

POLITIQUE BARRIERES D'INFORMATION WHOLESALE



Title	Owner	Approved by	Date of publication	Version	Security class
Wholesale Information Barriers Policy	Thomas Roukens. Director, Regulatory & Compliance	Bart van Sprundel General Counsel	31.10.2025	2.0	Internal

Contenu

1. INTRODUCTION	2
1.1 OBJECTIF	2
1.2 CHAMP D'APPLICATION	3
2. INFORMATIONS COMMERCIALEMENT SENSIBLES	3
3. PRINCIPES GENERAUX.....	4
4. QU'EST-CE QUE LES BARRIERES D'INFORMATION ?	5
5. POLITIQUE	6
6. PROCEDURES	7
7. ARRANGEMENTS PHYSIQUES (OU FONCTIONNELS)	8
8. CHOSES A FAIRE ET A NE PAS FAIRE POUR LES MEMBRES DU PERSONNEL DES EQUIPES WHOLESALE AUTORISEES ET LES EQUIPES NEED-TO-KNOW AYANT ACCES A DES INFORMATIONS COMMERCIALEMENT SENSIBLES	9
10. CONTROLE DES DOCUMENTS	10



1. INTRODUCTION

1.1 OBJECTIF

Telenet SRL et Telenet Group SA (collectivement « **Telenet group** ») obtiennent l'accès aux informations des clients wholesale dans le cadre de l'exécution et de la mise en œuvre des obligations d'accès au câble, des accords MVNO et/ou d'autres accords wholesale (y compris dans le cadre d'accords d'interconnexion et/ou d'itinérance et les SME/LE Carrier Sales Team). Certaines de ces informations sont sensibles sur le plan stratégique et/ou commercial, car elles réduisent l'incertitude quant au comportement futur du marché sur les marchés retail en aval sur lesquels le client wholesale est en concurrence avec Telenet group et/ou peuvent être utilisées d'une autre manière dans le cadre de la relation concurrentielle avec le client wholesale (« **Informations Commercialement Sensibles** » (ICS)).

L'objectif de cette politique est d'expliquer les règles et les mesures visant à empêcher la diffusion et/ou l'utilisation abusive (ou l'apparence de celle-ci) d'Informations Commercialement Sensibles de clients wholesale obtenues dans le cadre des opérations wholesale de Telenet group.

Les employés de Telenet group doivent également s'abstenir de divulguer des Informations stratégiques et/ou Commercialement Sensibles de Telenet group à des clients wholesale ou d'un client wholesale à un autre. L'interdiction d'une telle divulgation résulte des obligations générales de confidentialité et de l'obligation de respecter le droit de la concurrence qui s'appliquent à tous les employés de Telenet group (voir [Droit de la concurrence](#)).

Aux fins de la présente politique, l'accès aux Informations Commercialement Sensibles est basé sur **trois niveaux d'autorisation distincts**, chacun correspondant à des rôles, responsabilités et besoins opérationnels spécifiques au sein de Telenet group.

Équipes Wholesale Autorisées :

Tout Membre du personnel dont les responsabilités principales sont liées aux activités wholesale de Telenet group (y compris les SME/LE Carrier Sales Team) sera considéré collectivement comme membre des 'Équipes Wholesale Autorisées' de Telenet group :

- 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

POLITIQUE BARRIERES D'INFORMATION WHOLESALE



Équipes Non Autorisées :

Aux fins de la présente politique, tout Membre du personnel dont les responsabilités principales sont dans le retail, marketing, sales et care sera considéré comme un membre des « **Marketing, Sales & Care Departments** » de Telenet group et n'est donc pas autorisé à accéder à **des Informations Commercialement Sensibles** relatives aux clients wholesale, principalement :

- Commercial - Residential Circle
- Commercial - B2B Circle
- Customer Operations Circle

Équipes Need-to-know :

De plus, les membres des équipes ci-dessous peuvent rencontrer des **Informations Commercialement Sensibles** dans le cadre de leurs responsabilités habituelles. Ces équipes traitent toutes **les Informations Commercialement Sensibles** wholesale avec le plus haut niveau de confidentialité, ne les partageant que sur la base stricte du « besoin d'en savoir » au sein de leurs Circles. Il est également garanti que tout conseil juridique ou réglementaire lié aux clients wholesale n'est jamais divulgué aux Équipes Non Autorisées.

