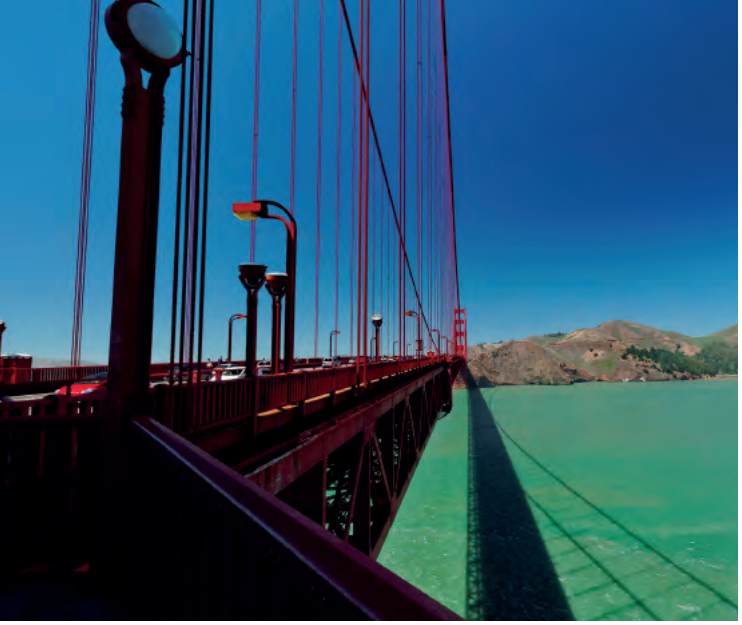


FBT
AVOCATS

FBT NewsLex

N° 9 - MAY 2015

CONTACT

Marco Villa

mvilla@fbt.ch
T. +41 (0)22 849 60 40
www.fbt.ch

PERIODIC LEGAL AND TAX INFORMATION REVIEW

TABLE OF CONTENTS

OUTSOURCING AND PROCESSING OF ELECTRONIC CLIENT DATA

The reduced profitability of banking institutions, which results from a legal and regulatory framework and an international environment that is growing ever stricter, increases the pressure related to operating costs. Banks are constantly looking for solutions allowing to control these costs. The outsourcing of some activities is an option often contemplated. However, delegation to third parties presents a risk for the delegating institution. FINMA has set some principles regarding outsourcing and will probably implement new rules relating to the outsourcing of the processing of electronic client data.

Due to an increase in transparency, in particular in terms of international taxation, and the progressive dismantlement of banking secrecy rules, banking institutions have progressively lost their competitive advantage (almost protectionist) stemming from banking secrecy, with a subsequent erosion of their margins. In this context, the outsourcing of certain activities to third parties may represent interesting costs savings. It is particularly the case of the processing of electronic data, where the costs related to the creation, maintenance and regular updating of an efficient computer infrastructure are often huge. Even if the computer tool is absolutely necessary for the performance of the bank's tasks (account monitoring, accounting or reporting), it is highly qualified staff consuming (IT specialists, chief systems, data administrator, etc.) It needs constant monitoring; it must function on a permanent basis and be adapted to the evolution of the technologic environment and to the clients' requests (e-banking, mobile services, etc.) and it must present all guarantees of security in terms of data protection.

FINMA'S CIRCULAR ON BANKING OUTSOURCING LAYS ITS PRINCIPLES

The outsourcing of banking activities is governed by FINMA's Circular 2008/7 "Capital adequacy requirements for operational risks within the banking sector", which lays the regulatory principles of the outsourcing of "essential" activities. An activity is deemed "essential" when it may affect the identification, mitigation and monitoring of different financial, but also legal, reputational and operational risks.

Circular 2008/7 sets the conditions to which outsourcing is subject. Hence, save for some exceptions, the relationships between the delegating company and the services provider to which a task is delegated must be governed by a written agreement. In particular, this agreement must establish the expected standards of performance and provide for the quantitative and qualitative evaluation of the performance. The delegatee must be carefully chosen, instructed and monitored; its skills must be established and precisely defined. Finally, the delegator and the delegatee must set the security requirements and draft the appropriate provisions.

Data, in particular client data (notably electronic data), must be protected by means of appropriate organisational and technical measures in order to avoid any unauthorised processing. The measures implemented must guarantee that data shall not be destructed accidentally or without authorisation, lost, affected by an error, falsified, stolen, copied, unlawfully used, modified, or made available to unauthorised third parties. Moreover, these measures must be periodically examined; the evolution of the technique, the environment and threats justifies that the protective measures undertaken be re-evaluated and, if need be, adapted thereto on a regular basis, or immediately after an incident.

Moreover, when client data are transferred abroad in the framework of an outsourcing operation, the delegating banking institution must ensure they will also be protected abroad in accordance with Swiss law.

FINMA'S CIRCULAR ON OPERATIONAL RISKS IMPOSES ORGANISATIONAL RULES ON THE PROCESSING OF ELECTRONIC CLIENT DATA

The requirements mentioned above are further developed in FINMA Circular 2008/21 on "requirements

for operational risks for financial institutions", completed by a new appendix on the "Processing of electronic client data" (Appendix 3), which entered into force on 1 January 2015.

