



Association Luxembourgeoise
des Compliance Officers
du Secteur Financier

News Bulletin

NO. 10

26 MARCH 2007

Editorial



Dear friends, members of the ALCO,

The association's bulletin continues to be a great success. Every month we examine in detail the statistics of visits to our Internet site (www.alco.lu) and, every month, we see that the bulletin is the rubric that is most in demand.

We also observe that the visitors don't only call for the most recent issues; rather, they also go to the « library » to find articles that have been published over the last few years.

Thank you for your interest in our bulletin, which the team gathered around Karine Vilret-Huot has been preparing with artistry and expertise for more than three years without interruption.

In order to make the bulletin a living link with the members of the ALCO, we plan to introduce a means for them to exchange ideas with us. Hence, we will open on the Internet site a specific rubric that enables the members to ask questions regarding the various subjects related to Compliance. These questions will be analyzed and grouped, and specific responses will be given in the bulletin.

Ask us questions, but also bring us your draft articles on all subjects in which the Compliance Officers of the Financial Sector might be interested. The range is wide!

I think this current issue aptly proves the point. You will find in it three articles that concern all of us.

- Marie-France de Pover discusses the new European regulation regarding information accompanying transfers of funds;
- Pierre-François Wéry, a partner in the recently formed Auditing Company, « Audit and Compliance », analyzes the role of a Compliance Officer confronted with fraud ;
- and Karine Vilret-Huot, publishes a lengthy documented article on personal data protection, certain provisions of which will be clarified at the urging of the State Council.

Don't forget our **General Assembly** that will be held on:

March 29, 2007 at the Novotel Hotel at 5:30 p.m..

That meeting is an important occasion in the life of our association. In particular, the Assembly will renew the Board of Directors of the ALCO pursuant to the charter, which specifies reappointment of the Board every two years. Hence, your presence is very important.

At this meeting, Mr. Philippe Dupont will address the subject of putting the « Market abuse» Act into practice in Luxembourg.

I look forward to seeing you very soon.

Jean-Marie Legendre
President

Legislative news

Actualités européennes :

Règlement CE n°1781 /2006 du parlement européen et du conseil du 15 novembre 2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds JOCE L 345/1 du 8 décembre 2006

Actualités luxembourgeoises :

La loi du 13 février 2007 relative aux fonds d'investissement spécialisés publiée au Mémorial A – N° 13 du 13 février 2007, abrogeant la loi du 19 juillet 1991 relative aux organismes de placement collectif dont les titres ne sont pas destinés au placement dans le public.

Règlement grand-ducal du 27 février 2007 pris en application de la loi du 13 février 2007.

Loi du 18 décembre 2006 portant transposition de la directive 2002/65/CE concernant la commercialisation à distance de services financiers auprès des consommateurs et portant modification de la loi du 27 juillet 1997 sur le contrat d'assurance, la loi modifiée du 14 août 2000 relative au commerce électronique, l'article 63 de la loi modifiée du 5 avril 1993 relative au secteur financier – memorial A n° 223 du 21 décembre 2006 page 3802.

Lettre circulaire CSSF 07/283 du 28 février 2007 concernant l'entrée en vigueur de la loi du 13 février 2007 relative aux fonds d'investissement spécialisés.

Lettre circulaire CSSF 07/281 du 27 février 2007 concernant l'entrée en vigueur de la loi du 18 décembre 2006 relative aux services financiers à distance portant transposition de la directive 2002/65/CE concernant la commercialisation à distance de services financiers auprès des consommateurs.

European news :

Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds JOCE L 345/1 8 December 2006

Luxembourg news :

Law dated 13 February 2007 on specialised investment funds published in Memorial A – N°13 of 13 February 2007, the law of 19 July 1991 relating to undertakings for collective investment whose securities are not meant for placement with the public.

Grand Ducal Regulation of 27 February 2007 pursuant to the Law dated 13 February 2007

Law of 18 December 2006 implementing Directive 2002/65/EC concerning the distance marketing of consumer –Memorial A n° 223 of 21 December 2006 page 3802

Circular CSSF 07/283 dated 28.02.2007 relating to the entry into force of the law of 13 February 2007 relating to specialised investment funds

Circular CSSF 07/281 dated 27.02.2007 relating to the entry into force of the law of 18 December 2006 on financial services provided at distance.

Bulletin

Lettre circulaire CSSF 07/280 du 5 février 2007 concernant les modalités d'application de la loi du 9 mai 2006 relative aux abus de marché.

Circular CSSF 07/280 dated 05.02.2007: relating to the implementation rules of the law of 9 May 2006 on market abuse

Karine VILRET-HUOT

Opinions

APPLICATION OF EUROPEAN REGULATION 1781/2006 RELATED TO TRANSMISSION OF INFORMATION REGARDING THE PRINCIPAL IN THE CONTEXT OF TRANSFERS OF FUNDS

I - Introduction

Although the Financial Action Group (FAG) acknowledges¹ that the systems of electronic payments that permit the tracing of transactions are largely secure, it also observes that the progress that has been realized (an increase in the speed and volume of transfers combined with an absence of coherence in the methods permitting the recording of essential information regarding these transactions, thus preserving the tracing thereof and transmitting the necessary information at the same time as the transaction) is also, for the authorities a source of obstacles to the traceability of transactions.

The use of transfers of funds for criminal purposes has on numerous occasions been demonstrated by the work of the FAG, which specifically issued the special recommendation n° VII.

In the context of the European Union's anti-terrorism action plan, the Parliament and the Council has adopted a Regulation on November 15, 2006 that integrated the recommendation in European law, along with a note regarding the construction thereof.

The purpose of the community provisions, applicable without adaptation to national law since Last January 1², consists of a harmonious and uniform implementation of

these recommendations in the European territory in such a way as to avoid hindering the systems of payments within the Union.

These provisions apply to all transfers of funds, in any currency whatsoever, to the extent that the payments are initiated or received within the Community³.

By adopting the Act of November 12, 2004⁴, the Luxembourg legislation had already adapted the FAG's⁵ special recommendation to national law. Based on the State Council's opinion, the particulars relating to the principal were limited to the name or account number, according to the client's choice or the bank's policy.

II - Obligations

New obligations are imposed on various providers of payment services, such obligations varying according to whether they provide a payment service for the account of the principal or the beneficiary, or as an intermediary.

The regulation also establishes the general obligation to respond in a complete and timely way to governmental authorities' requests in matters of money laundering in the country in which the provider is located. These authorities may use this information only for the purposes of prevention, investigation and detection of money laundering.

The sanctions applicable for breach of these provisions fall within the purview of the member States, and must be established by December 15, 2007.

¹ 2003-2004 report regarding the typologies of money laundering and terrorism financing

² Circular CSSF 06/274 of December 22, 2006 thus specifies that the provisions of the Regulation prevail over those of article 39 of the Financial Sector Act and of § 145 of circular 05/211 of October 13, 2005, in accordance with the principle of primacy of community law.