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

Le respect de cette politique est **obligatoire** et chaque équipe est responsable d'assurer le respect de cette politique en ce qui concerne ses propres activités.

1.2 CHAMP D'APPLICATION

Cette politique s'applique à Telenet SRL et Telenet Group SA et à tous ses employés et consultants externes (« **Membre du personnel** » ou collectivement les « **Membres du personnel** »).

2. INFORMATIONS COMMERCIALEMENT SENSIBLES

Voici des exemples d'Informations Commercialement Sensibles :

- Des informations sur les **modalités du contrat wholesale** (envisagé) avec le client wholesale ;
- Informations non publiques sur la **stratégie commerciale**, les lancements de produits, les promotions et les campagnes de marketing du client wholesale, **y compris les informations sur le fait qu'un concurrent s'est renseigné sur un contrat wholesale ou négocie actuellement un contrat wholesale.**
- Informations non publiques sur les **infrastructures**/les investissements dans les infrastructures du client wholesale.

POLITIQUE BARRIERES D'INFORMATION WHOLESALE



- **La tarification future des plans tarifaires retail** du client wholesale.
- Informations non publiques sur les **abonnés** des clients wholesale (par exemple, numéro de téléphone, adresse géographique, adresse IP, numéro IMSI, type de produit, informations sur le trafic ou la facturation, historique d'utilisation, logs du service client), etc.
- **Données de vente** (par exemple, nouvelles activations, migrations, désabonnement) du client wholesale.
- **Données de trafic** telles que les volumes de trafic, les types de trafic (par exemple, le mix technologique), la localisation du trafic, les prévisions de trafic, etc. du client wholesale.

Par souci de clarté, les informations obtenues dans le cadre des accords branded reseller n'entrent pas dans le champ d'application de la présente politique, car les branded resellers ne sont pas des clients wholesale et leurs abonnés sont en réalité des clients de Telenet group.

En règle générale, toute (i) information non publique relative à un concurrent, (ii) à laquelle Telenet group n'aurait pas accès en l'absence d'une relation wholesale avec ce concurrent, et (iii) qui peut influencer le comportement de Telenet group sur le marché retail, est susceptible d'être considérée comme une Information Commercialement Sensible.

**EN CAS DE DOUTE SUR LE CARACTERE COMMERCIALEMENT SENSIBLE DES INFORMATIONS,
VEUILLEZ CONTACTER LE REGULATORY & COMPLIANCE TRIBE
VIA D_Regulatory.and.Compliance@telenetgroup.be**

3. PRINCIPES GENERAUX

La divulgation d'Informations Commercialement Sensibles aux Équipes Non Autorisées pourrait éliminer les incertitudes inhérentes au marché et pourrait permettre à Telenet group d'ajuster son comportement économique sur le marché retail et d'enfreindre le droit de la concurrence et/ou les obligations contractuelles et/ou réglementaires de Telenet group (y compris les décisions des régulateurs imposant l'accès). Par conséquent, la divulgation directe ou indirecte d'Informations Commercialement Sensibles aux Équipes Non Autorisées est strictement interdite et les Informations Commercialement Sensibles ne doivent jamais être utilisées pour déterminer la stratégie et le comportement de Telenet group sur les marchés retail. De même, la divulgation d'Informations Commercialement Sensibles de Telenet group à des clients wholesale ou d'un client wholesale à un autre pourrait permettre au client wholesale destinataire d'adapter son comportement économique sur le marché retail. Par conséquent, la divulgation directe ou indirecte de ces informations est strictement interdite.

Les Équipes Wholesale Autorisées ne doivent jamais partager d'Informations Commercialement Sensibles avec les Équipes Non Autorisées ou avec d'autres clients wholesale. En règle générale, ils ne devraient pas non plus divulguer d'Informations Commercialement Sensibles aux Équipes Need-to-know, sauf sur la base stricte du « besoin d'en savoir » aux fins de l'exécution des contrats wholesale et/ou de la gestion des Équipes Wholesale Autorisées, ou de l'évaluation de l'impact de l'activité wholesale sur Telenet group dans son ensemble (afin d'éviter toute ambiguïté, cela ne doit jamais être utilisé pour déterminer la stratégie retail et le comportement de Telenet group) et faire l'objet d'une confidentialité appropriée.



