



Association Luxembourgeoise
des Compliance Officers
du Secteur Financier

Le Bulletin d'informations

N°12

DECEMBRE 2007

Editorial



Chers amis, membres de l'ALCO,

Depuis le dernier Bulletin en juin, nous nous sommes réunis trois fois. En juillet pour la conférence sur MiFID organisée conjointement avec l'ALJB et l'IRE ; début octobre pour la réunion sur les groupes de travail, et plus tard dans le mois pour un drink amical.

En réalité, si nous étions très nombreux pour la conférence qui fut un vrai succès, nos rangs étaient plus clairsemés pour les deux réunions d'octobre.

Afin de bien ajuster nos propositions d'activités, comme toujours nous avons besoin de votre « feed-back ». N'hésitez pas à nous écrire, et nous faire part de vos idées et desiderata.

Le Bulletin

Dès maintenant, vous pouvez noter que notre prochaine Assemblée Générale est prévue pour la première quinzaine de mars 2008. Elle sera l'occasion de faire le point sur la nouvelle législation sur le blanchiment, en application de la III^{ème} Directive.

Comme d'habitude, je vous sollicite aussi pour participer activement à notre Bulletin, qui est devenu une composante incontournable de l'ALCO. Nous souhaiterions accroître le rythme de sortie des numéros, et passer de 3 à 4 par an. Ceci permettrait de serrer au plus près ce qui fait l'actualité de la compliance et l'évolution de son environnement.

Mais pour ce faire, il est indispensable que les membres nous proposent régulièrement plus d'articles. Communiquez-nous aussi vos idées sur les thèmes que vous souhaitez voir traités.

Dans ce numéro, vous trouverez deux très intéressants articles qui ont été directement écrits en anglais :

- Marco Zwick recherche « l'équilibre éthique » entre la protection des données personnelles et le secret bancaire d'une part, la nécessité toujours plus affirmée de la transparence en matière financière d'autre part;
- Evelyn McHale veut nous faciliter l'approche d'ICAAP et de ses règles, qui font maintenant partie des responsabilités de la fonction Compliance.

Merci à l'un et à l'autre.

Nous vous souhaitons de joyeuses de fêtes de Noël et de fin d'année.

Meilleurs vœux pour l'ALCO et ses membres.

A l'année prochaine !

Jean-Marie Legendre
Président

Actualités législatives et réglementaires

Actualités luxembourgeoises

Règlement grand-ducal du 1^{er} octobre 2007 relatif aux modalités d'application du Règlement (CE) n° 1889/2005 du Parlement européen et du Conseil du 26 octobre 2005 relatif aux contrôles de l'argent liquide entrant ou sortant de la Communauté. Memorial A N° 189 du 16 octobre 2007 ;

Circulaire CSSF 07/326 du 19.11.2007 : Dispositions relatives aux établissements de crédit et aux entreprises d'investissement de droit luxembourgeois établis dans un autre Etat membre par l'intermédiaire de succursales ou y exerçant leurs activités par voie de libre prestation de services ;

Circulaire CSSF 07/325 du 19.11.2007 : Dispositions relatives aux établissements de crédit et aux entreprises d'investissement originaires d'un autre Etat membre établis au Luxembourg par l'intermédiaire de succursales ou y exerçant leurs activités par voie de libre prestation de services ;

Circulaire CSSF 07/323 du 07.11.2007 : Portant modification de la Circulaire CSSF 07/280 concernant les modalités d'application de la loi du 9 mai 2006 relative aux abus de marché ;

Circulaire CSSF 07/327 du 21.11.2007 :
1) GAFI, déclaration concernant l'Iran
2) Lignes directrices du GAFI relatives à la mise en œuvre de certaines résolutions de l'ONU

Luxembourgish News

Grand Ducal Regulation of 1st October 2007 on regulation EC n°1889/2005 of the European Parliament and of the council of 26 October 2005 on controls of cash entering or leaving the Community Memorial A N° 189 dated 16 October 2007 ;

Circular CSSF 07/326 dated 19.11.2007: Provisions relating to credit institutions and investment firms incorporated under Luxembourg law established in another Member State through branches or carrying on their activities under the freedom to provide services;

Circular CSSF 07/325 dated 19.11.2007: Provisions relating to credit institutions and investment firms of another Member State established in Luxembourg through branches or carrying on their activities under the freedom to provide services;

Circular CSSF 07/323 dated 07.11.2007: Amending Circular CSSF 07/280 on the implementation rules of the law of 9 May 2006 on market abuse ;

Circular CSSF 07/327 dated 21.11.2007:
1) FATF statement on Iran
2) FATF guidance regarding the implementation of certain UN resolutions

Rubrique de Karine Vilret-Huot

**CSSF Circular 07/301 – ICAAP
Implementation**

Summary of Requirements

BACKGROUND

The European directives defining the new capital adequacy framework for credit institutions (i.e. banks) and investment firms, stemming from the Basel II Accord, were adopted by the Council of the European Union on 7 June 2006.

