WHOLESALE INFORMATION BARRIERS POLICY

Title	Owner	Approved by	Date of publication	Version	Security class
Wholesale Information Barriers Policy	Thomas Roukens. Director, Regulatory & Compliance	Bart van Sprundel General Counsel	29.10.2025	2.0	Internal

Content

WHOLESALE INFORMATION BARRIERS POLICY

1. INTRODUCTION

1.1 PURPOSE

Telenet BV and Telenet Group NV (collectively "***Telenet group"***) obtain access to information of wholesale customers in the course of the performance and implementation of the cable access obligations, MVNO agreements and/or other wholesale deals (including in the context of interconnection and/or roaming agreements and SME/LE Carrier Sales Team). Some of that information is strategically and/or commercially sensitive because it reduces uncertainty regarding future market behaviour on the downstream retail markets on which the wholesale customer competes with Telenet group and/or can be otherwise used in the competitive relationship with the wholesale customer ("**Commercially Sensitive Information"(CSI)**).

The purpose of this policy is to explain the rules and measures designed to prevent the spread and/or misuse (or the appearance thereof) of Commercially Sensitive Information of wholesale customers obtained in the framework of Telenet group's wholesale operations.

Telenet group employees must also refrain from disclosing strategically and/or Commercially Sensitive Information from Telenet group to wholesale customers or from one wholesale customer to the other. The prohibition of such disclosure results from the general confidentiality obligations and the obligation to comply with competition law which apply to all Telenet group employees (see Competition law policy).

For the purposes of this policy, access to Commercially Sensitive Information is based on **three distinct levels of authorisation,** each corresponding to specific roles, responsibilities, and operational needs within Telenet group.

Authorised Wholesale Teams:

Any Staff Member whose primary responsibilities relate to Telenet group's wholesale business (including SME/LE Carrier Sales Team) will be considered collectively as being a member of Telenet group's 'Authorised Wholesale Teams':

- Product and Technology > Network and Wholesale > Wholesale
- Product and Technology > Technology & Partnership Steering
- Product and Technology > Product Journey > Telenet Shared Services Journeys
- Product and Technology > Product Journey > Customer Journey Solutions
- Product and Technology > Product Journey > Journey Enabling Foundations
- Commercial B2B > B2B Operations > B2B Carrier Sales

Unauthorised Teams:

For the purposes of this policy, any Staff Member whose primarily responsibilities are in retail, marketing, sales and care will be considered a member of Telenet group's "***Marketing, Sales & Care Departments",*** and therefore unauthorised to access **Commercially Sensitive Information** relating to wholesale customers, primarily:

- Commercial - Residential Circle

- Commercial - B2B Circle
- Customer Operations Circle

Need-to-know Teams:

Additionally, members of the Teams below may encounter **Commercially Sensitive Information** as part of their routine responsibilities. These Teams handle any wholesale **Commercially Sensitive Information** with the highest level of confidentiality, sharing it only on a 'need-to-know' basis within their Circles. It is also ensured that any legal or regulatory advice related to wholesale customers is never disclosed to the Unauthorised Teams.

- Legal & Regulatory Circle
- Finance > Financial Planning & Controlling > Product and Technology, Finance and Strategy
- Strategy & Corporate Development > Corporate Strategy

Compliance with this policy is **mandatory** and each Team is responsible for ensuring compliance with this policy with regards to its own activities.

1.2 SCOPE

This policy applies to Telenet BV and Telenet Group NV and all their employees and external consultants (collectively "***Staff Members"***).

2. COMMERCIALLY SENSITIVE INFORMATION

Examples of Commercially Sensitive Information include:

- Information about the **terms and conditions** of the (contemplated) wholesale agreement with the wholesale customer.
- Non-public information about the **commercial strategy**, product launches, promotions and marketing campaigns of the wholesale customer**, including information about the fact that a competitor has enquired about or is currently negotiating a wholesale agreement**.
- Non-public information about the **infrastructure**/infrastructure investments of the wholesale customer.
- **Future pricing of retail tariff plans** of the wholesale customer.
- Non-public information about the **subscribers** of wholesale customers (e.g. telephone number, geographic address, IP address, IMSI number, product type, traffic or billing information, historical usage, customer care logs), etc.
- **Sales data** (e.g. new activations, migrations, churn) of the wholesale customer.
- **Traffic data** such as traffic volumes, traffic types (e.g. technology mix), traffic location, traffic forecasts, etc. of the wholesale customer.

For the sake of clarity, information obtained in the context of branded reseller agreements falls outside the scope of this policy since branded resellers are not wholesale customers and the subscribers of the branded resellers are in actual fact Telenet group customers.

