Association Luxembourgeoise des Compliance Officers

COMPLIANCE INSIDER 32

The New Wave of Regulation

SOMMAIRE

ALCO Association Luxembourgeoise des Compliance Officers

COMPLIANCE INSIDER 32

Rédacteurs en chef : Sandrine Wesquy & Thierry Grosjean
Contributeurs : Steven Curfs, Géranise Hurtis, Oumarou Ide, Jean-Sébastien Kroonen, Matthieu Sarrazin
Conception & coordination : 360Crossmedia
relations@360Crossmedia.com - 35 68 77
Directeur artistique : 360Crossmedia/FB
Photo couverture : © DR
Tirage : 500 exemplaires

DEAR COMPLIANCE OFFICERS, DEAR FRIENDS,

Mifid II on top of a wave of regulatory changes of an unknown magnitude has come into force. The big bang did not happen: Mifid II softly become a reality. It witnesses a new world that we, as Compliance Officers, need to manage: in Europe, the transposition of the directive in the national legislation has followed a bumpy road, in content and timing; NCAs have not digested this unprecedented complexity yet and practical guidance is often missing. Moreover the interdependencies between regulations have never been as large with a lot of different players (markets, issuers, information providers...). It creates a world of uncertainty where we crucially need guidance for all of us. ALCO has a key role in that and we, Compliance Officers, have never felt the necessity as much as today to gather information through ALCO, ABBL, ALFI working groups, private exchange groups or multiple bilateral talks to define what a proper interpretation or attitude is. Since last year, the newly elected Board has taken new initiatives to give you additional support. They are plenty of working groups or events where you can challenge your positions with the ones of your peers. Do not hesitate to apply or provide ideas for new groups or new discussion channels. In the meantime, new challenges have knocked at our door: GDPR is also becoming a new reality. The technicality of our job has significantly increased these last years due to the upcoming technologies and cryptocurrencies. Hopefully you will find some answers to your questions in the following pages.

Marie Bourlond – Laurent Moser – Vincent Salzinger
Présidents de l'ALCO

Marie Bourlond
Président de l'ALCO

She has been Chief Compliance Officer of the Banque Internationale à Luxembourg S.A. since May 2012. Before she held various positions in BIL group, notably in Internal Audit, Risk Management and Wealth Management.

She was appointed co-chairman of the Association of Luxembourg Compliance Officers in March 2017.

Laurent Moser
Président de l'ALCO

Since April 2011, Laurent Moser has held the position of Head of Compliance & Conducting Officer at Pictet Asset Management (Europe) S.A.. He was previously working for Pictet & Cie (Europe) S.A. as Fund Accountant and Head of the Transfer Agency department.

He was appointed co-chairman of the Association of Luxembourg Compliance Officers in March 2017.

Vincent Salzinger
Président de l'ALCO

After a first experience in the steel industry and having spent 3 years at Deloitte as Senior External Auditor, Vincent Salzinger joined KBL European Private Bankers, where he held various positions (Internal Audit, M&A and then Compliance). Since November 2007, he has been the bank's Group Chief Compliance Offer.

He has been a director of the Association of Luxembourg Compliance Officers since 2008 and was appointed co-chairman of the association in March 2017.

MIFID II COMPLIANCE MONITORING PLAN
JUNE 2018
ALCO - WORKING GROUP 51

© DR

In the aftermath of the financial crisis, the European Commission has revised the global regulatory framework applicable to markets in financial instruments in the European Economic Area by the adoption of new rules. These consist of new legal instruments that apply from 3 January 2018. The main documents are:

- Directive 2014/65 on markets in financial instruments (MiFID II) (https://eurlex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0065&from=EN),

© DR

Vincent Salzinger
Président ALCO

- Regulation 600/2014 on markets in financial instruments (MiFIR) (https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02014R0600-20160701).

Comprehensive online libraries of European and Luxembourg rules and supporting documents are published by:

- ESMA
- CSSF

Aiming at strengthening investor protection and transparency of the financial market, these legal instruments:

- ensure that organized trading takes place on regulated platforms,
- introduce rules on algorithmic and high frequency trading,
- improve the transparency and oversight of financial markets – including derivatives markets - and addressing some shortcomings in commodity derivatives markets,
- enhance investor protection and improving conduct of business rules as well as conditions for competition in the trading and clearing of financial instruments,

And set out requirements on:

> **" The purpose of the working group, composed of ALCO members, was to issue practical guidelines in the form of a table, that would assist Compliance Officers to implement MiFID II monitoring plans in investments firms. "**
> Vincent SALZINGER,
> Président ALCO

- disclosure of data on trading activity to the public,
- disclosure of transaction data to regulators and supervisors,
- mandatory trading of derivatives on organized venues,
- removal of barriers between trading venues and providers of clearing services to ensure more competition,
- specific supervisory actions regarding financial instruments and positions in derivatives.

In Luxembourg, the 2018 Law amended the law of 5 April 1993 on the financial sector (the «LFS») and the Law of 13 July 2007 has been replaced by the Law of 30 May 2018 on markets in financial instruments. In addition, the Grand-ducal Regulation of 30 May 2018 on the protection of financial instruments and funds belonging to clients, product governance obligations and rules applicable to the reception of fees, commissions or any monetary or nonmonetary benefits replaced the Grand-ducal Regulation of 13 July 2007 on organisational requirements and rules of conduct in the financial sector.

The *Commission de Surveillance du Secteur financier* (CSSF) had already published the Circular 17/665 on ESMA Guidelines for the assessment of knowledge and competence on 31 July 2017.
The purpose of the working group, composed of ALCO members, was to issue practical guidelines in the form of a table (the MiFID II Compliance Monitoring Plan) that would assist Compliance Officers to implement MiFID II monitoring plans in investments firms. It has been split into four sub-working groups:

Sub working group I:

- **Topics:** Suitability (including investor profile) & appropriateness (including complex and non-complex products), inducements & investment research, classification of clients.

Sub working group II:

- **Topics:** Corporate governance (including management bodies (ref CRD IV)), remuneration & conflicts of interest (including underwriting & placing), personal transaction, complaints handling, staff knowledge & competence, independent advice and non-independent advice.

Sub working group III:

- **Topics:** Product governance (manufacturer / distributor: target market), best execution and client order handling, record keeping / recording of phone conversations and electronic communications, safekeeping of client assets.

Sub working group IV:

- **Topics:** Client information, client reporting, costs & charges, transaction reporting. The MiFID II Compliance Monitoring Plan is not intended to cover all MIFID II topics but focuses on its main or most relevant topics helping investment firms to choose and determine the controls to be performed by theme in order to ensure regulatory compliance. It does not contain a full analysis of the applicable rules nor does it constitute an opinion of ALCO members. Furthermore, this document has not been vetted by the competent authority. It is each investment firm's responsibility to establish the relevant set of controls and to adapt its control plan with regard to its activities, size, structure and organisation.

Finally, the table does not aim to cover all MiFID II controls: considering the characteristics of the Luxembourg market and the time schedule available for performing

> **" The working group has been working on key controls to avoid key compliance risk "**
> Vincent Salzinger
> Président ALCO

this exercise, the following topics have not been covered in this control plan: systematic internalize regime, direct market access, algorithmic trading, pre and post trade transparency and derivatives (including commodity derivatives).

As the Luxembourg legislation was not implemented when this report was being drawn up, the legal references are based on the European legislation and regulation hereinafter detailed in the table by the following acronyms. The table also lists related existing regulation: (see table ›)

Some provisions mentioned in the report might be amended or clarified by the Luxembourg legislation.

The proposed controls with a detailed description have been defined in the two columns «Purpose of controls» and «Description of control (details) ». Depending on the organisation, the list of the controls can be performed by the Compliance function or by another department (probably a 2nd Line of Defense depending on the size and structure). Whatever the function/department in charge of carrying out these controls, it is up to the Compliance function to ensure that all the necessary controls have been put in place, to analyse the results of these controls, to put in place the relevant measures, to mitigate the risks, to track progress made based on raised issues and to report to its management bodies.

The working group has been working on key controls to avoid key compliance risk, but it is up to each's investment firm's business model and exposure to such topics to find its own appropriate risk rating.

The working group did not propose a frequency for these controls, which remains at the discretion of each investment firm and which should be performed on a risk based approach.

Sponsor of the ALCO working group: Vincent SALZINGER.

For Working Group 51,
Nuno CASAL,
Emmanuelle CAUMONT,
Inida CELOMEMAG,
Sylvain DALLE,
Béatrice DEBARNOT,
Karelle ENCLOS,
Alexander ENDRIKAT (co-chairman),
Oumarou IDE (cochairman),
Alexandra MELIS,
Christiane SCHON,
Céline TROQUET.