The Basel II Accord consists of three “pillars”:

- Pillar 1: Minimum Capital Requirements;
- Pillar 2: Internal Capital Adequacy Assessment Process (ICAAP); and
- Pillar 3: Publication of additional financial information regarding Capital Adequacy.

The Commission de Surveillance du Secteur Financier (“CSSF”) transposed the European directives in Luxembourg for banks in its Circular 06/273 – enforceable from 1 January 2007 and by Circular 06/290 for investment firms (or “PSFs”) from 3 May 2007. These two Circulars together lay out all the Pillars requirements.

On 17 July 2007, the CSSF published Circular 07/301 on the Implementation of an ICAAP for both banks and investment firms (hereafter “bank”). This Circular draws heavily on the Committee of European Banking Supervisors (“CEBS”) *Guidelines on the Application of the Supervisory Review Process under Pillar 2*.

Questionnaire:

The CSSF also issued a questionnaire/survey on 17 July 2007 with the aim of:

1. understanding where Luxembourg-based banks are in their ICAAP preparation;
2. benchmarking progress and
3. staffing the CSSF appropriately as the Capital Requirements Directive is expected to put a strain on CSSF resources.

PSFs were excluded from the questionnaire but banks had until **15 October 2007** to respond to the CSSF.

ICAAP

“The ICAAP is the means by which institutions identify and measure the risks to which they are exposed and determine internal capital needed to support these risks. The resulting internal capital adequacy has to cover all the risks the institution is exposed to and, consequently, complements the prudential capital adequacy under Pillar 1 which requires prudential capital to be held against certain types of risk only.”

M. Arthur PHILIPPE, Director of the CSSF, at the PRiM 10th Anniversary Event, June 2007.

In other words, ICAAP is a process which forces a bank to make an assessment of those risks which do not form part of Pillar 1 (minimum capital requirements), and to ensure that the bank has enough capital to cover those risks in excess of credit risks,

market risks, operational risks minimum capital requirements.

Note: The notion of capital is broader under Pillar 2 than under Pillar 1, meaning that a bank can use further sources of capital than the ones authorised under Pillar 1.

1. Definition/objective and scope of ICAAP

ICAAP stands for Internal Capital Adequacy Assessment Process and all banks (and PSFs) fall within its scope. It consists in a series of **internal** strategies/processes that enable a bank to assess and permanently hold own funds deemed appropriate to cover all the risks to which it is **or could be** exposed to.

2. Main Elements of ICAAP Circular

- the requirement to implement an ICAAP in banks (and PSFs);
- the basics an ICAAP should cover;
- the structure of the ICAAP;
- the general principles of an ICAAP;
- the responsibilities of the institution's Board of Directors (essentially, to establish; document and communicate to Senior Management the principles and objectives of the ICAAP – and to review it at least annually, copying it to the CSSF);
- the responsibilities of Senior Management (basically, the practical implementation of the ICAAP and regular oversight of its operation; and reporting at least annually on the subject to the Board);
- the role of Internal Audit, Compliance and Risk in the process;
- particular guidance on concentration risk; interest rate risk; and investment management risk;
- guidance on Stress Testing;

- details on the supervision of the ICAAP by the CSSF and guidance on implementation of an ICAAP in a Group context;
- sanctions for non-compliance; and
- entry into force - immediate on publication, but with an understanding it may take until 1 January 2008 (the ultimate deadline), as institutions implement CSSF Circulars 06/273 and 07/290.

3. Key Processes Required

ICAAP consists of two key processes:

- a) A process of identification; measurement; management; and reporting of **all risks** to which a bank is, **or could be**, exposed to (including risks linked to economic and regulatory environment, concentration etc).

ICAAP doesn't just take a bank's current situation into account but must include a view of its future situation. Also, ICAAP must be proportionate to the scale/organisation of the bank and of the diversity/complexity of its activities.

- b) A process of own funds planning/management that must ensure appropriate level of own funds on a permanent basis.

4. Evidence of ICAAP

An ICAAP must be evidenced through documentation. The documentation must cover strategy (principles and general objectives of risk taking); methodology; a description of internal processes; and all results and decisions regarding ICAAP.

The ICAAP must be assessed at least once a year to ensure that it is still relevant and reflecting reality.

A **written risk policy** must be established to include:

- Setting up of internal standards regarding risk taking/management;
- Implementation of efficient processes to identify; manage; follow up; and report risks;
- Implementation of processes that enable a bank to efficiently manage crisis situations (especially any liquidity crisis); and
- Designation of a member of senior management responsible for implementing the above.

A **Written internal own funds policy** must be established to include:

- Setting of internal standards regarding internal own funds management;
- Implementation of efficient processes to plan; follow up; report; and modify amount, type, and division of internal own funds;
- Implementation of processes that enable a bank to efficiently manage crisis situations (inappropriateness of internal or prudential own funds); and
- Designation of a member of senior management responsible for implementing the above.