Recent (and unpleasant) experiences of some banking institutions in Switzerland and abroad (theft of CDs containing client data, external hacking of banks databases, etc.) convinced the FINMA that the processing of electronic client data represents a major operational risk and may have serious economic but also reputational consequences for the bank. It is a fortiori the case when the processing of data is outsourced, which may imply a transfer of these data abroad.

Accordingly, in Appendix 3 of its Circular 2008/21, the FINMA sets out the principles governing the proper management of the risks related to the processing of electronic client data.

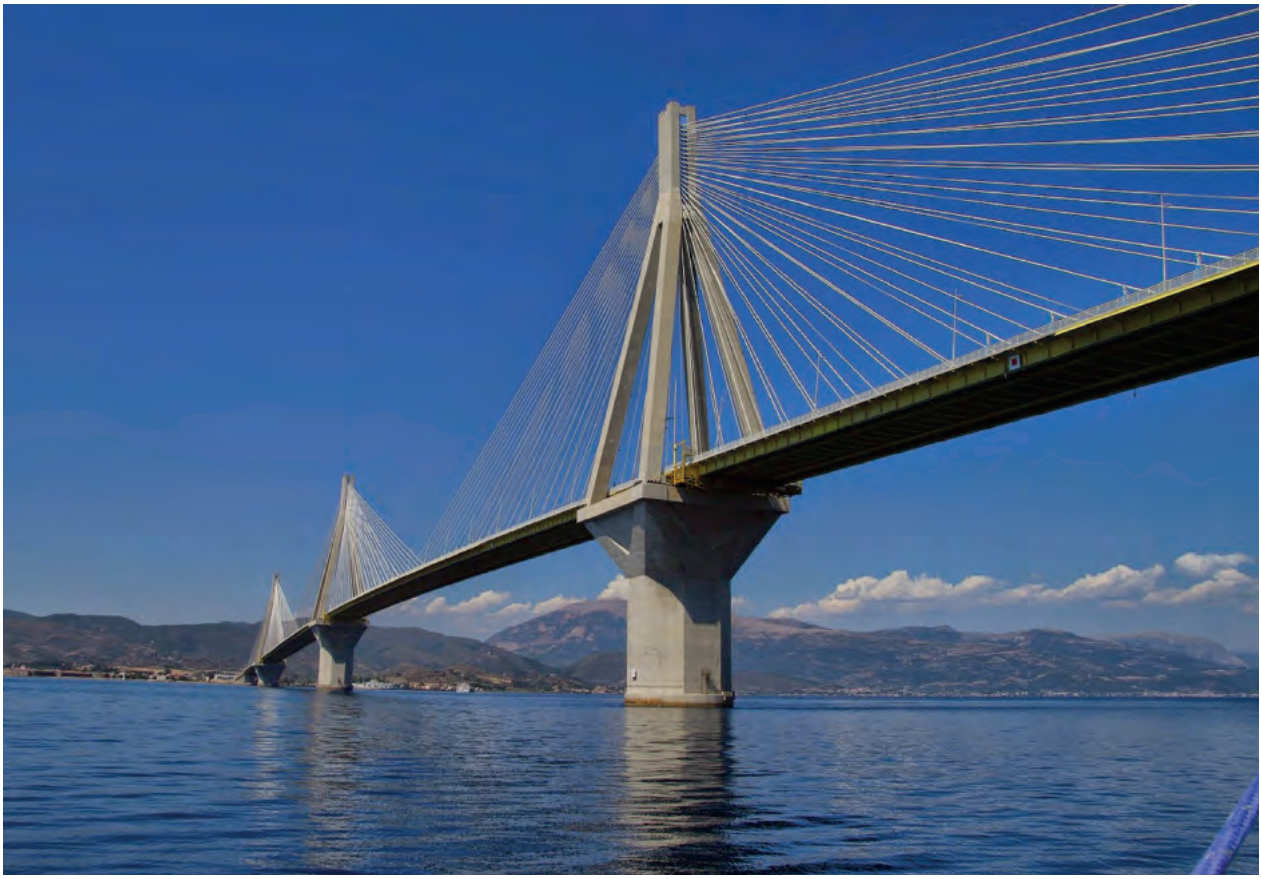
The FINMA now imposes on all banking institutions **the creation of an "independent unit"** reporting to the board of directors, whose mission consists in establishing, maintaining and monitoring a framework that secures the confidentiality of client data. This unit must be independent from other units in charge of the data processing. Moreover, banks must develop and document in writing a **framework concept relating to data confidentiality** by identifying the related risks and establishing a comprehensive list of the activities, processes and systems ensuring data confidentiality. This framework concept must take into account the categorization of the processed data according to their nature ("direct identification" data such as name, surname, etc., "indirect identification" data such as passport number, or "potentially indirect identification" data such as data resulting from the combination of date of birth and address, etc.) and provide for the implementation of protective measures (raw data, encryption, pseudonymisation, anonymisation) depending on the required confidentiality level and on the way data is processed.

