ACCORD DE COOPÉRATION
ENTRE L'AUTORITÉ DE CONTRÔLE PRUDENTIEL ET DE RÉSOLUTION (« ACPR »),
LA BANQUE DE FRANCE (BDF)
ET LA MONETARY AUTHORITY OF SINGAPORE (« MAS »)
EN MATIÈRE DE CYBER-SÉCURITÉ

1. Introduction

1.1. L'Autorité de contrôle prudentiel et de résolution veille à la préservation de la stabilité du système financier et à la protection des clients, assurés, adhérents et bénéficiaires des personnes soumises à son contrôle. Les missions de l'ACPR sont définies à l'article L. 612-1 du *Code monétaire et financier*. L'ACPR est chargée de superviser les établissements de crédit, les entreprises d'investissement (autres que les sociétés de gestion de portefeuille), les membres des marchés réglementés, les adhérents aux chambres de compensation, les entités du secteur des assurances et certains autres établissements financiers établis en France, y compris dans les territoires français d'outre-mer.

1.2. La Banque de France est la banque centrale nationale qui fait partie intégrante de l'Eurosystème. Dans ce cadre, la BDF veille à la stabilité du système financier, au bon fonctionnement et à la sécurité des systèmes de paiement, des infrastructures de marché et des moyens de paiement en application des articles L. 141-4, L. 141-5-1 du *Code monétaire et financier* et du paragraphe 2 de l'article 127 du Traité sur le fonctionnement de l'Union européenne.

1.3. L'Autorité monétaire de Singapour est la banque centrale et le superviseur des acteurs du secteur financier à Singapour, établie en vertu de la section 3 du *Monetary Authority of Singapore Act*. La MAS est responsable, entre autres, de la promotion de la cyber-résilience du secteur financier.

1.4. L'ACPR, la BDF et la MAS (ci-après collectivement dénommées « les autorités » et individuellement une « autorité ») conviennent que la coopération dans le domaine de la cyber-sécurité, en particulier l'élaboration de protocoles d'accord entre les autorités du secteur financier portant sur le partage d'informations liées à la cyber-sécurité (« informations ») et visant à accroître la connaissance du panorama des cyber-menaces, favorise une cyber-résilience accrue des écosystèmes financiers.

1.5. En vue de la coopération entre les autorités dans le domaine de la cyber-sécurité, le présent accord de coopération établit un cadre formel pour la conclusion de protocoles d'accord pour le partage d'informations, sur une base volontaire et au mieux des possibilités des autorités, conformément aux dispositions légales et réglementaires applicables.

1.6. Le présent accord de coopération ne crée en aucun cas, directement ou indirectement, de droits ou d'obligations pour les autorités.

2. Missions de la BDF, de l'ACPR et de la MAS

2.1. La coopération, promue par les instances décisionnaires des autorités, est inscrite dans les missions des autorités, au sein de leurs juridictions respectives.

2.2. La loi française applicable aux fins du présent accord est le *Code monétaire et financier*, notamment son article L. 632-7 qui autorise la BDF et l'ACPR à conclure le présent accord de coopération. Les dispositions relatives aux modalités de secret professionnel sont définies aux articles L. 142-9 et L. 612-17 du *Code monétaire et financier*.

3. Périmètre de coopération

3.1. Les autorités conviennent d'étudier des protocoles d'accord, notamment des règles et procédures définies conformément à l'article 6.1, pour le partage d'informations prévu à l'article 4, sur une base volontaire et au mieux de leurs possibilités.

3.2. Les autorités peuvent convenir de visites afin d'échanger des informations et d'encourager le partage de savoirs entre autorités ou faciliter des échanges de personnel, ou l'échange de publications de travaux de recherche communs, afin de promouvoir la coopération.

3.3. Les autorités peuvent envisager la mise en place d'activités liées au développement des compétences telles que la participation à la conduite d'exercices de crise transfrontières ou à des actions de formation du personnel, par l'une ou l'autre autorité, afin de tirer parti des connaissances et du soutien de l'autre autorité et de renforcer la coopération entre les autorités.

4. Périmètre du partage d'informations

4.1. Conformément aux articles 5, 7 et 8 du présent accord, les autorités conviennent de partager les informations pertinentes pour leurs juridictions, telles que :

(a) la loi applicable et les orientations en matière de cyber-sécurité, notamment en réponse à des cyber-incidents ;

(b) les cyber-incidents (notamment les cyber-attaques et les tentatives probables d'attaques) qui pourraient avoir des répercussions sur le secteur financier dans les juridictions respectives des autorités et ;

(c) les cyber-menaces et les enseignements relatifs à la cyber-sécurité en lien avec le secteur financier.

5. Principes directeurs pour le partage d'informations

5.1. Les autorités conviennent d'adopter les principes suivants en matière de partage d'informations :

(a) A titre volontaire – Chaque autorité peut, de manière flexible et à sa discrétion, partager des informations en tenant compte de leur degré de sensibilité et des répercussions de leur circulation. Toute réserve sur l'exactitude ou l'exhaustivité des informations relatives aux cyber-incidents, au moment du partage d'informations, devra être indiquée.

(b) Célérité – Chaque autorité partagera les informations au mieux de ses possibilités et dans les meilleurs délais, en fonction des circonstances. Les informations peuvent être partagées tant qu'un degré raisonnable de validité est établi, même s'il n'est pas totalement certain que les informations sont exactes ou exhaustives.