Decisions of senior management regarding ICAAP must be documented and filed.

Note: Unlike the minimum capital requirement (8%), the CSSF doesn't set any threshold for the internal own funds ratio.

5. Responsibility of Board of Directors regarding ICAAP

“In order to assume its role as the depository of the governance process, the Board must practice guidance and oversight in an efficient way. To start with, risk management must be embedded in governance practices and strategic planning. A Board’s role is to agree on objectives and strategies and to communicate on them. The Board can contribute here its expert judgement. It is also incumbent to the Board not only to fix the risk tolerance thresholds, but also to set the tone for ethical behaviour.

An enterprise wide framework of Risk Management, whose structure has been conceived by the Board, has to be implemented under its oversight. Once the framework has been put in place and authority has been assigned to the management to manage the risks on day-to-day basis, the Directors role will be to keep themselves informed on a regular basis, - should this apply through its audit committee -, on the risk profile, its management and the performance of risk limitation mechanisms. It is obvious that corrective action has to be taken at this juncture.”

M. Arthur PHILIPPE, Director of the CSSF, at the PRiM 10th Anniversary Event, June 2007.

The board is responsible for stating, documenting and communicating strategies regarding risk management, and management /appropriateness of own funds to senior management.

The board must approve ICAAP on a regular basis (at least once a year). This approval consists in determining the:

- Appropriateness of the ICAAP compared to the bank's structure and activities;
- Risk profile of the Company;
- Planning and appropriateness of Own Funds;
- Impact of internal Own Funds management on appropriateness of prudential own funds.

The document presented to the Board should be approximately 20 – 30 pages long (depending on the scale of the Bank's activities), but with supporting documentation behind it, held by the bank.

The ICAAP, approved by the board, must then be forwarded to the CSSF who will assess the initial, and annual review of the ICAAP, and the risks to which a bank may be exposed..

6. Role of Internal Audit and Compliance

The Circular states that ICAAP falls within the ambits of Internal Audit and Compliance and that the two functions should “participate in the realisation of the objectives of integrity and efficiency” in a regular review.

The Circular does not define more fully the involvement of Compliance and Internal Audit. However, depending on how a Bank (or PSF) is structured, and its scale:

Internal Audit is probably expected to:

- Ensure an ICAAP is in place;
- Regularly review the integrity of the process, after its implementation; in its Audit Plan; and
- Ensure that ICAAP remains adequate to the bank and its performance, and that it is integrated into the business.

Compliance may be expected to:

- Be involved in the establishment of the ICAAP – providing input on the breadth of risks covered and the appropriateness of the risks identified for the institutions business;
- To review the risks covered annually as part of its Compliance Monitoring Programme to ensure they remain relevant; and
- To ensure that the ICAAP is incorporated into the business.

Naturally, where a Bank or PSF has a Risk Management function, they would also be heavily involved in the ICAAP.

7. CSSF Oversight

The CSSF will assess at least once a year risks which the entity could be exposed to. This will be based on their review of the Board's annual update on the application of ICAAP. However, the CSSF will also enter into more frequent and regular dialogue with banks going forward – not just with senior management, but also with those responsible for certain areas such as Finance, Compliance, Internal Audit, Risk Management etc.

8. Practical implementation

8.1. Definition of risks

Potential risks listed in the circular (not exhaustive according to circular):

- concentration risk;
- credit and counterpart risk;
- country risk (transfer risk);
- market risk (interest rate risk trading portfolio excluded);
- liquidity risk;
- operational risk, included : IT risk, externalized processes, risks linked to new processes/activities
- payment/delivery risk ;
- reputation risk;

- compliance risk;
- legal risk;
- residual risk (risk that credit risk mitigation methods are less efficient than foreseen);
- Securitization risk;
- business and strategic risk;
- risks generated by macroeconomic and regulatory environment;
- model risk.

NB: “Administration services for UCI are exposed to reputation, compliance and operational risks that must be taken into account in ICAAP

8.2. Risks measurement

In theory, the Company must measure quantifiable risk and appreciate risk that is difficultly quantifiable.

83. Link between Risks and Internal own funds

In order to achieve the internal own funds appropriateness, the Company will have to define a link between risks and internal own funds.

8.4. ICAAP frequency

Frequency of ICAAP is the choice of the Company. For instance, depending on the scale of the Company and on the type of activities, internal own funds planning can be done less frequently than the follow up and measure of risks.

9. Approach

There is no template for completing the ICAAP. Therefore, each Bank or PSF will have to implement on a best efforts basis, following the guidance in the Circular, and tailored to size and complexity of the business.

26 October 2007

Evelyn McHale & Francois Meyers

Doctrine

The ‘ethical balance’ between data protection and banking secrecy as opposed to absolute transparency in the financial business, a success story ?

