Rabobank
CO Expertise & Operations - Market Abuse, Anti-Corruption and Conflicts of Interest (MAC)

Global Standard on Information Barriers

Coöperatieve Rabobank U.A.
Registered at the Chamber of Commerce, no. 30.046.259

Information sheet

Title	Global Standard on Information Barriers
Domain:	Compliance
Department:	CO Expertise & Operations- Market Abuse, Anti-Corruption and Conflicts of Interest (MAC)
Type of Global Policy Document:	Global Standard
Global Policy Document Owner:	Angelique Keijsers
Global Policy Document Primary Contact Person:	Edwin van Bruggen
Global Policy Document Writer:	MAC unit
Stakeholder Panel:	Central PPM coordinator Syward Couperus for LB (on behalf of the Focus Groep CFG) Eduard Blommendaal for RN (on behalf of the 'Klankbordgroep'), DLL and Obvion Remco Voogt for WRR (on behalf of the EWG MA, EWG CoI and Rabo Development) Lynda O'Reilly for IDB
Approved By:	Management Team Compliance (Risk Management Committee informed)
Date and version:	08 June 2017, v 1.0
Effective date:	08 June 2018
Next review date:	08 June 2019
Related documents:	Please see Definitions MAC
Applicability:	Rabobank Group

Table of Content

1 Introduction

Rabobank respects the confidentiality of information it receives from its Clients and Business Partners. Rabobank operates a 'Need to Know' approach. Three 'types' of information have been identified and have been described (§2.1).

Information handling measures such as Information Barriers (also known as 'Chinese walls') are in place and detailed in §2.2. Information Barriers are designed to prevent, control or monitor the exchange of information between different persons and/or areas of the bank and to prevent that any Confidential Information is leaked.
Subsequently, specific situations have been described in further detail in §2.3 (crossing an Information Barrier), §2.4 (Above the Information Barrier/ wall) and §2.5 (Employees changing roles). In §2.6 the process concerning information leaks is detailed and, finally §2.7 describes contractual confidentiality arrangements.

Other relevant documents include:

- Global Standard on Insiders & Inside Information
- Global Procedure on Price Sensitive Information
- Global Procedure on Wall Crossing.

1.1 Objectives

This Global Standard gives direction on how the Global Policy on Market Abuse and Global Policy on Conflict of Interest (Policies) should be applied and executed.

This Global Standard has deliberately been kept as short, clear and readable as possible. Further explanation of the terminology used can be found in the Definitions MAC (definitions as amended from time to time) that has been made available separately, in this and any other Global Standards and/or Global Procedures that apply.

For market abuse topics, this Standard, the relevant Global Policy and Global Procedures are primarily based on the requirements as stipulated in European laws and regulations in respect of market abuse as set forth in the Market Abuse Regulation (MAR) together with all level 2 and level 3 regulations pertaining thereto. However, the Policy, the Global Standards and Global Procedures also takes into account the laws and regulations of other jurisdictions in which Rabobank operates.

This Standard, the relevant Global Policy and Global Procedures do not intend to limit the application of MAR (together with all level 2 and level 3 regulations pertaining thereto) respectively the applicable local laws and regulations. In case of discrepancy MAR respectively the applicable local laws and regulations shall prevail.

If you have any questions or doubts, please contact your Compliance Officer for guidance.

1.2 Scope

This Standard applies to departments, locations (branches), local Rabobanks and Entities of Rabobank and their Employees.

1.3 Key definitions & related documents

To make sure definitions are used consistently throughout the Global Policy Documents owned by MAC, please refer to the Definitions MAC which is available separately. The document 'Definitions MAC' also contains a list of relevant/related documents and roles & responsibilities.

2 Requirements of the Global Standard

2.1 Three types of information

The minimum standards of this Standard contain requirements concerning three 'types' of information:

A. **public information**
B. **Confidential Information** - which is all information obtained in the course of an Employee's employment, which is not in the public domain and is related to Rabobank, its Employees, its Clients and/ or its Business Partners;
C. **Inside Information** which is specific Confidential Information:
    i. relating to Financial Instruments including (commodity) derivatives, commodity contracts, (auctioned products based on) emission allowances that;
    ii. has not been made public; and
    iii. which would likely have a significant impact on the price (you would use it as part of your basis for an investment decision) if it were made public.

