

BEMO Europe Market Abuse Policy

Publication Date: April 2024

Table of Contents

1	INTRODUCTION	3
2	DEFINITIONS	3
3	SCOPE	6
4	LEGAL FRAMEWORK	6
5	RULES AND EXCEPTIONS	7
5.1	Insider dealing	7
5.2	Disclosure and Unlawful disclosure of insider information	7
5.3	Market manipulation	7
6	MEASURES TO PREVENT AND DETECT MARKET ABUSE	8
6.1	List of insiders and central register	8
6.1.1	Responsibility to notify regarding insider status	8
6.1.2	Responsibility to maintain insiders list.....	9
6.1.3	Handling of inside information by its owner.....	9
6.2	Compliance responsibilities	9
6.3	Market abuse detection measures	10
6.3.1	Monitoring system	10
6.3.2	Investigation of suspicious transactions	10
6.3.3	Suspicious Transactions and Orders Reporting	10
7	GOVERNANCE	11
7.1	First line of defence	11
7.2	Second line of defence	11
7.3	Third line of defence	11
8	TRAINING	11
9	NON-COMPLIANCE WITH THE POLICY	12
10	OWNERSHIP AND REVISION PERIOD	12

1 Introduction

BEMO EUROPE BANQUE PRIVÉE (hereafter referred as “BEMO” or the “Bank”), is a public limited company governed by the law of the Grand-Duchy of Luxembourg. It is registered with the Registre de Commerce et des Sociétés de Luxembourg under number B176452, with its registered office at 26, Boulevard Royal, L-2449 Luxembourg.

The Bank is authorized by the CSSF to carry out their activities pursuant to Article 2 of the Law of 5 April 1993.

BEMO EUROPE with the agreement of the CSSF and the ACPR has a branch in France, denominated as BEMO EUROPE BANQUE PRIVÉE – Succursale de Paris (“Branch”). It is registered under RCS number 998269518 / CIB 17619 with its registered office at 63, Avenue Marceau, 75116 Paris.

BEMO is committed to preserving market integrity and public confidence in financial markets by preventing and detecting market abuse.

The purpose of this Market Abuse Policy (hereinafter referred to as the “Policy”) is to set up a framework and minimum requirements for BEMO for preventing, detecting and reporting market abuse. Non-compliance with market abuse rules could entail a risk of reputation and of administrative and penal sanctions for BEMO and its employees. Consequently, the participation of any employee in any activity described in this Policy as strictly prohibited will result in appropriate internal sanctions in addition to other possible regulatory or legal sanctions.

BEMO should regularly (at least annually), assess and update, if necessary, systems and procedures to detect and report the suspicious orders/transactions.

This Market Abuse Policy has been prepared in order to provide common standards for the prevention, detection and reporting of market abuse and to comply with the legal requirements as described in Section 4.

2 Definitions

Term	Definition
Market Abuse Regulation (MAR)	Regulation (EU) 596/2014 of the European Parliament and of the Council of 16 April 2014 on Market Abuse.
Market Abuse	Unlawful behaviour in financial markets which prevents full market transparency and created an unfair advantage for an individual exercising the behaviour.
Inside information	Inside information is information: <ul style="list-style-type: none"> - Of a precise nature (information is considered as precise when it indicates circumstances or events which have occurred or which may occur, in such a manner as to have an effect on the prices of the financial instruments); - Which has not been made public;

	<ul style="list-style-type: none"> - Which relates, directly or indirectly, to listed financial instruments or issuers of listed financial instruments; - And which, if it were made public, would be likely to have a significant effect on the prices of those financial instruments or related derivatives (information may have a significant effect on the prices of financial instruments when a reasonable investor would be likely to use this information as a basis of his investment decision).
Insider	<p>Individuals who have access to insider information and/or who are working for such under a contract of employment, or otherwise performing tasks through which they have access to inside information.</p> <p>An insider is a person who has obtained the inside information through:</p> <ul style="list-style-type: none"> - His position in the management of the issuer (management or supervisory bodies of the issuer); - His holding in the capital of the issuer (shareholder); - His profession or his duties (lawyer banker, auditor...); - Criminal activity; - Other circumstances in which the person knows or should know that it is inside information.
Insider dealing	<p>Insider dealing means:</p> <ul style="list-style-type: none"> - Possessing and using inside information: <ul style="list-style-type: none"> • To acquire/dispose of (or to attempt to acquire/dispose of), for his/her own account or for the account of a third party, directly or indirectly, financial instruments to which the information is related; or • To cancel/amend an order if the order was placed before the person possessed the inside information; • To recommend, on the basis of that information, to another person to acquire/dispose of financial instruments or to cancel/amend an order. - Using a recommendation to give/amend/cancel orders or carry out transactions when the person knows or should know that this recommendation is based on inside information. <p>Exemptions:</p> <p>Legitimate behaviour as defined by the Regulation on market abuse is not considered as insider dealing:</p> <ul style="list-style-type: none"> - Where market makers, counterparties or brokers acquire/dispose financial instruments on behalf of third parties in the course of the exercise of their professional functions; - Where the transaction is the discharge of an eligible obligation and that obligation results from an order or an agreement concluded before the concerned person has inside information; - Where the person uses information only in order to conduct a public acquisition or merger provided that at the moment of the approval of the acquisition/merger, any inside information has been made public.
Unlawful disclosure	<p>Unlawful disclosure of inside information means:</p>