“Data-processing systems are designed to serve man; they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy (...).”
(European Parliament and Council, 1995)

This press article aims at assessing the ongoing claim for data transparency by public authorities and the associated costs and benefits for the main stakeholders, i.e. individuals, collectivities and authorities. For this purpose, it will focus on a limited number of examples to evidence the sensitivity of the topic. The Luxembourg legislation on the protection of personal data and banking secrecy would appear to be in direct contradiction to the estimated need for absolute transparency in all financial business areas. But is a reconciliation of these apparently diametrically opposed concepts still possible?

The above consideration by the European Parliament and Council dates back to 1995 and to the years of discussions preceding the completion of the European Directive on data protection. This demonstrates that the concern to grant a fundamental right to privacy is not anchored in the Luxembourg banking secrecy exclusively, first made official by way of the Banking Act of 23 April 1981 and applicable to “the directors, the individuals responsible for supervision,

management, employees and other persons working for credit institutions and other professionals in the financial sector (... who ...) are required to keep secret all information confided to them in the course of their professional activity” (article 41 (1) of the Luxembourg Banking Act, 1993). If we acknowledge that banking secrecy rules have been set up to protect financial data of private persons and legal entities and hence their personal and operational lives respectively, data protection legislation is a bit different in its scope and application: “*Personal data* shall mean any information relating to an identified or identifiable natural person (*data subject*); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity” (European Union, 1995, *op cit*). It is noteworthy that the Luxembourg Law on Data Protection dated 2 August 2002, currently being amended, extended the scope to all natural *and legal* persons whose data is processed. In line with the European Directive of 1995, the Luxembourg Law applies to the *processing of personal data*, meaning “any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.” The review of the above legal definitions helps to understand that: (i) the Luxembourg Law on Data Protection is more stringent than the respective European Directive, as it protects

legal entities in their quality as data subjects as well; and (ii) data protection applies to all types of personal data, including but not limited to financial data.

What circumstances justify the request for absolute transparency relating to financial actors and their transactions? Or, if we put the question the other way round for illustrative purposes, has the Belgian banking co-operative SWIFT (Society for Worldwide Interbank Financial Telecommunications) defined new standards for justifying the transmission of sensitive personal data outside the European Union in order to assist the U.S. authorities in their fight against terrorist financing? In June 2006, American journalists quote the under secretary of the U.S. Treasury Department that a data mining programme run out of the Central Intelligence Agency and overseen by the Treasury Department “has provided (them) with a unique and powerful window into the operations of terrorist networks and is, without doubt, a legal and proper use of (their) authorities“ (The New York Times, 2006). The under secretary is referring to a programme founded on a secret agreement between SWIFT and the U.S. dating back to late 2001 by which SWIFT has been transferring enormous quantities of data relating to international financial transactions to assist American investigators in the fight against terrorist financing. Privacy International states that this practice could have impacted more than 2.5 billion messages for 2005 alone and confirms that “SWIFT told the (European) Commission that the U.S. government has the complete right under its laws to require that all SWIFT messages are placed within that black box” (Privacy International, 2006). The so-called *black box* contains all data provided by SWIFT on a regular basis, is maintained by the U.S. Treasury Department and being analysed in accordance with a name retrieval software designed by the U.S. authorities.

Just to summarise: (i) SWIFT¹ is a co-operative owned by financial institutions in order to facilitate electronic financial data transfers between them; (ii) international financial institutions, whether subject to banking secrecy and data protection regulation or not, have ‘outsourced’ to SWIFT the exchange of formatted financial messages (payment, transfer, free text instructions, etc.); they have *not* outsourced the responsibility to comply with data protection laws in their respective countries of residence and operations, i.e. they remain fully accountable with regard to duly protecting private data of their underlying clients; (iii) SWIFT claims to be a data messenger centre rather than a financial professional bound by data secrecy and protection rules; (iv) by transmitting personal data of financial institutions and their underlying clients to state authorities without the prior consent of the data subjects concerned, SWIFT may have breached European legislation on data protection. In this debate, the legal question as to whether SWIFT should be qualified as a *data processor*² rather than a *data controller*³ is second ranking, in consideration of the potential disrespect of the spirit of the European regulation. In the same light, the

¹ SWIFT is the industry-owned co-operative supplying secure, standardised messaging services and interface software to nearly 8,100 financial institutions in 207 countries and territories. SWIFT members include banks, broker-dealers and investment managers. The broader SWIFT community also encompasses corporates as well as market infrastructures in payments, securities, treasury and trade. (www.SWIFT.com, 6 March 2007)

² ‘Processor’ shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. (European Directive 95/46/EC)

³ ‘Controller’ shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. (European Directive 95/46/EC)

question of eligibility for ‘safe harbour’ data protection to be granted by the U.S. Federal Trade Commission should have been raised and answered prior to SWIFT freely exporting sensitive data outside the European Union. By doing this, the banking co-operative has taken the risk to expose its professional clients to severe legal and reputation damage, notwithstanding the presumed ‘good cause’ for their decision to transmit data to and actively assist U.S. investigators in the fight against terrorist financing. The intention here is not to dispute this good cause, but to assess the most suitable method to achieve it.

