PROTECTION MAGAZINE

SPECIAL EDITION 2018

SGSS2018 SISYP

SELECTING GLOBAL CUSTODIANS: A PARADIGM SHIFT IN ASSET PROTECTION?

UNDERSTANDING INITIAL COIN OFFERINGS: TECHNOLOGY, BENEFITS, RISKS, AND REGULATION

...AND 5 OTHER EXCITING CONTRIBUTIONS

BLOCKCHAIN AND ACCOUNTABILITY: 7 QUESTIONS TO HUBERT DE VAUPLANE

DATA PROTECTION: IS THERE A NEW SHERIFF IN TOWN?

FULL AGENDA FOR SISYPHUS!

SOCIETE GENERALE
Securities Services

BUILDING TEAM SPIRIT
TOGETHER

SISYPHUS GREEK MYTHOLOGY

In Greek mythology, Sisyphus was sentenced to endlessly roll a huge boulder up a hill and watch it roll back down again, just before he reached the top. Protection is another task that is never-ending...

CONTENTS

PROTECTIONS

Protection, whether in the context of people or of tangible or intangible assets, refers at the same time to both the state of being protected and the act of protecting. The distinction is important, as the state of being protected is clearly transient - protection requires constant adaptation to the prevailing risks. *Nothing endures but change*[1].

During the sub-prime crisis, many bankers and investors thought it was the end of the world. As it turned out, it was the end of the world as they had known it or as they could envisage at the time.

REGULATION AS A PROTECTION

The crisis was a catalyst for regulators, who felt compelled to make markets more **transparent,** intermediaries more **responsible** and investors better **protected** through increased regulation. There is no doubt that most of these regulations were necessary, even if it can be argued that some were inappropriate or ineffective, but one thing is clear - they will not be sufficient. *"There is no way regulators can keep up with the speed of technology, but they can play a role in accountability"*[2].

DEFINING AND ASSESSING PROTECTION

Therefore, investors and intermediaries should **question** their choices and re-assess the level of protection provided, or more accurately, the level of risk they knowingly accept to take. Assessing your risk appetite and position relative to others is not easy: leader, laggard, or just in the *Golden Mean*[3] *(or the Middle Way*[4]*)?* This will clearly have implications on the level of protection afforded. Similarly you need to assess your clients and suppliers, the level of protection they offer and the level of trust you give them. For instance, when selecting a bank as a trusted partner, it is customary to scrutinize its services, its relative position in the market, its capital structure and its global solidity.

FUNDAMENTAL CHANGES

But how deep should such questioning go? Should some foundations, usually seen as **immutable,** be put in question? For example, should we go so far as to question the system of trust in society based on the State, its constitution and laws? The emergence of new social trends among the next generation of tech-savvy world citizens is being reinforced by Blockchain technology that allows trust to be created within a group, eliminating the need for a trusted third party. Could a technology fundamentally change our organizations and eradicate our national systems? And if this vision becomes reality, when will the turning point be reached?

INCREMENTAL CHANGES

Or on the other hand, could it be that some incremental changes in fact become game changers? Digitization is advancing and techniques in the digital space are evolving. The expansion of outsourcing and the reliance on external resources like **cloud computing** or **Anything-As-A-Service**[5] create a strong dependency on third party suppliers who are entrusted with key processes and confidential data. With suppliers in turn depending on other suppliers, this interdependency can become either a strength or a weakness, unless it is properly managed.

CORPORATE IMPACT

Any failure in protection can result in **direct costs** to an organization. With media exposure, it can also turn into a major public **reputation risk.** This is the reason why communication managers will typically need to be involved in crisis management together with executive management, operations, IT, risk, legal, and compliance.

PERSONAL ACCOUNTABILITY

All regulators consider that corporate responsibility alone is not sufficient and more and more, they are introducing personal liability for management and operations, sometimes up to **criminal responsibility**. The message is consistent - there is no delegation of responsibility when using a third party.