	<ul style="list-style-type: none"> - Disclosing inside information to another person except where the disclosure is made in the normal exercise of the person's functions as legitimate behaviour, internal control, etc. - Giving recommendations to acquire/dispose of a financial instrument or to cancel/amend an order when the person knows or should know that these recommendations were based upon inside information. <p>Exemptions:</p> <ul style="list-style-type: none"> - Disclosure of inside information in the exercise of professional functions provided that the receiver of the inside information has a need to know in order to perform his/her professional function e.g. employee of an internal control function; - Reception of inside information, prior to the announcement of a transaction, in order to gauge the interest of (potential) investors.
Market Manipulation	<p>Any behaviour which:</p> <ul style="list-style-type: none"> - Gives false or misleading signals as to the supply, demand or price of a financial instrument; - Secures the price of a financial instrument at an artificial level, unless such is carried out for legitimate reasons and conform with accepted market practice; - Affects the price of a financial instrument by using a fictitious device; - Disseminates information on a financial instrument through the media in order to give false or misleading signals or to secure its price at an abnormal level when the person knows or should know this information was false or misleading; - Disseminates false or misleading information/input on a benchmark when the person knows or should know the information/input was false or misleading.
Insiders List	A list maintained by the Bank of individuals who have access to the insider information.
Reasonable investor	An investor, who bases their investment decision on information already available publicly at the time of such investment decision.
Research disclosure	Disclosure by an individual responsible for research.
Market Sounding	Act of communicating information before a transaction is announced in order to measure potential interest from prospective investors.
Disclosing market participant	Individual that performs Market Sounding as described above.
MTF	Multilateral Trading Facility
eRIIS	Electronic Reporting of Information concerning Issuers of Securities platform managed by the CSSF.
Financial instrument	Instrument as defined by the Annex I – Section C of the Directive 2014/65/EU of the European Parliament of 15 May 2014 on markets in financial instruments.
Securities	Includes:

	<ul style="list-style-type: none"> - Shares and other securities equivalent to shares; - Bonds and other forms of securitised debt; - Securitised debt convertible or exchangeable into shares or into securities equivalent to shares.
STOR	Suspicious Transactions and Order Report.

3 Scope

This Policy shall apply to all employees of the Bank and the Branch and covers:

- Financial instruments (which include emissions allowances and derivative instruments) admitted to trading on regulated markets, multilateral trading facilities and organised trading facilities;
- Transactions, orders, behaviours, conduct, actions or omissions which could have an effect on the price, value, supply of, or demand for such financial instruments;
- Spot commodity contracts which could potentially impact the price or value of financial instruments;
- Behaviours in relation to benchmarks and auctioning on an auction platform.

4 Legal framework

Jurisdiction	Legislation
European Union	<ul style="list-style-type: none"> • Regulation (EU) No 596/2014 of 16 April 2014 on Market Abuse • Criminal Sanction for Market Abuse Directive (CSMAD)
Luxembourg	<ul style="list-style-type: none"> • The Law of 5 April 1993 on the financial sector as amended • The Law of 23 December 2016 on market abuse implementing the Regulation (EU) n° 596/2014 of European Parliament and of the Council of 16 April 2014 relating to the market abuse (the “Law of 23 December 2016) • CSSF circular 12/552 as amended on Central administration, internal governance and risk management • CSSF Circular 17/648 • CSSF Circular 17/653 • CSSF Circular 22/813
France	<ul style="list-style-type: none"> • Code Monétaire et Financier • Code du Commerce

5 Rules and exceptions

5.1 Insider dealing

It is prohibited to individuals identified as insiders to use insider information as defined in this Policy to:

- Make investment decisions for their own account or that of a third party;
- Make recommendations or inducing other individuals to make an investment decision.