³ The Regulation provides a number of exemptions, particularly regarding transfers between providers of payment acting for personal account or transfers made from an account, of less than 1,000 EUR.

⁴ Act adapting the 2nd money laundering directive (2001/97)

⁵ Article 16 of the Act 12.11.04, amending article 39 of the Act of 05.04.93.

1. *Obligations of the principal's bank*

The bank must ensure that the transfers of funds are accompanied by complete, accurate and useful information regarding the principal⁶.

The term “complete information” designates the principal’s given name, surname, address (which can be replaced by the client’s date of birth, identification number or national identity card number) and account number. The account number may be replaced by a single identifier only if an account number does not exist.

Prior to a transfer, the bank must verify the information based on documents, data or information obtained from a reliable and independent⁷ source.

However, in the case of transfers of funds from an account, the verification must be deemed to be completed if the client has been identified pursuant to the principles of identification set out in the 3rd money laundering Directive⁸.

These data must be retained for 5 years.

The Regulation promulgates two different regimes according to whether the transfers are effectuated within the community or are destined for a third party country.

Transfers of funds to a third party country must in all circumstances include complete information regarding the principal⁹.

By dispensation, transfers of funds within the Community need include only the account number or a single identifier for access to the principal.

Upon request of the beneficiary bank, the principal bank must provide it with complete information within 3 days thereof.

The data to be transmitted by banks are thus now more extensive than those that have been required previously by the Luxembourg legislation.

However, the possibility of dispensation that is offered may be difficult to use considering:

- the risk that correspondents may systematically require all of the information and automatically reject transfers that include only the account number ;
- the beneficiary bank’s right to claim all of the data from the principal bank ;
- the extra work required if the banks must satisfy these requests within 3 days.

It appears that the banks have not adopted a common position in that regard: banks that are focused on « private banking » might opt for this dispensation, as distinct from those whose business is more orientated to « retail banking ».

A. Breach of banking secrecy?

European regulation 1781/2006 related to the transmission of information regarding the principal in the context of transfers is, as we know, immediately applicable without the necessity for any particular adaptation to national law.

Consequently, it is apparently permitted to consider that this is an exception to the banking secrecy prescribed by article 41 of the Financial Sector Act. Article 41§2 thereof indeed stipulates that the obligation of secrecy ceases when the disclosure of information is authorized/ imposed by force of law.

The Regulation restricts the use of this data by the authorities to the sole purposes of prevention, investigation and detection of capital laundering.

⁶Article 2§3) : The natural person or legal entity that is the holder of an account authorizing a transfer of funds **therefrom**, or, in the absence of **an** account, the natural person or legal entity that gives the order to effectuate a transfer of funds

⁷ However, for transfers that are not effectuated from an account, the provider checks the information only if the amount exceeds 1,000 EUR, unless the transaction is effectuated in one or more operations that seem to be connected or which jointly exceed 1,000 EUR.

⁸ The regulation refers to articles 9§6 and 30(a) of directive 2005/60.

⁹ Exception provided for transfers in blocks if the block file includes the complete information, and the transfers include the account number or a single identifier.

In this context, according to some commentators, it appears that the client's authorization for the bank to transmit the necessary information for execution of a transfer that he has initiated is not indispensable.

Nevertheless, some think that it preferable to inform the clients and perhaps, at least from a commercial point of view, take additional precautions with clients who opted for accounts other than those registered by name, considering the increased confidentiality that they are seeking. The opinions in this regard are not unanimous and the issue remains a subject of discussion

B. Definition of the principal

Although the Regulation states basic rules of a rather simple character, difficulties in application might arise when a transfer order comes jointly from several holders or a representative, and is executed from an « estate » account or initiated by an individual merchant.

What is in fact the information to be provided in such cases, considering the limitations of transfer applications, particularly when several names of signatories/holders must be indicated?

This question has not been clearly addressed in the text itself or in the « guidance notes » published by the European Banking Federation. We note that the ultimate goal of the Regulation is to enable the traceability of transfers for prevention of the risks of money laundering and financing of terrorism, and that it is this objective which must be given the highest priority.

C. Risks of fraud ?

As noted by the Chamber of Commerce in its opinion regarding the Bill adapting the second laundering directive¹⁰, indication of the principal's name along with his account number exposes the transaction to major risks of fraud.

Hence, it was with the view of preventing such risks that a majority of banks decided not to transmit to the beneficiaries the principal¹¹'s account number. But no guarantee is provided in that regard, as the transmission falls within the individual responsibility of each bank.

Unfortunately, this issue has not been taken up by the European Banking Federation. In any event, even if a common position were to be adopted by the Banks in the Community, that would not result in any commitments on the part of banks located in third party countries.

2. Obligations of the beneficiary's bank

The beneficiary's bank must be able to detect the absence of information regarding the principal when it receives the transfer, and take the appropriate measures to correct this situation, in such a way that the transfers of funds received do not remain anonymous¹².

Since incomplete items of information are to be considered as risk criteria when assessing the suspicious nature of a transaction, the bank may reject a transfer or require further information; but it must be particularly vigilant vis-à-vis such transfers and, according to the risks, take other pertinent factors into consideration, with a view to declaring suspicious transactions to the authority. Collected data must be retained for 5 years.

Recital 16 nevertheless acknowledges that « some flexibility should be authorized as a function of the risk, regarding the extent of information to be provided ».

If the principal's bank regularly fails to provide the required information, the beneficiary's bank takes measures that may, at first, include the issue of warnings and the setting of deadlines, before refusing any new transfer of funds or deciding whether or not to restrict or put an end to its commercial relationship.

¹⁰ Opinion of the Chamber of Commerce 16.09.03 relating to Bill n°5165, article 16.

¹¹ In the case of transmission of complete information regarding the principal.

¹² Therefore, the control shall be on the pertinence of data, even if the bank must ensure that the fields used in the messaging system have been filled out with characters or elements compatible with this system.

This fact is to be declared to the Public Prosecutor's Office.

ad hoc procedures.

In line with the approach based on risk, the statement of grounds of the regulation expressly sets forth that « when the principal's provider of the payment service is located outside of the Community, obligations of vigilance vis-à-vis the clientele should be applicable »¹³.

Nancy Carabin
28.02.07

3. Obligations of banks acting as intermediaries

Intermediary banks must act in such a way that the information regarding the principal in the context of a transfer is transmitted therewith or filed appropriately. They retain all information received for five years

III - Conclusion

The fight against use of the financial sector for money laundering or financing of terrorism is a priority in a global economy in order to guarantee both the stability and reputation of the financial sector and the trust of participants in the entire financial system. Let's us only regret that it is again the financial institutions themselves on which additional constraints of surveillance are imposed.