BALANCING

Following on from system backups, Disaster Recovery and Business Continuity, the concept of **resilience** has emerged. Should a production facility and its staff become inoperative, the objective of resilience is to complete the activities of the day and resume at least 75% of activities by the next day. To reach such a level of continuity, at least three production centres are required with load balancing and extra manpower, or manpower that can be made available and operational overnight. When vital or essential activities are outsourced, they too must be operative within the same standards with different third party suppliers and the possibility to rapidly balance operations between them. Obviously third party suppliers need proper monitoring and supervision.

In August 2015, an operating system upgrade of Sungard Invest-One at BNY Mellon caused a corruption of data and back up generated errors in valuations of 1,200 funds for a week. *"Financial institutions like BNY Mellon are expected to oversee their third-party vendors and have back up plans if the vendor's system fails," Massachusetts Secretary of the Commonwealth William Galvin said in a statement.*

"This is particularly important when the third party vendor performs a critical business function that impacts mom and pop investors."[6]

PRESERVING

The usual key words for the security of information are authentication[7], integrity[8], confidentiality[9], scalability[10], traceability[11], availability[12] and sometimes also comprehensiveness[13]. For each of these areas, there are potential weaknesses whenever information is stored or exchanged. The increase in the exchange of data over networks makes **cybersecurity** a constant preoccupation.

The most secured messaging system for the banking industry, SWIFT, has been used in 2015 and 2016 to steal hundreds of millions of dollars from the Bangladesh Central Bank[14]*.*

In the European Union, the Directive on the security of network and information systems (**NIS**)[15], expected to be transposed into national law by 9 May 2018, aims to boost overall security. Similarly, the EU General Data Protection Regulation (**GDPR**)[16] is designed to protect the data privacy of all EU citizens, empower individuals with regard to their personal data and reshape the way organizations across the region approach data protection.

PREPAREDNESS

Hacking is inevitable. Greed is the primary motivation of the hacker, but often such attacks are simply motivated by the thrill, by fame-seeking or in pursuit of a particular 'cause'. This is why it is essential to envisage hacking scenarios, establish responses to these scenarios and play them in order to be prepared.

CONDUCT AS PREVENTION

It is estimated that in almost two cases out of three (63%)[17], hacks are linked to a company's own employees, including consultants. *"Social engineering has become about 75% of an average hacker's toolkit, and for the most successful hackers, it reaches 90% or more"*[18]. So the first formula against cybercrime is **company culture**.

(1) Heraclitus. **(2)** Dara Khosrowshahi, Uber CEO, Davos 2017. **(3)** Theano (Pythagoras' wife). **(4)** (Gautama) Buddha. **(5)** XaaS, for Data, Software, Storage, Platform, Infrastructure, Desktop – as a Service. **(6)** http://triblive.com/business/headlines/10184410-74/mellon-bny-funds. **(7)** Authentication illustration: identity fraud, the most common fraud . Phishing is a type of reverse identity fraud where hackers pretend to be a company to retrieve sensitive information from its customers. **(8)** Integrity illustration: tempered or corrupted data. For instance, change of beneficiary owner of assets. **(9)** Confidentiality illustration: unauthorised data access or data theft. A social security number with a date of birth sells at over 10 euros on the darknet. **(10)** Scalability illustration: unability to cope with volume (sometimes included in availability). **(11)** Traceability illustration: capacity to monitor who has provided or changed information, like an audit trail. **(12)** Availability illustration: no or limited access to information. For instance, Denial Of Service (DOS) attacks aim to saturate a server and prevent access of other users. It is often used as a decoy and hide other simultaneous attacks. **(13)** Comprehensiveness illustration: dataset without erroneous or missing values. **(14)** https://en.wikipedia.org/wiki/2015%E2%80%932016_SWIFT_banking_hack. **(15)** DIRECTIVE (EU) 2016/1148. **(16)** REGULATION (EU) 2016/679. **(17)** Source Deloitte Enjeux Cyber 2018. **(18)** John McAfee, founder of McAfee Associates.