MiFID II	Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU
MiFIR	Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012
Dir 2017/593	Commission Delegated Directive (EU) 2017/593 of 7 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to safeguarding of financial instruments and funds belonging to clients, product governance obligations and the rules applicable to the provision or reception of fees, commissions or any monetary or non-monetary benefits
Reg 2017/565	Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive
Reg 2017/590	Commission Delegated Regulation (EU) 2017/590 of 28 July 2016 supplementing Regulation (EU) No 600/2014 of the European Parliament and of the Council with regard to regulatory technical standards for the reporting of transactions to competent authorities
ESMA/2016/1451	Final Report on Guidelines on transaction reporting, order record keeping and clock synchronisation under MiFID II
ESMA/2016/1452	Guidelines on Transaction reporting, order record keeping and clock synchronisation under MiFID II: Transaction reporting validation rules published by ESMA on 20 July 2017
CSSF 17/674	Circular CSSF 17/674 of 30 November 2017 on the transposition of ESMA Guidelines on transaction reporting and order record keeping under MiFIR and clock synchronisation pursuant to MiFID II and details on transaction reporting on financial instruments under MiFIR
ESMA 71-1154262120-153 (ESMA/1886 FR)	ESMA Guidelines for the assessment of knowledge and competence (rev) of 3 January 2017
CSSF 17/665	Circular CSSF 17/665 of 31 July 2017 on the implementation of ESMA Guidelines for the assessment of knowledge and competence
Q&A Inv Prot	Questions and Answers on MiFID II and MiFIR investor protection and intermediaries topics ESMA35-43-349
ABBL Guidelines	ABBL Industry Guidelines on Markets in Financial Instruments Directive 2014/65/EU, Version 1.0 of 28 September 2017
CSSF Reg 16-07	CSSF Regulation N° 16-07 of 11 November 2016 relating to out-of-court complaint resolution
Dir 2013/11/EU	Directive 2013/11/EU of the European Parliament and the Council on consumer Alternative Dispute Resolution
CSSF 12/552	Circular CSSF 12/552 of 11 December 2012 (as amended) on central administration, internal governance and risk management
Reg 596/2014/EU	Regulation (EU) No 596/2014 of 16 April 2014 of the European Parliament and of the Council on market abuse (market abuse regulation)

RGPD : OBLIGATIONS ET MISE EN CONFORMITÉ

Depuis le 25 mai dernier, le nouveau règlement général 2016/679 relatif à la protection des données à caractère personnel (« RGPD ») est entré en vigueur.

© DR

Dans le cadre de ses activités quotidiennes, chaque entreprise est amenée à traiter des données personnelles, à savoir, des données permettant d'identifier directement ou indirectement une personne physique (nom, prénom, adresse email même professionnelle, signature, coordonnées bancaires, cv, copie de pièce d'identité, données liées au salaire ou à l'expérience professionnelle, etc.). Ces données peuvent concerner des employés et leurs familles, des postulants envoyant leur cv, des consultants externes, des sous-traitants (personnes de contact, employés, etc.),

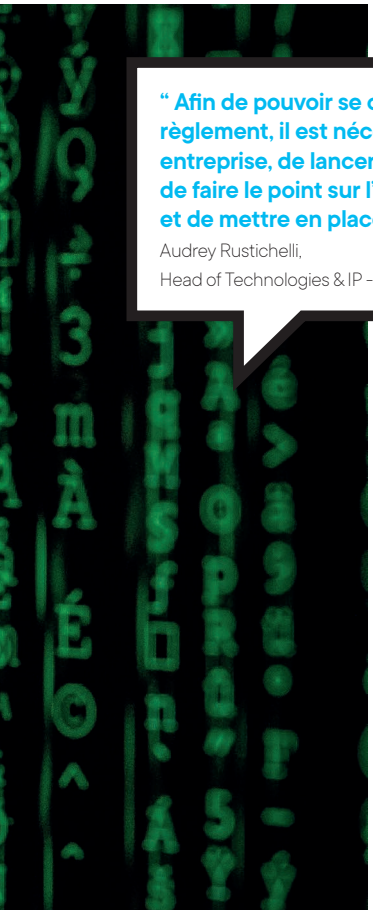
© DR

Audrey Rustichelli
Head of Technologies & IP

des clients (employés, personnes de contact, directeur, etc.) et autres tiers avec lesquels une entreprise contracte et interagit ou au sujet desquels elle obtient des données personnelles directement ou indirectement (bénéficiaires économiques dans le cadre de vérifications liées aux obligations AML, etc.).

Le RGPD introduit un certain nombre de nouvelles obligations à la charge des entreprises agissant en tant que responsable de traitement (entité qui détermine les finalités et les moyens du traitement) ou comme sous-traitant traitant des données à caractère personnel pour le compte du responsable du traitement.

Le RGPD s'applique (i) au traitement des données à caractère personnel effectué dans le cadre des activités d'un responsable du traitement ou d'un sous-traitant établi sur le territoire de l'Union Européenne, que le traitement ait lieu ou non dans l'Union, mais également (ii) au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées à une



> **“ Afin de pouvoir se conformer à ce nouveau règlement, il est nécessaire, pour chaque entreprise, de lancer un projet en interne afin de faire le point sur l’état actuel de conformité et de mettre en place les mesures nécessaires. ”**
>
> Audrey Rustichelli,
> Head of Technologies & IP -mnks

offre de biens ou de services à ces personnes concernées dans l’Union, qu’un paiement soit exigé ou non desdites personnes, ou au suivi du comportement de ces personnes.

Afin de pouvoir se conformer à ce nouveau règlement, il est nécessaire, pour chaque entreprise, de lancer un projet en interne afin de faire le point sur l’état actuel de conformité et de mettre en place les mesures nécessaires.

Qu’est-ce que le fameux principe « d’Accountability » et comment s’y conformer?

Le RGPD transforme la manière dont les entreprises protègent les données personnelles en supprimant les formalités administratives (notifications préalables, demandes d’autorisation, etc.) devant auparavant être effectuées auprès des autorités locales compétentes (pour le Luxembourg, la Commission Nationale pour la Protection des Données « CNPD »). Depuis le 25 mai 2018, les entreprises sont tenues (i) de mettre en place les mesures qu’elles estiment nécessaires au regard de la nature, de la portée, du contexte et des finalités des traitements qu’elles effectuent ainsi que des risques potentiels pour les droits et libertés des personnes concernées et (ii) de documenter cette mise en conformité.

- La première étape consiste à procéder à un inventaire des traitements de données effectués. Cet inventaire doit notamment permettre d’identifier la nature des données personnelles traitées, pour quelles finalités et sur laquelle des bases légales listées dans le RGPD, le lieu et la durée de conservation de ces données, les potentiels destinataires, etc.

Le RGPD donne quelques pistes concernant les éléments à mettre en place. Notamment, les entreprises doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Ces mesures de sécurité peuvent être variées et doivent permettre de pouvoir garantir la confidentialité, l’intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitements ainsi que la disponibilité des données et l’accès à celles-ci dans des délais appropriés en cas d’incident physique ou technique.

Dans le cadre de l’inventaire réalisé, il est important que chaque entreprise implique ses équipes IT afin d’identifier les mesures de sécurité encadrant les traitements effectués et pose les bonnes questions : les accès aux applications IT ou serveurs contenant des données personnelles sont-ils bien gérés et suffisants ?; les employés ont-ils la possibilité d’encrypter leurs emails sortants ou de protéger certains documents par un mot de passe ?; les systèmes sont-ils bien protégés contre les intrusions externes et contre une utilisation abusive de la part des employés (encadrement et restriction des connexions de ports USB, etc.) ?; avons-nous un programme de continuité des opérations ?; avons-nous une procédure d’archivage, de classification ou de destruction de documents ?.

Le RGPD prévoit également l’obligation de nommer un délégué à la protection des données (« DPO »)

Audrey Rustichelli est en charge du département Technologies & IP chez MNKS.

Elle conseille ses clients sur un large éventail de questions liées aux technologies de l’information et les assiste dans le cadre de leurs projets de mise en conformité avec le GDPR.

Audrey gère également régulièrement la rédaction et à la négociation de contrats commerciaux (contrats de services, de distribution, d’agents commerciaux, de franchise, etc.).

dans certains cas spécifiques. Si l'entreprise ne tombe pas dans le champ de cette obligation, il est tout de même fortement conseillé de désigner une personne en interne qui sera en charge de maintenir une gouvernance appropriée en matière de protection des données personnelles et de vérifier que l'entreprise reste en conformité avec ses obligations.

Les entreprises sont en outre tenues de maintenir un registre des activités de traitement qui doit contenir un certain nombre d'informations listées par le RGPD. Un inventaire préalable bien fait donne une base solide pour préparer ce registre. Les autorités belges et françaises ont publié un modèle de registre.

Enfin, certains types de traitements listés par le RGPD et d'autres traitements identifiés comme pouvant constituer un risque devront faire l'objet d'une analyse d'impact. L'autorité française a publié un formulaire qui peut être utilisé dans ce cadre.

Comment gérer les droits des personnes concernées?

Le RGPD est venu renforcer les droits existants des personnes concernées en ce qui concerne la gestion de leurs données personnelles par des tiers et les a complété avec de nouvelles prérogatives pour les individus.

Les entreprises ont l'obligation de fournir un certain nombre d'informations préalables aux personnes concernées afin d'expliquer la manière dont ces données seront conservées et traitées. Le RGPD vient ajouter des informations à la liste déjà existante.

- Afin de se conformer à cette obligation il va falloir adapter les documents correspondants (clauses dans les contrats de travail, dans les conditions générales ou contrats signés par les clients ou sous-traitants, information dans les emails de réponse envoyés suite à la réception de cv par un candidat, etc.).

