Sumitomo Mitsui Trust Bank (Luxembourg) S.A.

General Data Protection Regulation Policy

1. Introduction

1.1. Purpose of this Policy - Privacy by Design and by Default

This Policy sets out the SMTB Luxembourg (The Bank)'s framework which allows it to comply with the General Data Protection regulation (GDPR)[1]. This will be achieved by controlling and/or processing personal data using technical and organisational measures that ensure its protection.

1.2. General Data Protection Regulation

The GDPR is the European Union (EU) regulation which sets out the rights of individuals and principles[2] for personal data management. The fine for failure to comply with the regulation is up to €20 million or 4% of global annual turnover, whichever is higher. It comes into force on 25th May 2018.

The Bank is accountable for compliance with the GDPR to the supervisory authorities, namely the Commission de Surveillance du Secteur Financier (CSSF) and the Commission Nationale pour la Protection des Données (CNPD and, together with the CSSF, the Regulators).

1.3. Application of GDPR

The GDPR applies to any company that is a controller[3] and/or processer[4] which processes personal data[5] of an individual who is a resident in the EU. Even if a company is based outside of the EU, if the company is a controller and/or a processer of personal data of an individual who is resident in the EU, the company is required to adhere to the regulation.

Therefore, any entity within the SMTB Group (the Group) must comply with certain elements of the GDPR if it controls and/or processes[6] personal data of an individual who is resident in the EU.

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN)

[2] Article 5 of GDPR (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN)

[3] A "Controller" is defined in Article 4 of GDPR as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."

[4] A "processor" is defined in Article 4 of GDPR as a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."

[5] "Personal Data" is defined in Article 4 of GDPR as "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."

[6] "Processing" is defined in Article 4 of GDPR as "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."

This means that, among other things, all entities within the Group must comply with the stipulations on intra group transfers and execute the Intra Group Transfer Agreement (IGTA) (see below).

1.4. SMTB Group Global GDPR Policy

In order to comply with the regulation, the Group has established an SMTB Group Global GDPR Policy known as the "EU GDPR Implementation Rule" which sets out the Group's standard approach and compliance with the regulation and is consistent with this Policy.

1.5. The Bank's Vision

Recognising the significance of GDPR to the Bank, our vision is to accomplish a commensurate response to GDPR taking into account the nature and size of the Bank's business, incorporating systems, policies and controls into the framework of daily activity.

1.6. Intra Group Transfer Agreement

As referred to above, personal data cannot be transferred outside of the EEA without certain safeguards, the most appropriate available to the Group being to sign up to standard contractual clauses. These have been drafted by the EU and are designed to protect the privacy rights of data subjects within the EEA. These clauses are found in the IGTA which has been executed by each Group member and thereby legalises the transfer of personal data within the Group.

2. Personal Data Classification

Based on the nature of the Bank's business, the Bank classifies personal data into three categories, as explained below. Classifying personal data allows the Bank to identify high risk areas of personal data and implement an appropriate control framework in keeping with the Bank's vision.

The Bank provides wholesale banking and global markets services. For these business purposes, the Bank holds limited amounts of personal data as follows:

- Wholesale banking and global markets clients business contact details
- Ancillary business contact details
- Personal data required to conduct the businesses (e.g. AML/KYC/CDD related)
- Employee's personal data

2.1 General Personal Data

Definition: personal data which is neither Sensitive Personal Data nor High Risk Personal Data (see below); notification of a data breach in relation to which is required to be made to the Regulators within 72hrs of having become aware of it unless the breach is unlikely to result in a risk to the rights and freedoms of a data subject. Examples of General Personal Data are:

- Name
- Address (work)
- Telephone (work)
- Email address (work)
- Social networking details: Facebook, Twitter, etc (work)
- Professional bio (of Senior Management/business contacts – not a CV)

It is in the Bank's normal course of business to process this type of data. It is unlikely that the Bank will receive any kind of request from a data subject to disclose, amend or delete this type of personal data.

2.2 High Risk Personal Data

Definition: personal data that is neither Sensitive Personal Data nor General Personal Data; notification of a data breach in relation to which is required to be made to the data subject without delay, and to the Regulators without delay an in any event within 72hrs of having become aware of it. Examples of High Risk Personal Data are:

- Address (home)
- Telephone numbers (home/personal mobile if not on business card)
- Email address (personal)
- Social Networking details: Facebook, Twitter, LinkedIn etc
- Age
- Date of birth
- National Insurance/Tax code
- Bank Account
- Passport number and photo
- CV (used for recruitment purposes)
-

This data is held by the Bank mainly for human resources or KYC/CDD purposes. The Bank has established strict rules on internal data management of High Risk Personal Data which are as follows:

- Must only be held by the GA Department and subject to the retention policy
- Any other member of the Bank receiving AML/KYC/CDD High Risk Personal Data must transfer it to GA as soon as practicable and delete all records of it immediately

2.3 Sensitive Personal Data[7]

Definition: as defined in GDPR Article 9(1) "Special categories of personal data"; may require greater technical and organisational measures to be put in place before processing if necessary; the notification regime is the same as for High Risk Personal Data. Examples of Sensitive Personal Data are:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation
- Data concerning children under 16 years old (Article 6(1)(f))

[7] This is equivalent to "special categories of personal data" in Article 9 of GDPR

This data is held by the Bank in the GA Department and the senior management of the Bank who require the information for the purposes of managing the Bank. It will not be held by any other person within the Bank.