The member States will have to include in their legislation effective, proportionate and dissuasive sanctions, applicable as of December 15, 2007.

But particularly, the consequences of failure to abide by the Regulation can range from a refusal to execute or accept a payment to termination of a bilateral relationship when a bank systematically contravenes these provisions.

It is this principal commercial risk, and the risk of damaged reputation that must be curbed by adopting surveillance measures and

¹³ Recital 16

Opinions

THE COMPLIANCE OFFICER CONFRONTED WITH FRAUD

The purpose of this article is to share some thoughts regarding the problem of fraud with which every Compliance Officer is confronted in one way or another, but which is not treated as such by the banking regulations of Luxembourg. The discussion does not pretend to be a legal treatise; rather it merely aims to emphasize the importance of the Compliance Officer's role in dealing with this costly phenomenon.

After having defined fraud and the various phases that are generally present for analysis of the risk thereof, we will briefly review the banking regulations of Luxembourg with respect to their references regarding fraud. Finally, we will conclude with our personal opinion regarding the involvement of a Compliance Officer vis-à-vis the subject of fraud.

I. Fraud and its various aspects

Fraud is defined differently according to the professional bodies or associations involved; but, put simply, four essential characteristics emerge from the prevailing definitions: Fraud is a deceit deriving from an intentional act, which can be internal or external, for the purpose of extracting profit for the account of an organization or for the person committing the fraudulent act.

Generally, three types of fraud, depending on the actors involved, are most often distinguished:

- Internal fraud: a fraudulent act that is committed by employees of a company (for example: misappropriation of cash deposited by the customers of a bank or falsification of transfer orders deposited by customers),
- External fraud: a fraudulent act that is committed by employees who are not

bound to the company under an employment contract (falsified transfer order sent by a third party to a bank),

- Mixed fraud: a fraudulent act that is committed through complicity between a person inside the company and an outside person.

II. Phased approach to the risk of fraud

Before discussing the role of a Compliance Officer in respect to fraud, we think it pertinent to first indicate the various phases that usually exist in analysis of the phenomenon. Indeed, a Compliance Officer may be more or less involved in the fight against fraud depending on the different phases described below.

1. Prevention

The primary objective of prevention is to limit the number of cases, as well as the magnitude, of frauds to which banks are exposed. Several studies have concluded that it is not possible to completely prevent fraud, but that banks which have installed a preventive system have greatly reduced their risk in that regard.

Here are a few elements that are usually mentioned in the specialized literature as components of a preventive fraud system:

- definition and distribution of an ethics and internal control policy;
- definition and distribution of a general policy in line with the ethics and internal control policy ;

The Bank must ensure that its general policy and its operational particularities in implementation thereof comply with the ethics and internal control policy.

For example:

- management policy with physical and logical aspects
- policy for management of the relationships

with partners
- policy of powers;

- establishment an organization in conformity with the code of ethics;
- definition of a culture of control;

The culture of control should include three essential elements: raising of the employees' awareness of the risk of fraud, human resources policy and operational and control procedures.

- surveillance of the quality of the anti-fraud system.

2. Detection

The following phase consists of fraud detection, with a review of various means that are customarily used to achieve it.

2.1. Monitoring of complaints

Establishment of a rigorous procedure regarding the receipt and processing of complaints is a key element in an effective anti-fraud system.

This procedure must address two fundamental aspects:

- securing of receipt of complaints (via letter, fax, e-mail or telephone) by ensuring that they are not « detoured »;
- effective processing (from the anti-fraud point of view as well as from a commercial point of view) and independent monitoring of complaints.

2.2. Disclosure of fraudulent facts: The « whistleblowing »

The disclosure of fraudulent facts is one of the most effective means for detecting frauds. Indeed, according to statistics published by the Association of Certified Fraud Examiners, one-third of frauds are discovered on the basis of information obtained from employers, suppliers, customers, etc.

A professional alert or “whistleblowing” system is an arrangement established by a private or public entity to encourage

employees to report problems that can substantially affect its business or seriously engage its liability, thus contributing to the fight against attitudes that are contrary to the professional code of ethics, and against corruption and financial crimes in the areas of banking, accounting, internal supervision of accounts and audits. It does not replace any other existing channels of warnings (via the hierarchy, employee representatives, a public authority, etc....), but supplements them.

Such systems have frequently been set up by companies of an international scope, especially in the banking area. The professional alert system may take the form of a telephone number (« ethics line ») or an electronic mail that directs the alerts to people with special training. It then provides for the verification of facts collected in a confidential context, and enables the employer to decide, with full knowledge of the matter, on the measures to be taken in order to remedy the dysfunctioning that is observed.

2.3. Monitoring of errors and abnormalities

Any abnormal situation can be a reason for suspecting fraud. That is why the monitoring of errors and abnormalities is a key element in an anti-fraud system. The effectiveness of this activity may be maximized through the monitoring of fraud indicators.

The principal fraud indicators identified by the literature, set forth by category, are the following:

- **2.3.a) Personnel :**

An internal fraud is characterized by the involvement of an employee of the bank. Statistical studies enable a fairly precise definition of the profile of a typical fraudulent person in the corporate world: in Belgium or in France, it is usually a male employee of the company around forty years of age, who holds a diploma granted by an education institution. The monitoring of certain qualitative and quantitative indicators enables detection of elements that may lead to a suspicion of fraud.

Qualitative indicators:

- A lifestyle that is excessive in relation to the employee's income;
- Existence of other business activities outside of the bank;
- Involvement in high-risk interests (gambling, antiques,...)
- Abnormal vacation periods or working hours.

Quantitative indicators :

- High number of operational errors or reversing entries;
- Losses of documents ;
- Unauthorized operations (Exceeding of limits, operations not registered « in stand-by », unauthorized time limits).

- **2.3.b) Logical and physical access:**

The average number of comings and goings in the facility's banking area; the number of lost or forgotten entry badges; the average number of erroneous password encodings in an application; the number of breakdowns in access control (logical or physical) are many of the indicators for identification of frauds.

- **2.3.c) Abnormal performance:**

One should constantly be mindful of a potential risk of fraud, and be on the lookout for indicative abnormalities. Hence, when reviewing the company's activities, it is important to pose the question of whether the performance of these activities is normal. A product whose sale suddenly shows unexpected results should draw the attention of internal controllers and/or of the management. Conversely, a sudden loss of profitability in a company should raise questions, as it might be explained by fraudulent acts.

2.4. Monitoring of accounts

Without talking about money laundering

which, in itself, is a specific form of fraud, it is fundamental to monitor in detail the accounts and other management control indicators.

Based on analyses of the evolutions of accounting balances, abnormal movements that might be detected must be subject to a thorough inquiry. Movements may be considered abnormal because of their incoherence with the category of the account (for example, an expense account that is credited) or because the amounts involved are very substantial or small, but are repetitive, or even because the accounts being used are usually dormant...

