COMPLIANCE

DECEMBER 2012

NEWSLETTER

ISSUE 7

Forum Compliance be

IN THIS ISSUE:

SPECIAL POINTS OF INTEREST:

- More than 3.500 documents in the on-line STORI database of the FSMA
- Circular of the NBB on the issue of covered bonds
- Fine of £10.5 million in the UK for misselling insurance products
- Internet crime schemes: some recommendations

Dear Colleagues,

Dear Members,

In this last and shorter issue of the year, you will a.o. note that the EU Commission plans to take some measures wrt on-line gambling and that data protection remains a concern especially in case of outsourcing. More specifically in the context of cloud computing, the UK ICO has produced guidelines to businesses to be compliant and has also published guidance on deleting and archiving electronically stored data.

Some guidance are also provided regarding the FATCA timelines for due diligence knowing that most EU countries will sign an agreement with the IRS so that reporting and withholding duties will most certainly be more governed by domestic approaches.

I also draw your attention on the last article as EBA has now issued guidelines on the suitability of Management and key function holders including internal control functions. I refer here as well to the EBA Guidelines on Internal Governance, both having an impact on the Compliance function.

Above all, I would like to provide you here with a high level summary of the brillant presentation on the ESMA guidelines on the Compliance function and on suitability requirements made by Mr. Guillaume Berard in his personal name (and not on behalf of the FSMA) at the last Forum information session on November 28th. This is especially addressed to those of you who were not able to attend.

Zoals iedereen weet, zal de Belgische Circulaire inzake de Compliance functie door onze toezichthouders, de FSMA en de Nationale Bank, aangepast worden in principe voor het einde van het jaar. De verwachte Circulaire gaat verder dan de Compliance bevoegdheden rond MiFID en is gebaseerd op verschillende bronnen, onder andere de bestaande regelgeving, het Basel document, de ontwikkelingen in verschillende landen en zeker vast de ESMA guidelines, ten minste voor wat MiFID betreft.

Le risk assessment, les rôles de conseil et de monitoring, la proportionnalité, la risk based approach, le training, le rôle dans les Comités de nouveaux produits, la collaboration avec les fonctions proches et le reporting d'exception particulièrement détaillé quant a son contenu sont consacrés dans les récentes orientations de l'ESMA. Tout cela est peut-être déjà connu mais très largement précisé aujourd'hui. Les orientations de l'ESMA soulèvent en sus d'autres questions qui ont été abordées. Ainsi, l'identification du risque de Compliance relève bien de la fonction Compliance qui pourra se faire assister par le business qui connaît les spécificités des différents métiers.

(continued on next page)

ESMA gaat redelijk ver inzake de suitability vereisten, een van de belangrijkste aspecten van MIFID inzake beleggersbescherming sinds 2007 , zonder de ontwikkelingen maar de toekomst toe in rekening te nemen, gaat ESMA tamelijk ver. Elk advies, zelfs een advies om een financieel instrument te bewaren of te verkopen moet geschikt zijn. Financiële instellingen moeten zeker zijn dat de cliënt het risico begrijpt. Suitability is de verantwoordelijkheid van de financiële instelling waarbij ze zich niet mag baseren op het self assessment van de cliënt. De financiële instrumenten moeten goed begrepen worden door de instellingen die moeten evalueren of ze aan de behoeften en karakteristieken van de cliënt beantwoorden. Kennis en ervaring van de medewerkers van de distributienetwerken moeten bijgevolg toenemen. Een verhoogd suitability proces is noodzakelijk voor meer risicovolle of complexe producten.

Gegevens over kennis en ervaring van de cliënten mogen minder gedetailleerd zijn voor portfolio management. Inzake portfolio management moeten de cliënten het risico van de portfolio in het algemeen en elk financieel instrument in de portfolio in het bijzonder begrijpen.

Zelfs voor professionele cliënten is informatie vereist indien ze een risico willen hedgen.

