerning the identity of the natural person making the request referred to in section 5.3 to section 5.9, the Bank may request the provision of additional information necessary to confirm the identity of the data subject.

5 Rights of the data subject

5.1 Information to be provided where personal data are collected from the data subject

I. Where personal data relating to a data subject are collected from the data subject, the Bank shall, at the time when personal data are obtained, provide the data subject with all of the below information. To the extent possible the Bank shall provide such information in the Bank's General Terms and Conditions ("GTC"). Where GTC is not used, such as employment or other types of business relationship, the information should be provided through other means such as in Employment contract, or standalone document.

a) the identity and the contact details of the Bank and, where applicable, of the relevant department/staff;

b) the contact details of the data protection officer;

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d) where the processing is based on point (d) of point 3.1, the legitimate interests pursued by the Bank or by a third party;

e) the recipients or categories of recipients of the personal data, if any;

f) where applicable, the fact that the Bank intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission (via EU implementing act on decision that the third country, or the international organisation in question ensures an adequate level of data protection), and in the absence of such decision reference to the basis and the suitable safeguards as per GDPR Article 46 or 47, or the second subparagraph of Article 49(1) (derogation on specific situation), and the means by which to obtain a copy of them or where they have been made available.

II. In addition to the information referred to in I, the Bank shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b) the existence of the right to request from the Bank access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

c) where the processing is based on client consent as stipulated in point 3.1(a) or 3.3(a), existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

d) the right to lodge a complaint with a supervisory authority;

e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

f) the existence of automated decision-making, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Where the Bank intends to further process the personal data for a purpose other than that for which the personal data were collected, the Bank shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred in II (a) to (f) above.

5.2 Information to be provided where personal data have not been collected from the data subject

I. Where personal data have not been obtained from the data subject, the Bank shall provide the data subject with the following information:

a) the identity and the contact details of the Bank and, where applicable, of the relevant department/staff;

b) the contact details of the data protection officer;

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d) the categories of personal data concerned;

e) the recipients or categories of recipients of the personal data, if any;

f) where applicable, the fact that the Bank intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission (via EU implementing act on decision that the third country, or the international organisation in question ensures an adequate level of data protection), and in the absence of such decision reference to the basis and the suitable safeguards as per GDPR Article 46 or 47, or the second subparagraph of Article 49(1) (derogation on specific situation), and the means by which to obtain a copy of them or where they have been made available.

II. In addition to the information referred to in paragraph 1, the Bank shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b) where the processing is based on point (d) of point 3.1, legitimate interests pursued by the Bank or by a third party;

c) the existence of the right to request from the Bank access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

d) where processing is based on point 3.1(a) or 3.3(a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

e) the right to lodge a complaint with a supervisory authority;

f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

g) the existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

III. The relevant department/staff shall provide the information referred to in I and II;

a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

Where the Bank intends to further process the personal data for a purpose other than that for which the personal data were obtained, the Bank shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in II (a) to (f) above.

IV. Paragraphs I to III shall not apply where and insofar as:

a) the data subject already has the information;

b) the provision of such information proves impossible or would involve a disproportionate effort, or in so far as the obligation referred to in paragraph I above is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the Bank shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

c) obtaining or disclosure is expressly laid down by Portuguese law which provides appropriate measures to protect the data subject's legitimate interests; or

d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by EU or Portuguese law, including a statutory obligation of secrecy.

5.3 Right of access by the data subject

I. The data subject shall have the right to obtain from the Bank confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

a) the purposes of the processing;
b) the categories of personal data concerned;

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request from the Bank rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f) the right to lodge a complaint with a supervisory authority;
g) where the personal data are not collected from the data subject, any available information as to their source;
h) the existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

II. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to GDPR Article 46 (or refer to section 14) relating to the transfer.

III. The Bank shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the Bank may decide to charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

5.4 Right to rectification

The data subject shall have the right to obtain from the Bank without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

5.5 Right to erasure ('right to be forgotten')

I. The data subject shall have the right to obtain from the Bank the erasure of personal data concerning him or her without undue delay and the Bank shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) the data subject withdraws consent on which the processing is based according to point 3.1(a) or 3.3(a), and where there is no other legal ground for the processing;
c) the data subject objects to the processing pursuant to section 5.9 (I) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to 5.9 (II);
d) the personal data have been unlawfully processed;
e) the personal data have to be erased for compliance with a legal obligation in Portugal;

II. In the event that the Bank has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the Bank shall take measures as per GDPR article 17 (2).

III. The above I and II shall not apply to the extent that processing is necessary:

a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation which requires processing by Portuguese law; or
c) for the establishment, exercise or defence of legal claims.