In an official press release, SWIFT states that “all (their) members were informed in the 1990s about SWIFT’s general policy on member data retrieval including that SWIFT could be subject to judicial requests such as subpoenas. Informing (their) members on the specifics of the U.S. Treasury Department requests would have been inconsistent with (their) published policy of not commenting on sensitive activities such as subpoenas” (SWIFT, 2007). SWIFT objects to the “advisory opinions of the Belgian Data Privacy Commission and the Article 29 Working Party claim that SWIFT failed to respect the provision of EU Data Protection Directive 95/46/EC”, because “they reflect serious interpretation issues surrounding current data privacy laws.” SWIFT is right in raising the issue of legal uncertainty on specific data protection interpretation questions, putting them potentially into a difficult ‘political’ situation. But legal uncertainty is not providing a license to automatically disclose sensitive information to requesting state authorities without previously sorting out all legal interpretation issues, especially considering the fact that legal uncertainty has been subsisting from late 2001 to date with concerns being publicly voiced as late as in June 2006. It only evidences the unfortunate fact for

SWIFT to be “caught in the middle of a conflict between Belgian data privacy laws and US counter-terrorism laws” (SWIFT, 2007, *op cit*).

What makes organisations feeling pressurized by state authorities to act in such a way? Has ‘data liberalism’ and the associated claim for complete data transparency reached a stage where the violation of basic privacy protection rules can always be justified by the good cause? In this context, non-criminal frequent flyers and other travellers may be interested to know that the U.S. authorities request access to airline passenger data without these authorities offering adequate and legally acceptable data protection measures (EurActiv.com, 2007). Again the question is not whether this information is essential to assist state authorities in their legitimate attempt to stop terrorists from high-jacking airplanes. The answer needs to focus on identifying suitable legal means to combat crime; if these means require the inclusion of measures to adequately protect sensitive private data, so be it. It is positive to note that these examples have triggered discussions between the European Union and the United States to hopefully agree on a legal framework for exchanging financial intelligence in compliance with respective data protection requirements.

Even though the above two examples relate to the U.S., it would be unfair to finger-point unilaterally without also highlighting the exceptions foreseen by Luxembourg regulation in terms of waiving banking secrecy and data protection. In accordance with recommendation 4 issued by the Financial Action Task Force on Money Laundering in June 2003, secrecy laws cannot inhibit the implementation of measures ensuring the fight against money laundering and terrorist financing. In that sense, article 41 (2) of the Luxembourg

Banking Act of 1993 specifies that the obligation of secrecy shall cease where the disclosure of information is permitted or imposed by or pursuant to a legislative provision. One such important provision is the obligation of active and passive co-operation of financial professionals with the Luxembourg public prosecutor in the case of suspected money laundering or terrorist financing (article 5 of the law of 12 November 2004 on the fight against money laundering and terrorist financing). It differentiates, however, from the above SWIFT case study in the sense that the waiver of banking secrecy is granted locally and that the Luxembourg public prosecutor will ensure international co-operation by restricting the use of any information to the fight against money laundering and terrorist financing exclusively. Article 3 of the law of 12 November 2004 defines the obligation of financial professionals and their employees to know their clients. This includes the need to examine with utmost care every transaction that would appear suspect in terms of its *nature, surrounding circumstances and the quality of the persons* involved. The European Directive 2006/73/EC implementing the famous MiFID directive⁴ defines the financial professional's obligation to assess the suitability of its clients by requiring that "the information regarding the financial situation of the client or potential client shall include, where relevant, information on the source and extent of his regular income, his assets, including liquid assets, investments and real property, and his regular financial commitments."

⁴ Article 35 of Commission Directive 2006/73/EC of 10 August 2006 as regards organisational requirements and operating conditions for investment firms. Implementing European Directive 2004/39/EC of the European Parliament and Council of 21 April 2004 on markets in financial instruments ("MiFID").

What do these definitions imply in practice for the professionals concerned? *Nature of the transaction* and *quality of the persons involved* are to be verified during the initial identification process of the account holders and beneficial owners, if different from the account holders, and during the ongoing relationship. This includes the clarification of many questions exceeding the formal identification process in itself, which essentially consists in the verification of identification documents to determine client name and contact details: Who really is this natural or legal person I am supposed to deal with? What business is this person involved in, i.e. what is the source of any assets to be deposited? Has the person any official mandate as a director in a private or public company? Is the client to be considered as a 'politically exposed person (PEP)'? Does the client's name appear on any 'blacklist'? The concept of *surrounding circumstances* relates to the identification of the source of incoming assets and of the destination of outgoing payments and transfers of assets. Let us focus our interest on PEPs and blacklisted persons. Who are they and how to check them?