Un débat a eu lieu entre autres en ce qui concerne les portefeuilles. Bien que l'approche transactionnelle soit retenue, il ne semble pas devoir être exclu qu'un client au profil défensif puisse se voir conseiller un instrument financier dynamique pour autant que le portefeuille dans sa globalité garde son caractère originel, ne soit pas déséquilibre et que l'on puisse raisonnablement penser et idéalement établir que le client a parfaitement compris les risques inhérents a la transaction spécifique. Par contre, un instrument très dynamique dans un portefeuille très défensif paraît a priori moins aisément justifiable. De même, des changements de profils massifs moins défensifs avant l'émission d'un instrument plus dynamique suscitera sans doute le questionnement. Le "produit du mois" ne sera peut-être pas toujours per se "suitable" pour tous les profils de risque. Une analyse au cas par cas semble dans les cas de figure précités être de mise...

Quelques précisions ou assouplissements sont évoqués pour les compte-joints et les personnes morales ou une scission est opérée entre la connaissance et l'expérience a récolter dans le chef de leur représentant et la situation financière ainsi que les objectifs d'investissement a apprécier en fonction des personnes représentées dont on obtiendra le consensus. En l'absence d'accord, la partie la plus faible sera prise en compte. On mentionnera encore les obligations de mise à jour des données et le record keeping.

Ces orientations de l'ESMA méritaient toute notre attention même si elles n'ont pas une force contraignante absolue puisque les régulateurs doivent en principe en tenir compte dans leurs contrôles. La FSMA procèdera de la sorte.

Again, one more year has nearly gone and we have not seen the time passing.

We hope you have enjoyed the Newsletter in the course of the last 12 months. On behalf of the Forum Board, I would like to wish you all a nice year end, a merry, peaceful and enjoyable Christmas time with your families, friends and relatives and a bit in advance a fruitful beginning of 2013.

With kind regards

Marie-France De Pover

Chairwoman

The control environment sets the tone of an organization, influencing the control consciousness of its people

Forum Compliance .be

EUROPEAN COMMISSION SETS OUT AN ACTION PLAN FOR ONLINE GAMBLING

Online gambling is one of the fastest growing service activities in the EU, with annual growth rates of almost 15% and an estimated €13 billion in annual revenues in 2015. It continues to develop alongside the fast-paced progress of online technology. However, there are also thousands of unregulated gambling websites, often from outside the EU, to which consumers are exposed and which carry significant risks such as fraud and money laundering.

Online gambling in the EU is characterised by diverse national rules. Notwithstanding their obligation to comply with EU rules, Member States may indeed restrict or limit the supply of all or certain types of online gambling services on the basis of public interest objectives that they seek to protect in relation to gambling. An increasing number of Member States are seeking to address the challenges they face and are reviewing their national regulations and practices. However, the prevailing regulatory, societal and technical issues in the EU cannot be tackled adequately by Member States individually. This is especially true given the cross-border dimension of online gambling.

Key elements

The Commission is not proposing EU-wide legislation on online gambling. It is proposing a comprehensive set of actions and common principles on protection.

While Member States are in principle free to set the objectives of their policies on online gambling, ensuring compliance of national law with the Treaty on the Functioning of the EU (TFEU) is a prerequisite of a successful EU policy on online gambling. The Commission will establish an expert group to facilitate exchanges of experience on regulation between Member States. This will help to develop a well-regulated, safer online gambling sector in the EU, which will help turn consumers away from unregulated sites.

The Commission is encouraging the development of better age-verification tools and online content filters. It is also pushing for more responsible advertising and increased parental awareness of the dangers associated with gambling.

In addition, there is a responsibility to protect those citizens and families who have already suffered from a gambling addiction (between 0.5-3% of the population) or other forms of gambling-related disorders by finding effective methods of treatment and prevention.

Another important objective is to prevent and deter fraud and money-laundering through online gambling. Due to the cross-border nature, individual Member States cannot effectively apply anti-fraud mechanisms. An approach that brings together the EU, Member States and industry is necessary to tackle the problem from all angles.

To combat it, the Commission will promote faster information exchange, whistle-blowing mechanisms, and overall cooperation at national and international level between stakeholders, operators, and regulators to preserve the integrity of sports, as well as better education and increased awareness of sportspeople.

In concrete terms, the Commission will adopt three Recommendations addressed to the Member States, namely on i) common protection of consumers, ii) responsible gambling advertising and iii) the prevention and fight against betting-related match-fixing.