2.5. Reconciliation

Various tasks of internal control may afford an opportunity to bring to light incoherent elements that exist in the operation of an establishment. Such incoherence, which might appear substantial or slight, could possibly reveal fraudulent behaviour.

For example, the process for reconciliation of bank accounts serves, first, to ensure that the accounting entries are complete. However, a number of frauds are detected on the occasion of these reconciliation operations.

Under the term « reconciliation », one may group various types of more or less intensive internal controls for the detection of fraud: adjustments, conducting of inventories, exchanges of confirmations, systematic circulation of information and inquiries to customers and suppliers.

3. Investigation

As soon as suspicions of fraud arise, the investigative phase can be initiated and organized. The theoretical approach that is generally used for conducting an investigation is the following:

- *Validation of suspicions*
- *Establishment of the investigation's purpose*
- *Assembly of the investigation team*
- *Identification of the people in question*
- *Characterization of the fraud, and collection of proofs*

- *Determination of the amounts involved*
- *Determination of corrective measures to be taken*

III. Treatment of fraud in the Luxembourg regulations

In Luxembourg, fraud does not constitute a specific type of crime. However, the legislation defines certain types of crime that may be assimilated with the general notion of fraud: theft, abuse of trust, swindling, forgery, use of forgery, possession of stolen goods, money laundering, market abuse,.....

In the regulation of banking, the concept of fraud is treated in various circulars issued by the Commission for Surveillance of the Financial Sector (hereinafter CSFS), particularly those relating to internal control. However, it is obvious that the issues are not treated in a specific text.

We specify hereinafter the various texts issued by the CSFS which, in our opinion, are connected with the concepts of fraud.

- Circular **93/101**, relating to the rules regarding the organization and internal control of credit institutions' securities market business, specifies that « any institution that observes that a fraud (dissimulation of losses and positions, intentional deformation of the reality of transactions, etc...) has been committed in the market room, must immediately report it to the C.S.S.F».

- Circular **96/126** in many regards contains recommendations for the prevention of fraud. Hence, this circular relating to the administrative and accounting organization strongly insists on the principle of separation of tasks, as well as, for example, on the monitoring of dormant accounts.

- Circular **98/143** relating to internal control specifies that «the internal control system also provide for mechanisms designed to guard against errors of execution and frauds and to enable rapid detection». Regarding the internal control plan, this circular insists that « it pay particular

attention to the risk of errors of execution and that of fraud ».

- Also, even if the fraud is not explicitly mentioned in circular 2000/15 relating to the rules of conduct in the financial sector, this circular establishes a framework of ethics favourable to the prevention of, and fight against, fraud.

- Circular **04/155** instituted the Compliance function. The circular defines this as « an independent function aimed at identifying and assessing the risk of non-Compliance in an institution, as well at assisting the administration in the management and control of this risk ». The risk of non-Compliance may thus include various risks such as the risk to reputation, the legal risk, the risk of dispute, the risk of sanctions, as well as some aspects of operational risk». Unfortunately, these aspects are not detailed.

Intuitively, the reader of this text might consider that fraud is included in this definition of risk of non-Compliance. Nevertheless, it is remarkable that the word « fraud » appears only once in the entire text of the circular.

- Money laundering is a specific form of fraud. Circular **05/211** relating to the fight against money laundering and financing of terrorism clearly indicates that the person responsible for the Compliance function must be in charge of addressing this specific type of fraudulent conduct.

- Finally, it is appropriate to mention that, following the promulgation of the law on market abuses, two circulars have been published on that subject. Market abuses may consist of many kinds of fraudulent conduct. Circular **07/280** mentions that « the person responsible for the Compliance function (...) shall generally be responsible for compliance with the obligations specified in article 12 of the Act». This article 12 provides that every credit institution must report to the CSFS if there are reasons for suspecting that an operation might be that of an initiate in the system or of a manipulation of markets.

Conclusion

Even though fraud is sometimes explicitly mentioned in some circulars of the CSSF, the latter has not yet enacted a regulation specifically regarding fraud, which in some way would vest in the Compliance Officer a comprehensive mission relating to this theme.

However, especially regarding prevention, the Compliance function is logically at the head of the line, since ethics are systematically at issue in problems of fraud.

Regarding detection and investigation of fraud, the role of the Compliance officer is not as clear; and, in practice, the solutions applied by banks in the financial market vary greatly even if there is a trend to entrust these themes to internal service departments except for specific matters that constitute money laundering and securities market abuses.

We nevertheless think that the fight against fraud is a veritable subject in and of itself, which deserves from Compliance Officers a structured analysis, and which, in our opinion, must not be limited to prevention.

One observes that large institutions set up vast anti-fraud programs covering all aspects of the subject.

In addition to the preventive aspects, the Compliance Officer, when conducting his « Compliance Risk Assessment » and his « Compliance Monitoring Program » could define actions aimed at detecting frauds, even if those are handled by other departments.

As for the investigative phase, we think that involvement of the Compliance Officer, mainly for analysis of possible failures in the event of internal fraud, is desirable, especially in order to obtain information on dysfunctioning that are observed. However, during this phase, conflicts of interest, often latent, with which the Compliance Officer might be confronted, must be considered. Indeed, the investigation of a fraud may occur following a defect in the preventive system which the Compliance Officer himself has set up.

Pierre-François Wéry

Pierre-François Wéry is an associate founder of audit & compliance s.à r.l

Opinions

PROTECTION OF PERSONS WITH REGARD TO PERSONAL DATA PROCESSING IN LUXEMBOURG

Even though the principal objectives of the Luxembourg financial centre reside in the fight against laundering and terrorism, the fact still remains that the fundamental rights of everyone must be preserved, particularly with regard to compliance with the principles of personal data protection.

The importance of this requirement was recently underscored when the press made public the SWIFT company's failure to comply with the community provisions applicable to personal data¹⁴.

SWIFT, a company governed by Belgian law, operates a network of payments and financial messaging services aimed at facilitating international transfers. SWIFT stores all messages (personal data as well as the names of persons that effectuate and receive payments) in two operations centres, one in the European Union and the other in the United States. Since the terrorist attacks of September 2001, the Treasury Department has been asking SWIFT to give it access to data stored in the United States; SWIFT agreed to do so without advising the Belgium authority charged with responsibility for data protection.

The European authorities, particularly the European group of commissioners working on data protection (Group Article 29¹⁵), criticized SWIFT for its failure to comply with Belgian law regarding personal data protection adapting European directive 95/46 of October 24, 1995, in that it agreed to transmit to the American authorities banking data¹⁶ transiting through its network by confidential and non-transparent means,

failing to disclose said data without a legal basis for doing so and without the possibility of independent supervision by the European authorities responsible for data protection.

