SBERBANK CIB

SBERBANK CIB (UK) LIMITED

DATA PROTECTION POLICY

July 2018

SBERBANK CIB

TABLE OF CONTENTS

Preamble 2

1. Definitions 2

2. Purpose of the policy 3

3. Scope of this policy and main purposes of Data Processing 3

4. Standards for processing personal Data 3

5. Lawful processing of Personal Data 4

7. Management of Data Subject's Rights 5

8. Lodging an internal complaint 5

9. Data Security and Confidentiality 5

10. Personal Data Breach Reports 6

11. International transfers 6

12. Accountability 6

13. Training programs and other tools available 7

14. Audits 7

15. Supervising Authorities and sanctions 7

16. Your point of contact 7

17. Application date and Amendments 7

PREAMBULE

As a business and an employer, Sberbank CIB (UK) Limited and SIB (Cyprus) LTD, London Branch, (hereafter "CIB UK") collects and process many personal data from employees, candidates, customers (which include individuals and representatives/contacts from corporate clients), suppliers, distributors and other business partners. CIB UK recognizes the right for all data subjects to be protected from the abusive use of their personal data.

The present Data Protection Policy (hereafter "Policy") sets forth CIB UK's commitments on personal data protection, pursuant to Regulation (UE) 2016/679 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data or General Data Protection Regulation (hereinafter "GDPR").

The legal framework establishes obligations binding upon SBERBANK when they process Personal Data as well as the rights for Data Subjects whose' Personal Data are being processed. The GDPR also provides for specific sanctions for entities processing Personal Data in case of infringements.

1. DEFINITIONS

"**Personal Data**": any information relating to a Data Subject.

"**Data Subject"**: an identified or identifiable natural person to whom Personal Data relates. 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 (including IP addresses and logs) or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"**Data Controller**": the entity responsible for establishing the purposes and means of Processing of Personal Data.

"**Personal Data Breach"**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data that may be transferred, stored or otherwise processed.

"**Data Processor**": the entity which processes Personal Data on behalf of the Data Controller.

"**Processing"** : 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.

"**Special Categories of Personal Data**": Personal Data revealing data racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, as well as genetic data, biometric data, data concerning health, data concerning a natural person's sex life or data revealing sexual orientation.

"**Supervisory Authority**": an independent body which is in charge of: (i) monitoring the Processing of Personal Data within its jurisdiction, (ii) providing advice to the competent bodies in regards to legislative and administrative measures concerning the Processing of Personal Data, and (iii) hearing complaints lodged by Data Subjects regarding the protection of their rights as Data Subjects.

"**Transfer**": any mailing, communication, copy, transmission, distribution or remote access to Personal Data, via any way of communication or medium.

"**Third Country**": a country located outside the European Union ("EU").

2. PURPOSE OF THIS POLICY

This Policy presents all the obligations and requirements that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal data within CIB UK pursuant to GDPR.

This policy should be read in conjunction with the section on data protection in the Employee Handbook.

The Data Privacy Manager is responsible for ensuring compliance with this policy. Any questions or concerns regarding this policy should be referred in the first instance to the Data Protection Manager. This position is held by the Head of Business Administration for CIB UK.

3. SCOPE OF THIS POLICY AND MAIN PURPOSES OF DATA PROCESSING

This Policy applies to CIB UK, which has to ensure that all employees and/or departments having access to personal data have been informed of it (i.e., employees but also interns and contractors - hereafter "CIB UK employees").

This Policy applies to the Processing of all Personal Data (i.e., of employees, candidates, customers, suppliers, distributors, business partners, etc.) implemented by CIB UK.

CIB UK may process Personal Data for the following purposes:

- Screening of clients- KYC (including onboarding and periodic refresh)
- Screening of vendors
- Management of personnel account dealing and outside business interests
- Monitoring of market abuse and insider dealing
- Anti-fraud management
- Prevention, detection, investigation and prosecution of financial crimes (including but not limited to money laundering, terrorism financing, fraud and other financial crimes) in any jurisdiction, identity verification, government sanctions screening and due diligence checks.
- Compliance with applicable local or foreign law, regulation, policy, voluntary codes, directive, judgement or court order, as well as any contractual obligation pursuant to agreements between any member of CIB UK and any authority, regulator or enforcement agency or body or any request coming from said entities.
- Compliance with reporting obligations under Mifid II
- Risk management
- Management of client orders receipt, transmission, execution of clients orders)
- Recruitment management
- On boarding new employee
- Payroll management / salary review
- Personnel administrative file management
- Training management
- Career management
- Whistleblowing.
- Management of Expenses
- Management of Invoices

- Management of vendors/suppliers relationship management
- IT access management
- Security and control of access for visitors
- Organisation of board committees
- Allocation of IT equipment
- Telephony management
- Market research and marketing-related Data Processing

4. STANDARDS FOR PROCESSING PERSONAL DATA

Data Processing shall always respect the principles relating to processing of Personal Data in accordance with the GDPR. As such, Data Processing must be:

4.1 – ACCURATE AND KEPT UP TO DATE

CIB UK must take appropriate steps to ensure that the Personal Data used for Processing is accurate, corrected if necessary, and kept up to date.