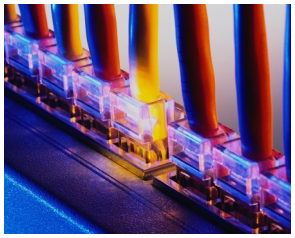
Other measures foresee, inter alia, support to the benchmarking and testing of parental control tools; the extension of the scope of the anti-money laundering directive; the promotion of international cooperation for the prevention of match-fixing.

Next steps

A first expert group meeting with the Member States is foreseen for December 2012, and in 2013, the Commission will organise a stakeholder conference.

In 2011, the annual revenues generated by the gambling service sector were estimated to be 84,9 billion EUR

IBM RECEIVED REQUEST FROM U.S. SECURITIES AND EXCHANGE COMMISSION OVER DEALINGS WITH IRAN



IBM recently received a request from the U.S. Securities and Exchange Commission to describe its interactions with Iran, following reports that ZTE Corp. resold some IBM products in the country.

As IBM's business partner, ZTE is required to comply fully with U.S. regulations, including economic sanctions and export laws.

"Iran is designated as a state sponsor of terrorism by the State Department and is subject to U.S. economic sanctions and export controls," the SEC said in a letter to IBM. "Please describe to us the nature, duration, and extent of your past, current, and anticipated contacts with Iran, whether through subsidiaries, distributors, resellers, or other direct or indirect arrangements."

The SEC also requested information about IBM's contacts with Syria, Sudan and Cuba.

"IBM takes its obligations regarding export compliance with great seriousness," Doug Shelton, a spokesman for Armonk, New York-based IBM, said in an e-mail. "Our agreements with our business partners specifically prohibit them from the transfer of IBM products to Iran. If any of IBM's business partners are breaching our export compliance agreements, IBM will take appropriate actions."

U.S. lawmakers asked ZTE and another Chinese telecommunications company, Huawei Technologies Co., for details about their business dealings as part of an investigation into how their expansion may affect U.S. security. In the letter, they questioned whether ZTE sold "highly sophisticated surveillance technology" to the Iranian government.

The House Intelligence Committee began an investigation last year "to review the threat posed to U.S. national security interests by telecommunications companies with potential ties to the Chinese government," according to a committee statement.

Banks face greater scrutiny from the authorities about how they conduct their business

BRITAIN EXAMINES 4.000 HSBC ACCOUNTS IN A TAX HAVEN

Her Majesty's Revenue and Customs, Britain's tax authority, is investigating more than 4.000 accounts in Jersey that belong to British clients after receiving details from a whistle-blower. The list includes a drug dealer and a man convicted of possessing more than 300 weapons at his home in the south of England.

"We have received the data and we are studying it," a tax authority spokesman wrote in an e-mailed statement. "Clamping down on those who try to cheat the system through evading taxes and over-claiming benefits is a top priority for us, and we value the information we receive from the public and business community."

HSBC said in a statement that the bank was "investigating the reports of an alleged loss of certain client data in Jersey as a matter of urgency."

HSBC said it had not yet been informed of any investigation but would fully cooperate with the authorities. "HSBC remains fully committed to adoption of the highest global standards, including the procedures for the acceptance of clients," it said.

HSBC clients are also on another list that was recently in the spotlight. Kostas Vaxevanis, editor of the investigative magazine Hot Doc was acquitted in November 2012 on charges of breaching privacy laws when he published a list of more than 2.000 Greeks believed to hold accounts at a Geneva branch of HSBC. The list was given to the Greek authorities two years ago by Christine Lagarde, then the French finance minister and now managing director of the International Monetary Fund, to help the government in Athens investigate evasion.

Forum Compliance .be

COUNCIL FINED £250,000 AFTER EMPLOYEE RECORDS FOUND IN SUPERMARKET CAR PARK RECYCLE BIN

A Council whose former employees' pension records were found in an over-filled paper recycle bank in a supermarket car park have been fined £250,000 for the data breach.

Scottish Borders Council employed an outside company to digitise the records, but failed to seek appropriate guarantees on how the personal data would be kept secure.

That prompted the UK Information Commissioner to use his powers under the Data Protection Act to impose a Civil Monetary Penalty of £250,000 on the Council.

The Data Protection Act requires that, if you decide to use another organisation to process personal data for you, you remain legally responsible for the security of the data and for protecting the rights of the individuals whose data is being processed.

But Scottish Borders Council put no contract in place with the third party processor, sought no guarantees on the technical and organisational security protecting the records and did not make sufficient attempts to monitor how the data was being handled.