For all types of information goes:

1. Exercise caution- don't openly read Confidential or Inside-information in public places, password-protect your files and digital data carriers (USB) etc.
2. Information has an owner: if you are a Client owner, you are responsible for the Confidential Information concerning your Client, if you are a deal captain, you are responsible for the information concerning the transaction, etc. Take your responsibility in managing this.
3. Report to your Compliance Officer if you have seen information that falls into categories B and/or C and was not meant for you. See below 2.6 about information leaks. This will help Rabobank improve its processes and help avoid an appearance of a Conflict of Interest.
4. Be particularly careful when you share information that could be a Rumour[1] or an Investment Recommendation[2].

2.1.1 Minimum standards for Confidential Information

This duty of confidentiality involves two related duties:

- the duty not to disclose Confidential Information (except if the bank is compelled by law or has a public duty to disclose or where the Client or Business Partner has agreed to the information being disclosed); and
- the duty not to use Confidential Information for anything else than for the purpose for which it was given.

Rabobank operates a strict Need to Know principle: only Employees who really need the information in the normal exercise of an employment, a profession or duties should have access to the information but access is limited to the necessary amount. If you have received

[1] See the Global Standard on Market Manipulation
[2] RMI programme has published a Compliance Advisory Note on their SharePoint: http://sharepoint.rabonet.com/sites/RMI/RMIPROJECT/mifid2/MAD2MAR/Forms/AllItems.aspx?RootFolder=%2Fsites%2FRMI%2FRMIPROJECT%2Fmifid2%2FMAD2MAR%2F3%2E%20Investment%20recommendations&FolderCTID=0x012000D7E15706CA6184419583960AF958D8E3&View=%7B52FD9301%2D29AF%2D43D2%2DA791%2D8383696DBB5E%7D

Confidential Information that is not intended for you to use for Rabobank, a Client and/or Business Partner, please report this to your Compliance Officer.

This means that information is only allowed to be shared for commercial purposes if:

- it is necessary in the normal exercise of duties;
- it is limited to the necessary amount of / type of information;
- it was given by the Client or Business Partner to share and if sharing of this information internally will not go against any contractual or legal obligations.

2.1.2 Minimum standards for Inside Information

A non-exhaustive list of information that may constitute Inside Information[3] is provided here:

- amendments to the management or supervisory board of an issuer;
- a takeover is going to occur;
- a decision is taken by the Issuer to repurchase its own shares.

Important information regarding the Issuer's financial position and/or results:

- the announcement of periodic financial results;
- significant differences from previous forecasts;
- the development of important new products;
- substantial changes in loans and collateral provided for loans, including the breaking of covenants;
- the cancellation of important credit facilities by one or more banks;
- substantial changes to the financial reporting procedure;
- negative equity;
- change of auditor (under unusual circumstances);
- important legal proceedings/claims/product liability/environmental damage/etc.

Important information regarding the company's strategy:

- the purchase or sale of important shareholdings/business units;
- the initiation or termination of important joint ventures;
- sizeable reorganisation;
- changes to strategy; radical changes to the business of the company;
- dissolution of the company;
- filing for suspension of payments or bankruptcy.

Important information on capital and governance:

- stock splits or reverse splits;
- changes to the rights associated with the various categories of Financial Instruments;
- dividend announcements, including the ex-dividend date or changes thereto and changes to dividend policy;
- significant changes to the distribution of share ownership and/or free float;
- the initiation or implementation of protective measures.

Please note that there is a Global Standard on Insiders & Inside Information and a Global Procedure on Price Sensitive Information Disclosure. Furthermore, specific rules are available on Market Sounding, these are available from the Regulatory Market Infrastructure

[3] See for instance https://www.afm.nl/~/profmedia/files/.../inside-information.ashx

team. Also, there is a Global Procedure on Price Sensitive Information which describes Inside Information relating to Rabobank.

2.2 Information Barriers

Information Barriers are the system of organisational, physical, technical and administrative controls used to secure the 'Need to Know' principle and prevent and monitor the exchange of information between Employees performing different activities. Normally, Information Barriers will at least be placed between:

- Public side; persons who work there only have access to public information;
- Private side; persons who work there, in the ordinary course of their work have access to Inside Information concerning a Client and/or transaction they are working on (see annex 4.1 for examples from Wholesale, Rural & Retail (WRR) domain).

