Politique de Prévention et de Détection des Abus de Marché

1. Introduction

1.1. Définitions

Conformément au règlement MiCA, la prévention et l'interdiction des abus de marché s'appliquent :

- *« aux actes accomplis par toute personne concernant des crypto-actifs admis à la négociation ou ayant fait l'objet d'une demande d'admission à la négociation ;*
- *toute transaction, tout ordre ou tout comportement concernant des cryptoactifs, indépendamment du fait que cette transaction, cet ordre ou ce comportement ait lieu sur une plate-forme de négociation ;*
- *dans l'Union et dans des pays tiers concernant des crypto-actifs. »*

Il existe trois types d'abus de marché définis comme suit :

- le délit d'initié ;
- la manipulation de marché ;
- la divulgation illicite d'informations privilégiées.

1.1.1. Délit d'initié

Le délit d'initié désigne l'acte d'utiliser une information privilégiée pour acquérir, céder ou modifier des ordres concernant des crypto-actifs associés, directement ou indirectement, pour soi-même ou pour autrui. Cela inclut également l'annulation ou la modification d'ordres passés avant l'obtention de l'information privilégiée, ainsi que le fait de recommander ou d'inciter autrui à effectuer de telles actions de négociation.

La prévention et l'interdiction du délit d'initié s'appliquent à toute personne qui détient une information privilégiée en raison de :

- son appartenance aux organes administratifs, de gestion ou de surveillance de l'émetteur, de l'offreur ou de la personne demandant l'admission à la négociation ;
- sa détention d'une participation dans le capital de l'émetteur, de l'offreur ou de la personne demandant l'admission à la négociation ;
- son accès à l'information dans le cadre de l'exercice d'un emploi, d'une profession ou de fonctions, ou en relation avec son rôle dans la technologie des registres distribués ou une technologie similaire ;
- son implication dans des activités criminelles.

1.1.2. Manipulation de marché

Les comportements suivants sont considérés, entre autres, comme de la manipulation de marché :

- l'obtention d'une position dominante sur l'offre ou la demande d'un crypto-actif, ayant pour effet (ou susceptible d'avoir pour effet) de fixer, directement ou indirectement, les prix d'achat ou de vente, ou de créer (ou susceptible de créer) des conditions de négociation déloyales ;

- le passage d'ordres sur une plateforme de négociation de crypto-actifs ou auprès d'un service d'échange, y compris toute annulation ou modification de ces ordres, par tout moyen de négociation disponible, et ayant l'un des effets mentionnés au paragraphe 2, point (a), notamment :

    - perturber ou retarder le fonctionnement de la plateforme de négociation de crypto-actifs, ou engager des activités susceptibles d'avoir cet effet ;

    - rendre plus difficile pour d'autres personnes l'identification des ordres authentiques concernant des crypto-actifs, ou engager des activités susceptibles d'avoir cet effet, y compris en passant des ordres entraînant une déstabilisation du fonctionnement normal de la plateforme ;

    - créer un signal faux ou trompeur sur l'offre, la demande ou le prix d'un crypto-actif, notamment en passant des ordres pour initier ou aggraver une tendance, ou en engageant des activités susceptibles d'avoir cet effet ;

    - tirer parti d'un accès occasionnel ou régulier aux médias traditionnels ou électroniques en exprimant une opinion sur un crypto-actif, tout en ayant préalablement pris position sur ce crypto-actif, puis en tirant profit de l'impact de cette opinion sur son prix, sans avoir simultanément divulgué ce conflit d'intérêts au public de manière appropriée et efficace.

1.1.3. Divulgation illicite d'informations privilégiées

La divulgation illicite d'informations privilégiées survient lorsqu'une personne en possession d'une information privilégiée la divulgue à une autre personne.

Afin d'interdire la divulgation illicite d'informations privilégiées :

- aucune personne en possession d'une information privilégiée ne doit la divulguer de manière illicite à une autre personne, sauf si cette divulgation est effectuée dans le cadre normal de l'exercice d'un emploi, d'une profession ou de fonctions ;

- la divulgation ultérieure de recommandations ou d'incitations basées sur une information privilégiée concernant des crypto-actifs constitue une divulgation illicite d'informations privilégiées lorsque la personne qui divulgue la recommandation ou l'incitation sait ou devrait savoir qu'elle était basée sur une information privilégiée.

1.2. Champ d'application de la politique

Dans le cadre de ses activités, Paymium peut être confrontée à des situations pouvant potentiellement générer des abus de marché. La présente Politique a pour objectif de présenter le cadre juridique que Paymium met en place pour prévenir, contrôler et gérer les abus de marché.