(c) Anonymat – Chaque autorité partagera les informations sans nommer ni ses sources, ni l'identité des établissements financiers ni aucun de leurs clients.

(d) Confidentialité – Chaque autorité partagera les informations conformément aux articles 7 et 8, aux règles et procédures mentionnées à l'article 6.1 du présent accord, afin de garantir le traitement approprié et la transmission sécurisée des informations à des destinataires identifiés au sein des autorités.

6. Classification des informations et modalités d'échange

6.1. Afin de garantir que le partage des informations relatives à la cyber-sécurité est effectué conformément aux principes directeurs énoncés aux articles 5, 7 et 8, les autorités conviennent d'établir des règles et procédures supplémentaires pour : (i) identifier et classifier les informations en fonction de leur sensibilité, (ii) identifier les personnes qui peuvent recevoir des informations en fonction de cette classification et (iii) établir et arrêter les modalités de communication des informations, avec chaque autorité.

6.2. Les règles et procédures visées à l'article 6.1 devront être soumises à la gouvernance et au dispositif de contrôle interne de chaque autorité.

7. Utilisation autorisée de l'information

7.1. Chaque autorité n'utilisera les informations non publiques obtenues de l'autre autorité dans le cadre du présent accord que pour les fins auxquelles ces informations ont été transmises.

RWJ

D DS

7.2. Si une autorité souhaite utiliser des informations non publiques transmises dans le cadre du présent accord pour une fin différente de celles mentionnées à l'article 7.1, elle doit au préalable consulter l'autre autorité afin d'obtenir son consentement écrit pour l'utilisation qu'elle souhaite faire de ces informations. Si ce consentement est refusé, les autorités se concerteront afin d'examiner les raisons du refus et, le cas échéant, les conditions dans lesquelles l'utilisation que l'autorité souhaite faire de ces informations pourrait, malgré tout, être autorisée.

7.3. Au sein de leurs autorités respectives, l'information non publique échangée dans le cadre du présent accord ne sera transmise qu'aux personnes identifiées selon les règles et procédures prévues à l'article 6.1 (ii) ou aux personnes dont le nom aura été notifié, par écrit, à l'autorité qui a fourni l'information. Les autorités ne partageront l'information non publique échangée dans le cadre du présent accord avec aucune autre personne de leur autorité, sans l'accord préalable de l'autorité qui a fourni l'information et uniquement pour les fins auxquelles cette autorité a donné son accord.

8. Confidentialité des informations

8.1. Sauf disposition contraire des articles 8.2 et 8.3, chaque autorité préservera la confidentialité des informations non publiques échangées dans le cadre du présent accord, des requêtes d'information et des suites apportées dans le cadre du présent accord et de leur contenu et de toute autre partage d'information intervenu au titre du présent accord, conformément à la loi applicable.

8.2. Chaque autorité doit obtenir le consentement préalable écrit de l'autre autorité avant de partager les informations non publiques reçues dans le cadre du présent accord avec toute entité non signataire du présent accord. L'autorité dont le consentement est recherché devra prendre en compte le degré d'urgence de la demande et répondre rapidement. Si ce consentement est refusé, les autorités se concerteront afin d'examiner les raisons du refus et, le cas échéant, les conditions dans lesquelles la divulgation d'informations prévue par l'autorité pourrait être autorisée.

8.3. Dans la mesure du possible, toute autorité qui est juridiquement tenue de divulguer une information non publique obtenue dans la cadre du présent accord, informera l'autre autorité. Lorsqu'elle répond à la demande, l'autorité invoquera les exemptions et privilèges appropriés, s'il en existe.

8.4. Les autorités prévoient que le partage ou la divulgation d'informations non publiques, notamment de documents délibératifs et consultatifs tels que des analyses, des avis ou des recommandations écrits en lien avec les informations non publiques, préparés par ou pour le compte d'une autorité, conformément aux dispositions du présent accord, ne constitueront pas une levée de l'obligation de confidentialité.

9. Consultation

9.1. Les autorités réexamineront régulièrement le présent accord et se concerteront, si nécessaire, en vue d'améliorer sa mise en œuvre ou en cas de difficultés.

9.2. Les autorités se consulteront en cas de changement de leurs lois respectives ou de toute autre difficulté qui pourrait rendre nécessaire un amendement du présent accord.

9.3. Les autorités se consulteront en cas de différence d'interprétation ou de difficulté dans la mise en œuvre du présent accord.

10. Entrée en vigueur, résiliation et modification

10.1. Le présent accord entre en vigueur à la date de signature par les autorités et restera en vigueur sauf si l'une des autorités souhaitait le résilier, par notification écrite adressée aux autres autorités, dans un délai de 30 jours.

10.2. Dans tous les cas, après résiliation, les dispositions des articles 5.1(d), 7 et 8 continueront de s'appliquer à toute information relative à la cyber-sécurité déjà transmise dans le cadre du présent accord.

Signé par les parties :

Pour l'ACPR

Denis BEAU
Président désigné
Date : 31 OCT. 2019

Pour la MAS

Ravi MENON
Directeur général
Date : 13th November 2019

Pour la Banque de France

François VILLEROY de GALHAU
Gouverneur
Date : 31 OCT. 2019