© DR

Parmi l'ensemble des droits octroyés aux personnes concernées, figurent également notamment (i) le droit d'obtenir la confirmation que ses données personnelles sont traitées par l'entreprise, et si oui, de demander l'accès à ces données ainsi que certaines informations relatives au traitement, (ii) le droit d'obtenir que les données soient rectifiées ou complétées, (iii) le droit d'obtenir l'effacement de ses données, (iv) le droit d'obtenir la limitation du traitement, (v) le droit de recevoir les données et de les transmettre à un autre responsable de traitement et (vi) le droit de s'opposer au traitement de ses données. Le RGPD pose des conditions spécifiques dans le cadre desquelles de telles demandes peuvent être effectuées.

La réception et la gestion de ces demandes doit se préparer en interne et faire l'objet de plusieurs actions préparatoires au sein de chaque entreprise afin d'être à même de gérer au mieux toute requête :

- Mettre en place un système de réception des plaintes. Il peut s'agir de la création d'une adresse email dédiée ou de la mise en place d'un outil de

gestion des plaintes qui assistera l'entreprise dans ce processus, tel que l'outil MyDPRights. Peu importe le canal de réception choisi, il est important que les personnes concernées puissent trouver facilement et sans frais le moyen de contacter une entreprise.

- Identifier la ou les personne(s) qui seront en charge de recevoir, coordonner en interne et gérer ces demandes (DPO ou autre). Cette personne devra vérifier que chaque demande est traitée dans le délai d'un mois prévu par le RGPD.
- Créer une procédure interne à suivre afin d'encadrer par écrit le processus de réception des demandes, de vérification de l'identité de la personne contactant l'entreprise et de préciser les critères à prendre en compte afin de déterminer (i) si une demande est valide ou non et (ii) si l'entreprise peut favorablement y répondre. En effet, une entreprise ne pourra faire droit à une demande d'effacement si cette dernière est toujours légalement tenue de conserver les données visées ou est en relation contractuelle avec cette personne (ex. les données KYC).

Comment gérer ses sous-traitants ?

L'utilisation d'un sous-traitant doit être encadrée par un contrat écrit ou tout autre acte juridique contenant des mentions obligatoires, mentions largement étendues par le RGPD afin de couvrir les obligations des sous-traitants dans le cadre du règlement.

Ainsi, les actions suivantes devront être prises :

- Effectuer un inventaire de ses sous-traitants actuels et vérifier si les contrats signés avec ces derniers contiennent des clauses adaptées dans le cadre du RGPD. En fonction du type de données auxquelles le sous-traitant peut avoir accès et de la nature des services proposés, il peut être nécessaire de contacter ce dernier afin de lui faire signer un avenant contenant les mentions contractuelles liées au traitement de données personnelles ou un contrat spécifique encadrant ce traitement ;
- Si l'entreprise agit elle-même en tant que sous-traitant (société proposant des services de gestion, fiduciaire, etc.), il sera nécessaire d'adapter les modèles existants de contrats ou conditions générales signées par les clients afin d'y insérer les clauses obligatoires visées par le RGPD et de proposer si nécessaire la signature d'un contrat encadrant les traitements de données personnelles.

> **" L'utilisation d'un sous-traitant doit être encadrée par un contrat écrit ou tout autre acte juridique contenant des mentions obligatoires. "**
> Audrey Rustichelli,
> Head of Technologies & IP - mnks

Comment gérer les transferts de données ?

Toute entreprise transférant des données personnelles hors de l'Espace Economique Européen vers un pays considéré comme n'offrant pas un niveau de protection suffisant, doit s'assurer que les garanties appropriées prévues par le RGPD sont bien mises en place. Il pourra s'agir de la signature avec le destinataire des données (intra groupe ou vers des tiers) de clauses contractuelles types se trouvant sur le site de la Commission Européenne, de la collecte du consentement préalable des personnes concernées par ce transfert ou de la mise en place de Règles d'Entreprises Contraignantes au sein d'un groupe d'entreprises.

Comment gérer ses obligations en matière de violation de données personnelles ?

Le RGPD impose aux entreprises responsables de traitements de notifier une violation de données personnelles à l'autorité de contrôle compétente, et dans certains cas aux personnes concernées, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes concernées.

La CNPD a mis à disposition sur son site Internet un formulaire de notification de violation, qu'il est recommandé d'utiliser.

- Afin de pouvoir réagir vite dans le cadre du délai imparti en cas de violation, il est conseillé d'établir en amont une procédure écrite interne à suivre afin (i) de déterminer les personnes responsables en interne pour gérer et prendre la décision de notifier ou non, (ii) de préciser les critères à prendre en considération afin d'établir si la violation est susceptible d'engendrer un risque pour les personnes concernées, (iii) de lister les informations devant être fournies à la CNPD et établir la procédure à suivre afin de les collecter et (iv) de déterminer le format de communication aux personnes concernées le cas échéant.

KYC : LE PROCESSUS DE CONNAISSANCE DU CLIENT

Le processus de connaissance du client (KYC : "Know Your Customer") est, avec la surveillance des opérations, l'un des deux piliers de la lutte contre le blanchiment d'argent et le financement du terrorisme (LAB/FT), et du respect des règles sur les embargos et les sanctions financières internationales. Traditionnellement, ce processus est supporté par les acteurs clés que sont les métiers commerciaux, accompagnés par la fonction Compliance.

© DR

Pour renforcer la maîtrise de ces risques et dans un contexte réglementaire de plus en plus exigeant, en 2016 le Groupe BNP Paribas a décidé de se doter d'**un ensemble de normes exhaustives et homogènes** en la matière, applicables dans tous les métiers et dans toutes les géographies, dans le respect des réglementations locales.

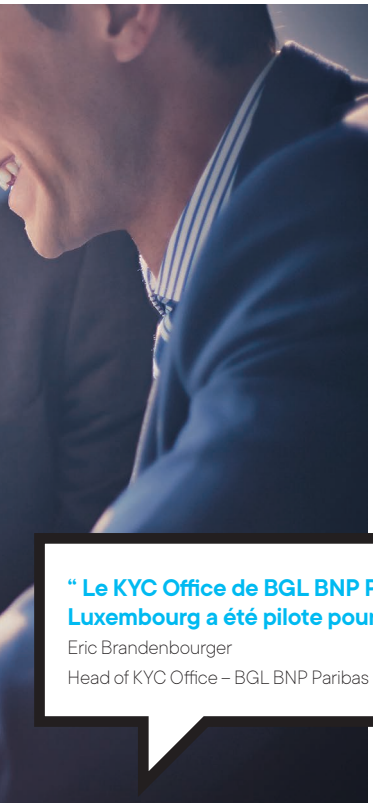
Afin d'être en mesure de se conformer de manière efficace aux nouvelles exigences (pression réglementaire croissante, 4e directive AML *Anti Money Laundering*, etc.), BGL BNP Paribas a décidé d'être précurseur en professionnalisant la filière par la **création de centres de compétences clients** (Due Diligence Team) et d'un **parcours professionnel au sein d'une nouvelle structure** : le **KYC Office**, qui a vu le jour en janvier 2017.

Le KYC Office de BGL BNP Paribas a été «pilote» pour le Groupe BNP Paribas.

Le **rôle des Due Diligence Team**s, situés entre les métiers commerciaux et la fonction Compliance et rattachés à la Direction des Opérations, consiste notamment à :

- assurer un support aux Relationship Managers (collecte d'informations ou documentation auprès des clients ou d'autres sources, mise à jour des dossiers et des systèmes, etc.) ;
- assurer la qualité, la complétude et la cohérence des dossiers KYC ;
- réaliser l'analyse transactionnelle ;
- piloter les programmes de révision ;
- réaliser des recherches de sanctions ou de notoriété ;
- pré-analyser les risques AML (Anti Money Laundering) ;
- participer au processus de décision (préparation, organisation et secrétariat des Comités d'Acceptation Clients, suivi des décisions et des réserves) ;
- prendre en charge le reporting vers la Direction de la banque et/ou du Groupe BNP Paribas.

Les KYC Officers sont en charge d'apporter les éléments à la décision de poursuivre ou non la relation commerciale.
Cette construction d'envergure



> **“ Le KYC Office de BGL BNP Paribas Luxembourg a été pilote pour le groupe ”**
> Eric Brandenbourger
> Head of KYC Office – BGL BNP Paribas


© DR

Jean-Christophe Schmitz
Deputy Head of KYC Office

Titulaire d'un DESS en Mathématiques et Informatiques appliqués à la Finance et à l'Assurance à Sophia Antipolis (Nice), Jean-Christophe Schmitz rejoint la Banque Générale du Luxembourg en 2005. Après plusieurs projets au Luxembourg et en Belgique en tant que responsable de la maîtrise d'œuvre puis maîtrise d'ouvrage, Jean-Christophe rejoint la Direction des Opérations de BGL BNP Paribas en 2013. Au sein du département Administration Comptes et Clients, il prend en charge la responsabilité de l'Administration Comptes avant de devenir responsable d'Administration Clients en 2015. A la création du KYC Office en janvier 2017, il est nommé Deputy Head of KYC Office, département dont il prendra la responsabilité en octobre 2018.