Cette politique vise à garantir que Paymium empêche toutes les formes d'abus de marché, telles que le délit d'initié, la divulgation illicite d'informations privilégiées ou la manipulation de marché.

2. Surveillance et détection

2.1. Surveillance

Paymium effectue une surveillance de conformité basée sur une approche par les risques afin d'assurer un contrôle efficace de ses activités. La surveillance des abus de marché se concentre sur la réception potentielle d'informations privilégiées tout au long du processus d'investissement, avec des mesures en place pour gérer et atténuer ce risque.

Dans le cadre de ses contrôles quotidiens, le service de conformité examine l'activité de négociation en temps réel afin d'identifier toute transaction suspecte.

Il est important de reconnaître que des indications suffisantes d'abus de marché peuvent n'apparaître qu'après qu'un ordre ait été passé ou qu'une transaction ait eu lieu. Le personnel de surveillance doit rester attentif à la possibilité qu'une séquence d'événements sur plusieurs jours puisse indiquer un abus de marché potentiel, nécessitant une enquête approfondie pour déterminer si un rapport d'ordre ou de transaction suspecte (ci-après dénommé « STOR ») doit être déposé.

2.2. Technologies de l'Information et de la Communication

Paymium utilise des systèmes TIC (Technologies de l'Information et de la Communication) et a mis en place des procédures qui aident à la détection des abus de marché ou des tentatives d'abus de marché. Ces systèmes TIC sont adaptés et proportionnés par rapport à son échelle, sa taille et la nature de ses activités.

Paymium a conçu son propre système TIC pour surveiller les transactions et les ordres, ainsi que son moteur de négociation.

Paymium garantit une conformité totale avec le Règlement Général sur la Protection des Données (RGPD). Cela inclut :

- des normes, notamment la minimisation des données, les mesures de sécurité et les limites de conservation ;
- des garanties pour le traitement des données personnelles ;
- la protection des droits des personnes concernées et la sécurité des données personnelles.

L'outil et ses paramètres respectent les exigences de la Politique de Sécurité du Système d'Information de Paymium, en conformité avec les règlements MiCA et DORA.

3. Prévention

Paymium a mis en œuvre un ensemble complet de mesures visant à prévenir toute situation impliquant des abus de marché.

Ces mesures sont conçues pour garantir la conformité avec les réglementations applicables et promouvoir la transparence dans toutes les opérations.

3.1. Protection des informations privilégiées

Les employés de Paymium doivent présumer que toutes les informations obtenues dans le cadre de

leur emploi au sein de Paymium ne sont pas publiques, à moins que ces informations n'aient été publiquement divulguées.

Voici quelques scénarios identifiés où les employés de Paymium peuvent être exposés à un risque élevé de recevoir des informations privilégiées :

- immeuble de bureaux partagé ;
- contact avec des sociétés cotées en bourse ;
- relations personnelles.

Afin de garantir la confidentialité des informations privilégiées, les règles suivantes sont mises en œuvre au sein de Paymium :

- toute communication impliquant des informations privilégiées doit être traitée avec une extrême prudence. Les employés qui entrent en possession d'une information privilégiée potentielle ne doivent pas la partager avec qui que ce soit, ni en interne ni en externe, sauf avec le service de conformité. Les discussions sur les informations privilégiées doivent être évitées dans les lieux publics tels que les couloirs, les ascenseurs ou les événements sociaux, et une attention particulière doit être portée lors de l'utilisation de téléphones dans des lieux où les conversations pourraient être entendues ;
- les informations non publiques liées aux stratégies d'investissement et aux participations de Paymium ne doivent pas être partagées avec des tiers, sauf si nécessaire pour exécuter des décisions d'investissement, mener des activités commerciales légitimes ou se conformer aux obligations réglementaires. Les employés sont interdits de divulguer des détails sur des accords proposés ou en cours ou d'autres sujets sensibles à des tiers sans l'approbation préalable du service de conformité ;
- les personnes exposées doivent faire preuve de vigilance supplémentaire lorsqu'elles travaillent dans des environnements de bureau ouvert. Les discussions sur les informations privilégiées ne doivent avoir lieu que dans des zones privées, telles que les salles de réunion ;
- les documents contenant des informations privilégiées doivent être traités avec le plus haut niveau de discrétion et stockés de manière sécurisée. Cela inclut :
    - éviter de laisser des documents sensibles en évidence ;
    - stocker les documents dans des armoires ou dossiers fermés ;
    - verrouiller les zones de stockage, en particulier en dehors des heures de bureau ;
    - limiter l'accès aux personnes autorisées à consulter les informations ;
    - détruire correctement les documents en double ou inutiles.

Toute fuite d'informations privilégiées par un employé peut entraîner des sanctions disciplinaires.