Etienne DENIAU, Head of Strategic Marketing SGSS. Etienne Deniau started working in 1990 at Fimat, the Futures and Options brokerage arm of Societe Generale, for which he ran the Tokyo office from 1993 to 1997. He then moved to London to head Societe Generale's local branch for Global Banking and Securities Services. In early 2000, he left the Societe Generale group to pursue different opportunities in retail banking. He returned to Societe Generale in October 2004 and has held the following positions: Deputy Head of Investor Services within SGSS and became Head of Custody and Trustee Services, Head of Business Development, Asset Managers and Asset Owners, and Head of Product Engineering. Etienne was appointed Head of Strategic Marketing in January 2017. Etienne Deniau is a graduate of the École Polytechnique and Mines Paris Tech.

SELECTING GLOBAL CUSTODIANS: A PARADIGM SHIFT IN ASSET PROTECTION?

The world of global custodians has undoubtedly seen one of the greatest waves of new regulations changing not only their landscape, but also the way their institutional clients review their custody providers.

REGULATIONS AND MARKET STIMULI

Regulations such as the Alternative Investment Management Directive (AIFM-D), Undertakings for Collective Investment in Transferable Securities V (UCITS V), and soon to be implemented Directive for Institutions for Occupational Retirement Provision 2 (IORPII) all have in common to increase investor protection amongst others.

Other stimuli that are aimed at increasing transparency and protection which are relevant for the global custody market are:

- the resolution planning exercise under the Dodd-Frank Wall Street Reform and Consumer Protection Act,
- the finalization of the post-crisis reforms under Basel III,
- Basel Committee's suggested changes to the assessment methodology for Globally Systemically Important Banks,
- And the European Commission's ambition on structural reform of banking in the EU through for instance Capital Requirement Directive IV (CRDIV).

In varying degrees all these regulations and market stimuli affect the way institutional investors are interconnected to the global custody industry.

RESEARCH

Societe Generale Securities Services recently completed research on the historical evolution of the global custody industry. The research reveals that institutional buying behavior in the global custody industry has emphasized on price as one of the most important buying criteria, and, simultaneously, global custodians tend to compete on price as a key differentiator when entering into competitive bidding.

Using applied microeconomics, it can be concluded that the market over the past 25 years has continuously found its equilibrium, but it can also be concluded that the number of global custodians offering services to European institutional investors has decreased substantially in some countries due to the economies-of-scale challenge global custodians have faced under price pressure.

However, as per the Financial Conduct Authority's (FCA) Business Plan for 2017/2018: custody banks provide critical support services to the funds industry and trading activities, which require them to be accurate, secure and resilient. The FCA has therefore planned a review of the global custody sector over the next two years.

ENHANCED METHODOLOGY FOR SELECTION

Historical experience and research shows that institutional investors have focused mainly on two critical lines of defence of a global custodian's business practice when selecting a global custodian. **The first line of defence** is segregation of client securities from the custodian's balance sheet and a high-quality sub-custodian selection and monitoring process.

The second line of defence is the global custodian's strategic, tactical and operational risk framework including security measures against material events. Both lines of defence are pre-event risk mitigations.

Under aforementioned regulations such as AIFM-D and UCITS V, and in the unlikely, low-probability event of loss of assets, **a third line of defence** becomes equally important, namely a global custodian's credible capital position versus the risks they are exposed to. Empirical research suggests that capital protection as the third line of defence may increase in the future as a more dominant factor when selecting a global custodian. With regards to capital protection the market has not found its equilibrium as of yet under new regulations. To support adequate analysis and decision making on capital protection, new methodologies have been developed to support institutional investors based on increased information and transparency available to the market. In a market where transparent decision making by financial institutions is fundamental to society under new regulations and investor protection is paramount, enhanced methodologies for custodian selection are welcomed by institutional investors.