Eric Brandenbourger
Head of KYC Office

Eric Brandenbourger a débuté sa carrière chez Paribas Luxembourg en octobre 1989 dans le cadre de la 1re édition de la Formation bancaire de l'ABBL. Il a occupé diverses fonctions de management opérationnel et gestion de projets transverses au sein des Opérations de la banque : Euro, An 2000, missions de qualité / productivité / organisation, fusions BNP Paribas Luxembourg et BGL BNP Paribas. Lors de cette dernière, il prend la responsabilité du Département Administration Comptes et Clients avant de contribuer à la création en janvier 2017 du KYC Office dont il est nommé responsable. Il poursuivra son parcours en prenant la responsabilité du Département Paiements, Comptes et Flux de BGL BNP Paribas à partir d'octobre 2018.

s'est étalée tout au long de l'année 2017. Après les fondations, l'enjeu est maintenant d'industrialiser le dispositif.

18 mois plus tard...

Le KYC Office a rejoint les acteurs clés du dispositif LAB/FT en devenant un véritable partenaire des métiers et de la fonction Compliance.

Il joue un rôle de facilitateur dans l'appropriation des changements et l'harmonisation des processus et procédures entre les différents métiers de la banque. Il lui offre une vue précise de sa base de coût en matière de KYC et enfin, il permet de l'optimiser au travers de la polyvalence et l'allocation dynamique des ressources.

Ses défis à court/moyen termes en 4 axes :

KYC OFFICE

Ressources Humaines Poursuivre la montée en compétence de KYC Officers.	**Conformité/ Réglementation** Suivre l'évolution des normes et réglementation. *Reliance* au sein du Groupe BNP Paribas
Data Management Assurer la qualité des référentiels sur lesquels se base le dispositif KYC.	**Digitalisation** Poursuivre l'intégration des nouveaux outils de workflow digitaux.

Le KYC Office, en plus de ces 4 axes de développement devra composer avec l'évolution de l'écosystème KYC sur la Place. En effet, l'arrivée de nouveaux acteurs spécialisés en matière de KYC et les évolutions réglementaires majeures telles que la création du registre des bénéficiaires effectifs (cf. transposition de la Directive UE 2015/849) façonnent les challenges de demain.

BGL BNP PARIBAS

Yuri **Broodman** (China Construction Bank (CCB))

The life of a Compliance Officer

What is your career path?

During my career as navy officer in The Netherlands I completed additional studies in operational audit which helped me to start working in the private sector within audit. When I moved to Luxembourg in November 2008 (a very snowy month in my memory) I shortly worked as internal auditor with RBC (still RBC Dexia at that time) before starting my Compliance journey at HSBC's Private Bank in a brand new building on boulevard d'Avranches.

Few years later I was Country Head of Compliance at HSBC and besides a few extra grey hair I had gained a great deal of Compliance experience - especially during the last few years while HSBC was operating under a Deferred Prosecution Agreement. In 2016 I continued my Compliance career as CCO for PayPal in Luxembourg where I expended my Compliance experience in a different part of the financial services.

" Compliance Officers need to be eager to learn about new trends and business developments to be able to identify any potential compliance issues at an early stage. "

Yuri Broodman

(China Construction Bank (CCB))

Time has flown since and it is with great pleasure that I recently continued my Compliance career with China Construction Bank adding yet another facet of global financial services to my work Compliance career path.

What do you enjoy most in your role?

I enjoy many aspects in my role as Chief Compliance Officer, but most of all I enjoy leading multi cultural teams of often young enthusiastic Compliance professionals. Separate from mentoring them in their Compliance career as I was mentored by my previous Compliance managers, and empowering them in their day-to-day work I love seeing my team engaging with business colleagues as a trusted partner who helps them to navigate through the ever increasingly complex world of rules and regulations.

Furthermore, I love the fact that as Compliance Officer you get a pretty broad view of any organisation you work in and with formulating good recommendations we can help Senior Management running the business in a compliant way - so that we all can sleep better at night.

What skills does someone working in the area need?

In my view the Compliance Officers of this time and age require much more than only knowledge about rules and regulations; they certainly also require strong soft skills in terms of people management and even broader stakeholder management in general. An average Compliance Officer nowadays probably has around 5 different (groups of) stakeholders ranging from his/her own team to a Board of Directors, Authorised Management, Regulatory bodies, Group internal Compliance in case one works for an international organisation, other department heads and potentially also remote Compliance team members in branches of other offices abroad.

Keeping this in mind the skill of maintaining a good work-life balance is certainly one a Compliance Officer can't lack, should he / she wish to be successful on the longer term.

Furthermore I think that the current Compliance Officers need to be eager to learn about new trends and business developments to be able to identify any potential compliance issues at an early stage.

Last but certainly not least a Compliance Officer needs to work as a partner to the business, while keeping his/her back straight and being able to explain complex regulatory matters in a simple way to other colleagues including Senior Management.

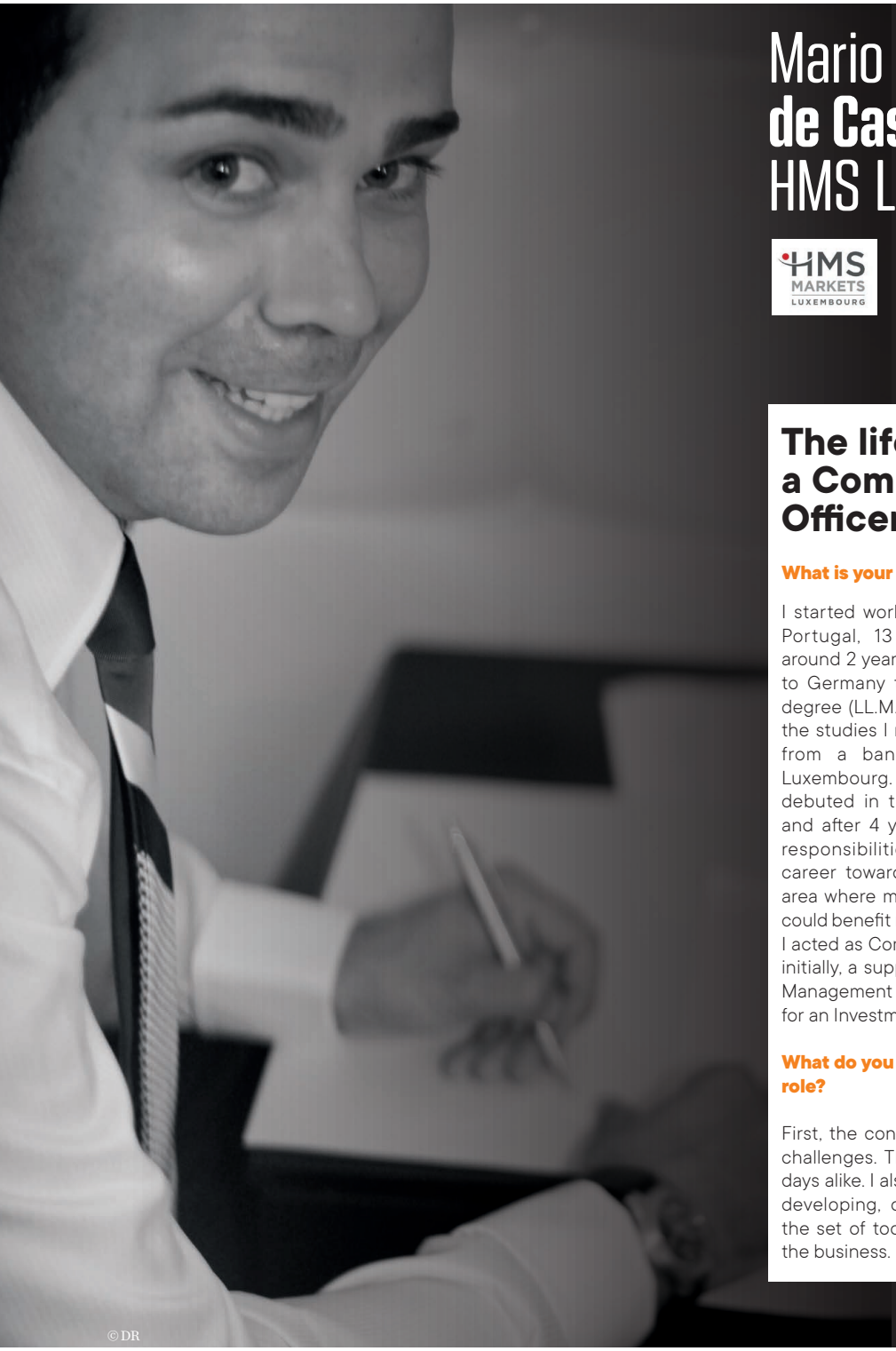
How do you see the Compliance Officer of the future?

The Compliance Officer of the future will certainly have to adapt with the fast moving financial industry and regulatory change in general. Even thou I love all aspects of Compliance I predict that there will be division between the different Compliance disciplines - Financial Crime Compliance and Regulatory Compliance which require different knowledge and experience.

What do you want to share with other Compliance officers?

In particular to the younger Compliance colleges I would like to say: work hard, stay informed about the developments in Compliance, stay curious and keep challenging colleagues if needed so that you can look yourself in the eyes at the end of each day.