En d'autres termes, la relation wholesale légitime de Telenet group avec ses clients wholesale ne doit pas aboutir à l'échange et/ou à la divulgation d'Informations Commercialement Sensibles (ce que l'on appelle le « overspill »).

Afin de limiter le risque d'un tel « overspill » :

- La divulgation par les clients wholesale d'Informations Commercialement Sensibles aux Équipes Wholesale Autorisées et aux Équipes Need-to-know doit être limitée à ce qui est strictement nécessaire à la mise en œuvre de la relation wholesale.
- Les Informations Commercialement Sensibles ne doivent être divulguées qu'aux Équipes Wholesale Autorisées et aux Équipes Need-to-know sur la base du « besoin d'en savoir ».
- Aucune communication directe ne doit avoir lieu entre les Équipes Non Autorisées et les Équipes Need-to-know, d'une part, et les clients wholesale, d'autre part.
- Aucune Information Commercialement Sensible ne doit être divulguée par les Équipes Wholesale Autorisées aux Équipes Non Autorisées et/ou à d'autres clients wholesale.
- La divulgation d'Informations Commercialement Sensibles aux Équipes Need-to-know devrait être limitée à ce qui est strictement nécessaire à la mise en œuvre de la relation wholesale, à la gestion des Équipes Wholesale Autorisées ou à l'évaluation de l'impact de l'activité wholesale sur Telenet group dans son ensemble (pour éviter toute ambiguïté, cela ne devrait jamais être utilisés pour déterminer la stratégie retail et le comportement de Telenet group) et faire l'objet d'une confidentialité appropriée. Dans des cas exceptionnels, l'accès aux Informations Commercialement Sensibles peut être autorisé aux Membres du personnel des Équipes Need-to-know, sous réserve de l'approbation préalable du Legal & Regulatory Circle de Telenet group.
- Les Informations Commercialement Sensibles ne doivent jamais être utilisées pour déterminer la stratégie retail et le comportement de Telenet group.

Toute Information Commercialement Sensible divulguée directement ou indirectement à des Équipes Non Autorisées sera présumée être utilisée par Telenet group dans ses décisions concernant son comportement futur sur le marché. En conséquence, il sera réputé qu'il en résulte une infraction au droit de la concurrence et/ou aux obligations contractuelles et réglementaires de Telenet group (y compris la décision de la CRC imposant l'accès au câble wholesale !)

4. QU'EST-CE QUE LES BARRIERES D'INFORMATION ?

Le principe des Barrières d'Information signifie qu'il existe une séparation fonctionnelle et/ou physique entre les fonctions et les lignes hiérarchiques wholesale et retail, plus précisément entre les Membres du personnel et les départements qui ont accès à des informations potentiellement sensibles sur le plan commercial (c'est-à-dire les Équipes Wholesale Autorisées et un nombre limité de Membres du personnel des Équipes Need-to-know) et les Membres du personnel et les équipes qui n'ont pas un tel accès (c'est-à-dire les Équipes Non Autorisées et les autres Membres du personnel des Équipes Need-to-know). En tant que tel, la Barrière d'Information est conçue pour fonctionner comme une barrière à la transmission (ou au « overspill ») d'Informations Commercialement Sensibles.



La séparation fonctionnelle et/ou physique entre les fonctions wholesale et retail n'empêche **pas** :

- Telenet group de déterminer une stratégie wholesale cohérente avec sa stratégie retail. Telenet group peut par exemple décider **unilatéralement** de se concentrer sur certains segments de marché par l'intermédiaire de son département wholesale. Toutefois, une telle intention ou décision ne doit pas être convenue, discutée ou révélée aux concurrents (y compris les clients wholesale). De même, cela ne devrait pas conduire à la divulgation directe ou indirecte d'Informations Commercialement Sensibles aux Équipes Non Autorisées et Équipes Need-to-know.
- La SLT et le Conseil d'administration de Telenet group d'approuver les termes des accords de gros. Cependant, les représentants des Équipes Non Autorisées ne peuvent pas être impliqués dans ce processus d'approbation, ce qui devrait éviter la divulgation directe ou indirecte d'Informations Commercialement Sensibles aux Équipes Non Autorisées.