MAXIMISE PREVENTION AND PARADIGM SHIFT

New regulations are now mostly implemented, and the interconnected stimuli of supervisors and regulators have fueled the market. As more information and methodologies become available to institutional investors to evaluate global custodians, buying behavior of institutional investors is likely to turn towards maximizing prevention and investor protection. The emphasis on three lines of defence, rather than the historical two, allow for the paradigm shift in asset protection to reach new heights.

Roel van de Wiel is Head of Coverage, Sales & Relationship Management, Nordics and The Netherlands SGSS and is based in Amsterdam. He is the author of the research paper: "Paradigm Shift: Review of the Historical Evolution of the Global Custody Industry Using Applied Microeconomics"

PROTECTING DATA

A SIGNIFICANT INCREASE OF DATA VOLUME

That's a fact : the world is changing increasingly fast and becomes highly digital. Growth of data is exponential. IDC forecasts that by 2025, the global datasphere will grow to 163 zettabytes (163 trillion gigabytes), i.e 10 times of data generated in 2016[1].

Last year[2], we emphasizes the emerging technologies in Finance such as Artificial intelligence and Machine learning. All these technologies require a huge amount of data to build the models, then to apply them on a daily basis, for experience, adjustment and production: data mining, data cleansing & sorting.

And data remains everywhere in our professional and personal lives, from personal assistant to automated cars, from newspaper to financial reports. The more we go, the more data becomes critical in all aspects of our life. Level of criticality of data might be assessed: according to IDC, 10% is hyper-critical, 20% is critical, almost 90% is sensitive, but only less than a half being secured.

From a business perspective, risks are increasing at the same rhythm than technology: from malicious payments, to ransomwares, including all kinds of attacks, individuals and companies are widely exposed to cyber-criminals.

Only in France[3], in 2017, 92% of companies have faced 1 or more cyber-attacks. 64% of companies will increase cyber-security budget this year and more than 40% are seriously considering cyber-insurance.

OPENING THE DATA ?

Then, companies are facing a contradiction between the willingness to open and expose their data and IT systems, to create more valuable offers to their customers, and develop partnerships with other institutions and partners (such as FinTechs and RegTechs), and on the other hand the necessity to secure data and IT environments.

FROM A FORTRESS MODEL TO AN AIRPORT MODEL

To solve this issue, a new paradigm is emerging from the security sphere: we are gently moving from a security model based on "Fortress" (nobody enters, everything is safe and secure inside) to a model of "Airport" (multiple zones, with different level of security adjusted on the level of protection of the data, adequately proportional to the risks related to the value of the underlying asset).

NEW EU REGULATIONS ABOUT DATA

GDPR regulation is about to be issued in Europe and includes some basic principles for data protection : among them, "privacy by design", identification of data protection officers, and accountability of companies managing personal data. It also offers new and reinforced rights for EU residents, in a simple and explicit manner. All companies which collect, store and process EU residents personal data are concerned, including outside the European borders.

This harmonization across Europe of basic principles related to data protection is just a recall that protection is not an option to consider, it is at the heart of any new development of financial activity. And beyond personal data, we all know that the same principles should be applied to any data manipulated by our companies: privacy, transparency, and proportionality have been introduced for many years in local and EU rules and directives. Let's just consider now them as part of our daily business, and information shared with our customers.

As trustful and long-lasting partners, banks and financial institutions are providing their customers with adequate level of security, to protect all kind of assets, during all phases of activity: safekeeping and securing transactions.

A COMMON UNDERSTANDING WITH BANKS

The Digital economy forces banks and financial institutions to revise their security models as well; bringing confidence into their systems and the process linked to the dematerialization of information. Number of cases of frauds have shown in a recent past, that protection of data is not only a struggle between hackers and some IT specialists in cyber-protection, this might become the major risk against the safe of a company. Data protection is under the responsibility of everybody from the top manager until any operator in our systems, a common asset to manage carefully.