For those who do this and persist a very interesting and rewarding career in Compliance is only a matter of time.



© DR

Mario **de Castro** HMS LUX S.A.

The life of a Compliance Officer

What is your career path?

I started working as a lawyer, in Portugal, 13 years ago. After around 2 years of practice, I went to Germany to get my Master's degree (LL.M.) and at the end of the studies I received a job offer from a bank operating from Luxembourg. So, 10 years ago I debuted in the financial sector and after 4 years in operational responsibilities I directed my career towards the Compliance area where my legal background could benefit me more. Ever since, I acted as Compliance Officer for, initially, a support PSF, then for a Management Company and, now, for an Investment firm.

What do you enjoy most in your role?

First, the constant alternation of challenges. There are never two days alike. I also particularly enjoy developing, often from scratch, the set of tools that will support the business.

In that sense, the current "ever-changing" regulatory landscape is very stimulating. In the last 3 or 4 years we have witnessed a succession of "heavy weight" regulations that have been taking (and will still take) its toll on us, COs, but it has also brought several new challenges.

What skills does someone working in the area need?

An inquisitive mind and attention to detail. The persons interested in steering a Compliance function must be on top of the changes to be able to keep up. If possible, even to anticipate issues. For that, I believe the best thing is to be curious, mainly about the new regulations but also about what other players are doing or thinking of doing. If you are curious you don't see the "new" as an additional burden but rather as an opportunity to do something different. The attention to detail is essential to not lose track of all the aspects that keep being requested, demanded or expected. A detailed plan should be the first output of that curiosity.

How do you see the Compliance Officer of the future?

As the legislator(s) and supervising authorities become more intervening, I believe the COs will be required to assume more roles (!), having to participate in all (or nearly) of the decision processes in each Company, including those only used to consult the COs, like product development or business strategy' decisions. In turn, this will require more time and attention from an already busy agenda so, hopefully, he/she will also have more (and cheaper) automation tools than the currently available ones.

What do you want to share with other Compliance officers?

A thought of solidarity. The COs are often placed in the back-back-office, with few or no contact with the outside of the company. And also inside to each company, the function is often "segregated" because of its nature. Nonetheless, networking is a social need that gets more acute when one is functionally detached from the group. I believe that networking among peers addresses that need and further helps to learn new methods and approaches. On this point, ALCO is to be commended for its work.

" I particularly enjoy developing, often from scratch, the set of tools that will support the business. "

Mario de Castro
HMS LUX S.A.

© DR

> **“ Avant tout investissement, que ce soit dans une nouvelle crypto, une ICO ou autre faites une analyse poussée. ”**
> Christophe Chudy,
> Membre du core team de la cryptocurrency Zclassic(ZCL)

Blockchain:
DON’T PANIC!

Blockchain, smart contracts, bitcoin, ethereum, ICO… sont des termes très à la mode en ce moment. Beaucoup de personnes en parlent, et vont peut-être même vous conseiller sur des investissements à fort rendement. Mais dans ce monde de la Blockchain un terme revient souvent : DYOR (Do Your Own Research). Alors, faites votre propre analyse.

© DR

Christophe Chudy
MCD TEAM CONSULTING COMPANY

Christophe Chudy, 47 ans, diplômé de l’école supérieur de l’électronique de l’Armée de Terre(France), a plus de 25 ans d’expériences en IT/Finance, Caisse des dépôts et Consignations à Paris, Clearstream au Luxembourg, gestion de plusieurs cabinets de conseils avant de créer son propre cabinet de conseils en IT/Finance & Assurance(2012), MCD TEAM.

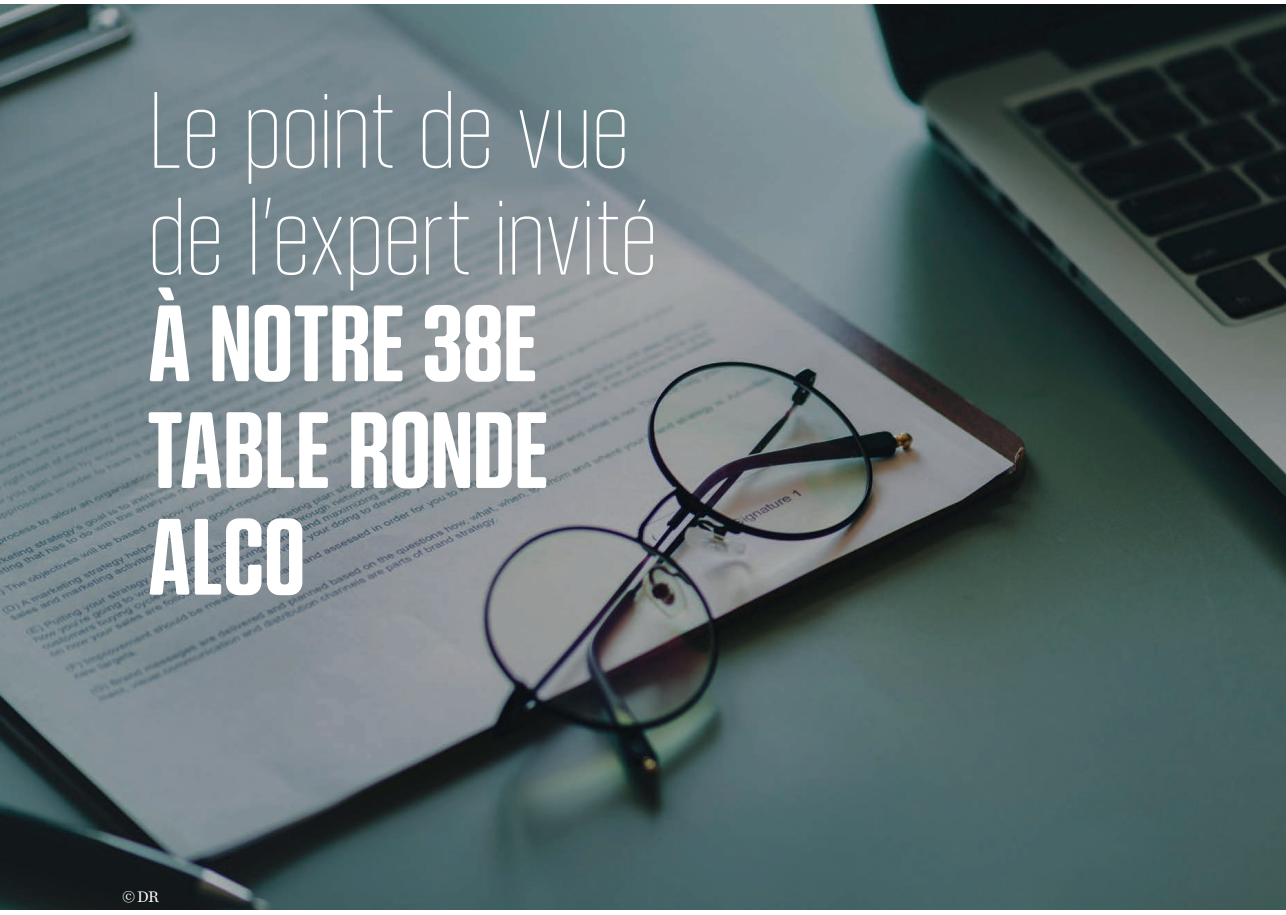
Membre du core team de la cryptocurrency Zclassic(ZCL), conseil & formation sur la Blockchain et les cryptocurrencies.

Ne vous fier pas aux rumeurs, aux informations. « Le bitcoin chute, c'est la panique, il faut tout vendre ! » C'est ce que beaucoup de personnes vous diront, prenez quelques heures, analysez l'évolution du bitcoin, en 2009 il valait moins de 1$, aujourd'hui plus de 6000$, certes cette nouvelle monnaie virtuelle a connu des 'crashs' mais elle s'est toujours relevée. Vous voulez rentrer dans ce monde, il y a des règles, les règles du monde de la 'crypto', rappelez vous que ce monde n'est pas encore régulé, il y a et aura encore des dérives. Le scam(arnaque) qui lance une ICO Savedroid, cette même ICO lève jusqu'à $50 millions et qui change la page d'accueil de son site avec ce message 'AANNND IT'S GONE', plusieurs jours après la même personne twittera 'Thanks guys, Over and out'.

Pour résumer, avant tout investissement, que ce soit dans une nouvelle crypto, une ICO ou autre faites une analyse poussée, ne vous fiez pas au beau site web, lien LinkedIn de la soit disant équipe, vérifier les groupes de discussion (telegram, discord, twitter....). Attention également aux sites de trading de crypto sans KYC, ayant beaucoup de soucis de support ou bloquant même vos retraits, contentez-vous des sites de référence, Bitflyer & Bitstamp ont des représentations locales aux Luxembourg, limitez vos trades à quelques sites ou le KYC est obligatoire, Binance par exemple. Pensez qu'un jour vous allez devoir justifier vos plus-values, trading, ICO..... sans justification cela sera plus que compliqué de convertir vos cryptocurrencies en FIAT (Euros, Dollars....).
Cette nouvelle technologie décentralisée et virtuelle est et sera de plus en plus présente dans la vie de tous les jours, les Compliance Officers vont être confrontés aux analyses AML et flux crypto-financiers, plusieurs conseils, commencez par référencer les sites de trading(rating par exemple en fonction du niveau de KYC), les ICO, faites une listes d'alertes, une check/list et informez vos clients sur ces alertes afin qu'ils puissent les suivre et ne pas se retrouver avec des cryptocurrencies sans pouvoir les convertir en Euros. Certains site de trading de référence vont commencer à proposer à leurs clients corporates de trader en cryptos (https://www.bloomberg.com/news/articles/2018-05-31 bittrex-gets-bank-agreement-to-help-you-buy-bitcoin-with-dollars).