As a rule of thumb, any (i) non-public information relating to a competitor (ii) that Telenet group would not have access to in the absence of a wholesale relation with such competitor, and (iii) which can influence Telenet group's behavior on the retail market, is likely to be considered as Commercially Sensitive Information.

IN CASE OF DOUBT WHETHER INFORMATION QUALIFIES AS COMMERCIALLY SENSITIVE, PLEASE CONTACT THE REGULATORY & COMPLIANCE TRIBE VIA D_Regulatory.and.Compliance@telenetgroup.be

3. GENERAL PRINCIPLES

The disclosure of Commercially Sensitive Information to the Unauthorised Teams could take away the uncertainties that are inherent to the market and could enable Telenet group to adjust its economic behaviour on the retail market and infringe competition law and/or Telenet group's contractual and/or regulatory obligations (including regulator decisions mandating access). Therefore, the direct or indirect disclosure of Commercially Sensitive Information to the Unauthorised Teams is strictly prohibited and Commercially Sensitive Information should never be used to determine the strategy and behaviour of Telenet group on retail markets. Likewise, the disclosure of Commercially Sensitive Information from Telenet group to wholesale customers or from one wholesale customer to another could enable the receiving wholesale customer to adjust its economic behaviour on the retail market. Therefore, the direct or indirect disclosure of such information is strictly prohibited.

The Authorised Wholesale Teams should never share Commercially Sensitive Information with the Unauthorised Teams or with other wholesale customers. It should as a general rule not disclose Commercially Sensitive Information to Need-to-know Teams either, except on a strict 'need-to-know' basis for the purpose of the performance of the wholesale agreements and/or management of the Authorised Wholesale Teams, or the assessment of the impact of the wholesale business on Telenet group as a whole (for the avoidance of doubt, this should never be used to determine the retail strategy and behaviour of Telenet group) and made subject to appropriate confidentiality.

In other words, Telenet group's legitimate wholesale relation with its wholesale customers should not result in the exchange and/or disclosure of Commercially Sensitive Information (so-called 'overspill').

To limit the risk of such 'overspill':

- The disclosure by wholesale customers of Commercially Sensitive Information to the Authorised Wholesale Teams and Need-to-know Teams should be limited to what is strictly necessary for the implementation of the wholesale relationship.
- Commercially Sensitive Information should only be disclosed to the Authorised Wholesale Teams and Need-to-know Teams on a 'need-to-know' basis.
- No direct communication should take place between Unauthorised Teams and Need-to-know Teams on the one hand and the wholesale customers on the other hand.

- No Commercially Sensitive Information should be disclosed by the Authorised Wholesale Teams to the Unauthorised Teams and/or to other wholesale customers.
- Disclosure of Commercially Sensitive Information to Need-to-know Teams should be limited to that what is strictly necessary for the implementation of the wholesale relationship, the management of the Authorised Wholesale Teams, or the assessment of the impact of the wholesale business on Telenet group as a whole (for the avoidance of doubt, this should never be used to determine the retail strategy and behaviour of Telenet group) and made subject to appropriate confidentiality. In exceptional cases access to Commercially Sensitive Information may be allowed to Staff Members of Need-to-know Teams subject to prior approval of the Telenet group Legal and Regulatory Circle
- Commercially Sensitive Information should never be used to determine the retail strategy and behaviour of Telenet group.

Any Commercially Sensitive Information directly or indirectly disclosed to Unauthorised Teams will be presumed to be used by Telenet group in its decisions regarding its future market behaviour. Accordingly, it will be deemed to result in an infringement of competition law and/ or Telenet group's contractual and regulatory obligations (including the CRC decision mandating wholesale cable access!).

4. WHAT ARE INFORMATION BARRIERS?

The Information Barriers principle means that there is a functional and/ or physical separation between wholesale and retail functions and reporting lines, more specifically between Staff Members and Departments that have access to information that is potentially Commercially Sensitive Information (i.e., the Authorised Wholesale Teams and a limited number of Staff Members of Need-to-know Teams) and Staff Members and Teams who do not have such access (i.e. the Unauthorised Teams and the other Staff Members of the Need-to-know Teams). As such, the Information Barrier is designed to operate as a barrier to the passing (or 'spilling over') of Commercially Sensitive Information.

The functional and/or physical separation between wholesale and retail functions does not prevent:

- Telenet group from determining a wholesale strategy which is consistent with its retail strategy. Telenet group may for example **unilaterally** decide to focus on certain market segments through its wholesale department. However, such intention or decision should not be agreed, discussed or revealed to competitors (including wholesale customers). Similarly, it should not lead to the direct or indirect disclosure of Commercially Sensitive Information to the Unauthorised and Need-to-know Teams.
- The Telenet group SLT and Board of Directors from approving the terms of wholesale agreements. However, representatives of the Unauthorised Teams may not be involved in this approval process, which should avoid the direct or indirect disclosure of Commercially Sensitive Information to the Unauthorised Teams.