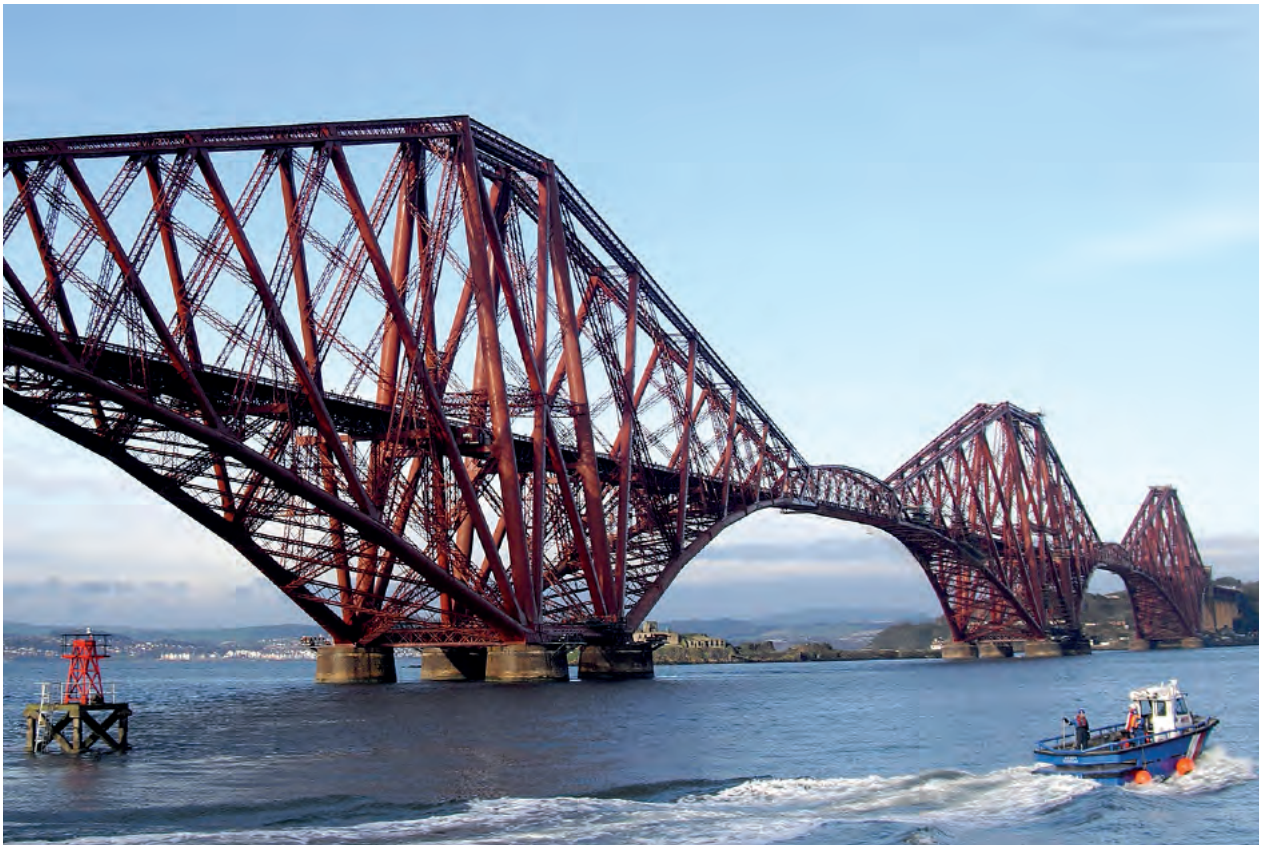
It also provides rules on **the security of the storage location and the access to data** (keeping of an inventory of applications and infrastructures used to store data, secured storage places, authorisations to access data and storage places on a "need-to-know" basis). These rules remind that the data storage outside of Switzerland or access to data from abroad imply increased risks that must be adequately mitigated and that the institution must provide for more

important security measures if need be. Infrastructure and technology used for the data storage and processing must notably allow to ensure data security not only at the data endpoint (personal computers, notebooks, mobile devices, etc.) but also during the transfer from the storage place (security of the network used, notably if data are split between several places) and of course at the storage place. Banking institutions must **follow the developments of IT** and regularly adapt their security measures to the market practices.

The human factor must also be taken into account: employees must be carefully selected and their level of accreditation regularly reviewed as regards access to data from a confidentiality point of view. Employees with access to mass data (for example IT specialists) must comply with stricter confidentiality measures.

Finally, in the event of outsourcing of activities and services related to the processing of client data, the capacity of the delegatee to ensure confidentiality is a decisive criterion in its choice. When outsourcing the provision of services related to mass client data, the delegator must establish evaluation criteria setting the expected standards for security and confidentiality. The contemplated services provider may only be selected if it complies with these criteria, being specified that this evaluation must be made prior to the signature of any new contract, even if the provider has been previously selected. The contract with the third party services provider must provide that it shall comply with the confidentiality and security standards established by the banking institution as they result from the framework concept which shall have been communicated to the services provider.