La technologie de la Blockchain et les cryptocurrencies/smart contracts associés sont en place et vont se développer, il faudra adapter les outils, outil que nous sommes en train de développer.
Pour ma part, je fais partie du core team de l'équipe Zclassic (ZCL), qui a l'avantage de rendre complètement anonyme la transaction à l'inverse d'une transaction en Bitcoin qui est quant à elle 'transparente', l'adresse d'envoi, de réception ainsi que le montant peuvent être consultés par tous sur internet, à quoi cela peut-il bien servir, une transaction en bitcoin n'est pas complètement anonyme, en ayant l'adresse ou le numéro de transaction de votre correspondant vous avez accès en lecture à son portefeuille(wallet), l'inverse, c'est à dire votre correspondant à également accès à votre Wallet. A titre de comparaison, en faisant un virement SEPA, grâce à l'IBAN vous auriez accès aux données de votre correspondant, ce qui est impensable, le Zclassic résout ce problème en ne protégeant les données des utilisateurs.

Suivez les règles de conduite que vous aurez mis en place, parlez à votre banque, demandez-leur ce qui est accepté et ce qui est interdit avant de vous lancer dans ce monde décentralisé en pleine évolution.



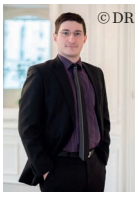
© DR

Le point de vue de l'expert invité

À NOTRE 38E TABLE RONDE ALCO

Les crypto-actifs, auparavant simples curiosités libertariennes ou liées aux geeks, sont en train d'entrer, qu'on le veuille ou non, en interférence avec le monde de la finance classique.

Du jeune étudiant qui a acheté 10 000 Bitcoin à l'époque où cela ne représentait que le prix d'une pizza, au mineur chevronné qui multiplie les machines, les fortunes (bien réelles) construites sur ces actifs intangibles se multiplient. Alors comment intégrer ces sommes dans le système classiques ? Comment réaliser la due diligence des fortunes faites sur les crypto-actifs ?



© DR

Jean-Baptiste Pleynet
Actuaire Manager au sein de Pericles group

Débordant de traçabilité

Commençons par une bonne nouvelle : dans une blockchain classique (type Bitcoin), tous les échanges sont publiquement accessibles. Il est donc possible de tracer l'histoire de tous les Bitcoins de leur création à aujourd'hui.

Mais rendons-nous à l'évidence : cela n'est pas la solution miracle.

Comment interpréter en effet qu'une crypto-devise, il y a 10 ans soit 1000 transactions passées, ait été utilisée pour des activités frauduleuses? Quel billet de banque ne peut pas en dire autant?

Cette traçabilité absolue peut donner une illusion de contrôle, alors qu'elle risque de nous inonder dans un océan d'information qu'il faudra ensuite traiter et interpréter.

D'autant que ces échanges, même s'ils sont publics, sont sous pseudonyme : seules les adresses publiques sont connues.

Le problème des actifs anonymes

En plus de cela, s'ajoutent les actifs permettant de jeter un voile sur cette transparence des blockchains primitives. Ainsi, avec la crypto-devise Monero, il n'est plus possible de savoir quelle adresse en détient combien, et quelle adresse a échangé avec qui. Du moins, c'est impossible sans la clé privée.

> **“ Monero, la crypto-monnaie anonyme la plus utilisée, permet de divulguer des « clés de visions », qui permettent à une personne tierce de voir les opérations, sans pour autant pouvoir disposer des fonds. ”**
>
> Jean-Baptiste Pleynet
>
> Actuaire Manager au sein de Periclès group

Rappelons que les blockchains sont basées sur un principe fondamental : celui de la cryptographie asymétrique. Il met le binôme clé privée / clé publique au centre de son fonctionnement. La clé publique, c'est plus ou moins l'équivalent du numéro IBAN : connaissant un numéro de compte, il est possible d'y verser de l'argent, mais impossible d'en prélever (du moins sans autorisation). La clé privée, qui va de pair avec cette clé publique, permet quant à elle de faire des virements sortants du compte et donc de dépenser les sommes qui s'y trouvent. Cette clé privée, comme son nom l'indique, doit donc impérativement rester secrète, sous peine de vol des sommes détenues.

Dans une blockchain et, à plus forte raison, si elle est anonyme, la clé privée peut être utilisée pour ouvrir les registres et démontrer, de façon certaine, les opérations passées. Ainsi, quiconque souhaite démontrer sa bonne foi et sa bonne volonté peut partager ses opérations passées.

Monero, la crypto-monnaie anonyme la plus utilisée, permet de divulguer des « clés de visions », qui permettent à une personne tierce de voir les opérations, sans pour autant pouvoir disposer des fonds.

Comment devenir riche en 4 leçons

Il existe plusieurs façons de constituer un patrimoine, grâce aux crypto-actifs, chacune apportant sa complexité et ses spécificités.

Dans ce domaine comme dans les autres, un principe immuable s'applique. Celui de Pareto, autrement appelé principe des 80-20 : 80% des cas seront simples et 20% représenterons 80% du travail.

Le trading

Aujourd'hui, généralement, pour acquérir des crypto-actifs et profiter de leur hausse, il faut en acheter. Pour cela, il est possible de recourir à des plateformes d'échange, qui permettent à tout un chacun d'échanger des euros (ou autres devises classiques) contre des crypto-monnaies. Ces échanges peuvent être régulés (comme le sont, au Luxembourg, BitFlyer et Bitstamp) ou non.

Dans le cas où ils sont régulés, les échanges intègrent déjà un dispositif anti-blanchiment. Dans le cas où ils ne le sont pas, ils peuvent ou non en intégrer un, selon leur organisation interne.

La traçabilité découle moins de la blockchain que de la plateforme d'échange : si quelqu'un fait fortune en achetant et vendant des crypto-actifs aux bons moments, il doit être en mesure de le prouver en partageant son carnet d'ordre. Si tous les actifs sont centralisés sur une même plateforme, alors la traçabilité est assurée.

Une question demeure : a-t-il payé ses impôts sur les plus-va-

lues ? Question simple mais dont la réponse est complexe. En effet, il faut d'abord identifier l'administration fiscale compétente et vérifier si elle a pris position sur l'imposition des plus-values en crypto-actifs ? Dans bon nombre de pays, cette question n'a pas encore de réponse satisfaisante.

Le minage

Pour faire (trop) simple, miner c'est dépenser (énormément) de puissance de calcul pour créer des nouvelles unités de crypto-devises. Un mineur est donc quelqu'un qui laisse tourner de puissants ordinateurs(souvent 24/24) pour, en récompense, obtenir des unités de crypto-monnaies nouvellement générées.

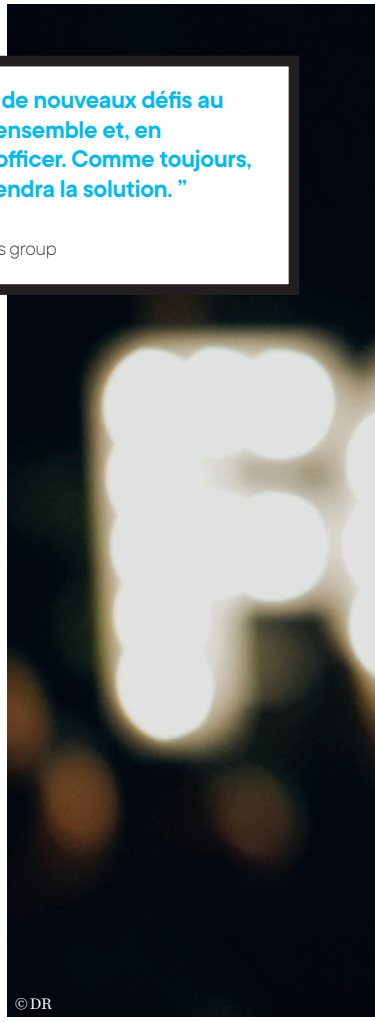
Ici, la traçabilité des actifs peut être la plus simple : la monnaie est créée et créditée en faveur du mineur. C'est par ce biais qu'il constitue sa fortune. Simple, sauf qu'en réalité, les mineurs le font en passant par des « pools », qui sont des coopératives de minage. Ils se présentent sous la forme de sites internet, et ce sont eux qui sont les propriétaires de la fortune créée, qu'ils recréditent ensuite à leurs membres-utilisateurs. Pour ceux qui ont pignon sur rue, refaire l'histoire de tels échanges n'est pas compliqué. Pour d'autres, moins connus, voire éphémères, l'historique disparait lorsque le site internet disparait...