The Compliance Officer, whose responsibility is especially to oversee and verify conformity of the company's activities with the legal, regulatory and ethics standards in effect, must take cognizance of the data protection legislation and ensure that the legal and regulatory provisions are applied by his bank, particularly when he is in charge of the processing. To that end, he must establish and conduct a national and international regulatory vigil, and must report any potential impacts on the organization and/or activities.

Protection of persons with regard to the processing of personal data is provided in Luxembourg by the Act of August 2, 2002. This Act frames the rules governing the processing of data of a personal character, protects the rights and liberties of natural persons and legal entities in respect thereto, and appoints the National Commission for data protection, which is an independent administrative authority with the responsibility of inspecting and verifying the legality of personal data, and of ensuring application of the law.

The present analysis summarizes the obligations of persons or entities that process personal data, describes the rights of persons subject to personal data protection (« the person involved ») and highlights the possibility of a future evolution of the legislation by virtue of Bill n° 5554.

¹⁴ European directive 95/46 of October 24, 1995 regarding data protection

¹⁵ Article 29 of European directive 95/46/CE of October 24, 1995 designated an independent working group comprised of representatives of each authority of the member States of the European Union dealing with data protection.

¹⁶ The banking data involved are personal data such as the names of persons that effectuate and receive payments.

I. Obligations of persons processing personal data

Any natural person or legal entity that processes personal data is subject to a certain number of obligations. Before analyzing the obligations to be met during a processing of data, vis-à-vis the person involved and vis-à-vis the National Commission in charge of data protection, it is necessary to describe the actors that participate in this processing.

A. Various participants in the processing of personal data.

The law defines the roles, missions and relationships of persons and entities working in the field of data processing.

1. Processing manager

The law defines the processing manager as being « the natural person or legal entity, the public authority, the department or any other body that, alone or jointly with others, determines the purposes and means of personal data processing. When such purposes and means are determined by, or by virtue of, the legal provisions, the processing manager is determined by, or by virtue of, specific criteria pursuant to the legal provisions»¹⁷.

The processing manager is the person who has the authority to determine the purposes of a processing and the means to be implemented in view of this processing.

2. Subcontractor

The subcontractor is different from the one that is responsible for the material execution of all or part of the processing¹⁸, since it is « the natural person or legal entity, the public authority, the department or any other body that processes data for the account of the processing manager »¹⁹.

3. Person in charge of data protection

Another participant that can process personal data is the one in charge of data protection, whether as a natural person or a legal entity approved by the National Commission for data protection. The processing manager may appoint a person in charge of data protection²⁰. This appointment exempts the processing manager from the obligation to notify his processing to the National Commission. The processing manager must transmit thereto the identity of the person in charge of data protection that it has appointed for the establishment thereof, in order to be exempt from said notification. The Luxembourg regulation establishes the modes of appointment and dismissal of the person or entity in charge of data protection, particularly by imposing independence thereon vis-à-vis the processing manager that appoints him²¹.

4. In practice

It is important to distinguish between the function and role of a processing manager and a subcontractor. For example, an insurance company is considered to be a processing manager, whereas the general insurance agent must have the status of a subcontractor ; a unit trust or a company managing a mutual fund is to be considered responsible for the processing, whereas a depository bank or an administrative agent must have the status of a subcontractor since it executes the orders of the processing manager²².

In the SWIFT case, SWIFT is not deemed to be an entity acting for its own account, but as a subcontractor at the service of various banks for which it executes international banking orders. Banks are to be considered processing managers; therefore, they have the duty to prohibit SWIFT from transferring to the United States banking data that do not relate to a transaction coming from or destined for

¹⁷ Article 2 (o) of the Act of August 2, 2002.

¹⁸ Parliamentary document 4735-13 p. 6

¹⁹ Article 2 (p) of the Act of August 2, 2002.

²⁰ Article 40 of the Act of August 2, 2002.

²¹ Article 40 of the Act of August 2, 2002, and the Grand Ducal regulation of November 27, 2004.

²² P. Santer, T. Hoss, «The Act of August 2, 2002 dealing with the protection of persons in respect to personal data processing: a new data for the financial centre», *Banking and financial law in Luxembourg, collection of legal opinions, volume 1*, p 376.

an American bank account; indeed the role of banks is to determine the purposes and means of personal data processing.

In the event of violation of legal provisions, the processing manager engages its own civil and criminal liability, not the subcontractor.

When the means and purposes of processing are determined by law, the law also designates the processing manager. Hence, the law that sets the modes and purposes of processing data provided by students in public or private schools designates the minister of national education as processing manager. A processing manager in the public sector is any ministry, administration or department of the State that processes personal data.

These participants, particularly the processing manager, are subject to a number of obligations vis-à-vis the person involved when they process personal data.

B. Principles to be observed upon the collection of personal data

A processing manager is a person that must observe the rules governing data protection, and engages its liability in the event of failure; it must ensure that the data it processes comply with certain principles.

1. Principle of legitimacy and legality

Data processed by the processing manager must meet the requirements of legality, legitimacy and fairness.

In other words, only a legitimate reason justifies the collection of data.

For example, the processing of data is permitted for the execution of a contract, to satisfy a legal obligation, or if the person or entity involved consented thereto.

2. Principle of purpose and proportionality

Data may be collected only for purposes that are determined in advance; therefore, the use of said data must be strictly limited to such purposes, and to that which is necessary to

fulfil them. The data must be useful and necessary for the person or entity that processes them; they shall not be excessive in relation to the established purpose.

3. Principle of accuracy in data

Data that are processed must be accurate and current; they must be processed confidentially, and stored in secured areas and in secure equipment.

The collection, registration, use and transmission of data must be effectuated in good faith and not without the knowledge of the person involved – i.e. they must be deleted as soon as they are no longer useful for their initial purpose.

4. Data subject to reinforced protection

Some data that are defined as particularly « sensitive » -- e.g. those relating to racial or ethnic origin, political opinions, religious or philosophical conviction, union membership, health, and sexual orientation and activity – cannot be processed except in cases that are expressly specified by law²³, such as compliance with the processing manager's specific obligations and rights in matters of labour law, when the person involved gives his express, unambiguous, free and specific consent with full knowledge, when the data have been provided by the person involved or when the processing is required for protecting the vital interests of the person involved (e.g. processing in the event of a medical emergency) or of another person if the person involved is in a state of physical or legal incapacity that prevents him from giving his consent.