PEPs include " (a) heads of State, heads of government, ministers and deputy or assistant ministers; (b) members of parliaments; (c) members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances; (d) members of courts of auditors or of the boards of central banks; (e) ambassadors, *chargés d'affaires* and high-ranking officers in the armed forces; (f) members of the administrative, management or supervisory bodies of State-owned enterprises" as well as their immediate family members and persons known to be close associates (European Commission, 2006/70/EC). PEPs are no longer to be considered as such where they

have ceased to be entrusted with a prominent public function for a period of at least one year. Even though the critical reader of the Commission Directive may get the firm impression that this restriction has been invented by politicians for the benefit of politicians, it does not help the financial professional in complying with his duty to ensure complete transparency about the PEP status of his clients; it is even making the monitoring of PEP transactions more complicated. It is worth highlighting that the European Commission has not published a list of PEPs and that the identification of PEPs is being left to the entire responsibility of the financial professionals. Even though one might argue that the identification of persons falling under the categories (a) and (b) of the above PEP definition should be easy to achieve, because data on these persons is often publicly available, the identification of persons falling under (c), (d), (e), (f) and of immediate family members and persons close to PEPs reveals to be a real challenge. The verification of prospective new and existing clients against 'blacklists' would appear to be more straightforward and ready for implementation without delay, as the European Commission publishes terrorist blacklists on the basis of the United Nations sanction lists; in addition the Luxembourg public prosecutor informs financial professionals about criminals to be checked against their books.

A number of data vendors have discovered a lucrative business opportunity in selling 'blacklist' databases to financial professionals in order to assist them in monitoring their clients and transactions. These databases are said to be sourced from public information channels exclusively. They contain personal data, including but not limited to name, date of birth, address, involvement in criminal activities, link to terrorist organisations, link to other persons,

etc. The data is not limited to criminals, terrorists or PEPs, as one would first imagine. The desire for client transparency would appear to be a sufficient justification to extend the database content to other *client risk* categories. It is questionable to what extent the reliance on interconnected data, even if resulting from different official sources, can still be considered as fair data processing. Lawyers may well argue that this does not make the distribution of 'blacklist' databases illegal. It is interesting to note that some data vendors assemble the data for their databases outside the European Union in countries that do not offer equivalent data protection measures. It is also worth considering the question why these data vendors do not offer any guarantee with respect to the accuracy of the data sold to financial professionals. If you asked, they would probably – and quite rightly – respond that they are not in a position to warrant the accuracy of the public sources on which they rely for their sales. These databases have undoubtedly become a powerful tool to assist professionals in client identification, the detection of potentially suspicious (money laundering / terrorist financing) transactions as well as fraud prevention. What about the errors contained in public sources, what about the reputation impact on the natural and legal persons concerned? Would this be another example of 'good cause' justifying the risk of damage to individuals and collectivities that has not been clearly assessed beforehand?

The various case studies outlined above best evidence the existence of grey zones in terms of what is legally permitted and what may be ethically disputable in terms of sacrificing personal data protection for the sake of enhanced transparency. Interestingly enough, you will usually be able to find specialists providing advice on the lawfulness of data processing. You may, however, find it quite difficult to identify

persons capable of assisting you in the decision making process as to whether enhanced transparency in relation to individuals and collectivities – being your clients at the same level as being data subjects relying on your professional judgment – always matches up with your understanding of ethics. No wonder, it is and needs to remain your professional judgment! There will be nobody do make it on your behalf! The individual understanding of ethics is visibly influenced by ethical benchmarks set by state authorities of what is considered to be right and wrong. In this sense, it is interesting to view these authorities' priorities that focus on *PEPs* and *terrorists*, showing that they have agreed upon political priorities in the fight against money laundering and terrorist financing.

How to best set up the 'ethical balance' between data protection / banking secrecy and absolute transparency in the financial business? In an earlier attempt to identify possible ways of maintaining and improving the credibility and acceptance of banking secrecy jurisdictions such as Luxembourg, I recommended the establishment of a PESTL⁵ balance by its actors. The 'S' stands for "socio-regulatory balance between customer data protection, ensured by means of banking secrecy, and transparency of financial transactions." It means that "even though the right to privacy of customer information is fully justifiable, it can never be invoked to conceal any components of a financial transaction" (Zwick, 2003). And it is true to say that Luxembourg financial

⁵ Political balance between banking secrecy and international co-operation, Economic balance between profit and cost inherent to the attraction of foreign capital, Socio-regulatory balance between personal data protection and financial data transparency, Technological balance between new innovation and customer/transaction data tracking means, Legal balance between national legislation and common definition of money laundering.