Mais demeure toujours la facture d'électricité nécessaire pour nourrir des machines à l'appétit gargantuesque.

Les ICO's

Une ICO est une levée de fonds utilisant des crypto-devises. Ce type de levée de fond peut être réglementé ou non. Certains pays ont défini un cadre légal. En échange de son investissement, un investisseur reçoit habituellement des « tokens ». Ce sont des jetons numériques un peu selon le modèle les crypto devises. Ces jetons peuvent avoir la valeur d'une action ou, encore, être plutôt une prévente d'un produit futur (comme une place de la finale de la coupe de monde de foot, achetée avant de savoir quelles équipes seront qualifiées). Les ICO's réglementées ne devraient pas poser de grands problèmes à la Compliance, mis à part le payement par l'investisseur d'éventuelles taxes sur les plus-values réalisées, rien d'insurmontable. Quant aux ICO's non règlementées, elles peuvent être plus ou moins opaques, certaines proposant un processus de lutte contre le blanchiment et d'autres absolument pas.

> **" Les cryptos actifs posent de nouveaux défis au monde financier dans son ensemble et, en particulier, au compliance officer. Comme toujours, c'est de l'innovation que viendra la solution. "**
>
> Jean-Baptiste Pleynet
>
> Actuaire Manager au sein de Periclès group



© DR

Le commerce en crypto-devises

Les crypto-monnaies ont, comme leur nom l'indique, vocation à servir de moyen de payement. Certains jouent le jeu en faisant du commerce en utilisant ces actifs. Soit du commerce de biens réels, soit de la prestation de service, par exemple des casinos

ou des contrats d'assurance.
La traçabilité de ce type d'opérations est les plus complexe : comment distinguer, uniquement sur base des adresse (Bitcoin ou autre), l'achat d'un jeux vidéo sur la plateforme Steam d'un achat de programme pirate sur le dark web?

Il n'y a pas de problème sans solution

Les cryptos actifs posent de nouveaux défis au monde financier dans son ensemble et, en particulier, au compliance officer. Ce dernier est aujourd'hui encore souvent en première ligne dans ces problématiques. Mais aucun problème ne demeure longtemps sans solution.
Lors de la création de Bitcoin il y a moins de 10 ans, tout était à faire. Aujourd'hui, de nombreuses startups proposent des outils et services de lutte anti-blanchiment sur crypto-actifs automatisés. Ces outils et services génèrent des rapports d'analyse détaillés sur base d'une adresse : Est-elle impliquée dans des opérations sur le dark web ? Est-elle liée à l'utilisation de « mixer », des outils pour brouiller la provenance des fonds ? Combien d'opérations effectue-t-elle et à quelle fréquence ?
S'il n'est plus aujourd'hui possible de fermer les yeux sur leur existence, l'arrivée des crypto-actifs dans le monde de la finance classique s'accompagne d'une série de services nouveaux qui sont amenés à se développer eux aussi exponentiellement le Bitcoin ne l'a fait. Comme toujours, c'est de l'innovation que viendra la solution.

SHORT OUTLINE OF THE CHALLENGES OF THE COMPLIANCE OFFICER IN (REGULATED) START-UP ENVIRONMENTS

There are different ways in which (regulated) start-ups may be formed depending on the activity, size and preference of its (future) shareholders or legal/tax advice obtained from local advisors. This article describes the process from a situation in which nothing exists at the beginning until the point where the company is no longer to be considered as a start-up as business has been launched.
As opposed to integrating an existing entity or department as a compliance officer ("CO"), managing or integrating the compliance function in regulated start-up environments represents additional challenges on top of the already quite heavy burden on CO's nowadays, as set out hereafter.

© DR

Starting point

The Law of 5 April 1993 on the financial sector, as amended (the "1993 Law"), provides, in general terms, for the following regulated entities to be set-up:

- Banks
- Investment firms
- Specialised PSF's
- Support PSF's
- Payment agents

Each category of entities carries different rules and regulations and as a consequence, requirements. However, similarities exist for all of them, and it is those that we will focus on.

A regulated start-up is usually set-up with one or more (future) members of the entity's (the "Entity") board and management being appointed with the task of initiating the so-called licence request (demande d'agrément) with the CSSF.[1] A simple private or public limited liability company may be set-up by the (future) shareholders (the "Shareholders") to enable these members to be employed, to attract office space, to set up a first IT environment, and so on, although this is not mandatory. It is also usual for the Shareholders to obtain prior legal and tax advice from advisors locally or abroad to ensure that their project has a chance of being accepted by the CSSF.


© DR

Steven Curfs
Associate Director
Ocorian
OCORIAN

The dedicated CO may already be employed at this time by the Entity to assist with the different phases of the licence request, the drafting of documents, structure charts, policies and procedures, and so on. It is also possible that advisors or consultants provide the CSSF with these documents based on standard forms, which will later be adapted by the Entity's CO to the specific needs of the Entity. The CSSF permits a member of the daily management of certain Entities to act as CO for a limited period of time upon obtainment of the rele-

1 Entities possibly falling within the supervision of the EBA are not taken into consideration in this article.

> **" Another important task for the CO is to create an electronic and physical filing environment in line with the IT set-up, as described in the licence request file. "**
>
> Steven Curfs
>
> Associate Director Ocorian

vant licence according to the proportionality principle. This is not the case for financial institutions, payment firms or investment firms, which need a CO right away.

CO's tasks and priorities during the licence obtainment process

Depending on the solidity of the licence request file, the obtainment process may last more or less time. A CO employed from the outset should ensure that any additional document or clarification request from the CSSF be treated as a top priority. An electronic track of the initial request as well as all follow-up requests from the CSSF + answers sent to the CSSF in return should be kept for future reference (see below).

The Entity's CO should use as much time as possible during this period to start setting-up the skeleton of the compliance function. A good starting point is to take the applicable laws and regulations applicable to the Entity and to map those out (for instance using an excel sheet). Once this has been done, an analysis can be made as to what needs to be put in place in terms of policies and procedures to ensure satisfactory compliance with such requirements. The licence request file will also be a good help as it sets out in some detail the specific requirements which the CSSF imposes on the Entity. It is recommended to use a separate excel sheet or tab to line out the requirements and the answers given by the Entity to the CSSF in that document as well as any follow-up between the Entity and the CSSF prior to licence obtainment. This is particularly important in the light of the requirement of the newly introduced article 15(9) of the 1993 Law which obliges the Entity to inform the CSSF of any "important" changes made in comparison with the original licence request.

Steven is responsible for the legal and compliance department in Luxembourg. He also acts as the accredited data protection officer and serves as secretary to the Board of Directors.

Steven started his career as a corporate lawyer in a magic circle law firm before joining a leading global financial institution where he was co-responsible for all alternative investment products.

In the last six years he has specialised in setting-up and managing regulated entities such as management companies and service providers for alternative investment funds in Luxembourg and has experience in both emerging and established markets. He acts as a Director on several regulated and unregulated entities in Luxembourg and abroad and is a member of ALCO & ALFI working groups in the field of alternative investments. Steven has been an ILA certified director since 2016.

Steven holds a Master of Laws from Maastricht University and a LLM in International Business Law from McGill University, Montréal. He also speaks eight languages including French, English, German, Dutch, Luxembourgish, Spanish, Portuguese and Italian.

The mapping document referred to above is also crucial to enable the CO to put a yearly compliance monitoring plan in place once the Entity will be up and running (see below).

Another important task for the CO during this period is to create an electronic and physical filing environment in line with the IT set-up as described in the licence request file. Thought should be given to the actual implementation of the policies and procedures, checklists and KRI/KPI documents, reporting to the Entity's authorised management and its board of directors, and so on. A coherent electronic and physical filing system will allow for the reduction of errors and thus the reduction of the legal & compliance risk for the Entity from the outset. Standard reporting can already be prepared in draft form for use at launch.

The CO may very well also be involved in the operational set-up of the Entity, reviewing operational procedures, the set-up of Entity bank accounts, signing powers, selection and set-up of relevant third party client software to be used to service the Entities clients, and so on. Standard service agreements and other documents

binding the companies to its future clients may well also need to be reviewed by compliance (and might even need to be included in the original licence request, depending on the licence sought).

Finally, the CO will inevitably be involved in the scrutiny of any outsourced activities (for instance finance, payroll, IT, and so on) and will usually also have to be informed on the proposed set-up in regards of the internal and external auditor of the Entity.

Upon obtainment of the licence

Once the Entity has gotten the green light from the CSSF and has obtained its licence from the Ministry of Finance, the activity can be launched. If not yet launched, the Entity can formally be incorporated and its governing bodies and external auditor appointed, if already launched, the bylaws may now be changed to reflect the required changes needed for regulated entities. The CO should not forget to ensure that the board of directors and/or the authorised management of the Entity approve of the relevant policies, procedures and other documents that shall apply throughout the Entity's duration and are required by law or regulation. Where applicable, these decisions and/or documents should be provided to the CSSF for information (for instance the internal audit charter, tri-annual internal audit plan, remuneration policy, formal appointment of governing bodies and external auditors, and so on). Others might be laid down with the Luxembourg Business Register ("LBR"), such as an authorised signatories list of the Entity. Infrastructural and IT requirements must now be in line with the description set-out in the licence request (secured office space, Chinese walls for IT systems where required, and so on). External and internal auditors, IT and other service provider may now be hired through engagement letters or service contracts.