Surveillance (audio, video, electronic) of identifiable persons is framed by law²⁴, and requires the consent of the person involved, or the informing thereof by appropriate means such as road signs, circulars, etc.. Also, processing data for the purpose of surveillance at the workplace is possible only if the person involved, the joint committee, the employee delegation or the labour and mining department have been informed

²³ Article 6 of the Act of August 2, 2002

²⁴ Article 10 of the Act of August 2, 2002

beforehand²⁵ ; but it is not necessary to have their agreement in order to organize this processing. The processing of data for surveillance at the workplace is possible only if necessary for the workers' safety and health, for protection of the company's properties, for inspection of the production process, but only on machines, and for temporary inspection of the employee's production or work when such a measure is the only way to determine the employee's exact remuneration²⁶.

Use of personal data for the purposes of advertising or commercial prospecting, and any transmission of data to third parties must never be effectuated without the consent of the person involved.

In any event, the processing of personal data shall not infringe upon the privacy of the person involved, with any contrary use being prohibited and sanctioned.

If these principles are breached, the processing manager's liability is engaged, even if the breach is due to the subcontractor's wrongful act or omission.

In addition to compliance with these principles, in cases that are specified by law the processing manager must notify the National Commission of the processing of personal data, or ask the latter for its authorization prior thereto.

C. Obligation of prior notification and authorization for the processing of personal data

Most operations of personal data processing must be notified; and others must be authorized by the National Commission prior to initiation of the processing.

1. Prior notification to the National Commission

Processings of personal data must be notified by the processing manager to the National

Commission beforehand.

The notifications must be effectuated to the National Commission by means of forms provided thereby, on paper or electronic medium; notifications on « plain unheaded paper » are not accepted.

All notifications must be made on a paper version; however, they may be sent by electronic means in addition to the paper version for ordinary and simplified notifications, and for those that relate to changes in the processing.

A notification must contain at least the following information (without being limited thereto) : the processing manager's name and address, the legitimacy and purposes of the processing, the description of categories of the persons involved, the addressees ,

Although notification is the rule, some processing (apart from processing that must be authorized) may not be subject to notification; for example when a processing has no impact on the rights and liberties of the persons involved²⁷.

The designation of a person in charge of protection exempts the processing manager from the obligation of notification, subject to that person's identity having been transmitted to the National Commission; in that event, the obligation of notification is incumbent on the person in charge of data protection.

The law specifies that a number of processings under the same processing manager's responsibility, and with identical or related purposes, may be subject to a single notification²⁸.

There are two types of notification:

- The simplified notification is possible for processing operations whose execution does not infringe on fundamental liberties and rights, particularly the privacy of the persons involved.

The National Commission adopted six directives allowing simplified notifications of processing:

²⁵ Article 11 of the Act of August 2, 2002

²⁶ Article 11-1 of the Act of August 2, 2002

²⁷ Article 12 of the Act of August 2, 2002

²⁸ Article 12(1)(b) of the Act of August 2, 2002.

- Management of members of nonprofitmaking foundations and associations and de facto associations;
- Personnel administration;
- Shareholder registries;
- Management of contacts and public, social and professional relations;
- Administration of suppliers, including prospecting of potential suppliers;
- Customer administration, including prospecting of new customers, marketing and personalized advertising.

A fee must be paid before introduction of the notification, the amount of which varies according to the form of notification (100 € for notifications only in paper version, and 75 € for those in paper version and by electronic means).

- The ordinary notification is specified when a data processing to be notified does not correspond to the directives for a simplified notification; the processing manager must declare such a processing to the National Commission by ordinary notification.

Article 13 of the Act of August 2, 2002 sets forth the information that the ordinary notification must contain. The form of ordinary notification is identical to that of the simplified one; but the amount of fee differs (125 € for notifications only in paper version, and 100 € for those in paper version and by electronic means).

The processing manager must notify the National Commission of any change in the contents of the original notification, the end of the data processing and the transfer of data.

Processing for which notification is not required or which is exempt from notification, must be authorized beforehand.

2. *Authorization prior to processing*

The law specifies two different categories of prior authorizations:

- Reinforced control is provided for processing that may present particular risks of infringement on the rights and liberties of the persons involved²⁹. Processing of « sensitive »³⁰ data, processing for surveillance, processing for surveillance at the workplace³¹, and processing regarding the credit and solvency of the persons involved are subject to this procedure.

- Processing regarding the interconnection of data must also be authorized by the National Commission.

An interconnection is « any form of processing that consists of correlating data processed for a particular purpose with data processed for identical or related purposes by one or more processing managers. »³². One refers to interconnection of data when one or more processing managers put into correlation data that it processes for identical or related purposes. The interconnection may involve processing that is authorized by, or notified to, the National Commission. It is possible to ask for an interconnection concomitantly with one or more authorization applications or one or more notifications. The purposes of processing for which an interconnection is asked, must be identical or related.

- The National Commission must also authorize the processing of data for a determinate purpose, provided that such data are intended to be processed subsequently for historical, statistical or scientific purposes, including data that are used for purposes other than those for which they were collected; such processing must be authorized by the person involved and, if said person is deceased, by his/her heirs.

- Generally, the transfer of data to countries outside of the European Union is prohibited, but the law provides exceptions:

²⁹ Article 20 of directive 95/46/EC

³⁰ Article 6 of the Act.

³¹ Articles 10 and 11 of the Act

³² Article 2 (j) of the Act

Transfers of data to third party countries that do not guarantee adequate protection may be authorized by the National Commission³³ if the processing manager provides sufficient guarantees in respect to the privacy and to the fundamental rights and liberties of the persons involved, as well as to the exercise of related rights³⁴.

Regarding the authorization procedure, the National Commission may authorize by a single decision a number of processing operations that have the same purpose and involve several categories of addressees.

Since the authorization precedes the commencement of a processing, the processing manager must categorically commit to initiate it by virtue of the authorization that it received.

The content of an authorization application is similar to that of a notification. However, the information regarding the data in question, the processing envisaged and the security measures are more detailed than for a notification.

Having described the obligations in respect to personal data processing, and the administrative procedures prior to processing, it is appropriate to describe the rights of the persons involved.

II. Rights of the persons involved

The reconciliation of the principle of free circulation of data with the fundamental rights and liberties of the person involved requires that the latter be given several rights in respect to his data that are processed -- the rights of information, access and objection.

A. The right of the person involved to be informed

The law confers on the person involved the right to be informed³⁵ -- a right that is not

absolute, the exceptions being specified in the principle.

1. The principle

When data are collected directly from the person involved, the law requires the processing manager to provide directly to that person, upon or prior to the collection and regardless of the means and medium employed, certain items of information (the identity of the processing manager (s) or, if such applies, its representative, or the purposes for which the data are intended)³⁶.

The processing manager must provide all further information that is necessary in view of the circumstances in which the data are collected, or the purposes of the processing, such as the data involved, the potential addressees, the existence of a right of access, the duration of retention of the data.

The law requires the processing manager to inform the person involved of the existence of a right of objection in the event that the processing is for purposes of canvassing. Hence, the fact that the person involved may consult the public registry does not exempt the processing manager from providing him with complete information.