3.2. Barrières d'information

Paymium empêche et contrôle l'échange d'informations entre les personnes concernées impliquées dans des activités présentant un risque d'abus de marché.

Paymium restreint l'accès aux informations privilégiées sur la base du « besoin d'en connaître », en permettant uniquement aux personnes dont les rôles nécessitent spécifiquement ces informations d'y accéder pour exercer leurs fonctions.

Paymium met en œuvre des restrictions d'accès aux systèmes informatiques pour gérer l'accès aux informations privilégiées, telles que :

- la gestion des permissions utilisateurs : des révisions et mises à jour régulières des permissions utilisateurs garantissent que les niveaux d'accès sont actuels et appropriés pour chaque rôle ;
- les contrôles de sécurité physique : l'accès aux infrastructures et systèmes informatiques qui stockent ou traitent des informations privilégiées est restreint par des mesures de sécurité physique, telles que des salles serveurs verrouillées et des zones restreintes ;
- la protection par mot de passe : l'accès aux informations privilégiées est sécurisé par des mots de passe uniques et robustes, attribués uniquement aux utilisateurs autorisés ;
- le chiffrement des informations : Paymium peut chiffrer les messages contenant des informations privilégiées.

3.3. Médias et divulgation

Paymium suit une politique de communication et une politique commerciale stricte.

Paymium maintient une surveillance vigilante pour éviter la diffusion de signaux trompeurs ou d'informations non autorisées pouvant affecter l'intégrité du marché ou ses opérations.

Les activités médiatiques et les interactions des membres exposés de Paymium, ainsi que celles de Paymium elle-même, sont étroitement surveillées.

En cas de fuite détectée ou d'activité suspecte, des mesures immédiates sont mises en œuvre pour contrôler la situation et empêcher une diffusion ultérieure, y compris des enquêtes internes et, si nécessaire, une coordination avec les autorités de régulation.

4. Signalement

L'équipe dédiée, composée du Directeur Général, du Responsable de la Conformité en matière de Lutte contre le Blanchiment d'Argent (LCB-FT) et du Directeur Technique, est chargée des obligations de signalement.

4.1. Processus interne de signalement

Paymium établit et maintient des procédures efficaces qui lui permettent d'évaluer, aux fins de soumission d'une STOR, s'il existe des circonstances indiquant qu'un abus de marché a été commis, est en train d'être commis ou est susceptible de l'être.

Paymium a mis en place un processus interne de signalement organisé en 3 étapes :

1. Identification / suspicion d'un cas potentiel d'abus de marché ;
2. Évaluation initiale ;
3. Escalade.

L'intégralité du processus de signalement doit être achevée dans un délai de cinq (5) jours ouvrés pour déterminer si une STOR sera transmis à l'AMF.

4.2. Confidentialité

Paymium garantit et maintient la confidentialité des informations à tout moment.

Des procédures sont en place pour éviter la divulgation à la personne concernée par le STOR ou à toute personne non autorisée à être informée en raison de son rôle au sein de Paymium. Cela inclut la protection des informations liées à :

- la génération d'alertes ou les évaluations menant à la soumission d'une STOR, en veillant à ce que l'équipe dédiée complète le STOR sans demander d'informations à la personne impliquée pour remplir des champs spécifiques ;
- la soumission d'une STOR ou toute intention de le soumettre à l'autorité compétente.

Les données personnelles dans le cadre de cette politique et de ses procédures de mise en œuvre sont traitées conformément au Règlement sur la Protection des Données.

4.3. Transmission d'une STOR à l'AMF

Paymium a mis en place un processus de signalement qui garantit la soumission rapide d'une STOR dès qu'un soupçon raisonnable d'abus de marché est identifié.

En cas de retard, l'équipe dédiée doit inclure dans le STOR une explication détaillée, abordant les raisons du retard et décrivant les circonstances spécifiques ayant conduit à la soumission tardive, comme l'exige l'AMF.

Paymium transmet, sans délai, une STOR, ainsi que tout document justificatif ou pièce jointe, à la Division de la Surveillance des Marchés de l'AMF.

4.4. Conservation des STOR et des observations de marché

Paymium conserve les informations documentant les analyses effectuées concernant les ordres, transactions et aspects du fonctionnement de la technologie des registres distribués pouvant constituer des abus de marché pendant une période de dix (10) ans. Ces informations incluent :

- les analyses réalisées ;
- les raisons de la soumission ou de la non-soumission d'une STOR.

Ces informations seront fournies à l'AMF sur demande.

Les personnes ayant accès au stockage des données sont le Directeur Général, le Responsable de la Conformité LCB-FT et le Directeur Technique.

*
* *