PERSPECTIVES

FINMA takes the issue of the security and confidentiality of electronic client data seriously, in particular when they are outsourced. With good reason. Modern technologies allow large-scale and rapid data processing; a failure in the security or a breach of confidentiality, in particular regarding mass data, may rapidly have serious consequences on the bank's operations. The risk is all the more important when data processing is outsourced. In a world where banks as well as their clients wish to be able to access data almost anywhere, notably through mobile devices, and when outsourcing appears to be an attractive or even necessary option, protection requirements – and the implementing costs resulting thereof – will continue to grow, triggering, as curiously as it may seem, an increased need to outsource.

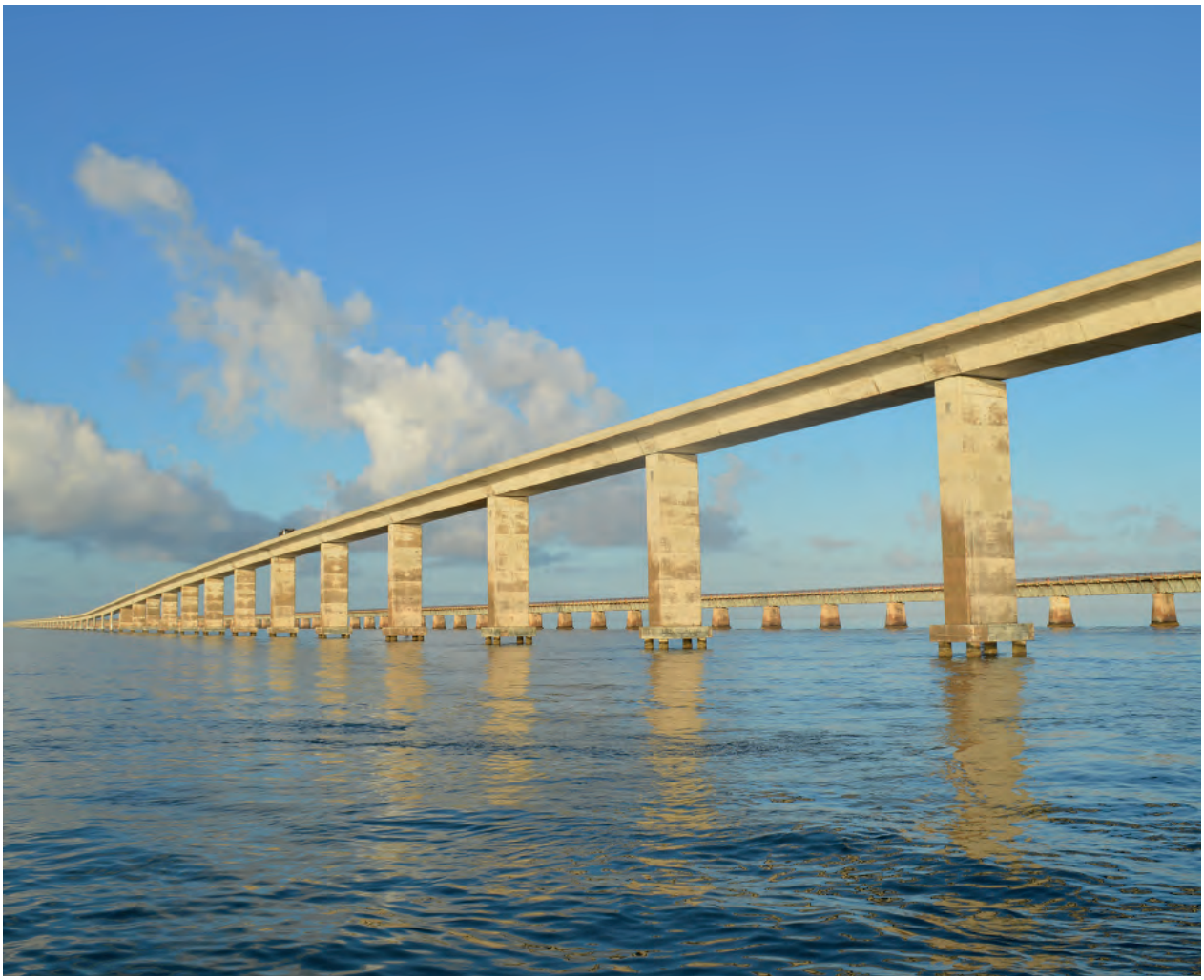
Contacts : Marco Villa and Frédérique Bensahel

DISTRIBUTION OF FOREIGN FUNDS TO QUALIFIED INVESTORS: FINAL STRETCH TO ADAPTING TO THE NEW SWISS REGULATORY REQUIREMENTS

The distribution in Switzerland of foreign collective investment schemes has experienced a significant turning point. While to date foreign funds reserved to qualified investors could be offered in Switzerland to all types of qualified investors with no regulatory constraints, the legislator has decided otherwise. The revision of the Federal Act on Collective Investment Schemes ("CISA") of 23 June 2006 introduced a new regime applicable to distribution. It imposes new regulatory requirements on foreign funds, that had to be met before 1 March 2015, failing which the distribution of the funds should be suspended.