professionals respect this socio-regulatory balance via the implementation of sound customer identification and transaction monitoring procedures. The main priority questions to be answered by *data processors* and *data controllers* are as follows: (i) What data is essential to enable me to conduct my business in accordance with prevailing regulation? Your answer should refer to the need to collect data on the basis of the "need to know" principle; data quality and quantity needs to be in line with the purpose of processing. (ii) Am I in a position to verify compliance with legal data quality and data processing requirements on an ongoing basis? The answer to this question will determine your ability to process and control data as well as to potentially act as a data vendor. Data must always be adequate, relevant and non-excessive when considering the purpose for which it is collected and processed. In addition, data must be accurate, up to date and stored only during the period necessary to meet that purpose. How to measure the proportionality of the risk of processing or transmitting inaccurate data in comparison to the estimated benefit for the community, if that risk has not been clearly assessed beforehand⁶? Even tough transparency of personal data bears a measurable direct cost for data processors, controllers and purchasers, your interest needs to focus on the ultimate cost for the data subjects concerned as well. (iii) Are my Information Technology and operational security measures sufficient to warrant a controlled and appropriate data processing? You may wish to consider personal data as a highly valuable asset entrusted to you and that you would like to protect from destruction, loss, alteration, unauthorised publication or access and from abuse for illegal purposes. (iv) Under which conditions am I authorised, or

⁶ Reference is also made to the previous discussion on 'blacklist' database vendors.

even legally required to disclose sensitive personal data to third parties? How can I best assess that the principle of proportionality is respected by those state authorities requesting access to personal data?

The right for privacy and for protection of personal data is a key concept in liberal democracies. It does not imply that persons who benefit from this right would de facto have something to hide from any public authorities. It may occasionally mean that persons simply want to hide something from other individuals, collectivities or state authorities for various reasons. If we agree that banking secrecy and data protection rules must never be designed to offer immunity to criminals and their transactions, any waiver to these rules must, however, be granted in a controlled way. As stated above, governments and authorities are now challenged to agree immediately on a legal framework for exchanging financial intelligence in compliance with respective data protection requirements. By the way, the same will need to apply to the exchange of personal data between international financial actors intending to shift data inside their group between several jurisdictions and outside their group to third parties to which they outsource part of their IT operations. Any other way of exchanging personal data is purely negligent and raises the pertinent question as to who is finally watching the controller, i.e. the state authorities themselves. Data processing and exchange may be legal, but does this make it defensible in all cases from an ethical standpoint? The existence of grey zones in terms of scope of data protection puts, in that sense, additional responsibility on *data processors* and *data controllers* to avoid any abusive behaviour. Being grown-up actors in the financial business who do not need to have detailed regulation covering all possible scenarios, we have now once more the opportunity to demonstrate that we are

ready to meet this challenge and make the co-existence of data protection and transparency become a success story.

by Marco Zwick, March 2007

published in the April 2007 Forum

References:

EurActiv.com, *Data transfer to US: MEPs raise pressure*, 1 February, 2007.

European Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, November, 1995.

European Directive 2004/39/EC of the European Parliament and Council of 21 April 2004 on markets in financial instruments.

European Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis.

European Commission Directive 2006/73/EC of 10 August 2006 as regards organisational requirements and operating conditions for investment firms.

Luxembourg Banking Act dated 5 April 1993, relating to the financial sector, as amended, 1993.

Le Bulletin

Luxembourg Law of 2 August 2002 relating to the protection of persons with regard to the processing of personal data, Luxembourg Law on Data Protection, 2002.

Luxembourg Law of 12 November 2004 on the fight against money laundering and terrorist financing, 2004.

Privacy International, *Belgian Prime Minister condemns SWIFT data transfers to U.S. as 'illegal'*, 28 September, 2006.

SWIFT, *US terrorist financing investigations and the role of SWIFT, A summary of developments to date on SWIFT compliance*, 11 February, 2007.

The New York Times, *Bank Data Is Sifted by U.S. in Secret to Block Terror*, Lichtblau, Eric, and Risen, James, 23 June, 2006.

The Register, *SWIFT sides with US in data spat with EU*, Ballard, Mark, 24 February, 2007.

Zwick, Marco, *Banking Secrecy and Money Laundering, The Challenge of Consolidating Luxembourg Banking Secrecy Rules and the Active Fight against Money Laundering*, Editions Promoculture, 2003.