And the perimeter of the environment to secure is also moving rapidly, including all partners included in the value chain, from producers to final consumers. The purpose here is not to frighten everybody and stop making business, trying to avoid to exchange data. At the contrary, the objective is to increase number of exchanges, and share the business value linked with the quality of data we provide each other. But to do it carefully, managing the right proportion of security and confidence between partners.

SOCIETE GENERALE PROTECTION STRATEGY

At Societe Generale level, many actions have been put in place to secure data: creation of CERT (real time analysis of activity, potential frauds & attacks, analysis of weak signal thanks to AI & machine learning), increase of awareness programs & all-staff training about new cases of frauds (Advanced Persistent Threats, Social engineering), permanent surveys of inbound/outbound flows of data, identity management upgrade.

Identification of stakeholders in an electronic exchange is a way to bring the right level of confidence, and open the doors to the right friends. The data protection engages any part of the chain, consciously.

And, by analogy with Artificial Intelligence, don't fear to be left behind, we get smarter by improving our systems, and protecting our assets. Just we have to remember that Darwin is still alive today : the ones which will not adapt data protection to the current risks may face major issues in the future.

(1) Data age 2025: the evolution of Data to Life-Critical, IDC White Paper, April 2017. **(2)** SGSS Tech magazine, Special Edition 2017. **(3)** Les Echos, Jan 23rd 2018, « Cybercriminalité : nette augmentation des attaques en France en 2017 » ; https://www.lesechos.fr/tech-medias/hightech/0301193349879-cybercriminalite-nette-augmentation-des-attaques-en-france-en-2017-2147347.php

Yvan MIROCHNIKOFF, Head of Innovation & Digital Transformation, SGSS. Associated Professor, Paris-Est University. Supervises 8 experts at Business Line level : Chief Digital Officer, Chief Data Officer, Head of Digital Marketing, Head of Innovation, Digital Projects managers.

UNDERSTANDING INITIAL COIN OFFERINGS:

TECHNOLOGY, BENEFITS, RISKS, AND REGULATIONS

Organizations have raised $3,700,682,293[1] in 2017 through Initial Coin Offerings (ICOs). The popularity of ICOs has rocketed in 2017 and we are currently seeing a lot of discussions on whether investors should look into this investment given the associated risks.

Regulators all around the world are currently assessing cryptocurrencies and ICOs to determine if current regulation applies or if there are necessary adjustments.

In a whitepaper produced in collaboration with Stellar[2], we aim to explain the functioning of ICOs, why they are favored by new businesses (and particularly those active into blockchain technology), what are the benefits, the risks for issuers and investors; as well as the regulatory considerations to keep nurturing innovation.

An initial coin offering (ICO), also known as a token sale, token generating event, or initial token offering, is an event in which an organization sells digital tokens for the purpose of obtaining public capital to fund software development, business operations, business development, community management, or other initiatives. Tokens can have various attributes, and contrarily to an Initial Public Offering (IPO), those are rarely linked to an ownership in the organization.

We currently hear a lot about risks associated to ICOs but we rarely speak about the benefits for the issuer or investor. Why is it gaining attractiveness? Why does it become the go-to solution for innovative projects when it comes to raising fund? The benefits for the organizations rely on, but are not limited to the positive network effects, the built-in customer base, the marketing power of such actions and the investors' outreach which can be qualified as non-discriminatory and global.

The risks are threefold, first, the consumer protection which must be paramount. Given the nature of ICOs, their reach, some investors could be subject to phishing scam.

In addition, it might prove difficult to know what is the jurisdiction of the ICO and the regulation applicable. In terms of market risks, price volatility, market manipulation and network lag constitutes the biggest challenges of such market at the moment. Finally, using blockchain does not prevent from complying with the existing regulations.

Raising money via ICOs will be more and more frequent in the future. Numerous countries are taking drastic measures against ICOs such as bans or categorizing tokens as securities but these measures should be temporary, to protect the investors, while the authorities work on a set of adapted regulations, nurturing the innovation. Moreover, existing regulations can apply to a certain extent to the ICOs, it is then necessary to perform a thorough analysis and assessment of what is in place to adapt it and know how does that apply. ICOs and cryptocurrencies also bring opportunities to the financial industry and could be part of the diversification strategy of some investment funds for example. We're only witnessing the birth of an additional capital market, a decentralized one. It will grow and learn from its mistakes, similarly to the capital market we know today.

