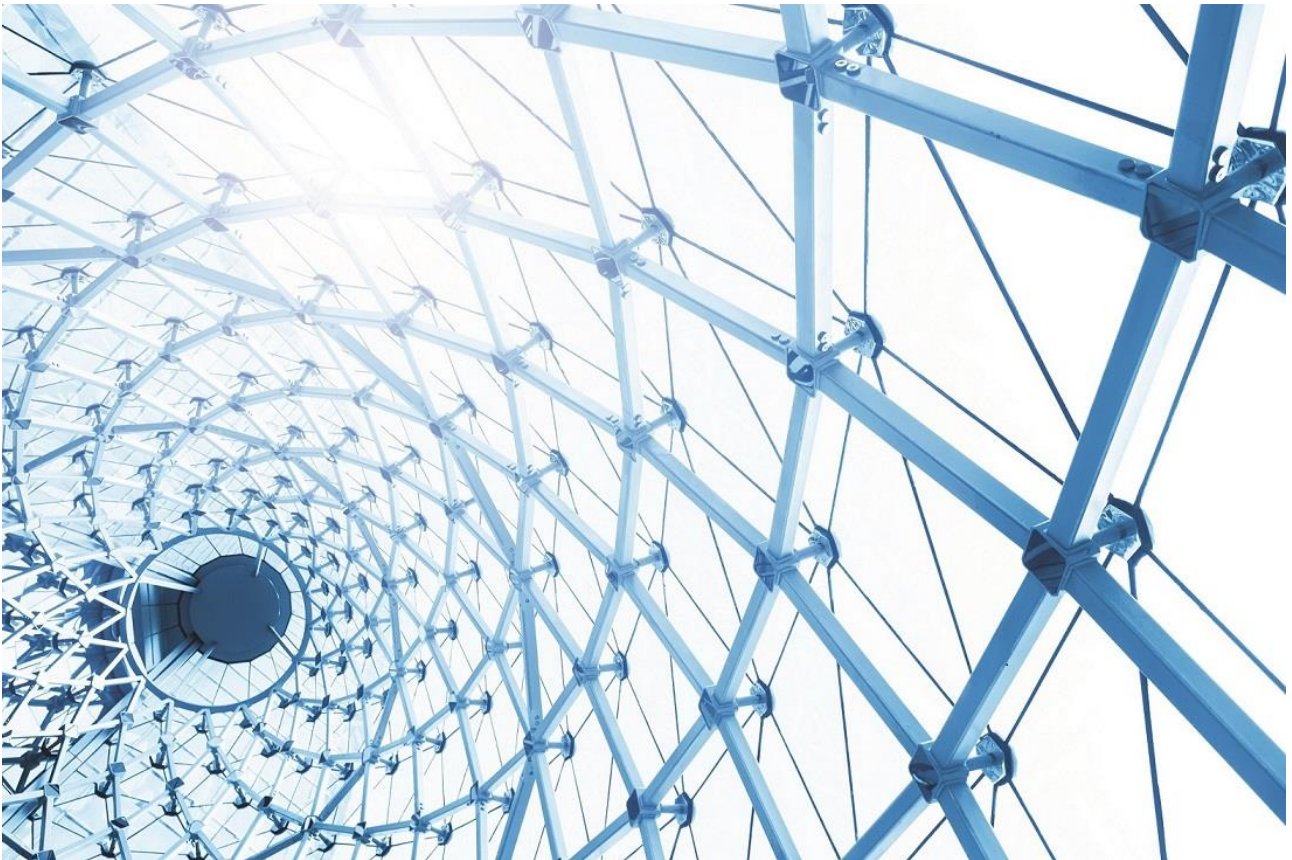




BOSWME GDPR Policy

BOS Wealth Management Europe S.A.

Approved by BOSWME Board of Directors



February 2024

Version No. 4

Owner: DPO

Author: Dorin Draghici

Review Cycle: Annually

Document Change Record

Date	Version	Updated By	Change Details
07/10/2019	1	Compliance	1 st version
16/09/2021	2	Compliance	Annual review, no changes
15/11/2021	3	Compliance	Annual review, references to the UK Branch added
02/02/2024	4	Compliance	Annual review, HACA clarifications and additions

Document Version Control	
Document owner	BOSWME DPO
Version (Effective Date)	15.02.2024
Recommended by:	BOSWME DPO represented by the Compliance function
Reviewed by:	BOSWME Head of Compliance
Endorsed by:	NA
Approved by:	BOSWME ERC BOSWME Board of Directors

Contents

1.	Introduction.....	4
1.1.	Purpose.....	4
1.2.	Definitions.....	4
2.	Core Principles of data processing	5
3.	Records of processing activities	6
3.1.	Data Processing Register	6
3.2.	Transfer to third countries	6
4.	Rights of the Data Subject	7
5.	Data Protection Officer/ Contact for Data Protection Matters	7
6.	Data Breach	8

1. Introduction

1.1. Purpose

The purpose of this policy (the "**Policy**") is to ensure and be able to demonstrate that any processing of personal data performed by BOS Wealth Management Europe S.A. ("**BOSWME**"), in its capacity of Data Controller (as defined in the section 1.1. below) and within the context of its activity, is carried out in accordance with the following applicable data protection regulation and law:

- 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 ("**General Data Protection Regulation**" or "**GDPR**");
- Luxembourg Law of 1st August 2018 on the organisation of the National Data Protection Commission (the "**CNPD**") and the general data protection framework;
- any recommendations, guidelines issued by the CNPD;
- any other applicable data protection regulation, law, guidelines which may amend, replace, or supersede from time to time the above.

