Information Barriers Policy

An Ilomar Group policy designed to govern the relationship, interaction, and information flows between Louis Dreyfus Company B.V. as indirect shareholder, companies of the Ilomar Group and all other companies acting as supplier or customer of the Ilomar Group.

This policy applies to all operations within the Ilomar Group of Companies.

Version Number	1.7
Reviewed by	Filip Brion – IB manager
Last review date	**23 November 2021**
Approved by	Keir Ashton – Director Ilomar Holding NV Jean-Marc Foucher – CEO Ilomar Holding
Approval date	24 November 2021
Next review date	Annually

Table of Contents

1. Purpose and background

The relationship between the Ilomar Group (the "Group") and its principal indirect shareholder (Louis Dreyfus Company B.V. – hereinafter the "**Shareholder**") and its customers/suppliers needs to be carefully managed to ensure compliance with the existing regulations regarding warehouse company relationships with trading companies. These regulations include those of ICE Futures Europe (ICE EU) and ICE Futures U.S. (ICE US).

These rules exist to maintain a fair and competitive market within the said exchanges. In order to protect the interests of the customers of the Group, these rules will be applied also to private store commodities which are not regulated in the same way as exchange certified stocks.

Both customers and the above-mentioned exchanges are concerned that the Group puts in place proper measures to control the exchange of Confidential Information between the different companies in the Group and the Shareholder given that the Shareholder is part of a commodities trading group.

The present Policy is based upon the requirements of the ICE EU regulations (ICE EU Rule D 1.17.6) and the ICE US rules (ICE US Rule 7.24) as well as the Code of Conduct of the Group. This policy is also intended to support the fulfilment of certain other key principles of ICE EU/ICE US applicable to warehouse keepers such as observing "high standards of integrity" and "responsible entrepreneurship".

2. Policy governance and scope, monitoring

This policy applies **without exception** to **all** Group subsidiaries and majority controlled Joint Venture arrangements.

Each Business unit manager and Country Manager is ultimately responsible for the implementation and compliance of this policy within each their respective area(s) of responsibility, with oversight from the Board of Directors of Ilomar Holding NV (the "**Group Directors**") and the Group Information Barriers Manager (the "**IB Manager**").

The IB Manager is responsible for monitoring overall compliance with the requirements of this Policy and reporting issues to the CEO of the Ilomar Holding if they arise.

2.1. Annual review and sign off

All relevant Group staff members are required to acknowledge their understanding and compliance of this Information Barriers Policy each year as part of the annual appraisals/performance review process. The IB Manager will undertake annual training sessions for all staff in each location. This will be delivered either in person, by eLearning modules, or via teleconference. The Group HR Manager will communicate this policy to each new employee at the start of their career within the Group in parallel with explanation of the Code of Conduct.

2.2. Outsourced relationships

All third party outsourced relationships (e.g. warehouse operators and agents) must be reminded that they **must not** engage in any communication or other interaction with regards to Group business **without prior written consent**.

This can only be obtained via pre-approval from the Group IB Manager with approval from the Group Directors if the IB Manager feels necessary.

2.3. Compliance review

The Group, and any Group company, may be subject to internal audit and/or exchange (or other relevant regulatory body) review to demonstrate compliance and transparency.

3. Need to Know Policy

By adopting this Policy, the Group shall implement the "Need to Know" principle. This means access to Confidential Information must be given only to those personnel whose responsibilities could not reasonably be carried out without such access. The governance structure of the Group is organized to keep this number of personnel to a reasonable minimum.
The Group is a wholly owned by the Shareholder. Each of the Group companies has a statutory Board of Directors.

3.1. 'Confidential Information' definition

For the purposes of this Policy, "**Confidential Information**" is defined as follows:

- Stock figures by individual customer, both historical, current and forecasted;
- All information relating to proposed or actual shipments of Exchange deliverable commodities and privately owned commodities to be made or received by the Group. This can include any information of commercially sensitive nature given to the Group by the shipper, their agent or the recipient of that shipment, such as the identity of the customer, customers information etc.;
- All information related to the issuance, holding and cancellation of warrants or warehouse receipts by the Group; and
- Customer details, including payments made and balances owed.

It is essential that all Group Directors are able to perform their fiduciary duties whilst maintaining the integrity of the Information Barrier that exists between the Group and the Shareholder.

Where there is sharing of Confidential Information, this must be undertaken on a need to know basis. It is the responsibility of the Directors of the companies of the Group to ensure that this information is not used, distributed or otherwise transmitted across the Information Barrier other than on a need to know basis.

3.2 Sharing Confidential Information

Confidential Information is only shared with the Group Directors in accordance with this policy. If there is a genuine reason for the Group to share any Confidential Information with the Shareholder's staff, other than the Group Directors, a recommendation must be asked of the IB Manager and the final approval will be given by the Group Directors.

All approvals must be obtained in writing and include justification for the information share and what controls are to be operated to prevent any risk of information abuse or unintended transmission.

3.3 Areas of Concern

The following customary information and meetings require particular attention to ensure compliance, particularly with the need to know principle:

Information/meeting	Summary and issues	Comments and control requirements
Management Team Meeting	Biweekly and quarterly meetings to discuss the operational performance and internal control framework of the Group. Stock levels, warranting and cancellations are summarized.	Detailed customer information may be presented and discussed as reasonably required.
Logistics Synergy Group	Liaison working group to identify commercial synergies between the Shareholder's business areas and the Group	No Confidential Information to be shared with participants from the Shareholder
Board meetings	Business performance and operational management of each subsidiary with the board of Directors with respect to associated fiduciary duties.	Confidential Information is accessible to the Board of Directors on a need to know basis to support the undertaking of their fiduciary duties. Transmission of Confidential Information beyond the Board is subject to this Information Barriers Policy. All meetings should have an agenda and minutes recorded.