5.2 Disclosure and Unlawful disclosure of insider information

Any relevant person who receives or originates inside information is prohibited from disclosing that information to any other person, except where the disclosure is made on a need-to-know basis as part of the person's normal discharge of his or her professional duties, and provided that:

- a) The intended recipient acknowledges, in writing, the legal and regulatory duties related to being an insider, and the sanctions applicable to insider dealing and the unlawful disclosure of inside information; and
- b) The intended recipient is registered in the relevant insider list as per the relevant market abuse procedure for the setup of such lists.

The above prohibition supplements any professional secrecy or non-disclosure obligation, data protection requirement, or conflict of interest requirement which may otherwise exist, and which may require the creation of specific arrangements, such as segregation of information, segregation of duties, etc.

Where an employee of the Bank knows or should have known that a recommendation or inducement to make an investment decision was based on insider information, it is prohibited to further disclose it.

5.3 Market manipulation

It shall be prohibited to engage in behaviour qualified as market manipulation.

For the purposes of this Policy, the behaviour of market manipulation shall be defined as:

- Entering into a transaction, placing an order or any other behaviour which:
 - o Gives false or misleading cues regarding the supply, demand, or price of a financial instrument;
 - o Secures the price of a financial instrument at an artificial level, unless such behaviour has been carried out for legitimate reasons and conform with an accepted market practice.
- Using a fictitious device or any other form of deception;
- Disseminating information through media in order to give false or misleading cues when the person is aware or should be aware that the information is false or misleading;
- Transmitting false or misleading information or input on a benchmark when the person knows or should know that it is false or misleading and may impact the calculation of a benchmark;
- Behaviours aimed at ensuring a dominant position on the supply/demand of a financial instrument to fix its price and/or to create other unfair trading conditions;

- Placing, cancelling, or modifying orders to manipulate the supply, demand or price of a financial instrument via disrupting the trading system – making it more difficult for other persons to identify real orders – or executing orders to initiate or aggravate a trend;
- Publicly expressing an opinion via media on a financial instrument or its issuer after planning to profit from the impact of the opinion expressed, without disclosing this conflict of interest;
- Buying or selling emission allowances or related derivatives to fix their auction prices at artificial levels or to mislead bidders.

6 Measures to prevent and detect Market Abuse

The current section is only relevant to insiders who have obtained the inside information through:

- Their position in the management of the issuer (management or supervisory bodies of the issuer);
- Their holding in the capital of the issuer (shareholder);
- Their profession or their duties (lawyer banker, auditor...);
- Other circumstances in which the person knows or should know that it is inside information.

Inside information obtained through criminal activities can only be identified by the Compliance department through their monitoring of the business activities, and therefore be reported as required by the regulation.

6.1 List of insiders and central register

To manage appropriate access to inside information, a central register of lists of recipients of inside information (insiders lists) shall be maintained by the Bank. This register will facilitate cross-referencing and shall be updated when appropriated by duly authorised staff members.

Inside information cannot be contained or referred to, in whole or in part, in documents generally accessible to persons other than those on the insiders list and will therefore be stored in secure and restricted areas. Relevant persons accessing this area shall be considered insiders and entered on the appropriate insiders list.

6.1.1 Responsibility to notify regarding insider status

Whenever a person has gained access, or knows about another individual gaining access to insider information, they shall promptly inform the Compliance department of such event and provide the following information:

- Names and identification of insider employees or other individuals qualified as insiders;
- Date and time at which the individual obtain access to the insider information;
- Supplemental information as requested by the Compliance department on an individual basis.

6.1.2 Responsibility to maintain insiders list

The list of insiders shall be maintained by the Compliance department. In particular, the Compliance department shall perform the following functions and activities in relation to the list of insiders:

- Inform individuals listed in the insiders list about the legal and regulatory duties of insiders and about sanctions applicable to insider dealing and unlawful disclosure of information and require acknowledgement from the recipient of such communication;
- Update and review the list of insiders, particularly when:
 - o There is a change in the reason for including a person already in the list of insiders;
 - o A new individual gains access to insider information;
 - o An individual who previously had access to the insider information ceased to have such access.
- Maintain responsibility for recordkeeping of such lists for at least 5 years.

6.1.3 Handling of inside information by its owner

Any relevant person (hereafter the owner), who first receives or originates inside information in the course of his or her working activities, shall manage the appropriate classification and handling of such inside information within the Bank, until either:

- a) There is formal transfer of such duties to another relevant person;
- b) The inside information has been made public/or is declassified; or
- c) The relevant person's mandate, employment or contractual relationship with the Bank comes to an end.