Since the entry into force of the revised CISA on 1 March 2013, any marketing of collective investment schemes which is not aimed at super-qualified investors (notably banks, securities dealers, fund management companies) qualifies as a distribution activity subject to the law, with few exceptions. Thus, the marketing of foreign funds towards qualified (but not regulated) investors such as pension funds, high-net-worth individuals or independent asset managers (under certain conditions) is deemed a distribution activity subject to the law.

With this change of paradigm, the legislator introduced new requirements foreign funds reserved to qualified investors must imperatively meet to continue to be distributed in Switzerland. Accordingly, foreign funds must appoint a paying agent and a representative in Switzerland. Only a bank duly authorised in Switzerland may act as paying agent and make the payments requested by the investor. As for the representative, it must be a



Swiss entity duly authorised by the FINMA, which will act as a contact point in Switzerland. It shall represent the foreign fund vis-à-vis the FINMA and the investors and keep the fund documentation available to the latter.

The representative ensures that the distribution of the fund represented complies with the regulations and monitors the distributors. To this effect, it is a party to the distribution agreements between the foreign funds and the distributors. Finally, it ensures that the distributors comply with the rules of conduct imposed by the Swiss regulations and specified by the self-regulatory bodies.

PERSPECTIVES

Appointing a representative and a paying agent and concluding representation and distribution agreements are some of the steps necessary to pursue the distribution in Switzerland of foreign funds reserved to qualified investors after the expiry of the transitional period, i.e. 1 March 2015. On 26 March 2015, the Swiss Fund and Asset Management Association (SFAMA), with the consent of the FINMA, has extended the deadline to 31 August 2015 for the amendment of the foreign funds documents according to the new legal requirements and the SFAMA self-regulation. The intentional breach of the above mentioned duties is punishable by a term of imprisonment of up to three years. The breach of these duties by negligence is punishable by a fine up to CHF 250,000. Thus, it is imperative that any distributor of foreign funds reserved to qualified investors in Switzerland who would not have complied with these regulatory duties yet takes action with no further delay.

Contacts : Frédérique Bensahel,
Pierre-Olivier Etique
and Véronique Chatelain Gomez

NEW RULES ON THE TRADE ON DERIVATIVES: INSIGHTS ON THE DRAFT LAW ON THE FINANCIAL MARKETS INFRASTRUCTURE (FMIA)

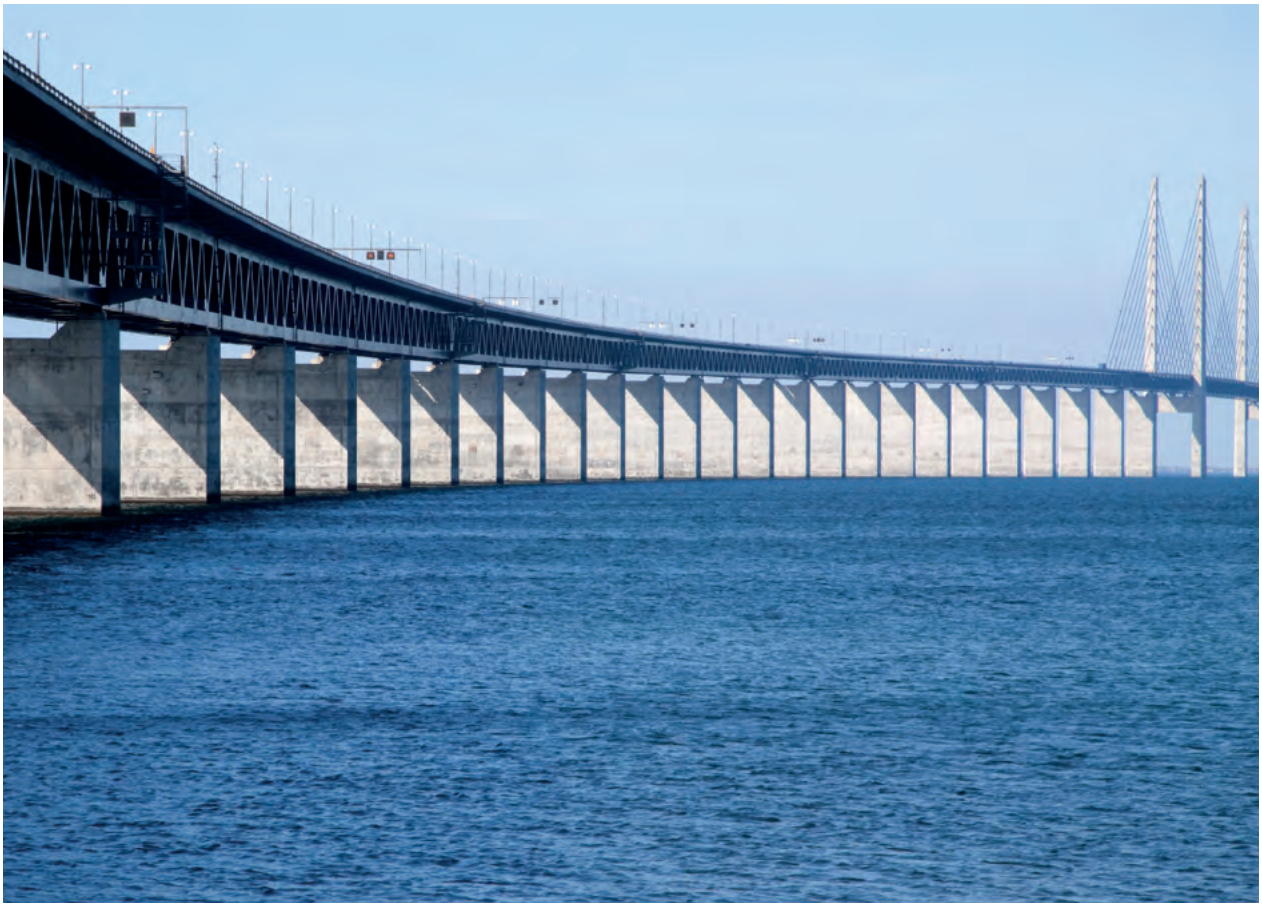
On September 3, 2014, the Swiss Federal Council adopted the dispatch on the Financial Market Infrastructure Act (FMIA). This draft law proposes a harmonised regulation of the financial market infrastructures and introduces new rules on the trading of derivatives, with a view of putting Swiss law in line with other international standards in this area (Dodd-Frank Act in the United States and the European regulation EMIR.)