It is believed more than 600 files were deposited at the recycle bins, containing confidential information and, in a significant number of cases, salary and bank account details. The files were spotted by a member of the public who called police, prompting the recovery of 676 files. A further 172 files deposited on the same day but at a different paper recycling bank are thought to have been destroyed in the recycling process.

For practical advice on this topic, read the ICO's guidance on outsourcing: A guide for small and medium-sized businesses'

Businesses can follow these top tips to make sure they keep personal data safe when outsourcing:

- Always select a reputable organisation to work with;
- Make sure the organisation has appropriate data security measures in place, including how it disposes of data;
- And make sure the organisation has appropriate security checks on staff too;
- Put a clear, enforceable contract in place;
- Make sure that contract requires the contractor to report any security breaches or other problems to you, and have procedures in place on how you will act if problems are reported.

A classic case of an organisation taking its eye off the ball when it came to outsourcing

SEC RECEIVES MORE THAN 3.000 WHISTLEBLOWER TIPS IN 2012

Over the past year, the Securities and Exchange Commission received more than 3,000 whistleblower tips from all 50 states and from 49 countries, according to the agency's 2012 Annual Report.

The report, which is required by the Dodd Frank Wall Street Reform and Consumer Protection Act, summarizes the activities of the SEC's Office of the Whistleblower.

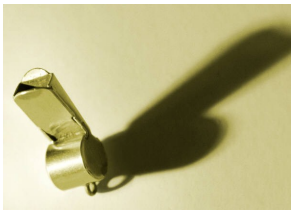
Among other things, the report notes:

The SEC made its first award under the new program to a whistleblower who helped the SEC stop an ongoing multi-million dollar fraud.

The whistleblower received an award of 30 percent of the amount collected in the SEC's enforcement action, which is the maximum percentage payout allowed by law.

The most common complaints related to corporate disclosures and financials (18.2 percent), offering fraud (15.5 percent), and manipulation (15.2 percent).

There were 143 enforcement judgments and orders issued during fiscal year 2012 that potentially qualify as eligible for a whistleblower award.



BP TO PAY 525 MILLION USD PENALTY FOR SECURITIES FRAUD DURING DEEPWATER HORIZON OIL SPILL

On November 15, 2012 the Securities and Exchange Commission charged BP p.l.c. with misleading investors while its Deepwater Horizon oil rig was gushing into the Gulf of Mexico by significantly understating the flow rate in multiple reports filed with the SEC.

The SEC alleges that the global oil and gas company headquartered in London made fraudulent public statements indicating a flow rate estimate of 5,000 barrels of oil per day. BP reported this figure despite its own internal data indicating that potential flow rates could be as high as 146,000 barrels of oil per day. BP executives also made numerous public statements after the filings were made in which they stood behind the flow rate estimate of 5,000 barrels of oil per day even though they had internal data indicating otherwise. In fact, they criticized other much higher estimates by third parties as scaremongering.

Months later, a government task force determined the flow rate estimate was actually more than 10 times higher at 52,700 to 62,200 barrels of oil per day, yet BP never corrected or updated the misrepresentations and omissions it made in SEC filings for investors.

BP agreed to settle the SEC's charges by paying the third-largest penalty in agency history at $525 million. The SEC plans to establish a Fair Fund with the BP penalty to provide harmed investors with compensation for losses they sustained in the fraud.

CLOUD ON THE HORIZON FOR DATA-HANDLING OUTSOURCING

The UK Information Commissioner's Office (ICO) has published guidelines to businesses today to underline that companies remain responsible for how personal data is looked after, even if they pass it to cloud network providers.

More and more businesses are looking to use cloud computing, with the economies of scale they offer giving access to a range of computer technologies and expertise that would be difficult to afford in-house.

But data protection regulator ICO is concerned that many businesses do not realise they remain responsible for how the data is looked after, even after passing it to the cloud network provider.