In the context of the branch of BOSWME (the "**UK Branch**") established in the United Kingdom, the applicable data protection regulation and law will be understood as the UK General Data Protection Regulation (the "**UK GDPR**") and the Data Protection Act 2018, and any recommendations, guide, guidelines provided by the Information Commissioner's Office (the "**ICO**").

The Policy should be read in conjunction with the applicable BOSWME data privacy notices and is a supplement to BOS General Personal Data Protection Policy, which should also be read in conjunction with this Policy.

1.2. Definitions

Articles 4 and 9 of the GDPR or UK GDPR define some key concepts which can be summarised as:

Anonymisation means removing personal identifiers, aggregating data, or processing this data in a way that it can no longer be related to an identified or identifiable individual

Controller means 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;

Personal data means any information relating to an identified or identifiable natural person (the "**Data subject**");

Personal data breach 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;

Processing means any operation or set of operations which is performed on personal data (collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, restriction, erasure, destruction);

Processor refers to a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller;

Pseudonymisation means processing of personal data in such a manner that the personal can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately;

Special category data refers to personal data consisting of or regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life or sexual orientation.

2. Core Principles of data processing

The data protection core principles are stated in Article 5 of the GDPR and Chapter 2 of the Data Protection Act 2018.

The personal data will be:

PRINCIPLE	DESCRIPTION
1. Lawfulness, fairness, and transparency	processed lawfully, fairly, and in transparent manner in relation to the Data Subject.
2. Purpose limitation	collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes
3. Data minimisation	adequate, relevant, and limited to what is necessary in relation to the processing purposes
4. Accuracy	accurate and, where necessary, kept up to date
5. Storage limitation	kept in a form that permits identification of Data Subject for no longer than is necessary for the purposes for which the personal data is processed
6. Integrity and confidentiality	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 measure, anonymisation or pseudonymisation of data

To fulfil its obligations, insofar as is necessary, and considering that such processing is not prohibited, BOSWME may process sensitive data, such as:

- information on a Data Subject's criminal record or convictions;
- health and medical data such as the number of sick days and the information contained in a doctor's certificate/medical certificate, information on work-related accidents, information on disability, and information on maternity leave;
- information contained in the marriage/civil partnership certificate; and
- holding of public office or political/non-governmental organisations' affiliations.

3. Records of processing activities

3.1. Data Processing Register

BOSWME has put in place a register of processing activities (the “**Data Processing Register**”) which is a live document subject to regular reviews and updates. The Data Processing Register contains all information requested as per the Article 30 of GDPR, such as the purposes of the processing activities, the categories of Data Subjects and of the personal data that might be collected from Data Subjects while performing its processing activities. It also contains information about the retention period, transfers to third countries, as well as technical and organisational security measures.

 applicable BOSWME [Data Processing Register](#), incl. BOSWME, UK Branch format

3.2. Transfer to third countries

The Data Processing Register referred in the above section also contains information in relation to the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries.

BOSWME is part of a wider global group which include Bank of Singapore Limited (established in Singapore) and its parent Oversea-Chinese Banking Corporation Limited (“**OCBC Bank**” - established in Singapore) and their respective affiliates. In such context, BOSWME may transfer some personal data to a third country, including locations which may not have the same level of protection of personal data as in the EU or the UK. Information about such transfers of personal data is further detailed in the data privacy notices and the Data Processing Register.

Such third countries are Singapore, Hong Kong and their offices located in Philippines, Malaysia, and Dubai. Despite the existence of comprehensive data protection laws in Singapore and Hong Kong, these countries are not part of the limited list of countries offering an adequate level of protection of personal data set out by the European Commission and/or the UK Parliament. For this reason, BOSWME, acting as data controller, has taken all reasonable steps necessary to ensure that the personal data is treated securely and in accordance with this Policy, data privacy notices as well as applicable data protection laws, including, where relevant, by entering into EU standard contractual clauses (the “**SCCs**”) with the party outside the EEA (available [here](#) for the UE and [here](#) for the UK).

In case BOSWME shares personal data with receiving group entities, it is our policy to limit the categories of individuals who have access to that personal data based on a need-to-know principle to the extent necessary to perform their obligations and responsibilities.