Financial market infrastructures are stock exchanges, multilateral trading facilities, central counterparties, central depositaries, "trade repositories" (mentioned below) and payment systems. Multilateral trading facilities differ from stock exchanges as there is no listing of the securities admitted for trading. Financial market infrastructures are subject to licensing requirements by the FINMA under the conditions set forth in the draft law. Particular requirements are imposed on financial market infrastructures deemed of systemic importance.

Subject to certain exceptions, the new provisions applying to derivatives trading are intended to financial and non-financial counterparties. They apply to derivatives trading, to the exclusion of structured products and securities lending and borrowing.

The draft FMIA introduces **three key obligations** in the area of derivatives trading: clearing through a central counterparty, reporting to a trade repository and risk mitigation.

The **obligation to clear through a central counterparty** is imposed on financial and non-financial counterparties, for as long as the derivatives are sufficiently standardised, according to criteria to be set forth by the FINMA. Currency swaps and forward transactions do not trigger any clearing duty. The draft FMIA provides for exceptions in favour of "smaller counterparties" (non-financial, but also financial), i.e. entities whose over-



the-counter derivatives average gross position does not exceed the thresholds which will be set in the implementing regulation.

All **derivatives transactions,** including currency swaps or forward transactions, must be **reported to a trade repository authorised or recognised by the FINMA,** whether the derivatives were traded on a regulated market or not. This duty applies with no exceptions to all financial and non-financial counterparties. They have the duty to report to the central repository the main features of each derivatives transaction. The duty to report applies to the identity of the counterparties, the type of transaction, the maturity date, the nominal value, the price, the settlement date and the currency.

When the derivatives traded are not sufficiently standardised and thus cannot be cleared through a licenced central counterparty, counterparties must **undertake to mitigate operating and counterparty risks.** This duty of risk mitigation does not apply to currency swaps and forward transactions. Reliefs are provided for small financial and non-financial counterparties.

Finally, in anticipation of international developments (in particular MiFIR), the draft FMIA introduces a legal basis allowing to impose on all financial and non-financial counterparties, to the exception of small counterparties, the duty to perform all standardised derivatives transactions via trading venues or organised trading facilities authorised or recognised by the FINMA. However, the entry into force of this obligation has been postponed until this standard is imposed on an international level, which could be the case at the time of the entry into force of FMIA.

PERSPECTIVES

The draft FMIA reinforces and broadens the harmonisation efforts undertaken by Switzerland in the area of financial market infrastructures, with the partial review of the National Bank Ordinance, which entered into force on 1 July 2013. Moreover, FMIA represents a necessary step towards the equivalence, according to international standards, of the Swiss regulations on derivatives trading. Failing this equivalence, financial groups could be penalised within the framework of their intra-group cross-border derivatives transactions. The compromise reached by the authors of the draft law should be welcomed; indeed, while taking over most of the European EMIR, the draft FMIA establishes a welcomed exceptional system in favour of small counter parties.

The draft could enter into force by 2016.

Market participants will have to examine the strategic, operational and legal consequences of the new provisions on derivatives trading on their business models. Counterparties will determine the extent of their obligations according to the exceptions or reliefs they may benefit from and adapt their agreements and internal procedures to the new requirements. Furthermore, the interaction between FMIA and other foreign regulations on derivatives trading, notably EMIR will require that financial intermediaries carrying out cross-border transactions precisely determine their regulatory duties and, if the case may be, solve any possible conflicts between the different regulations.