4.2 – PROCESSED FOR LIMITED PURPOSES

CIB UK must process Personal Data for specified, explicit, and legitimate purposes. It must not further process the data in a way that is incompatible with said purposes. Specifically, Personal Data must not be processed for secondary purposes without verifying that additional Data Protection requirements have been implemented, such as information or consent from the Data Subject.

4.3 – *RELEVANT AND NOT EXCESSIVE FOR THE PURPOSE OF PROCESSING*

CIB UK must limit the collection of Personal Data to the extent necessary for its business purposes, and in consideration of the rights of the individuals.

4.4 – *LIMITED IN TIME TO WHAT IS NECESSARY FOR THE PURPOSE OF PROCESSING*

CIB UK must not retain Personal Data for a period longer to what is necessary in regards to the purpose for which it was collected and processed.

Personal Data must be saved consistently with legal and business retention requirements. When the maximum retention period required by the applicable law or the retention period required for the purpose of collection is reached, CIB UK must take reasonable steps to destroy the Personal Data.

4.5 – IN LINE WITH THE PRINCIPLE OF TRANSPARENCY

In accordance with the principle of transparency, CIB UK must provide all Data Subjects with an information notice describing the Processing operation (including the contacts details of the entity acting as Data Controller, the contact details of the Data Protection Manager, the purposes of Processing, the recipients of the Personal Data, the storage period of the Personal Data, the rights of the Data Subjects, etc.).

The list of information to be included in the information notice is different where Persona Data has not been obtained directly from the Data Subjects[1].

The information provided must be intelligible and accessible for all the Data Subjects. The information must be presented in a concise, and easily accessible form, using clear and plain language in particular for any information addressed specifically to a child.

4.6 – PROTECTED BY APPROPRIATE SAFEGUARDS

[1] Article 13 and 14 of the GDPR.

When Personal Data is transferred to a Third Country, Transfer must be protected by appropriate safeguards (please refer to section 10 below).

5. LAWFUL PROCESSING OF PERSONAL DATA

5.1 – LAWFUL BASIS OF PROCESSING

At least one of the following lawful bases must applicable in regards to the Processing:

- The Data Subject has consented to the Processing for a specific purpose. This consent shall be revocable at all times;
- Processing is necessary for the execution of a contract to which the Data Subject is party[2]; for instance, Processing for payroll management, in execution of the contract of employment;
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject, such as, among others, compliance with Tax Law or anti-money laundering requirements*;*
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- Processing is necessary either for the performance of a task carried out in the public interest or for the exercise of the official authority vested in the Data Controller; such as, among others, reporting requirements related to fraud prevention and anti-money laundering in accordance with the Crime Act 2002;
- Processing is necessary for the purposes of the legitimate interests pursued either by the Data Controller or a third party. For instance, Processing might be necessary for the completion of a Merger transaction. Such Processing can only be limited in instances where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of Personal Data, in particular where the data subject is a child.

5.2 – LEGAL BASIS FOR THE PROCESSING OF SPECIAL CATEGORIES OF DATA

CIB UK must not process Special Categories of Personal Data unless:

- the Data Subject has given his/her consent in a clear an unequivocal manner (except where the applicable laws prohibit it); or
- Processing is necessary for carrying out the obligations and specific rights of CIB UK acting as Data Controller, in the area of Employment law, provided that said obligations or specific rights are authorized either by Union or national law, or by a collective agreement providing adequate safeguards; or
- Processing is necessary to protect the vital interests of the Data Subject or of another person, where the Data Subject is physically or legally incapable of giving his/her consent; or
- Processing is necessary for the establishment, exercise or defense of existing and potential legal claims; or
- Processing relates to Special Categories of Personal Data that have been made public by the Data Subject himself/herself; or
- Processing is necessary for reasons of substantial public interest;
- Processing is necessary for the assessment of the working capacity of an employee;

[2] or in order to take steps at the request of the data subject prior to entering into a contract

- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes (in accordance with article 89 of the GDPR).

6. MANAGEMENT OF DATA SUBJECTS' RIGHTS

In accordance with the GDPR, Processing shall respect the following rights:

- Right of access;
- Right to rectification;
- Right to erasure;
- Right to restriction of Processing;
- Right to data portability.