If data are collected from a third person, the processing manager must provide directly to the person involved the aforesaid items of information upon the recording of said data or, if a transmission of data to a third party is envisaged, upon or prior to said transmission³⁷, to enable the person involved to exercise his rights of access or objection.

The information provided to the person involved must be clear and targeted; verbal transmission of information may be sufficient. It is to be noted that an item of information published in a brochure or any other document seen by the person involved, even if his signature does not appear, must be deemed to be sufficient.

³³ Within the meaning of article 18 (2) of the Act

³⁴ Article 19(3) of the Act

³⁵ Article 26 of the Act

³⁶ Article 26 (1) of the Act.

³⁷ Article 26 (2) of the Act

The obligation to inform the person involved is an absolute obligation of result³⁸.

In the event of dispute regarding the existence or extent of information provided to the person involved, the obligation of proof is imposed on the processing manager.

The positive obligation of information has a certain number of exceptions.

2. Exceptions to the right to be informed

The right to information of the person involved is restricted when the data processing does not directly infringe upon his rights and liberties³⁹.

The processing manager is exempt from informing the person involved if the latter has already been informed prior to the collection or, when applicable, upon the recording of data or upon or prior to the initial communication of data. Also, the exception is effective only if the person involved has actually been informed, not merely if it may be reasonably assumed that he has been informed.

If data have voluntarily or spontaneously been provided by the person involved, the right to be informed is irrelevant.

But, if this voluntary and spontaneous transmission comes from a third person, the person involved must in any event be informed.⁴⁰

The right to be informed is not applicable when it is impossible to inform the person involved, or if the conveying of information requires disproportionate efforts, or if the recording or transmission of data are specified by law.

Therefore, the person involved has the right to be informed in cases that are specified by law; but, during the processing of his data, he may have access thereto and object to the use

thereof.

B. The rights of access and objection of the person involved

In addition to the right to be informed, the person involved is given the right of access to his own data and to object to certain uses thereof.

1. The right of access

The person involved or his beneficiaries who can prove their legitimate interest, may obtain without expense and within a reasonable time:

- Access to his own data;
- Confirmation that his data are or are not processed, as well as information regarding at least the purposes of the processing, the categories of data processed and the addressees or categories thereof to which the data are transmitted;
- Knowledge of the logic behind all automated processing of data regarding him⁴¹.

The right of access is subject to the condition that the person involved or his beneficiaries prove their identity.

If the person who exercises his right of access has « serious reasons for asserting that the data transmitted to him are not in conformity with the data processed », it may inform the National Commission, which proceeds to the necessary verifications⁴².

The processing manager must rectify, delete or seal the data that have not been processed in conformity with the law.

The National Commission may sanction the processing manager if it fails to do so. The processing manager must notify the addressees to which the data have been transmitted, of the rectification, deletion or

³⁸ Parliamentary document 4735-13, page 24

³⁹ Article 27 and those that follow of the Act.

⁴⁰ Article 26 of the Act.

⁴¹ Article 28 of the Act.

⁴² Article 28 (6) of the Act

sealing of data⁴³, unless said notification cannot be effectuated for material or technical reasons.

The exceptions to the right of access are identical to those for the right to be informed.

The right of access is also limited:

- in respect to data that are processed solely for scientific research,
- data retained for a duration that does not exceed the time that is necessary only for the establishment of statistics,
- when there is obviously no risk of infringement upon the privacy of the person involved,
- when the data cannot be used for imposing a measure or making a decision relating to the specific persons⁴⁴.

The processing manager must always indicate to the requesting party the reasons for limitation of the right of access. If it only defers the exercise of this right, the processing manager must specify the date on which the right of access may again be exercised⁴⁵.

After being informed of the refusal to give access, the National Commission may exercise its right of investigation, and may order the rectification, deletion or sealing of data that has not been processed in conformity with the law. The Commission may advise the person involved of the result of its investigations, « without, however, jeopardizing the purposes of the particular processing.»⁴⁶

2. The right of objection

The person involved may object to certain uses of his data.

The right of objection involves specific data or a processing for prospecting purposes.

The person involved may object to the processing of his data, unless such processing is enabled by a legal provision⁴⁷. The objection must be for preponderant and legitimate reasons related to the particular situation of the person involved. If the objection is deemed to be for good cause by the processing manager to which the objection is addressed, or by the National Commission if it had to intervene, the processing may continue, but cannot be effectuated on disputed data. The person involved, who is duly informed of the prospecting purpose of the processing and of the existence of his right of objection, may gratuitously object to the processing as such. The law specifies any form of prospecting, even for non-commercial purposes⁴⁸.

The present legislation regarding the protection of persons in respect to personal data presents a few difficulties that were raised by the National Commission. In its annual business reports, the national legislature took note thereof, and a Bill was submitted to the Chamber of Deputies on March 16, 2006.

III. Bill n°5554 for amendment of the Act of August 2, 2002

The purpose of this bill is, first, a simplification of the required formalities, which translates into an easing of the prior authorization procedure and an essential simplification of the procedure for notification of processing, without putting at issue the protection of the person involved; and, second, to clarify certain provisions of the law for a more accurate and complete adaptation of directive 95/46/EC of the European Parliament and the Council of October 24, 1995 related to natural persons with regard to personal data and free circulation of data.

⁴³ Article 28 (7) of the Act

⁴⁴ Article 29 (2) of the Act

⁴⁵ Article 29 (3) of the Act

⁴⁶ Article 29 (4) of the Act

⁴⁷ Article 30 of the Act

⁴⁸ Parliamentary document 4735-13, page 27.

A. Easing of the prior authorization procedure

Easing of the prior authorization procedure results essentially in a reduction of the processing categories that are subject to prior authorization. This simplification was desired by the National Commission, which, in its activity report for 2003, expressed its dissatisfaction with being materially incapable of dealing with the authorization applications within a reasonable time.

One of the main objectives of the bill is exemption of the processing of the most ordinary data, which is unlikely to infringe upon the privacy of individuals, from the administrative formality. The bill's purpose is to make the authorizations delivered by the National Commission more efficient while enabling it to focus its resources on matters that are deemed to be a priority.

For simplification of the notification procedure, an expansion of the list of cases of exemption from the obligation of notification, and elimination of the simplified notification by virtue of its obsolescence in view of the proposed exemptions, are essential.

These simplifications will not infringe upon the privacy of individuals since the legislature specifies that the basic rules applicable to personal data processing will remain unchanged, particularly compliance with the principles of legitimacy, legality and purpose of the processing; the person involved will retain his rights of information, access to his data, and objection.

