

September 2018

# **SIB (Cyprus) Limited DATA PROTECTION POLICY**

# Contents

<b>PREAMBULE .....</b>	<b>3</b>
<b>1. DEFINITIONS.....</b>	<b>3</b>
<b>2. PURPOSE OF THIS POLICY .....</b>	<b>3</b>
<b>3. SCOPE OF THIS POLICY AND MAIN PURPOSES OF DATA PROCESSING .....</b>	<b>4</b>
<b>4. STANDARDS FOR PROCESSING OF PERSONAL DATA .....</b>	<b>4</b>
<b>5. LAWFUL PROCESSING OF PERSONAL DATA .....</b>	<b>5</b>
<b>6. MANAGEMENT OF DATA SUBJECTS' RIGHTS.....</b>	<b>6</b>
<b>7. LODGING AN INTERNAL COMPLAINT.....</b>	<b>6</b>
<b>8. SECURITY AND CONFIDENTIALITY .....</b>	<b>7</b>
<b>9. PERSONAL DATA BREACH REPORTS .....</b>	<b>7</b>
<b>10. INTERNATIONAL TRANSFERS .....</b>	<b>7</b>
<b>11. ACCOUNTABILITY.....</b>	<b>7</b>
<b>12. TRAINING PROGRAMS AND TOOLS AVAILABLE.....</b>	<b>8</b>
<b>13. AUDIT PROGRAMS .....</b>	<b>8</b>
<b>14. POWER OF THE SUPERVISORY AUTHORITIES AND SANCTIONS.....</b>	<b>8</b>
<b>15. YOUR POINT OF CONTACT .....</b>	<b>8</b>
<b>16. APPLICATION DATE AND AMENDMENT .....</b>	<b>8</b>

## PREAMBULE

As a business and an employer, SIB (Cyprus) Limited (hereafter "SIB CY") collects and processes various personal data from employees, candidates, customers (which include individuals and representatives/contacts from corporate clients), suppliers, distributors and other business partners. SIB CY 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 SIB CY'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 SIB CY when they process Personal Data as well as the rights for Data Subjects whose Personal Data is being processed. The GDPR also provides for specific sanctions for entities processing Personal Data in case of infringements.

## 1. DEFINITIONS

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

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

**"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.

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

**"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.

**"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.

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

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

## 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 SIB CY pursuant to GDPR.

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 Privacy Manager.

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

This Policy applies to SIB CY, 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 "SIB CY employees").

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

SIB CY may process Personal Data for the following purposes:

- Screening of clients - KYC (including onboarding and periodic refresh)
- Screening of vendors
- Management of personal 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 code, directive, judgement or court order, as well as any contractual obligation pursuant to agreements between any member of SIB CY and any authority, regulator or enforcement agency or body or any request coming from the said entities
- Compliance with reporting obligations under relevant directives (e.g. MiFID II)
- Risk management
- Management of client orders (receipt, transmission and execution of clients orders)
- Recruitment management
- On-boarding of a 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
- IT access management
- Security and control of access for visitors
- Organisation of board committees
- Allocation of IT equipment and software
- Telephony management

The above list is an indicative non-exhaustive one.

### **4. STANDARDS FOR PROCESSING OF 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*

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

#### *4.2 PROCESSED FOR LIMITED PURPOSES*

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

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

SIB CY 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*

SIB CY 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, SIB CY 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, SIB CY 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 Personal Data has not been obtained directly from the Data Subjects<sup>1</sup>.

The information provided must be intelligible and accessible for all the Data Subjects.

#### *4.6 PROTECTED BY APPROPRIATE SAFEGUARDS*

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 be 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<sup>2</sup>; 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;

---

<sup>1</sup> Article 13 and 14 of the GDPR.

<sup>2</sup> or in order to take steps at the request of the data subject prior to entering into a contract

- 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*

SIB CY must not process Special Categories of Personal Data unless:

- the Data Subject has given his/her consent in a clear and unequivocal manner (except where the applicable laws prohibit it); or
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject, such as, among others, compliance with anti-money laundering requirements;
- Processing is necessary for carrying out the obligations and specific rights of SIB CY 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;
- 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:

## **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. Please refer to Data Subjects' Complaint Management Procedure.

## 8. SECURITY AND CONFIDENTIALITY

SIB CY 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 SIB CY on its Processors.

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

## 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.

SIB CY must ensure that adequate means are in place to respond to this obligation. Please refer to Data Breach Notification Procedure.

## 10. INTERNATIONAL TRANSFERS

SIB CY shall not transfer Personal Data to recipients located in Third Countries unless the 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>.

## 11. ACCOUNTABILITY

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

### *11.1 RECORDS OF PROCESSING ACTIVITIES (DOCUMENTATION)*

SIB CY must maintain internal records of Processing activities involving Personal Data<sup>3</sup>. These records must be available to any competent Supervisory Authority for purposes of an investigation.

### *11.2 DATA PROTECTION BY DESIGN AND BY DEFAULT*

SIB CY 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 SIB CY 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

---

<sup>3</sup> See Article 30 of the GDPR.

Personal Data, pseudonymisation and anonymisation are appropriate measures participating to demonstrate Data Protection by design and by default.

### *11.1 DATA PROTECTION IMPACT ASSESSMENTS*

SIB CY 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<sup>4</sup>.

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 SIB CY.

Appropriate training has to be carried out for all SIB CY employees.

## **13. AUDIT PROGRAMS**

Data Protection audits shall be carried out by SIB CY on a regular basis by internal or external accredited audit teams. These audits must be carried out in accordance with the general SIB CY audit methods and in collaboration with the internal audit teams.

## **14. POWER OF THE SUPERVISORY AUTHORITIES AND SANCTIONS**

The Supervisory Authorities have the power to request documents and information from SIB CY such as records of Processing activities<sup>5</sup> or any other document which demonstrates Data Protection compliance<sup>6</sup> 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 Privacy 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.

---

<sup>4</sup> 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).

<sup>5</sup> Article 30.4 of the GDPR.

<sup>6</sup> Articles 5.2 and 24 of the GDPR.