4. Physical interaction

The Group office locations are deliberately not co-located with the headquarters of the Shareholder. The shareholder's headquarters are located in Rotterdam. The Group is headquartered separately across different locations in Antwerp (BE), Barcelona (ES) and Tucson (US).

4.1. Exemptions List

The following teams and personnel are exempted from the Information Barriers approvals process on the basis that the interaction is purely as a back-office service and the possibility of Confidential Information sharing is remote and therefore does not pose a threat to any breach of the Information Barriers:

- Group Security & Investigations;
- IT Support functions:
    - Desktop Support
    - Global Network Services
- All Compliance, Legal and Internal Audits in areas with the group Warehouses;
- All HR staff having responsibility for Group staff worldwide; and
- Finance and Corporate Taxation teams.

4.2. Guidance on prohibited discussions

The following items must not be discussed under any circumstances during any meetings with the Shareholder or other clients:

- Current and/or forecasted individual customer stock levels (i.e. you are able to discuss an individual customer's stock levels with them as this is relevant to their business; you are **prevented** from discussing any other client stock levels);
- Commodity detailed stock movements (deliveries in and out – planned and actual);
- Customer ownership/transactions (including planned or actual warrant/warehouse receipt cancellations or transfers); or
- Customer details.

This includes communications via meetings in person, report, telephone, instant messaging fax or email and also applies to informal, social meetings.

4.3. Access to information

Information security is essential to ensuring compliance with this policy.

4.4. Hard copy information

You must ensure that your desk is clear of all Confidential Information, specifically during any visits from the Shareholder's representatives and third parties/clients.
This also includes information that you take to their site or other meeting location. Care must be taken to ensure that there is no opportunity for this information to be shared with, or accessed by, them or any other party.

4.5. Electronic information

The Group has strong information access security controls to ensure that no members of staff of the Shareholder have direct access to the group systems and networks. Additional care needs to be taken when you communicate with the Shareholders' staff via email - **please take extra care over email content and recipient email addresses.**

If you believe that you have accidentally sent an email to the wrong recipient, you must:

- Try to recall the email immediately in Outlook via the IT helpdesk and
- Advise the Group IT team immediately.

5. Systems and system access:

The Group's systems and servers are managed by an external company called Econocom with offices in Zaventem, Belgium. Electronic mails are stored in the Microsoft data centre (Microsoft 365).

5.1. Navision LQS-Navision Finance

Ensuring controlled access to this system is critical to ensuring compliance with this policy. This system is only accessible by authorized and relevant personnel and **cannot** be accessed by any staff member that trades the commodities.
Access to this system is controlled via strict user entitlement procedures managed by the Group IT Manager.

5.2. Role-Based Access Management

Users are set up on the Navision system with user access rights commensurate to their role within the Group.

5.3. Requesting/amending access rights:

For all new starters, leavers or role changes, a ticket has to be created and sent to **the IT department** requesting the precise access and use modalities for the system.

This request must be reviewed and approved by the HR Manager in advance of any changes being made to the Navision system. Once the approvals are obtained, the access rights will be updated.

Appropriate segregation of duties will be maintained throughout the request, approval and update process.

5.4. User Entitlement Review ("UER")

A yearly UER shall be undertaken by the IB Manager to check:

- Whether users have the correct, and appropriately restricted, access rights
- Whether the access rights have been correctly updated in the event of dismissal or internal job changes
- Whether the level of security and access restrictions of the various access groups is sufficient for maintaining the business activities

5.5. Password updates and Multi-Factor Authentication

An MFA system is used for us to be sure that the correct user is logging in. Passwords no longer need to be changed (Microsoft's recommendation if in combination with MFA).

5.6. Shared data stations (drives)

The shared drives are stored in Azure from Microsoft but are gradually being phased out and replaced by OneDrive.

At the moment, anyone can share OneDrive with all third parties, but this can be limited by domain name, if desired. Logging does take place, though.

5.7. Restricting access

There is no restriction of access on OneDrive and the user is himself responsible for whom he grants access to and with whom he shares information. IT can retrieve the person who consulted information within a period of a few months.

5.8 Data classification

The user is responsible for the classification of his data. Here he can indicate the sensitivity as "personal", "public", "general", "confidential", "very confidential". This can be done in both emails and files.

5.9. Email

Extra attention must be paid when sending emails. **The email content and email addresses of the recipients will always be carefully checked.**

If you believe that you have accidentally sent an email to the wrong recipient, you must:

- Try to recall the email immediately in Outlook via the IT helpdesk
- Advise the Group IT team immediately
- Confidential Information must not be sent unless pre-approval is obtained from:
    - Country Managers/Directors
    - Group IB Manager

If desired, it can be enforced that certain emails with certain content are automatically redirected via the Country Managers/Directors.

5.10. System design and development

All system design and development requests will be coordinated by the IT Manager.

Any such changes or updates must not adversely impact upon the integrity of the Information Barrier controls within the systems.

6. Policy breaches

If employees become aware of any actual or potential breach of the Policies, including identification control failures that could lead to a breach of the Information Barriers policy, the issue must be reported to the Group IB Manager immediately, who will promptly take action and report to the relevant parties.

The IB Manager will work with the relevant parties to minimize any further risk and attempt to recover the information, if appropriate/able to do so.

The IB Manager will investigate the route cause(s) of the issue and ensure that corrective control measures are implemented immediately to prevent any further recurrence.

6.1. Deliberate breach

Any deliberate breach of the Information Barriers policy will be considered a breach of the Code of Conduct (available at: CodeOfConduct_ENG-v202102.pdf (molenbergnatie.com)) and as gross misconduct by the employee. Appropriate disciplinary action will be taken.

Signed copy available upon request.