These different activities involve a risk of a Conflict of Interest and exchanging this information could be harmful to the interests of the parties involved. These controls can include but are not limited to:

- locating Employees involved in certain transaction types in secure areas that are separate from other Employees and public areas; holding certain meetings off-site;
- using specifically trained administrative and IT support staff that are specially assigned to the specific project at hand;
- using code names to anonymise transactions with Confidential/ Inside Information and/ or even the parties involved in these type of transactions, to preserve confidentiality and to prevent the improper use and dissemination of Confidential Information;
- safe storage and disposal of documents and clean desk policy;
- providing specific training and/or awareness session for Employees regularly involved in transactions with Confidential/ Inside Information.

The Executive Board is responsible for these Information Barriers on an Entity level. Managers are responsible for identifying, placing and implementing Information Barriers in their department or Entity. Specifically, Management is responsible for making sure that proper controls (including reporting lines) are in place so that their teams can safely handle information. Management should decide which measures are reasonable and proportionate in certain cases.

Rabobank Entities with financial market activities must implement and maintain in addition to other Information Barriers, a physical segregation between organisational units with private activities and organisation units with public activities.

The IT department plays a big role in information security and together with managers and Compliance Officers they are responsible for creating awareness concerning the sharing of information. In particular attention should be paid to:

- information that is shared on platforms such as SharePoint;
- use of (e-mail)distribution lists;
- chat rooms on trading systems as well as on internal Rabobank systems; and
- Yammer.

2.3 Crossing an Information Barrier

In case of a transaction involving Inside Information it may be necessary to disclose that information to Employees outside the Information Barrier. The process for this so-called wall crossing is described in the Global Procedure on Wall Crossing.

2.4 Above the Information Barrier

- Members of the Executive Board of Rabobank, because of their position and always in line with the 'Need to Know' principle, do not need any prior approval to access Confidential Information from a Rabobank Entity and their activities. They are therefore permanently placed 'above the Information Barrier'.
- Management of Rabobank Entities because of their position and in line with the 'Need to Know' principle, do not need any prior approval to access Confidential Information within their Rabobank Entity. They are therefore permanently placed 'above the Information Barrier' for their Rabobank Entity.
- Only in very exceptional situations are Members of the Executive Board of Rabobank allowed to be actively involved in a transaction and become a Deal Team Member (i.e. take part in the execution of a transaction). Exceptions can be made; these must be approved by the Compliance Officer and the risks involved must expressly be accepted by higher management.
- In case a manager takes part in a deal team, that manager must step down from the Information Barrier for the specific Client/topic/related transactions. In such a case, higher Management must replace the manager who is stepping down from the 'above the wall' role.
- In line with the 'Need to Know' principle certain (risk) management functions can also be given access to certain Confidential Information on a case to case basis without approval in advance.
- Rabobank Group Credit Risk Management, if this is *required* for *risk management purposes* concerning the Client/ Business Partner that the Confidential Information pertains are considered Above the Wall.
- Compliance Officers and Legal staff are in general considered to be above the Information Barrier.

Employees that are above the Information Barrier do not need to be 'wall crossed'. However, they must be listed as a Deal Insider if the transaction involves Inside Information. If they get involved in the execution of the transaction they must actually step down from their 'above the wall' position for that transaction.

The table in Annex 4.2 shows which management roles are considered above the Information Barrier (applicable to WRR). In case of doubt, please contact the Compliance Officer.

2.5 Employees changing roles

If Employees have had access to Inside Information in their role and are moving to a new role, their new manager must assess the risk and decide if it is necessary to contact the Compliance Officer. The Compliance Officer may decide which requirements are necessary, such as a cooling off period.

2.6 Information leak (investigation)

If an Employee discovers or suspects that Confidential Information is being shared outside the 'Need to Know circle or has been leaked, the Employee must immediately contact the

Compliance Officer. Please note that an information leak can be intended or not, for example an information leak can be caused by accidently using the wrong email address.
The Compliance Officer will investigate and contact the relevant Control Room and/or the privacy officer (if it concerns personal data) to discuss the course of action. The Compliance Officer will advise the Employee on what actions should follow on his/ her part.

Depending on the findings, subsequent actions may include:

1) contacting the recipient to remove the information and ask them to confirm that it has not been read;
2) advising the receiving Employee that he/ she now has an Insider status;
3) informing the Client or Business Partner about the information leak;
4) advising the Client or Business Partner to immediately disclose the information;
5) contacting (senior) Management;
6) contacting a Competent Authority

If the suspicion is based on transactions or Orders being instructed, please see the Global Procedure concerning Market Abuse Reporting.