5.6 Right to restriction of processing

I. The data subject shall have the right to obtain from the Bank restriction of processing where one of the following applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the Bank to verify the accuracy of the personal data;
b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
c) the Bank no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
d) the data subject has objected to processing pursuant to section 5.9 (I) pending the verification whether the legitimate grounds of the Bank override those of the data subject.

II. Where processing has been restricted under paragraph I, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest as per applicable laws.

III. A data subject who has obtained restriction of processing pursuant to point 5.6. I shall be informed by the Bank before the restriction of processing is lifted.

5.7 Notification obligation regarding rectification or erasure of personal data or restriction of processing

The Bank shall communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Bank shall inform the data subject about those recipients if the data subject requests it.

5.8 Right to data portability

I. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the Bank, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the Bank to which the personal data have been provided, where:

a) the processing is based on consent pursuant to point (a) of section 3.1 or point (a) of section 3.3 (a) to (d) or on a contract pursuant to point (b) of section 3.1; and
b) the processing is carried out by automated means.

II. In exercising his or her right to data portability pursuant to paragraph 1, the Bank shall transfer the personal data of a data subject from the Bank to another controller directly at the request of the data subject, where technically feasible.

III. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to section 5.5.

IV. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

5.9 Right to object

I. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (d) of section 3.1, including profiling based on those provisions. The Bank shall no longer process the personal data unless the Bank demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

II. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

III. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

IV. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs I and II shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5.10 Automated individual decision-making, including profiling

I. Decision based solely on automated processing, including profiling, shall take place only in the following conditions

a) It is necessary for entering into, or performance of, a contract between the data subject and the Bank;

b) It is authorised by Portuguese law to

c) It is based on the data subject's explicit consent.

II. In the cases referred to in points (a) and (c) of paragraph 2, the Bank shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the Bank, to express his or her point of view and to contest the decision.

III. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in 3.3 (I), unless point (a) of section 3.3 applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

6 The Bank as the Controller

6.1 Data protection by design and by default

I. Taking into account of factors such as technical means, the cost of implementation and the nature, scope, context and purposes of processing as well as the associated risks posed by the processing, the Bank shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as

pseudonymisation and data minimization, which are designed to implement data-protection principles, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

II. The departments of the Bank shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

6.2 Joint controllers

I. In the event that the purposes and means of processing are determined jointly by the Bank and other parties, all parties are therefore joint controllers. Joint controllers shall in a transparent manner determine the respective responsibilities for compliance with the obligations under GDPR, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in sections 5.1 and 5.2, by means of an agreement which may designate a contact point for data subjects.

II. The agreement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the agreement shall be made available to the data subject.

7 The Bank as the Processor

I. In the event that the Bank, itself is not the controller and processes data on behalf of another controller, the Bank shall not engage another processor without prior specific or general written authorisation of the controller. Any changes shall the informed to the controller, thereby giving the controller the opportunity to object to such changes. In this situation, processing shall be governed by a contract under Portugal or other EU member state law as appropriate, setting out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller in accordance of Article 23 (3) of GDPR. The Bank shall not process those data except on instructions from the controller, unless required to do so by Portuguese authorities.

8 Records of processing activities

The Bank and specifically the relevant departments acting as controller and/or processor shall maintain a record of processing activities under its responsibility, namely:

- The data processing register for each department
- Documented procedure for each data processing activity

The above shall when considered together contain all of the following information:

a) the name and contact details of the controller and processor (if applicable), the data protection officer;
b) the purposes of the processing;
c) the categories of processing carried out
d) a description of the categories of data subjects and of the categories of personal data;
e) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
f) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), i.e in the absence of the EU adequacy decision of that third country and the appropriate safeguards stipulated in Article 46 of GDPR, the documentation of suitable safeguards in the circumstance;
g) where possible, the envisaged time limits for erasure of the different categories of data;
h) where possible, a general description of the technical and organisational security measures referred to in 10 (I).

9 Cooperation with the supervisory authority

The Bank shall cooperate, on request, with the supervisory authority such as CSSF and CNPD and make the record available to the supervisory authority on request promptly

10 Security of processing

I. The Bank shall implement appropriate technical and organisational measures to ensure adequate level of security appropriate to the risk, including inter alia as appropriate:

i) the pseudonymisation and encryption of personal data;
j) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
k) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
l) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

II. In assessing the appropriate level of security, it shall be taken into account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

III. The staff of the Bank who has access to personal data shall not process them except the processing is necessary for the performance of their job or under the instructions from their superior.

11 Personal data breach

11.1 Notification of a personal data breach to the supervisory authority

I. In the case of a personal data breach, the Bank shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority in Portuguese which is the CNPD, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

II. It shall be agreed formally with other third party processor that it shall notify the Bank without undue delay after becoming aware of a personal data breach.