In order to obtain more information in regards to your rights as a Data Subject, or the procedure to assert said rights, please refer to the Data Subject's Rights Management Procedure:

Data Subject's Rights Management Procedure

7. LODGING AN INTERNAL COMPLAINT

If you consider that the policy has not been followed regarding your Personal Data, you may lodge a complaint so as to obtain adequate correction measures.

Data Subject's Complaint Management Procedure

8. SECURITY AND CONFIDENTIALITY

CIB UK must implement all appropriate technical and organizational measures to ensure a level of security for the Personal Data appropriate to the risk and, in particular, protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to. The state of the art, the cost of implementation and the sensitivity of information shall be taken into consideration for implementing security measures.

The same level of protection must be contractually imposed by CIB UK on its Processors.

CIB UK employees who, in the course of their work, might have access to Personal Data must agree to hold it in the strictest confidentiality.

For more information, please refer to the Information Security Policy Procedure.

Information Security Policy Procedure

9. PERSONAL DATA BREACH REPORTS

Personal Data Breaches are subject to a notification regime before competent Supervisory Authorities and affected Data Subjects under certain circumstances.

CIB UK must ensure that adequate means are in place to respond to this obligation.

Data Breach Notification Procedure

10. INTERNATIONAL TRANSFERS

CIB UK shall not transfer Personal Data to recipients located in Third Countries unless said Transfer is appropriately secured, for instance:

- The Third Country is deemed with an adequate level of protection by the EU Commission;
- EU Standard Contractual Clauses approved by the EU Commission are signed with the non EU recipients of the Personal Data;
- The recipient is a US company certified Privacy Shield (please note US companies certified "Privacy Shield" are considered by the European Commission as providing an adequate level of Personal Data protection). Please visit the following link to obtain the list of companies which adhered to the Privacy Shield: https://www.privacyshield.gov/welcome.

Personal Data Transfers to Third Parties Procedure

11. ACCOUNTABILITY

In order to demonstrate compliance with the principles set forth in this Policy, CIB UK shall implement the following measures:

11.1 - RECORDS OF PROCESSING ACTIVITIES (DOCUMENTATION)

CIB UK must maintain internal records of Processing activities involving Personal Data[3]. These records must be available to any competent Supervisory Authority for purposes of an investigation.

11.2 - DATA PROTECTION BY DESIGN AND BY DEFAULT

CIB UK must implement appropriate technical and organizational measures designed to implement data protection principles in an effective manner and integrate the necessary safeguards into the Processing in order to meet Data Protection requirements and protect the rights of the Data Subjects, at the time of conception and during the Processing itself.

In addition, systems and technology implemented and used by CIB UK shall be designed in such a way so as to ensure that by default: (i) Processing is limited to what is necessary for the purposes for which the Personal Data was collected; and (ii) only the recipients who need to access the Personal Data can do so. Restricting access to Personal Data, pseudonymisation and anonymisation are appropriate measures participating to demonstrate Data Protection by design and by default.

11.1 - DATA PROTECTION IMPACT ASSESSMENTS

CIB UK must carry out Data Protection Impact Assessments (or DPIAs) when Processing is likely to result in a high risk to the rights and freedoms of Data subjects[4].

DPIAs are an assessment of a Processing of Personal Data that identifies the impact that Processing might have on the rights and freedoms of Data Subjects, and sets out recommendations for managing that impact.

12. TRAINING PROGRAMS AND TOOLS AVAILABLE

In order to facilitate compliance with applicable Data Protection obligations, a series of procedures and policies have been implemented in CIB UK**.**

[3] See Article 30 of the GDPR.

[4] More particularly when (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, or of Personal Data relating to criminal convictions and offences; or a systematic monitoring of a publicly accessible area on a large scale (see article 35 of the GDPR).

Appropriate training has to be carried out for any CIB UK employee.

13. AUDIT PROGRAMS

Data Protection audits shall be carried out by CIB UK on a regular basis (at least every year, subject to more stringent local applicable law) by internal or external accredited audit teams. These audits must be carried out in accordance with the general CIB UK audit methods and in collaboration with the internal audit teams.

GDPR Compliance Checklist

14. POWER OF THE SUPERVISORY AUTHORITIES AND SANCTIONS

The Supervisory Authorities have the power to request documents and information from CIB UK such as records of Processing activities[5] or any other document which demonstrates Data Protection compliance[6] in order to conduct investigations.

Any appropriate disciplinary sanction may be imposed, in accordance with local law and internal rules, on employees involved in a Data Breach violation.

15. YOUR POINT OF CONTACT

For any questions on this Policy, please contact the Data Protection Manager.

16. APPLICATION DATE AND AMENDMENT

This policy is reviewed annually by the Data Privacy Manager (in consultation with departments as may be appropriate) to ensure it is achieving its stated objectives.

[5] Article 30.4 of the GDPR.
[6] Articles 5.2 and 24 of the GDPR.