The Information Barrier is created by means of (i) policies and (ii) procedures as well as (iii) physical arrangements.

5. POLICY

The Authorised Wholesale Teams and Need-to-know Teams with access to Commercially Sensitive Information shall **strictly adhere** to the following principles:

a. Disclosure by wholesale customers of Commercially Sensitive Information to the Authorised Wholesale Teams will be limited to what is strictly necessary for the performance of the wholesale services.

b. Communication of Commercially Sensitive Information to the Unauthorised Teams or to other wholesale customers is strictly prohibited.

c. Within the Authorised Wholesale and Need-to-know Teams Commercially Sensitive Information can only be disclosed on a 'need-to-know' basis.

d. Communication of Commercially Sensitive Information to Need-to-know Teams should be limited to that what is strictly necessary for the implementation of the wholesale relationship, the management of the Authorised Wholesale Teams or the assessment of the impact of the wholesale business on Telenet group as a whole (for the avoidance of doubt, this should never be used to determine the retail strategy and behaviour of Telenet group) and made subject to appropriate confidentiality. In exceptional cases access to Commercially Sensitive Information may be allowed to Need-to-know Teams subject to prior approval of the Legal and Regulatory Circle.

e. Need-to-know Teams who, as a result of their function, may have access to Commercially Sensitive Information (e.g. IT, digital & data, engineering, regulatory, finance, legal, etc.), will:
   i. only access Commercially Sensitive Information on a strict 'need-to-know' basis (i.e. only the information which is strictly necessary);

   ii. have the responsibility to ensure that Commercially Sensitive Information is not spread to Unauthorised Teams (for instance during meetings attended by employees located on both sides of an Information Barrier) and/or Staff Members of Need-to-know Teams who do not need access to such information;

   iii. not participate, nor hold a position of which the function is to participate in decisions relating to Telenet group's retail strategy.

The Unauthorised and Need-to-know Teams without access to Commercially Sensitive Information, shall **strictly adhere** to the following principles:

a. No direct communication should take place between Unauthorised Teams or Need-to-know Teams on the one hand and the wholesale customers on the other hand.

b. The Unauthorised and Need-to-know Teams who do not need access to such information should not try to access or ask for Commercially Sensitive Information.

c. The Unauthorised and Need-to-know Teams who do not need access to such information should not participate in meetings during which Commercially Sensitive Information is being discussed.

KNOWN OR SUSPECTED BREACHES OF THE INFORMATION BARRIERS MUST BE REFERRED TO THE RISK AND COMPLIANCE TEAM (compliance@telenetgroup.be) IMMEDIATELY FOR FURTHER STEPS.

6. PROCEDURES

a. Telenet group will maintain and keep up to date an organisational matrix of the Authorised Wholesale and of Need-to-know Teams with access to Commercially Sensitive Information.

b. Each (new) Staff Member of the Authorised Wholesale Team must acknowledge in writing that he/she has read, understood and agreed to comply with this policy. The Authorised Wholesale Teams are responsible for ensuring compliance.

c. Each (new) Staff Member will follow the training and education relating to this policy. Participation will be monitored and documented.

d. The effectiveness of this policy will be periodically audited (internally and/or externally).

e. The Legal & Regulatory Circle will monitor compliance with this policy and serve as point of contact for questions regarding the interpretation and application of this policy.

f. Incidents should be reported to the Risk & Compliance Team (compliance@telenetgroup.be).

7. PHYSICAL (OR FUNCTIONAL) ARRANGEMENTS

The following arrangements shall be complied with in addition to the applicable policies relating to physical and IT security:

a. IT systems on which Commercially Sensitive Information is stored should be (functionally) separate from other IT Systems (separate servers or partitioning). The owners of the relevant IT systems are responsible for ensuring compliance in this respect.

b. Access to Commercially Sensitive Information must be password protected, with access available only to relevant persons within the Authorised Wholesale Team (and -as the case may be- Need-to-know Teams) on a strict 'need-to-know' basis. Telenet group will maintain and keep up to date an organisational matrix. Access management is applied to ensure that Tribes and Staff Members allowed to obtain access to Commercially Sensitive Information will only receive access to the specific category(ies) of Commercially Sensitive Information (e.g. MVNO data, wholesale fixed repair tickets) to which the Staff Member/Tribe needs access for the execution of its tasks.