3. Bank GDPR Breach Protocol[8]

The procedure for responding to a breach incident is stipulated in Section 2-1-6 Operational Incident Reporting (Bank-wide Procedure Manual).

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

If the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the Bank shall notify the Breach to the supervisory authority, where feasible, within 72 hours after having become aware of it.

If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.[9]

A breach incident must be recorded regardless of whether the supervisory authority was notified.

4. Fair Processing Notices

A Fair Processing Notice is required by Articles 12-14 to be provided to a data subject in order to provide accessible information about how the Bank will use their personal data

5. Subject Access Requests (SARs)

The Bank is required to respond to the request without undue delay and in any event within one month from receipt of the request.

6. Lawful basis of processing under GDPR

In order for any business area in the Bank to control and/or process personal data, it must have a valid lawful basis to collect and process such data, and it must be able to demonstrate that a lawful basis applies.

[8] 'Personal data breach' is defined in Article 4 of the GDPR. It means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

[9] The communication to the data subject is not required if the exemptions in Article 34-3 of GDPR are met.

The lawful bases for processing personal data by the Bank are one or more of the following set out in Article 6(1):

- Processing is necessary for the performance of a contract (Article 6(1)(b))
- Processing is necessary for compliance with a legal obligation (Article 6(1)(c)
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (Article 6(1)(e))

7. Governance

7.1 Bank Departments

Each head of department in the Bank is responsible for personal data management held in their department. This includes the accuracy of records registered in the GDPR Register.

In addition each department is also responsible for providing any information required in order to comply with a data request received for their department in the event of a SAR.

7.2 Information Security Officer (ISO)

The MD will be responsible for incorporating GDPR into the existing information security management framework, ensuring that personal data remains protected and accessed by authorised personnel only, conducting annual risk assessments, supporting breach management processes and promoting employee awareness through annual training on the GDPR.

7.3 GA Department

The GA Department is responsible for:

- Collaborating with Head Office on the review and maintenance of Head Office Global GDPR Policy
- Collaborating with Head Office on the review and maintenance of Intra Group Data Transfer Agreement
- Coordinating the maintenance of this Policy
- Coordinating the consistency of this Policy to the Head Office Global GDPR Policy
- Monitoring the Bank's compliance with GDPR
- Being the point of contact for the Regulators on GDPR matters
- Being the point of contact for GDPR matters internally

7.4 Customer Data Protection

It is critical to our business that the Bank is able to use personal data to conduct business with, and provide banking services to, customers, and manage our overall relationship with customers, as well as to provide information about new products and services that may be of relevance to the customer's business needs. In order to continue to be able to do so, customer's personal data must be controlled and processed with the utmost care, particularly High Risk Customer Data. Examples of High Risk Customer Data that the Bank processes relate to Anti-Money Laundering, Know your Client and Customer Due Diligence.

7.5 Employee Data Protection

Personal Data that are classified as High Risk Personal Data and Sensitive Personal Data must be controlled and processed with utmost care and within a strict management framework. The

Employee Data Policy summarises and describes how the Bank collects and uses personal information.

7.6 Information Security

Personal data must be controlled and/or processed in a manner that ensures its security. Under the management of the GA, information security aspects of personal data are set out in the policies and procedures.

7.7 Retention

Personal Data must not be retained longer that is necessary for the purpose for which it was obtained. The retention rules for personal data are stipulated in the Data Retention Policy.

7.8 Third party contracts

It is important to ensure that the counterparties with whom the Bank has a contract adhere to the GDPR where they are processing Bank personal data. This includes the third parties to which the Bank outsources a service. The Bank has set out a procedure to ensure third parties' compliance with the regulation. The procedure is set out in Outsourcing Operations procedure.

7.9 Monitoring

It is the responsibility of the Risk Management team to monitor the Bank's compliance with the GDPR as a second line of defence.

7.10 Audit

It is the responsibility of the Internal Audit Department to monitor the Bank's compliance with the GDPR and report the results to Management as a third line of defence.

8. Training and Contact

Training to all existing staff of the Bank will be conducted on an annual basis. The training will be managed by the GA. Training to all new staff will be provided by the GA Department upon joining the Bank. For any queries regarding the GDPR staff can contact the GA Departments for further advice.

END