La Barrière d'Information est créée au moyen (i) de politiques et (ii) de procédures ainsi que (iii) d'arrangements physiques.

5. POLITIQUE

Les Équipes Wholesale Autorisées et les Équipes Need-to-know ayant accès à des Informations Commercialement Sensibles doivent **respecter strictement** les principes suivants :

- a. La divulgation par les clients wholesale d'Informations Commercialement Sensibles aux Équipes Wholesale Autorisées sera limitée à ce qui est strictement nécessaire à l'exécution des services wholesale.
- b. La communication d'Informations Commercialement Sensibles aux Équipes Non Autorisées ou à d'autres clients wholesale est strictement interdite.
- c. Au sein des Équipes Wholesale Autorisées et Need-to-know, les Informations Commercialement Sensibles ne peuvent être divulguées qu'en cas de besoin.
- d. La communication d'Informations Commercialement Sensibles aux Équipes Need-to-know doit se limiter à ce qui est strictement nécessaire à la mise en œuvre de la relation wholesale, à la gestion des Équipes Wholesale Autorisées ou à l'évaluation de l'impact de l'activité wholesale sur Telenet group dans son ensemble (pour éviter toute ambiguïté, cela **ne doit jamais** être utilisés pour déterminer la stratégie retail et le comportement de Telenet group) et faire l'objet d'une confidentialité appropriée. Dans des cas exceptionnels, l'accès aux Informations Commercialement Sensibles peut être autorisé aux Équipes Need-to-know, sous réserve de l'approbation préalable du Legal & Regulatory Circle.
- e. Les équipes qui, en raison de leur fonction, peuvent avoir accès à des Informations Commercialement Sensibles (par exemple, IT, digital & data, engineering, regulatory, finance, legal, etc.), devront :
 - i. n'accéder aux Informations Commercialement Sensibles qu'à la base stricte du « besoin



d'en savoir » (c'est-à-dire uniquement les informations strictement nécessaires);

- ii. prendre la responsabilité de veiller à ce que les Informations Commercialement Sensibles ne soient pas transmises à des Équipes Non Autorisées (par exemple, lors de réunions auxquelles assistent des Membres de personnel situés des deux côtés d'une Barrière d'Information) et/ou aux Membres du personnel des Équipes Need-to-know qui n'ont pas besoin d'accéder à ces informations ;
- iii. ne pas participer, ni occuper une position ayant pour fonction de participer aux décisions relatives à la stratégie retail de Telenet group.

Les Équipes Non Autorisées et Need-to-know qui n'ont pas accès à des Informations Commercialement Sensibles doivent **respecter strictement** les principes suivants :

- a. Aucune communication directe ne doit avoir lieu entre les Équipes Non Autorisées ou les Équipes Need-to-know, d'une part, et les clients wholesale, d'autre part.
- b. Les Équipes Non Autorisées et Need-to-know qui n'ont pas besoin d'accéder à ces informations ne doivent pas essayer d'accéder ni demander des Informations Commercialement Sensibles.
- c. Les Équipes Non Autorisées et Need-to-know qui n'ont pas besoin d'accéder à ces informations ne doivent pas participer à des réunions au cours desquelles des Informations Commercialement Sensibles sont discutées.