(1) Source: https://www.coinschedule.com/stats.html accessed on 1st of February 2018. **(2)** Available for download : http://bit.ly/2hQRpT7.

Emilie Allaert - Head of Operations and Projects - Luxembourg House of Financial Technology (LHoFT). Emilie promotes the use of financial technology and innovation within the financial sector. As part of her role, she leads various projects and researches on trends and fintech topics.

COMPULSORY LICENSING FOR AIF DEPOSITARIES IN THE NETHERLANDS

PART OF A EU WIDE FOCUS ON SYSTEMIC RISKS OF THE ASSET MANAGEMENT SECTOR?

The Alternative Investment Fund Managers Directive (AIFMD) requires managers to appoint a depositary for each (alternative) investment fund (AIF) in scope of the AIFMD[1]. The rationale behind this requirement, succinctly put, is that such depositary will protect investors against a loss of their assets. To this end, the AIFMD introduced oversight requirements and provisions on the liability of depositaries for the loss of the (financial) instruments brought in custody[2].

Just before the 2017 Christmas recess, the Dutch Authority for the Financial Markets (AFM) announced in its newsletter[3] the introduction of a compulsory licensing for AIF depositaries[4] with effect from 18 March 2018. This is a logical next step on the path towards the objective of the EU to protecting to the extent possible the interests of investors (and their assets). The measure is in line with an EU-wide focus on the risks attached to the asset management sector and custodians in particular. Last year, for example, the UK supervisory authority FCA launched an investigation into the systemic risks run by the custody sector which investigation is ongoing. The FCA posed that amongst others custodians provide critical services to the funds industry which require them to be accurate, secure and resilient and argued that a lacking supply of parties, low profit margins, bundling of banking services (such as transfer agency and fund accounting) and custody services as well as a lack of investment in modern technology - triggered by the low profit margins - are factors posing a risk to the asset management sector and a stumbling block for managers to obtain compatible offers. The introduction of compulsory licensing will enable the AFM to test depositaries, reviewing those risks, but also governance and capitalisation.

So as of March 2018 licensing will be compulsory for all AIF with a few exceptions only[5]. In short, banks that are licensed to amongst others have in custody and manage securities as well as investment firms with a prescribed minimum share capital (in compliance with CRD) that also provide depositary services are exempt from the compulsory licensing scheme.

Depositaries of AIFs which for the first five years after acquiring the units do not offer any repurchase or redemption option and generally (i) do not invest in assets that can be given in custody or (ii) do invest in (unlisted) issuers in order to acquire governance and control[6] need not apply for a licence either.

It follows from the above that the consequences of compulsory licensing will chiefly be felt by depositaries of regulated open-ended AIFs that have appointed depositaries not being banks or investment firms. A depositary that intends to assume the duty of safekeeping an AIF would be well-advised to heed the new requirements. Compulsory licensing also affects managers of such AIFs and ultimately the investors. Of particular importance is the fact that the AFM will apply stricter tests to governance, operation (organisation (integrity and conduct), AIF acceptance policy, implementation of the depositary duties in compliance with the AIFMD, policy on conflicts of interests, due diligence in the event of delegation, compliance and audit functions) and business plans of depositaries. There is also more focus on sub-delegation of custody tasks. The depositary will obviously have to take account of initial and ongoing supervisory fee relating to - the application for - the licence. And last but not least, the AFM will also apply stricter screening of capital requirements by shifting the focus on minimum equity capital requirements to the minimum capital to be held in relation to the (custody) risks attached to the specific AIFs. Potentially, this shift in focus could lead to an increase in capital requirements for depositaries which would not only affect the entire custody industry but ultimately investors as well. This focus on adequate own capital would fit the EU wide trend of the shifted focus by legislators and regulators to the systemic risks of the asset management sector.