That's prompted the ICO to produce a guide to cloud computing, to help businesses comply with the law. The guide gives tips including:

- Seek assurances on how your data will be kept safe. How secure is the cloud network, and what systems are in place to stop someone hacking in or disrupting your access to the data?
- Think about the physical security of the cloud provider. Your data will be stored on a server in a data centre, which needs to have sufficient security in place.
- Have a written contract in place with the cloud provider. This is a legal requirement, and means the cloud provider will not be able to change the terms of the service without your agreement.
- Put a policy in place to make clear the expectations you have of the cloud provider. This is key where services are funded through adverts targeted at your customers: if they're using personal data and you haven't asked your customers' permission, you're breaking data protection law.
- Don't forget that transferring data internationally brings a number of obligations – that includes using cloud storage based abroad.

The BNB published its own expectations regarding cloud computing in a communication dated October 9, 2012.

Regulation on outsourcing data is very clear.
As a business, you are responsible for keeping your data safe

Forum Compliance .be

DELETING PERSONAL DATA OR PUTTING PERSONAL DATA 'BEYOND USE'?

The UK Information Commissioner's office has published guidance on deleting and archiving electronically stored personal data.

This guidance explains what organisations need to do to when they archive or delete personal data.

In the days of paper records it was relatively easy to say whether information had been deleted or not, for example through incineration. The situation can be less certain with electronic storage, where information that has been 'deleted' may still exist, in some form or another, within an organisation's systems.

In some cases an organisation may be required by law to delete an individual's personal data. This guidance is intended to counteract the problem of organisations informing people that their personal data has been deleted when, in fact, it is merely archived and could be re-instated.

There is a significant difference between deleting information irretrievably, archiving it in a structured, retrievable manner or retaining it as random data in an un-emptied electronic wastebasket.

Information that is archived, for example, is subject to the same data protection rules as 'live' information, although information that is in effect inert is far less likely to have any unfair or detrimental effect on an individual than live information.

However, the ICO will adopt a realistic approach in terms of recognising that deleting information from a system is not always a straightforward matter and that it is possible to put information 'beyond use'.

The ICO will be satisfied that information has been 'put beyond use', if not actually deleted, provided that the data controller holding it:

- is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
- does not give any other organisation access to the personal data;
- surrounds the personal data with appropriate technical and organisational security; and
- commits to permanent deletion of the information if, or when, this becomes possible.

It is, however, important to note that where data put beyond use is still held it might need to be provided in response to a court order. Therefore data controllers should work towards technical solutions to prevent deletion problems recurring in the future.

In the days of paper records it was relatively easy to say whether information had been deleted

INVESTMENT BANKER GUILTY OF INSIDER DEALING

Thomas Ammann was an investment banker working at Mizuho International plc (MIP). In late 2008 and 2009 MIP was advising Canon, the multi-national technology company, on its acquisition of Océ, a medium sized Dutch company making photocopiers, scanners, related software and accessories. Ammann was one of the very small team at MIP working on the acquisition and had access to inside price sensitive information.

Ammann passed information to Weckwerth and Mang and encouraged them to trade in the shares of Océ prior to the acquisition being announced. Both considered Ammann to be their boyfriend and had no idea of the existence of the other. Following the announcement of the acquisition of Océ both Weckwerth and Mang sold their shares for a substantial profit. Weckwerth made Eur 1 million and Mang £29,000 and both shared half their profits with Ammann.

In a prosecution brought by the Financial Services Authority (FSA) Thomas Ammann has pleaded guilty. Ammann will be sentenced on a date to be confirmed.

FATCA TIMELINES FOR DUE DILIGENCE ARE POSTPONED ANNOUNCEMENT 2012-42

The announcement 2012-42 outlines certain timelines for withholding agents and foreign financial institutions (FFIs) to complete due diligence and other requirements and provides certain additional guidance concerning gross proceeds withholding and the status of certain instruments as grandfathered obligations.

1. Timeline for Implementing New Account Opening Procedures

Withholding agents, including participating FFIs and registered-deemed compliant FFIs, generally will be required to implement new account opening procedures by January 1, 2014.

2. Transition Rules for Completing Due Diligence on Preexisting Obligations

2.1 Withholding and Documentation for Prima Facie FFIs

With respect to preexisting obligations, the final regulations will provide that withholding agents, other than participating FFIs, will be required to document payees that are prima facie FFIs by June 30, 2014.

With respect to a preexisting obligation, the final regulations will provide that a participating FFI will be required to perform the requisite identification procedures and obtain the appropriate documentation to determine whether a prima facie FFI payee is itself a participating FFI, deemed-compliant FFI, or nonparticipating FFI within six months after the effective date of its FFI agreement.