Furthermore, the SCCs are part of the Internal Group Data Transfer Agreement (the “**IGDTA**”) signed between BOSWME and BOS and OCBC.

These receiving entities will also monitor the compliance by their sub-contractors with the terms of their contractual arrangements. BOSWME may also transfer personal data to third parties such as governmental or regulatory agencies in or outside the EU and/or UK, in accordance with applicable laws and regulations.

For any other data transfer to third countries, the above EU or UK standard contractual clauses will be inserted in the contract/agreement to be entered between BOSWME and the third-party providers.

4. Rights of the Data Subject

- a. **Access.** The Data Subject has the right to request a copy of the personal data we are processing about you. In case of a request, BOSWME will provide you with the information on purposes of the processing, categories of data concerned, recipients to whom the data are disclosed, retention period. For your own privacy and security, at our discretion we may require you to prove your identity before providing the requested information.
- b. **Rectification.** The Data Subject has the right to have incomplete or inaccurate personal data that we process about you rectified.
- c. **Deletion.** The Data Subject has the right to request that we delete personal data that we process about you, except we are not obliged to do so if we need to retain such data in order to comply with a legal obligation or to establish, exercise or defend legal claims.
- d. **Restriction.** The Data Subject has the right to restrict our processing of your personal data where you believe such data to be inaccurate; our processing is unlawful; or that we no longer need to process such data for a particular purpose unless we are not able to delete the data due to a legal or other obligation or because you do not wish for us to delete it.
- e. **Portability.** The Data Subject has the right to obtain personal data we hold about you, in a structured, electronic format, and to transmit such data to another data controller, where this is (a) personal data which you have provided to us, and (b) if we are processing that data on the basis of your consent or to perform a contract with you.
- f. **Objection.** Where the legal justification for our processing of your personal data is our legitimate interest, the Data Subject has the right to object to such processing on grounds relating to your particular situation. We will abide by your request unless we have compelling legitimate grounds for the processing which override your interests and rights, or if we need to continue to process the data for the establishment, exercise or defence of a legal claim.
- g. **Withdrawing Consent.** If a Data Subject has consented to our processing of its personal data, data subject has the right to withdraw his/her consent at any time, free of charge. This includes cases where he/she wishes to opt out from marketing messages that you receive from us.

The Data Subject can make a request to exercise any of these rights in relation to his/her personal data by sending the request to Data Protection Officer.

 applicable BOSWME [Data Subject Request Procedure](#) & [Data Subject Request Register](#), incl. BOSWME, UK Branch formats

Data privacy notices provide detailed information on the categories of data that BOSWME collects about its employees, clients, and vendors, as well as on the purpose and legal bases for such processing.

5. Data Protection Officer/ Contact for Data Protection Matters

BOSWME appointed a Data Protection Officer (the "DPO"), which can be contacted at:

Data Protection Officer, by email to dpo@boswm.com or by letter to:

- For BOSWME – The Data Protection Officer, BOS Wealth Management Europe S.A., 33 Rue Sainte Zithe, L-2763 Luxembourg, Luxembourg
- For BOSWME, UK Branch – The Data Protection Officer, BOS Wealth Management Europe S.A., UK Branch, The Rex Building, 3rd Floor, | 62 Queen Street, London EC4R 1EB.

The DPO will notably:

- Inform and advise the controller or the processor and the employees on their obligations;
- Be involved in any questions pertaining to data issues;
- Monitor compliance with the Regulation, the Controller/Processor's policies, and Member States data protection provisions;
- Act as a point of contact for the authorities among others.

6. Data Breach

☰ applicable BOSWME Personal Data Breach & Incident Procedure & Data Breach Register (incl. BOSWME, UK Branch formats)

- Personal data breach can result both from accidental and deliberate causes which are likely to result in a risk to the rights and freedoms of natural persons. This includes risks like financial loss, breach of confidentiality, discrimination, reputational damage, or other significant economic or social disadvantages.
- Every data breach or an incident which might lead to a breach has to be recorded by BOSWME within a registry detailing the facts relating to the incident / breach, its effects, and the remedial actions taken. These are also documented appropriately using the ☰ applicable BOSWME Data Breach Assessment form (incl. BOSWME, UK Branch format).
- BOSWME as data controller has an obligation to notify a CNPD (or ICO in the UK, as applicable) of a data breach without undue delay and where feasible within 72 hours of discovery of a breach. Late notifications will have to be accompanied by a reasoned justification for the delay. The notification includes information on the breach itself, the measures taken to fix it, and possible consequences.
- Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller will in most cases communicate the personal data breach to the data subject without undue delay. Otherwise, if BOSWME has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the data breach (i.e., measures that render the data unintelligible to any person who is not authorised to access it, such as encryption), the high risk to the rights and freedoms of data subjects is likely to be mitigated. In such cases, notifying the data subjects may not be necessary.

Also, if notifying the data subjects would involve a disproportionate effort to notify each affected individual, public communication or a similar measure may be used instead.