In exceptional circumstances, when access to Commercially Sensitive Information cannot (temporarily) be restricted to relevant persons within the Authorised Wholesale Teams (and -as the case may be- Need-to-know Teams), periodic checks must be put in place by the relevant system owner to verify whether Commercially Sensitive Information has been accessed by Unauthorised Teams Circles or Need-to-know Teams who do not need access to such information. Unauthorised access should be reported to the Risk and Compliance team.

Any computer workstations used by Staff Members of the Authorised Wholesale Teams or of Need-to-know Teams who are authorised to access Commercially Sensitive Information, should be password protected and locked with a screen saver if unattended, with all information deleted when the computer is finished with.

c. When a Staff Member stops working for the Authorised Wholesale Team or for Need-to-know Teams requiring access to Commercially Sensitive Information, their access right should be revoked. Likewise, when the Staff Member no longer needs access to certain Commercially Sensitive Information, their access rights should be revoked. The manager responsible for the Staff Member should contact the relevant system owner to make the necessary changes to the access rights without undue delay.

   All Commercially Sensitive Information on the computer workstation of a Staff Member of the Authorised Wholesale Teams or of Need-to-know Teams who are authorised to access Commercially Sensitive Information, should be wiped when the Staff Member stops working for the Authorised Wholesale Teams or when the Staff Member of the Need-to-know Teams authorisation to access Commercially Sensitive Information is repealed.

d. The Authorised Wholesale Teams must be located in a physical location which is separate from the Unauthorised Teams.

e. Staff Members of the Authorised Wholesale Teams or of the Need-to-know Teams who have access to physical documents containing Commercially Sensitive Information shall apply a clean desk approach. Physical documents containing Commercially Sensitive Information will either be kept in a secure location and locked at the end of every day or shredded immediately.

8. DOS AND DON'TS FOR STAFF MEMBERS OF THE AUTHORISED WHOLESALE TEAMS AND NEED-TO-KNOW TEAMS WITH ACCESS TO COMMERCIALLY SENSITIVE INFORMATION

DO

- **Do** take all necessary steps to protect the confidentiality of Commercially Sensitive Information.
- **Do** apply a clean desk policy and keep your passwords safe.
- **Do** keep physical copies of Commercially Sensitive Information in a secure location.
- **Do** use Commercially Sensitive Information for the purpose of the legitimate performance and management of the wholesale relationship only ("***Legitimate Purposes***").
- **Do** only share Commercially Sensitive Information with colleagues for Legitimate Purposes and on a strict 'need-to-know' basis (with the necessary confidentiality caution).
- **Do** as much as possible aggregate Commercially Sensitive Information before reporting it to management.
- **Do** signal any compliance incidents to the Risk and Compliance team.

DON'T

- **Don't** ask wholesale customers to provide information that is not strictly necessary for the performance and management of the wholesale relationship.
- **Don't** try to access Commercially Sensitive Information you don't need.
- **Don't** share Commercially Sensitive Information with Unauthorised Teams. **Don't** disclose Commercially Sensitive Information to other wholesale customers.
- **Don't** share more Commercially Sensitive Information with Staff Members than strictly necessary for Legitimate Purposes.
- **Don't** use Commercially Sensitive Information to favour Telenet group's retail activities over the activities of wholesale customers.

9. DOS AND DON'TS FOR STAFF MEMBERS OF THE UNAUTHORISED TEAMS AND STAFF MEMBERS OF THE NEED-TO-KNOW TEAMS WITHOUT ACCESS TO COMMERCIALLY SENSITIVE INFORMATION

DO

- **Do** make clear to your colleagues that you cannot receive Commercially Sensitive Information.
- **Do** signal any compliance incidents to the Risk and Compliance team.

DON'T

- **Don't** try to access Commercially Sensitive Information.
- **Don't** ask your colleagues for Commercially Sensitive Information.
- **Don't** participate in meetings during which Commercially Sensitive Information is being discussed.
- **Don't** use Commercially Sensitive Information to favour Telenet group's retail activities over the activities of wholesale customers.

10. DOCUMENT CONTROL

Editor	Angeleena Kumar (Regulatory & Compliance)
Reviewers	Bart Van Sprundel (General Counsel), Thomas Roukens (Director, Regulatory & Compliance), Saskia Bellinkx (Director, Wholesale and Competition), Yasmina Oualmakran (Risk &Compliance), Annouk Van Rossem De Weyer (Risk & Compliance)
SLT Approval date	Bart van Sprundel (05.09.2025)
Update / amendment history	V1.0: original version V2.0 (05.09.2025) Organisational and terminology changes