2.2 Withholding and Documentation for other Preexisting Entity Obligations.

With respect to preexisting obligations, the final regulations will provide that withholding agents, other than participating FFIs, will be required to document payees that are entities other than prima facie FFIs by December 31, 2015.

Participating FFIs will be required to perform the requisite identification procedures and obtain the appropriate documentation to determine whether an entity, other than a prima facie FFI, is itself a participating FFI by the later of December 31, 2015, or the date that is two years after the effective date of its FFI agreement.

2.3 Withholding and Documentation Requirements of Participating FFIs for Preexisting Individual Accounts.

A participating FFI must perform the requisite identification procedures and obtain the appropriate documentation to identify preexisting individual accounts that are high-value accounts by the later of December 31, 2014, or the date that is one year after the effective date of the FFI's FFI agreement..

For preexisting individual accounts (other than high-value accounts) the due date is December 31, 2015, or the date that is two years after the effective date of the FFI's FFI agreement.

Summary of Timing	New Individual and Entity Accounts (Implementation of new account opening procedures)	Preexisting Accounts of Prima Facie FFIs (Date by which due diligence must be completed for all accounts)	Preexisting Accounts of Entities other than Prima Facie FFIs	Preexisting High Value Accounts of Individuals	Preexisting Accounts of Individuals other than High Value Accounts
Withholding Agents other than Participating FFIs and Deemed-Compliant FFIs	By January 1, 2014	By June 30, 2014	By December 31, 2015	N/A	N/A
Withholding Agents that are Participating FFIs	By later of January 1, 2014, or effective date of FFI agreement	By the later of June 30, 2014, or 6 months after the effective date of the FFI Agreement	By the later of December 31, 2015, or two years after the effective date of the FFI Agreement	By the later of December 31, 2014, or one year after the effective date of the FFI Agreement	By the later of December 31, 2015, or two years after the effective date of the FFI Agreement
Withholding Agents that are Registered Deemed-Compliant FFIs	By later of January 1, 2014, or date of Registration	N/A	N/A	N/A	N/A

FSA FINES SAVOY INVESTMENT MANAGEMENT LIMITED £412,000 FOR WEALTH MANAGEMENT FAILINGS

The Financial Services Authority (FSA) has fined Savoy Investment Management Limited (Savoy) £412,000 for failing to take reasonable care to ensure the suitability of the investment portfolios of its wealth management clients

Savoy allowed its investment managers a high degree of discretion to advise its wealth management clients on their investment portfolios. It had limited front office controls and its other processes failed to ensure the suitability of its advice and portfolio management. This included failures to collect and record know your client information and failures in its compliance monitoring processes.

As a result of these failings, a review of a sample of files found that 23% showed a high risk of unsuitability. Files often lacked information on clients' personal and financial circumstances and contained out of date and inadequate client information. This meant there was a high risk that investment managers were making investment decisions that did not match clients' expectations and their attitude to risk.

EBA PUBLISHED ITS GUIDELINES ON THE ASSESSMENT OF THE SUITABILITY OF MEMBERS OF THE MANAGEMENT

The European Banking Authority (EBA) published on November 22, 2012 its guidelines on the assessment of the suitability of members of the management body and key function holders. These Guidelines set out the process, criteria and minimum requirements for assessing the suitability of those persons and are ultimately aimed at ensuring robust governance arrangements and appropriate oversight.

The Guidelines contain provisions to be followed by both credit institutions and competent authorities when assessing the suitability of all members of the management body and extend also to key function holders.

Moreover, as financial and mixed financial holding companies have significant influence on their credit institutions, they are also included in the scope of the Guidelines.

The Guidelines set out the criteria for the assessment of experience and reputation and documentation requirements for credit institutions.

They also contain a notification requirement and provide that in cases where a member of the management body is not suitable, the credit institution and, if necessary, the competent authority shall take appropriate action.

A credit institution shall only be authorised when there are at least two suitable persons who effectively direct the business

Pour nous transmettre vos suggestions d'articles ou pour vous désabonner de la Newsletter une seule adresse : info@forumcompliance.be

Maak ons uw suggesties over artikelen over of laat u schrappen van de distributielijst van deze Newsletter op volgend adres : info@forumcompliance.be