Contacts : Pierre-Olivier Etique, Frédérique Bensahel and Véronique Chatelain Gomez

TAKING INTO ACCOUNT THE EMPLOYER'S BEHAVIOUR WITHIN THE FRAMEWORK OF THE DISMISSAL OF AN EMPLOYEE WITH IMMEDIATE EFFECT

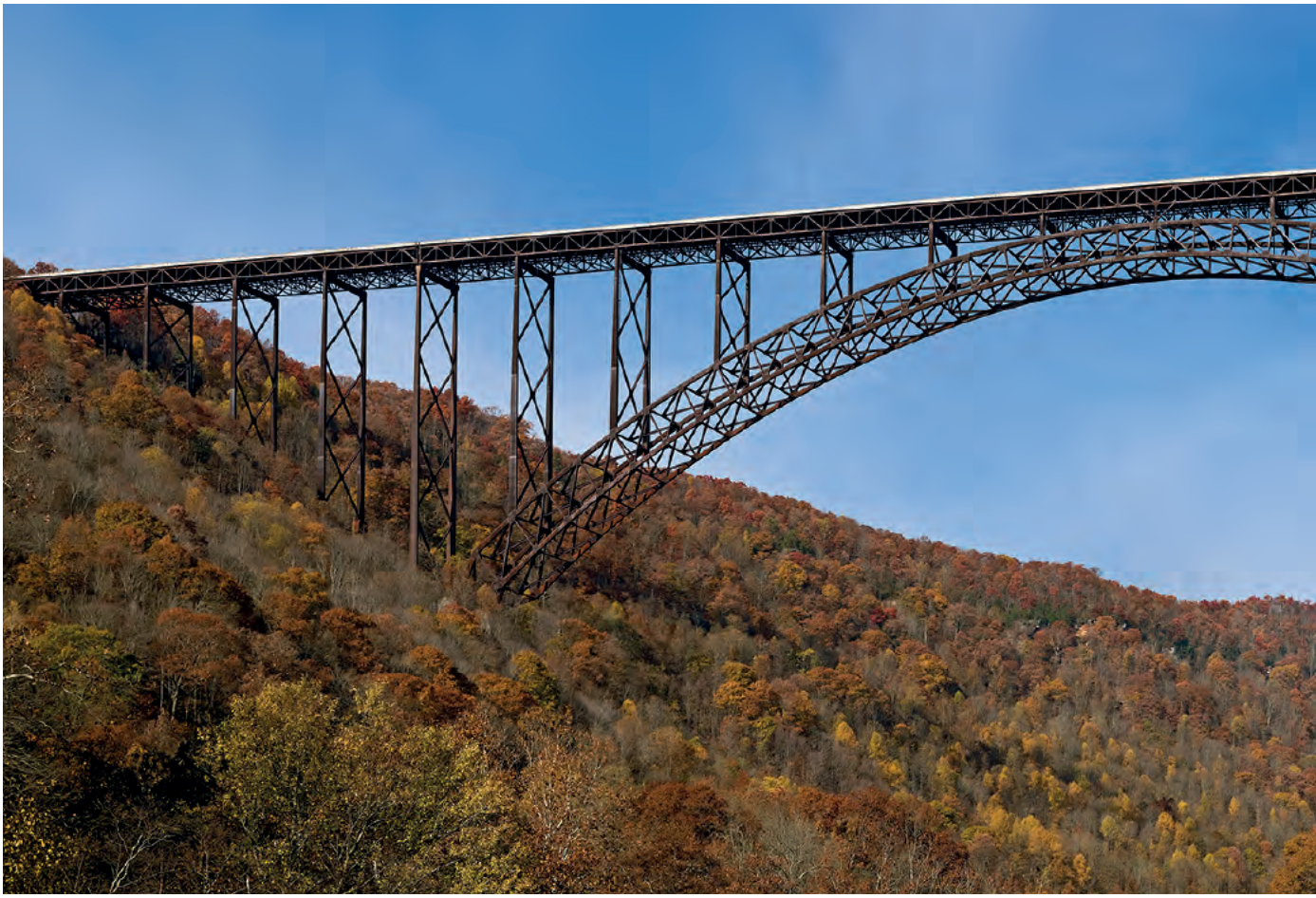
Even if the wrongful behaviour of an employee seems to be sufficiently serious to justify his dismissal with immediate effect, the employer's behaviour must also be taken into account. The employer could not avail himself on the consequences of his own breach of contract to justify the termination of the employment relationship.

Pursuant to Art. 337 of the Swiss Code of Obligations (CO), both employer and employee may terminate the employment relationship with immediate effect at any time for good cause. In particular, is deemed good cause any circumstance under which the continuation of the employment relationship would not be tenable for the party giving notice.

As a general rule, only a particularly serious breach of the contractual duties may trigger the termination of the employment relationship with immediate effect; such a termination must be permitted only in a restrictive way.

According to the Federal Court case law, the fact that an employee behaves aggressively towards one of his colleagues may, under certain circumstances, justify a dismissal with immediate effect.

However, when examining the existence of good reasons permitting a dismissal with immediate effect, the judge has to take into account the overall circumstances of the case at hand, among them, the unlawful or non-contractual behaviour of the employer, if it is directly related to the behaviour of the employee having led to the termination of the employment relationship. Indeed, the behaviour of the employer may be the source of the tense situation that has led the employee to commit a serious breach of his duty of loyalty. Thus, if an employer harasses an employee, or if it tolerates his harassment, he breaches the duties imposed on him by Art. 328 CO and he cannot avail himself of the consequences of his own breach of



contract to justify the termination of the employment relationship.