Now is also a good time to set-up and design the yearly compliance monitoring plan which will derive from the mapping (excel) document referred to earlier on. A risk and priority level can for instance be added to every single requirement of that document, which can then be translated into a multi-year compliance monitoring plan, taking into account the identified risks and priorities. Of course, such a plan is very likely to be a living document in a start-up environment for obvious reasons. Also, any comments received from the CSSF during a first courtesy visit as well as feedback from the internal and external audit functions and, last but not least, the compliance function itself after the first year of business should be taken into account and integrated.

In order to comply with the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended (the "2004 Law"), and CSSF Regulation 12-02 on the same topic (the "CSSF Regulation"), transaction monitoring checks, usually integrated in the Entity's KYC Policy and Procedure, should be put into place and carried out in line with such internal documents. ALCO offers a good model document, consisting of a (1) Client Profile and (2) Transaction Monitoring document, which can be used from the outset and until the activity of the Entity allows for it, taking into account the nature and frequency of transactions carried out by its clients.[2] Furthermore, the Entity must now ensure, in line with the CSSF Regulation, that any of its clients' UBO's are now screened on a regular basis vs. relevant defined watch lists. Several software solutions exist

2 An electronic system should be considered from the outset for payment institutions and banks as due the nature and frequency of its clients, these type of entities will usually be confronted quite soon to an overload which can not be effectively monitored based on a document-based system.

> **" The challenge of the CO in regulated start-up environments is that it requires deep knowledge of the applicable and current laws and regulations for the Entity. "**
>
> Steven Curfs
>
> Associate Director Ocorian

that can assist with this requirement if the Entity cannot base itself on group systems which will have been approved for use in Luxembourg by the CSSF.

In line with the requirements outlined here before, it is also wise to already request the "Go AML" access from the Cellule de Renseignement Financier attached to the State Prosecutor (Parquet) ("CRF"), by (1) obtaining a Luxtrust certificate for the CO and (2) register online on the CRF's website.

In order to allow authorised management, and thus indirectly the board of directors, of the Entity to be informed on a regular basis on the activity from an operational and support functions point of view, it is advisable to set-up internal KPI's/KRI's for each department which are filled-out and communicated to authorised management on a monthly basis. Any outsourced activities should be the object of similar reporting from the companies/persons to which such activities are outsourced, notwithstanding any annual reporting that may be made available to external/internal control functions. Authorised management can then use these KPI's/KRI's to compile a quarterly reporting to the Entity's board of directors.

Any regulatory or legal changes applicable to the Entity should be included in the aforementioned mapping (excel) document and translated into the multi-year compliance monitoring program. This will allow for (1) changing relevant policies and procedures whenever needed, (2) formal approval by the authorised management or board of directors of the Entity, (3) an audit trace and (4) compliance with these new regulations or laws. A good starting point is to subscribe to the newsletters from the CSSF and the Ministry of Finance (sanctions' lists) as well as those of the big four and magic circle law firms in Luxembourg and/or abroad.

Last but not least membership to professional bodies like ALCO, ALJB, ALFI, ILA, and so on may now be considered in order to stay up-to-date of industry standards and to be able to contribute to these organisations where this could be mutually beneficial.

Conclusion

As can be deducted from the short outline given here above, the challenge of the CO in regulated start-up environments is that it requires deep knowledge of the applicable and current laws and regulations for the Entity. Consequently, an affirmed and experienced person should be hired for this kind of function.

The chosen CO should also be very flexible and eager to work cross-functionally, at least at the start of the Entity's corporate life and during the licence request file, as in the absence thereof, the puzzle of building a regulated start-up Entity will not be able to be finished adequately. This is however also the charm of the CO's function in such a setting, as it will be very enriching and allow for a much broader view of the Entity's business, not limited to the mere "traditional" compliance tasks which one can imagine an established entity's compliance department.

LA COMPLIANCE À L'ÈRE DU NUMÉRIQUE

Le digital envahit désormais tous les services d'une entreprise. Les compliances officers n'y échappent pas. Jérôme Bloch, PDG de 360Crossmedia, détaille cette révolution culturelle.

Comment la transformation digitale en cours impacte-t-elle le domaine de la compliance ?

La compliance figure parmi les secteurs les plus impactés et donc, déjà très engagés dans une véritable révolution. Un état des lieux du quotidien dans d'autres départements d'une entreprise, notamment l'opérationnel, permet d'observer que le digital y relève encore du fantasme. Dans les esprits rôde le spectre de la machine toute puissante volant le travail des uns et le savoir-faire des autres. Les mots ou concepts, tels les blockchains, ne s'y traduisent pas concrètement. Sur le plan de la compliance, en revanche, la révolution numérique et digitale s'inscrit déjà dans la réalité. Je pense par exemple aux procédures de KYC, qui profitent largement des possibilités offertes par le digital pour améliorer la précision de leurs recherches ou aux systèmes informatiques sans lesquels il est devenu impossible de rester en conformité avec les innombrables obligations qui ne cessent d'émerger.

Jérôme Bloch
360Crossmedia

Comment le compliance officer doit-il s'adapter ?

Le temps où les compliances officers exerçaient en vase clos paraît bien révolu. Ils font désormais le lien entre différents métiers pour assurer à

> **“ Les compliance officers doivent disposer d’un double arsenal de compétences. ”**
> Jérôme Bloch, PDG, 360Crossmedia

leurs employeurs de rester en ligne avec les demandes des régulateurs. A ce titre, ils doivent disposer d’un double arsenal de compétences : une expertise métier très pointue d’une part, doublée d’une maîtrise parfaite de la communication. Cette dernière qualité leur permet de présenter clairement à leurs collègues les projets en cours, les deadlines et les obligations de chacun. Les meilleurs obtiennent un buy-in apte à accélérer la mise en œuvre des projets et à réduire les risques. Lorsque nous travaillons avec des compliance officers, nous commençons par un travail sur les documents : textes, structure des présentations powerpoint, vidéos. Même dans la compliance, trop d’information tue l’information. Nous observons souvent une tendance à exprimer toute la complexité de la matière, alors que le rôle principal du compliance officer consiste à absorber cette complexité pour présenter à ses collègues les points fondamentaux. Ensuite, nous travaillons sur les techniques de présentation : in fine, pour obtenir un support maximal de ses collègues, le compliance officer doit savoir leur ‘vendre’ son projet.

La digitalisation transforme donc la culture de l’entreprise ?

Absolument, d’autant qu’avec l’IT, c’est-à-dire les technologies de l’information, nous assistons à un double phénomène : moins de taches rébarbatives et davantage de possibilités pour gagner en compétence, via l’e-learning et le co-learning par exemple. Regardons les banques passant d’un fonctionnement extrêmement lourd à des workshops et à l’innovation en général. Je pense que le compliance officer doit réaliser la même évolution en passant d’un rôle de surveillance pure à un rôle de catalyseur pour aider l’entreprise à définir les meilleures stratégies au grès des multiples évolutions en cours.

ALCO'S COMMUNCIATION TEAM

RÉDACTEURS EN CHEF


© DR

Sandrine Wesquy
Head of Training & Communication Compliance
BGL BNP paribas


© DR

Thierry Grosjean
Conducting Officer –
Head of Compliance & Risk
Japan Fund Management Luxembourg

Fight against laundering of money of criminal origin and against terrorism financing; integrity of financial markets, respect for ethical principles, all these are now important parts of the financial sector today and that influences its activities widely.

The **Compliance Officer** function has appeared among credit institutions, PSFs, insurance companies. The Compliance Officer role is to make sure that these institutions comply with the current legislative, statutory and ethical standards.

Today, the Compliance function in the financial sector is officially recognised, on an international level by the Committee of Basel, and locally in Luxembourg by the CSSF. This function becomes compulsory in all the institutions of the financial sector in Luxembourg.

The "**A**ssociation of **L**uxemburg **C**ompliance **O**fficers" for the Financial Sector was created on 20 december 2000.

AUTHORS

Steven Curfs
Head of Legal & Compliance
Ocorian (Luxembourg) S.A.)

Oumarou Ide
Deputy Chief Compliance Officer
Mitsubishi UFJ Investor Services & Banking
(Luxembourg) S.A.

Matthieu Sarrazin
Legal Counsel & Compliance Officer
ONPEX

Géranise Hurtis
Senior Fund Compliance Officer
CF Fund Services
(Groupe BDO)

Jean-Sébastien Kroonen
Senior Compliance Officer
KBL epb Compliance Advisory
KBL European Private Bankers S.A.

SQOPE

INTELLIGENCE
FOR DECISION MAKERS

PROTECT YOUR REPUTATION AND BE FULLY COMPLIANT.

KNOWING IN ADVANCE: SQOPE YOUR CLIENTS | PROSPECTS | EMPLOYEES | PARTNERS

Sqope S.A. offers independent premium information reports on individuals and companies worldwide to allow its clients to develop their business in full respect of Anti-Money Laundering, Anti-Terror Financing and Anti-Corruptions laws.

LUXEMBOURG | **SWITZERLAND** | WWW.SQOPE.LU | INFO@SQOPE.LU