III. The Bank's procedure "BoC_Procedure for Identification and notification of breaches" shall be followed. The notification referred to in paragraph 1 shall at least:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) describe the likely consequences of the personal data breach;
d) describe the measures taken or proposed to be taken by the Bank to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

IV. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided to CNPD in phases without undue further delay.

V. The Bank shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this section 11.

11.2 Communication of a personal data breach to the data subject

I. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Bank shall communicate the personal data breach to the data subject without undue delay.

II. The communication to the data subject referred to in paragraph I above shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of section 11.1(III).

III. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
a) the Bank has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
b) the Bank has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph I is no longer likely to materialise;
c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

12 Data protection impact assessment (“DPIA”)

I. Where the processing is likely to result in a high risk to the rights and freedoms of natural persons, the Bank shall prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

II. The advice of the data protection officer or Personal Data Protection Committee shall be requested, when carrying out a data protection impact assessment.

III. DPIA shall in particular be required in the case of:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b) processing on a large scale of special categories of data referred to section 3.3, or
c) a systematic monitoring of a publicly accessible area on a large scale, which is not relevant to the Bank presently.

IV. The Bank's procedure for DPIA "BOC_Procedure for the Data Protection Impact Assessment" shall be followed. The DPIA methodology shall contain at least:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

V. If a code of conduct on data protection has been issued by the authorities in Portugal, it shall be taken into due account in assessing the impact of the processing operations performed in the data protection impact assessment.

VI. Where appropriate, the Bank shall seek the views of data subjects or their representatives on the intended processing. Where necessary the relevant department responsible for the processing in question shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing

12.1 Prior consultation with CNPD

I. The Bank shall consult CNPD prior to processing where a data protection impact assessment under indicates that the processing would result in a high risk in the absence of measures taken by the Bank to mitigate the risk. When consulting CNPD, the following shall controller shall provide the supervisory authority with:

a) where applicable, the respective responsibilities of the Bank as controller and/or processor, and joint controllers if any involved in the processing, the purposes and means of the intended processing;
b) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant GDPR where applicable, the contact details of the data protection officer;
c) the DPIA; and
d) any other information requested by CNPD

13 Data Protection Officer ("DPO")

13.1 Designation

I. The Bank shall designate a DPO who shall be appointed on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill the tasks referred to in section 13.3

II. The Bank shall establish a Personal Data Protection Committee (PDPC) which shall have the objective of assisting DPO in his/her tasks.

III. The Bank shall publish the contact details of the DPO and communicate them to the supervisory authority CNPD

13.2 Position of Data Protection Officer

I. DPO shall be involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

II. The Bank shall support the DPO in performing the tasks referred to in section 13.3 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

III. The Bank shall ensure that the DPO does not receive any instructions regarding the exercise of those tasks. DPO shall not be dismissed or penalised by the Bank for performing his tasks. The DPO shall directly report to the highest management level of the Bank.

IV. Data subjects may contact the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights under GDPR.

V. The DPO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Portuguese laws.

VI. The DPO may fulfill other tasks and duties. The Bank shall ensure that any such tasks and duties do not result in a conflict of interests.

13.3 Tasks of Data Protection Officer

I. The data protection officer shall have the following tasks:

a) to inform and advise the Bank and the employees who carry out processing of their obligations pursuant to GDPR and this Policy and to other Portuguese personal data protection provisions;

b) to monitor compliance with GDPR and this Policy, with other Portuguese personal data protection provisions, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to section12;

d) to cooperate with the supervisory authority CNPD;

e) to act as the contact point for the CNPD on issues relating to processing, including the prior consultation referred to in section 12.1 and to consult, where appropriate, with regard to any other matter.

II. The DPO shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

14 Transfers of personal data to third countries or international organizations

I. Any transfer of personal data to countries which are outside EEA shall subject to a DPIA by the department which originates the transfer. The results shall be reported to the DPO of the Bank who shall, based on the risks identified has the power to veto the data transfer.

II. EU may decide through an implementing act that a third country or an international organisation has framework in place which ensures an adequate level of protection of personal data. In this case transfer of personal data to that country or organization does not necessarily need a prior approval from the competent authority. However in the absence of a decision pursuant to Article 45(3), the Bank may transfer personal data to a third country or an international organisation only if the Bank has provided the appropriate safeguards, and that data subject freedom and rights are protected.

III. The appropriate safeguards provided for in GDPR Article 46 (2), without requiring any specific authorisation from a supervisory authority, are:

a) a legally binding and enforceable instrument between public authorities or bodies;
b) binding corporate rules in accordance with GDPR Article 47;
c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in GDPR Article 93(2);

d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
e) an approved code of conduct pursuant to GDPR Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
f) an approved certification mechanism pursuant to GDPR Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

IV. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:
a) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

The corporate binding rules shall need to be approved by relevant competent authority as per GDPR Article 47