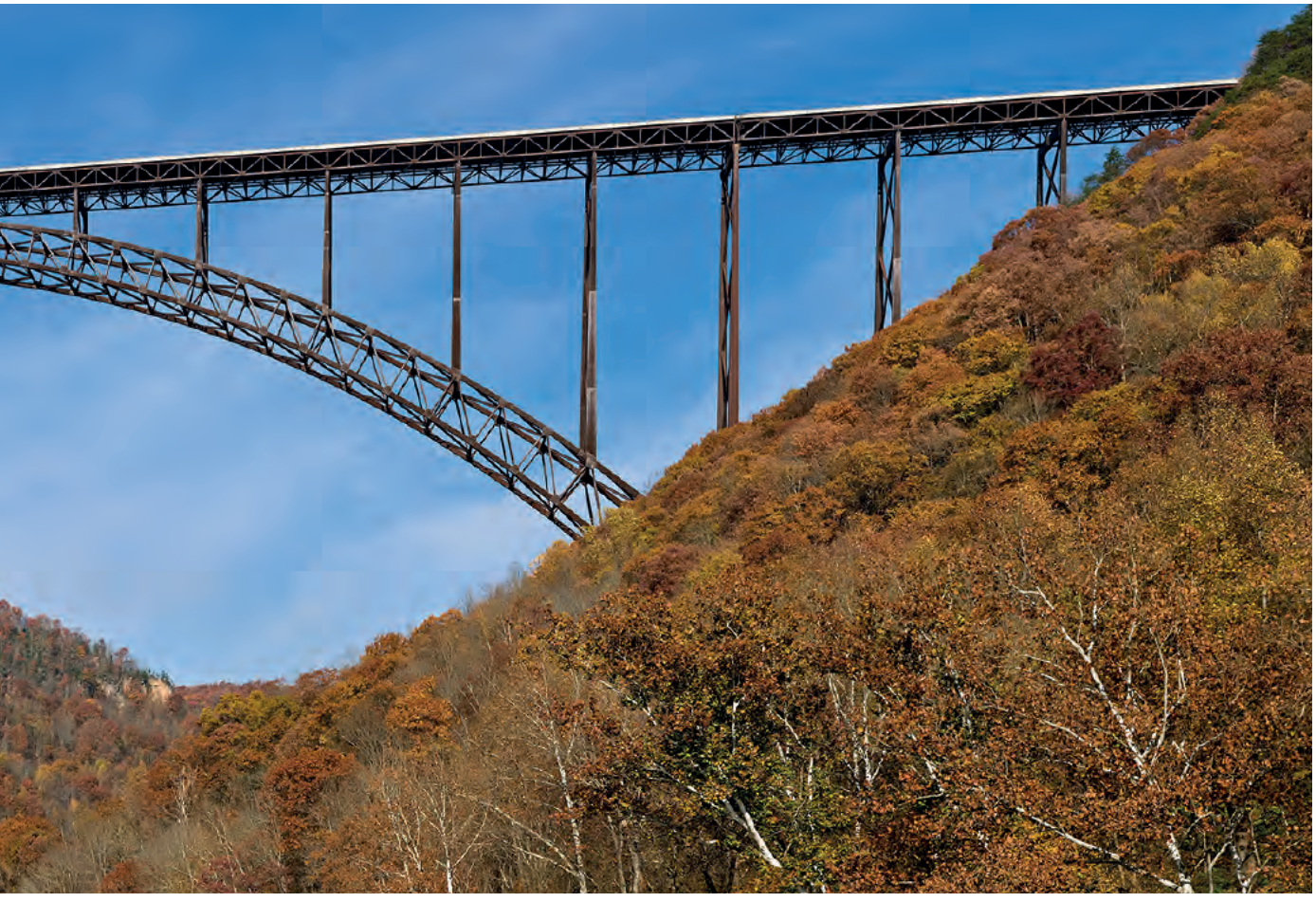
In a recent decision[1], the Swiss Federal Court refused to accept the dismissal with immediate effect of an employee who had physically assaulted his superior aged 61. Even if such behaviour is deemed in principle a good reason to pronounce a dismissal with immediate effect, the Swiss Federal Court considered that the wrongful behaviour of the employee was caused exclusively by the mobbing he had been facing for more than one year.

PERSPECTIVES

In view of this recent case law and in order to avoid any complaint about the inappropriate behaviour of an employer within the framework of a dismissal with immediate effect, which would entail the risk of indemnification of the employee dismissed, we would strongly advise all employers to take all necessary measures in accordance to Art. 328 CO in order to defuse any interpersonal issues that could arise.

Contacts : Michael Biot et Vincent Delaloye

1 Swiss Federal Court decision of 22 July 2014, 4A_60/2014.



FBT Avocats SA
Genève | Paris

www.fbt.ch

Rue du 31-Décembre 47
Case postale 6120
CH-1211 Genève 6
T. +41 22 849 60 40
F. +41 22 849 60 50

37-39 rue de la Bienfaisance
F-75008 Paris
T. +33 1 45 61 18 00
F. +33 1 45 61 73 99