**LES VIOLATIONS CONNUES OU SOUPÇONNEES DES BARRIERES D'INFORMATION DOIVENT
ETRE IMMEDIATEMENT TRANSMISES A L'EQUIPE RISK & COMPLIANCE
(compliance@telenetgroup.be) POUR DES DEMARCHES ULTERIEURES.**

6. PROCEDURES

- a. Telenet group maintiendra et tiendra à jour une matrice organisationnelle des Équipes wholesale Autorisées et des Équipes Need-to-know ayant accès à des Informations Commercialement Sensibles.
- b. Chaque (nouveau/nouvelle) Membre du personnel de l'Équipe Wholesale Autorisée doit reconnaître par écrit qu'il/elle a lu, compris et accepté de se conformer à la présente politique. Les Équipes Wholesale Autorisées sont chargées de veiller à la conformité.
- c. Chaque (nouveau/nouvelle) Membre du personnel suivra la formation et l'éducation relatives à la présente politique. La participation fera l'objet d'un suivi et d'une documentation.
- d. L'efficacité de cette politique fera l'objet d'un audit périodique (interne et/ou externe).



- e. Le Legal & Regulatory Circle surveillera le respect de la présente politique et servira de point de contact pour les questions concernant l'interprétation et l'application de cette politique.
- f. Les incidents doivent être signalés à l'équipe Risk & Compliance (compliance@telenetgroup.be).

7. ARRANGEMENTS PHYSIQUES (OU FONCTIONNELS)

En plus des politiques applicables en matière de sécurité physique et informatique, les dispositions suivantes doivent être respectées :

- a. Les systèmes informatiques sur lesquels des Informations Commercialement Sensibles sont stockées doivent être (fonctionnellement) séparés des autres systèmes informatiques (serveurs séparés ou partitionnement). Les propriétaires des systèmes informatiques concernés sont responsables de la conformité à cet égard.
- b. L'accès aux Informations Commercialement Sensibles doit être protégé par un mot de passe, l'accès n'étant accessible qu'aux personnes concernées au sein de l'Équipe Wholesale Autorisée (et, le cas échéant, des Équipes Need-to-know) sur la base stricte du « besoin d'en savoir ». Telenet group maintiendra et tiendra à jour une matrice organisationnelle. La gestion de l'accès est appliquée pour s'assurer que les Tribes et les Membres du personnel autorisés à obtenir l'accès aux Informations Commercialement Sensibles ne recevront l'accès qu'à la ou aux catégories spécifiques d'Informations Commercialement Sensibles (par exemple, les données MVNO, wholesale fixed repair tickets) auxquelles le Membre du personnel/le Tribe a besoin d'accéder pour l'exécution de ses tâches.

Dans des circonstances exceptionnelles, lorsque l'accès aux Informations Commercialement Sensibles ne peut pas (temporairement) être limité aux personnes concernées au sein des Équipes Wholesale Autorisées (et, le cas échéant, des Équipes Need-to-know), des vérifications périodiques doivent être mises en place par le propriétaire du système concerné pour vérifier si des Informations Commercialement Sensibles ont été consultées par des Circles d'Équipes Non Autorisées ou des Équipes Need-to-know qui n'ont pas besoin d'accéder à ces informations. Les accès non autorisés doivent être signalés à l'équipe Risk & Compliance.

Tous les postes de travail informatiques utilisés par les Membres du personnel des Équipes Wholesale Autorisées ou des Équipes Need-to-know qui sont autorisés à accéder à des Informations Commercialement Sensibles, doivent être protégés par un mot de passe et verrouillés à l'aide d'un écran de veille s'ils ne sont pas surveillés, et toutes les informations sont supprimées lorsque l'usage du poste de travail informatique est terminé.

- c. Lorsqu'un Membre du personnel cesse de travailler pour l'Équipe Wholesale Autorisée ou pour les Équipes Need-to-know nécessitant l'accès à des Informations Commercialement Sensibles, son/sa droit d'accès doit être révoqué. De même, lorsque le Membre du personnel n'a plus besoin d'accéder à certaines Informations Commercialement Sensibles, ses droits d'accès doivent être révoqués. Le responsable du Membre du personnel doit contacter le propriétaire du système concerné pour apporter les modifications nécessaires aux droits d'accès dans les meilleurs délais.



Toutes les Informations Commercialement Sensibles se trouvant sur le poste de travail informatique d'un Membre du personnel des Équipes Wholesale Autorisées ou des Équipes Need-to-know qui sont autorisées à accéder à des Informations Commercialement Sensibles, doivent être effacées lorsque le Membre du personnel cesse de travailler pour les Équipes Wholesale Autorisées ou lorsque l'autorisation du Membre du personnel des Équipes Need-to-know d'accéder à des Informations Commercialement Sensibles est abrogée.