In particular, the owner shall promptly:

- a) Make available in the central register the mandatory details required to maintain inside information and the related insider lists;
- b) Keep such lists and information up to date, and declassify the inside information as soon as it no longer qualifies as inside information.

6.2 Compliance responsibilities

Within the Bank, the Compliance department shall be responsible for maintaining a list of persons discharging managerial responsibilities and closely associated persons.

The Compliance department shall also be responsible for notifying the persons discharging managerial responsibilities regarding their obligation to notify the Bank and the CSSF about their personal transactions on financial instruments.

The list shall include, at the very least, the name of persons discharging managerial responsibilities.

6.3 Market abuse detection measures

6.3.1 Monitoring system

The Bank shall implement systems and controls to monitor the transactions performed by the Bank's and the Branch's employees acting for both themselves and on behalf of their clients. Such systems and controls shall enable the Bank and the Branch to:

- Monitor the trading activity based on predefined scenarios;
- Generate alerts for potentially suspicious transactions. Where such alerts are generated, they shall be further treated by the Compliance department on an individual basis in order to detect actual or attempted insider dealing or market manipulation.

Additionally, systems and control arrangements implemented by the Bank shall be:

- Proportionate to the scale, size, and nature of the Bank's activity;
- Regularly assessed by the Internal Audit function and Compliance department and, where appropriate, updated.

The Bank shall design and implement a specific Alerts Handling Procedure, which shall set forth the rules for the process of handling suspicious transactions alerts, their escalation, and STOR submission.

6.3.2 Investigation of suspicious transactions

All employees of the Bank or the Branch shall be responsible for reporting transactions and orders for which they have reasonable ground to suspect that such orders or transactions represent a market abuse practice.

In such cases, the employees shall alert the Compliance department about their suspicions and provide description of the order or transaction, and the reasons for suspecting that the order or transaction constitutes market abuse practice.

Where alert has been system-generated or has been notified by an employee, the Compliance department shall investigate such alert. The investigation of an alert shall consist of the following:

- Examination of a suspicion and analysis of alerts generated by the transaction monitoring system;
- Assessment of whether the client relationship should be terminated;
- Reporting of suspected market abuse to the competent authorities where suspicions have ground.

6.3.3 Suspicious Transactions and Orders Reporting

The Bank shall be responsible for submitting reports, without delays, to its supervisory authority on orders and transactions that could constitute actual or potential insider dealing or market manipulation. A STOR must be submitted to the supervisory authority as soon as there is a reasonable suspicion of market abuse.

Where suspicions have arisen in regard to historical orders or transactions, they shall also be reported to the supervisory authority.

7 Governance

7.1 First line of defence

All employees of the Bank and the Branch are responsible for the compliance with this Policy and their respective line managers are responsible for ensuring that their subordinates are in compliance with the rules laid down in this Policy.

7.2 Second line of defence

The Compliance department shall be responsible for acting as a second line of defence. The Compliance department shall be charged with the following responsibilities in regard to this Policy:

- Conducting monitoring activities of the compliance of the Bank with the Market Abuse regulatory environment;
- Performing investigations of suspicious transactions and preparation of STORs and their consequent submission to the regulatory authorities;
- Maintaining the list of insiders as well as the list of persons discharging managerial responsibilities accurate and up-to-date;
- Reviewing and updating this Policy as necessary;
- Designing and delivering training to the Bank's employees in relation to this Policy and the Market Abuse environment;
- Interpreting relevant regulations and providing them to the employees of the Bank as and when requested.

7.3 Third line of defence

Internal Audit shall be charged with the responsibility of providing independent assurance in regard to the compliance of the Bank with the relevant regulatory requirements and with this Policy.

Internal audit shall periodically reassess this Policy in order to ensure its effective design, application and implementation, ensure that the Bank has implemented the controls relevant to this Policy, and assess whether such controls are efficient and effective.

8 Training

All employees shall undertake annual training in relation to the rules set out in this Policy. Those employees, whose work responsibilities directly involve transaction monitoring activities shall undertake an in-depth training relating to the compliance with the Market Abuse rules annually.

9 Non-compliance with the policy

Relevant persons breaching the prohibitions laid down in this Policy may be subject to sanctions, penalties and disciplinary proceedings, notably under the relevant applicable Codes of Conduct and laws.

10 Ownership and revision period

This Policy shall be maintained by the Compliance department and shall be revised whenever deemed necessary, especially if any changes are made to the relevant regulation.