Vie associative

VIE ASSOCIATIVE

ASSOCIATION ACTIVITIES

GROUPES DE TRAVAIL ACTUELS:

CURRENT WORKING GROUPS:

A. SECTEUR TRANSVERSAL:

A. CROSS-SECTOR:

Groupe de travail 16

Commission permanente juridique et relations publiques / site internet

Responsable Karine VILRET-HUOT
Téléphone (+352) 26 44 14 13
kvilret@vilret-avocats.com

Responsable internet Olivier GILSON
Téléphone (+352) 49 49 30 888
olivier.gilson@eurizoncapital.lu

Working group 16

Legal and public relations / internet site

Owner Karine VILRET-HUOT
Telephone (+352) 26 44 14 13
kvilret@vilret-avocats.com

Internet Owner Olivier GILSON
Telephone (+352) 49 49 30 888
olivier.gilson@eurizoncapital.lu

Groupe de travail 27

Formations IFBL

Coordinateur Jean-Noël LEQUEUE
Téléphone (+352) 621 194 941
jean-noel.lequeue@skynet.be

Working group 27

Training IFBL

Coordinator Jean-Noël LEQUEUE
Telephone (+352) 621 194 941
jean-noel.lequeue@skynet.be

Groupe de travail 29

Abus de marché

Coordinateur Cyril MATTHIEU
Téléphone (+352) 40 46 46 400
cyrilmatthieu@lu.hsbc.com

Working group 29

Market abuse

Coordinator Cyril MATTHIEU
Telephone (+352) 40 46 46 400
cyrilmatthieu@lu.hsbc.com

Groupe de travail 30

Domiciliation de sociétés

Coordinateur Sophie RASE
Téléphone (+352) 40 25 05 408
sophie.rase@maitlandgroup.com

Working group 30

Domiciliary agents

Coordinator Sophie RASE
Telephone (+352) 40 25 05 408
sophie.rase@maitlandgroup.com

B. SECTEUR BANCAIRE:

B. BANKING SECTOR:

Groupe de travail 10

Contrôles de compliance

Responsable Patrick CHILLET
Téléphone (+352) 40 65 40 584
p.chillet@ing.lu

Working group 10

Compliance controls

Owner Patrick CHILLET
Telephone (+352) 40 65 40 584
p.chillet@ing.lu

C. SECTEUR FONDS:

Groupe de travail 21
Interprétation pratique des restrictions d'investissements de fonds
 Responsable Tim WINFIELD
 Téléphone (+352) 34 10 23 85
tim.winfield@jpmorganfleming.com

C. FUNDS SECTOR:

Working group 21
Practical interpretation of fund investment restrictions
 Owner Tim WINFIELD
 Telephone (+352) 34 10 23 85
tim.winfield@jpmorganfleming.com

D. SECTEUR ASSURANCE:

Groupe de travail 13
Compliance et intermédiaires
 Responsable Bruno GOSSART
 Téléphone (+352) 24 18 58 51 60
b.gossart@fortis.lu

D. INSURANCE SECTOR:

Working group 13
Compliance and intermediaries
 Owner Bruno GOSSART
 Telephone (+352) 24 18 58 51 60
b.gossart@fortis.lu

Coordinateur groupes de travail / Working groups coordinator:

Jean-Noël LEQUEUE
 Téléphone (+352) 621 194 941
icesa@pt.lu

MEMBRES ET VIE ASSOCIATIVE:

Nombre de membres (au 20/11/2007):

Banques	153
Fonds	74
Fonds / Banques	33
Assurances	35
Consultants / Réviseurs	25
Admin. et domiciliation de sociétés	13
Avocats	4
PSF	24
Gestion de fortune	4
Autres	10
Effectif total:	375
Membres effectifs	315
Membres d'honneur	60
Effectif total:	375

MEMBERS AND ASSOCIATION ACTIVITIES:

Number of members (as per 20/11/2007):

Banking sector	153
Funds sector	74
Funds / Banking sector	33
Insurance sector	35
Consultants / Auditors	25
Admin. and company domiciliation	13
Law firms	4
SFP	24
Asset management	4
Other	10
Total number:	375
Active members	315
Honorary members	60
Total number:	375

Le Bulletin

Réunions et activités:

Mensuellement	Réunions du conseil d'administration
1 / 2 x par an	Réunions plénières
2 / 3 x par an	Rencontres informelles autour d'un thème

Meetings and activities:

Monthly	Board meetings
1 / 2 x per year	Plenary assemblies
2 / 3 x per year	Informal meetings on a subject



Secrétariat de l'ALCO:

Laurence THILMANY-INCOURT

secretariat@alco.lu

BP 13 L- 2010 Luxembourg

Secrétariat du Président:

Solyane LORKOVIC

Téléphone (+352) 24 67 26 12

Fax (+352) 24 67 81 37

solyane.lorkovic@ca-luxembourg.com

Secrétariat du Bulletin:

Sophia OZOG

Téléphone (+352) 26 44 14 13

Fax (+352) 26 44 15 14

sozog@vilret-avocats.com

Comité de rédaction / Drafting committee:

Karine VILRET-HUOT, Marie-France DE POVER, Marie BOURLOND, Sophie PIROTTE, Claudine FRUTSAERT, Jean-Marie LEGENDRE, Leen BOM, Olivier GILSON, Philippe SCHNEIDER, Patrick SCHOTT

Visitez notre site / Visit our website:

www.alco.lu