- d. Les Équipes Wholesale Autorisées doivent être situées dans un lieu physique distinct de celui des Équipes Non Autorisées.
- e. Les Membres du personnel des Équipes Wholesale Autorisées ou des Équipes Need-to-know qui ont accès à des documents physiques contenant des Informations Commercialement Sensibles doivent appliquer une politique du bureau rangé. Les documents physiques contenant des Informations Commercialement Sensibles seront soit conservés dans un endroit sécurisé et verrouillés à la fin de chaque journée, soit déchiquetés immédiatement.

8. CHOSSES À FAIRE ET À NE PAS FAIRE POUR LES MEMBRES DU PERSONNEL DES ÉQUIPES WHOLESALE AUTORISÉES ET LES ÉQUIPES NEED-TO-KNOW AYANT ACCÈS À DES INFORMATIONS COMMERCIALEMENT SENSIBLES

À FAIRE

- **Prenez** toutes les mesures nécessaires pour protéger la confidentialité des Informations Commercialement Sensibles
- **Appliquez** une politique du bureau rangé et protégez vos mots de passe.
- **Conservez** des copies physiques des Informations Commercialement Sensibles dans un endroit sécurisé.
- **Utilisez** les Informations Commercialement Sensibles seulement aux fins de l'exécution et de la gestion légitimes de la relation de gros uniquement (« **Fins Légitimes** »).
- **Partagez** des Informations Commercialement Sensibles seulement avec des collègues qu'à des Fins Légitimes et sur la base stricte du « besoin d'en savoir » (avec la prudence de confidentialité nécessaire).
- **Faites** autant que possible agréger les Informations Commercialement Sensibles avant de les signaler au management.
- **Signalez** tout incident de conformité à l'équipe Risk & Compliance.

À NE PAS FAIRE

- **Ne demandez pas** aux clients wholesale de fournir des informations qui ne sont pas strictement nécessaires à l'exécution et à la gestion de la relation wholesale.
- **N'essayez pas** d'accéder à des Informations Commercialement Sensibles dont vous n'avez pas besoin.
- **Ne partagez pas** d'Informations Commercialement Sensibles avec des Équipes Non Autorisées.
- **Ne divulguez pas** d'Informations Commercialement Sensibles à d'autres clients wholesale.



- **Ne partagez pas** avec les Membres du personnel plus d'Informations Commercialement Sensibles que ce qui est strictement nécessaire à des Fins Légitimes.
- **N'utilisez pas** d'Informations Commercialement Sensibles pour favoriser les activités retail de Telenet group par rapport aux activités des clients wholesale.

9. CHOSE A FAIRE ET A NE PAS FAIRE POUR LES MEMBRES DU PERSONNEL DES EQUIPES NON AUTORISEES ET LES MEMBRES DU PERSONNEL DES EQUIPES NEED-TO-KNOW SANS ACCES A DES INFORMATIONS COMMERCIALEMENT SENSIBLES

À FAIRE

- **Indiquez** clairement à vos collègues que vous ne pouvez pas recevoir d'Informations Commercialement Sensibles.
- **Signalez** tout incident de conformité à l'équipe Risk & Compliance.

À NE PAS FAIRE

- **N'essayez pas** d'accéder à des Informations Commercialement Sensibles.
- **Ne demandez pas** d'Informations Commercialement Sensibles à vos collègues.
- **Ne participez pas** à des réunions au cours desquelles des Informations Commercialement Sensibles sont discutées.
- **N'utilisez pas** d'Informations Commercialement Sensibles pour favoriser les activités retail de Telenet group par rapport aux activités des clients wholesale.

10. CONTROLE DES DOCUMENTS

Editeur	Angeleena Kumar (Regulatory & Compliance)
Réviseurs	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)
Date d 'approbation par SLT	Bart van Sprundel (05.09.2025)
Historique de mise à jour et des modifications	V1.0: version originale V2.0 (05.09.2025) : Modifications organisationnelles et terminologiques