B. Clarification of certain provisions of law

The clarification of certain legal provisions will result in the exclusion of « legal entities » from the scope of application of the law; this

exclusion is explained by a more accurate adaptation of directive 95/46/EC (article 1 of the directive is directed only at natural persons) and serves the goal of clarity and simplification of the law. But this particular clarification does not have unanimous support; in its opinion rendered January 30, 2007 regarding Bill n° 5554/04, the State Council, to the contrary, considered it to apply the legislative provisions to legal entities. Indeed, the State Council stated « that the protection of natural persons through data regarding legal entities is frequent »; hence, if the legislature intended to exclude legal entities from the purview of the law, it would be a source of legal insecurity⁴⁹.

This clarification also results not only in a simplification of the legislative provisions in such a way as to make them clearer, but also in more precise definitions of the technical terms⁵⁰.

The interconnection procedure would also be simplified, and would result in a lifting of the restriction on the scenarios of interconnection subject to authorization; the interconnection, regardless of its purpose, would become possible on the condition that it is authorized, case by case, by the National Commission or that is subject to a legal or regulatory provision..

The legislature also intends to enlarge the circle of persons that can be designated as the person in charge of data protection. A relaxing of the procedure applicable to the person in charge of data protection will, in particular, make possible the appointment of an employee of the processing manager as the person in charge of data protection, by guaranteeing to him an adequate protection in the exercise of his functions. The legislature and the National Commission consider that a relaxing of the system will render this

Bulletin

⁴⁹ Opinion of the State Council of January 30, 2007 on Bill n° 5554 for amendment of the Act of August 2, 2002

⁵⁰ For example, the definition of the term « surveillance » is more precise than that which appears in the Act of 2002 ; surveillance would designate « any activity which, conducted by means of a technical instrument, consists of occasional observation, collection or recording of personal data, relating to behaviour, movements, communications or use of electronic or computerized devices. » whereas article 2(q) of the Act of August 2, 2002 designates the term « surveillance » as being « any activity using technical means for the purposes of detecting, observing, copying or recording movements, images, words, written documents, or the state of a fixed or mobile object or person ».

procedure more attractive.

Finally, the Bill also intends to enlarge the scope of application of the Act of 2002 by subjecting to the Personal Data Protection Act totally or partially automated processing and non-automated processing of data that are or will be contained in a file; any form of capturing, processing and dissemination of sounds and images that enables the identification of natural persons; processing of data regarding public safety, defence, pursuit and prosecution of criminal offences or the security of the State, even if related to a substantial economic or financial interest of the State, without prejudice to the specific provisions of national or international law governing these areas⁵¹.

The law provides for more or less severe sanctions in the event of violations of legal provisions by the processing manager. The processing manager is legally responsible for failure to comply with the provisions related to personal data protection, even if such failure is due to its subcontractor's wrongful act or omission.

The most severe sanction is imprisonment from eight days to a year and/or a penalty of 251 to 125,000 euros. The court dealing with the case may order the cessation of the disputed processing on pain of a penalty whose maximum amount is determined by said court. The absence of prior notification of data processing to the National Commission is punishable by a penalty of 251 to 125,000 euros.

In addition to these criminal sanctions, breaches of the law may be sanctioned by the National Commission, which has the power to impose suppressive measures⁵², such as sealing, deleting or destroying data, or prohibiting the processing.

Since practical experience has revealed loopholes in the existing legislation, modification of the law is imperative.

However, the legislation regarding data

Bulletin

protection must be taken seriously; and, as the institutions are not in conformity with the legal provisions, they must very rapidly set up secure and practical mechanisms of data protection or straighten out their situation without awaiting any possible changes in the law.

Karine VILRET-HUOT et Rabah LARBI
VILRET-AVOCATS

⁵¹ Article 3 of bill n° 5554 for amendment of the Act of August 2, 2002.

⁵² Article 32 and 33 of the Act.

Vie associative/Association activities

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

Groupe de travail 27

Formations IFBL

Coordinateur Jean-Noël LEQUEUE
Téléphone (+352) 62 11 94 941
jean-noel.lequeue@skynet.be

Groupe de travail 28

MiFID

Coordinateur Evelyn MCHALE
Téléphone (+352) 48 88 96 21
evelyn.mchale@hsbcib.com

Groupe de travail 29

Abus de marché

Coordinateur Cyril MATTHIEU
Téléphone (+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 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

Working group 27

Training IFBL

Coordinator Jean-Noël LEQUEUE
Telephone (+352) 62 11 94 941
jean-noel.lequeue@skynet.be

Working group 28

MiFID

Coordinator Evelyn MCHALE
Telephone (+352) 48 88 96 21
evelyn.mchale@hsbcib.com

Working group 29

Market abuse

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

Working group 30

Domiciliary agents

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

B. SECTEUR BANCAIRE:

Groupe de travail 10

Contrôles de compliance

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

B. BANKING SECTOR:

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) 62 11 94 941
jean-noel.lequeue@skynet.be

MEMBRES ET VIE ASSOCIATIVE:**Nombre de membres (au 01/03/2007):**

Banques	139
Fonds	82
Fonds / Banques	35
Assurances	41
Consultants / Réviseurs	25
Admin. et domiciliation de sociétés	14
Avocats	6
PSF	15
Gestion de fortune	3
Autres	11
Effectif total:	371

Membres effectifs	305
Membres d'honneur	66
Effectif total:	371

MEMBERS AND ASSOCIATION ACTIVITIES:**Number of members (as per 01/03/2007):**

Banking sector	139
Funds sector	82
Funds / Banking sector	35
Insurance sector	41
Consultants / Auditors	25
Admin. and company domiciliation	14
Law firms	6
SFP	15
Asset management	3
Other	11
Total number:	371

Active members	305
Honorary members	66
Total number:	371

Réunions et activités:

Mensuellement	Réunions du conseil d'administration
29/03/07	Assemblée Générale annuelle – Hôtel Novotel
16/05/07	Conférence annuelle (MiFID)
1 / 2 x par an	Réunions plénières
2 / 3 x par an	Rencontres informelles autour d'un thème

Meetings and activities:

Monthly	Board meetings
29/03/07	Annual General Meeting – Hotel Novotel
16/05/07	Annual conference (MiFID)
1 / 2 x per year	Plenary assemblies
2 / 3 x per year	Informal meetings on a subject



Association Luxembourgeoise
des Compliance Officers
du Secteur Financier

Secrétariat de l'ALCO:

Laurence THILMANY-INCOURT / Johanny LICK
Téléphone (+352) 47 67 26 44
Fax (+352) 47 67 36 12
secretariat@alco.lu
johanny.lick@ca-luxembourg.com
Adresse B.P. 1104
L-1011 Luxembourg

Secrétariat du bulletin:

Coralie CZERWINSKI
Téléphone (+352) 26 44 14 13
Fax (+352) 26 44 15 14
cczerwinski@vilret-avocats.com

Comité de rédaction / Drafting committee:

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

Visitez notre site / Visit our website:

www.alco.lu