2.7 Contractual arrangements

Confidentiality, exclusivity, non-disclosure agreements and stand still clauses are contractual arrangements which fall outside of the scope of this Standard. Note however that:

- In principle, exclusivity and stand-still agreements can only be entered into for the part of business or the activity the Employee is responsible for.
- Before signing any exclusivity or stand-still clause with a Client or Business Partner, the legal department of the respective Rabobank Entity must be consulted unless other arrangements with this legal department (such as a standard pre-agreed template) are in place.
- The Relevant Control Room must be informed of an exclusivity/ stand-still clause as soon as possible.

2.8 Sanctions

Any act by an Employee that goes against this Policy, the related Global Standards and/or the Global Procedures will be considered a significant violation of the Code of Conduct and/or your labour agreement and could lead to sanctions. Sanctions could include, but are not limited to:

1) a (written) warning
2) a letter in the Employee's personnel file;
3) (temporary) relief of duties/ suspension;
4) demotion; or
5) (immediate) dismissal.

Circumstances will be considered when determining the sanction is imposed. These may include:

1. the severity of the violation;
2. the duration of the violation;
3. the intent and
4. the cooperation upon/in view of discovery of the violation.

If an Employee does not agree with the sanction(s) imposed, the Employee may turn to the locally applicable appeal procedure.

In case of non-compliance, the Competent Authority and/or stakeholders could file administrative, legal or civil cases against the Employee and/or Rabobank.

2.9 Exception management process

If departments, locations (branches), local Rabobanks and Entities of Rabobank cannot comply with a Global Policy Document or a part of the Global Policy Document, the Management thereof must apply for a waiver. A waiver is a dispensation provided by the approval body of a Global Policy Document to an entity or a department from complying with a specific requirement of a Global Policy Document or with the whole Global Policy Document. Waivers are granted for specific periods of time or until further notice[4]. See the PPM-policy or annexure for a standard waiver form.

The Chief Compliance Officer of Rabobank shall have the power to take a decision in all cases not covered by this Standard.

[4] Policies and Procedures Management Policy, v1.0, 06 Jan 2015

3 Roles & Responsibilities

For more information on roles and responsibilities, please see the Definitions MAC. Alternatively, please see the Compliance Charter document.

4 Annexures

4.1 Private side functions WRR

Private side department
Mergers & Acquisitions (M&A)
Loan Products Group (LPG)
Asset Based Finance (ABF)
Senior Relationship Banking (SRB)
Acquisition Finance (AF)
Loan Syndication (LS)
Debt Capital Markets (DCM)
Equity Capital Markets (ECM)
Trade & Commodity Finance (TCF)
Global Client Solutions (GCS)
Global sector Heads
Capital Structuring
Private equity
Export & Project finance
Agency Desk

4.2 Above the wall examples from WRR

Managers	General	Product	Sector
Global	**MT Business Line Heads (Head GCC/GWPC)** Permanently above the wall globally for own products in their business line	**Global Product Heads** Above the wall globally for own product	**Global Sector Head** Can only be above the wall for own sector globally as far as not involved in a deal team
Regional	**Regional MT Member** Permanently above the wall for all products in own region	**Regional Product Heads** Can only be above the wall for own product in own region as far as not involved in a deal team	**Regional Sector Head** Can only be above the wall for own sector in own region as far as not involved in a deal team
Local	**General (country) Managers** Permanently above the wall for all products in own location if role is not combined with SRB role and deal team involvement, otherwise only be above the wall as far as not involved in a deal team	**Local Product Heads** Can only be above the wall for own product in own location as far as not involved in a deal team	N/a
Client owners	SRB or Relationship manager in product line: e.g. RM LPG or RM TCF	Client owners should have full overview of all opportunities where the bank is engaging directly with the client. They are so to speak "Above the wall for their client only", provided: • their client is not the target in the opportunity and • conflicting opportunities with other clients in their portfolio are managed so that information of one client is never used for the purpose of another client • The client does not withhold consent to share opportunity information with the Client owner	

Above the wall, members only in very exceptional situations can get involved in a deal team, need to know all client names for role as manager in engagement, pipeline

Above the wall in a management role, but management roles are regularly combined with operational roles that require participation in deal teams

Never above the wall, always on the client side of the wall

4.3 Waiver Template

Waiver template ver 1.0.docx