(1) The same requirement applies to undertakings for collective investments in transferable securities (UCITS) and has been laid down in the Undertakings for Collective Investment in Transferable Securities (UCITS) Directive. **(2)** Article 21(12) AIFMD. **(3)** Newsletter professionals December 2017, "Vergunningaanvraag bewaarder beleggingsinstelling/ICBE", www.afm.nl via website@afm.nl. **(4)** and UCITS. **(5)** Which are: section 2:3g(2) of the Dutch Financial Supervision Act (Wet op het financieel toezicht – (Wft) or Section 2:3h Wft in conjunction with Article 1c of the Exemption Regulations under the Wft (Vrijstellingsregeling Wft). **(6)** Within the meaning of the AIFMD as implemented in sections 4:37q and 4:37w Wft.

Minke Hoekstra, heads the Fund practice of Simmons & Simmons in the Netherlands and has over 18 years of experience in the asset management sector. Prior to joining Simmons & Simmons, Minke worked as in house lawyer for several global asset managers and was based in The Hague, Hong Kong and New York. She started her career in private practice at a leading Dutch law firm and was based in Rotterdam, Amsterdam and London.

DATA PROTECTION: IS THERE A NEW SHERIFF IN TOWN?

In the beginning, there were personal data being digitalized, accessible form everywhere by everyone. The new frontier, will, as always, generate abusive behaviours. Not long after, come threats and data breaches - such as ransomware or security breaches. Some are not brought to the attention of the public and the authorities, some are with delay... To deal with those security issues, once again the European Commission has turned into a shield to protect the people, as it had done it with MiFID II, IDD, PRIIPs, PSD2, etc. There's a new sheriff in town as goes the saying!

GDPR, THE EUROPEAN LEGISLATIVE RESPONSE

On May 25, 2018, the General Data Protection Regulation (GDPR) will come into force with a significant novelty compared to previous regulations: all companies are concerned, for all categories of data subjects. The GAFAs' sector is obviously a target, but so are service and industrial companies, be they international or local! As for the data subjects, if customers and employees naturally come to mind, the GDPR also aims at protecting personal data of prospects, former employees, candidates, legal representatives etc.

…WITH MEANS TO MATCH ITS AMBITIONS!

What are the purposes of this regulation? To strengthen data subjects' rights, of course, but also to make organisations more responsible, including subcontractors, and finally to standardise practices within the European Union. What about the means? Administrative penalties incurred in case of data breaches can go up to 4% of worldwide group turnover (or € 20 million for non-profit organisations). In comparison, in France the maximum penalty amount in case of personal data violation was set at € 150,000!

ALL RIGHT THEN, BUT BANKS ARE ALREADY PROTECTING DATA!

Yes. And at first, the gap does not seem to be that large (in France at least): GDPR is based at 90% on the French law "Informatics and freedom" from 1978. Lucky us! However, a closer look reveals a not so ideal situation considering the main tasks to complete: respecting data subject's rights, setting up security measures and adapting organisations around the Data Protection Officer (DPO) to state the obvious!

SO, IT'S ALL GOOD?

Not so fast! The GDPR covers different rights: the rights of access, opposition, rectification, limitation of processing, the right to be forgotten and the new right to data portability. If the first rights are generally respected (access, limitation, opposition, limitation), organisations mostly deal with them with manual procedures: the approach is then to ensure processing are documented and to evaluate the relevance of automating (in part?) some of them, depending on observed and anticipated volumes. No big deal, actually, even if the right of access might turn out to be complex to implement considering the scope of personal data to be communicated to the data subject.

WHAT'S THE CATCH, THEN?

Well, respecting the right to be forgotten and the right to data portability certainly raises deep IT issues. If you ask a CIO to purge his databases, he will probably refer to the non-existence of the data repository, to the IS legacy, to the lack of control over data propagation and interdependencies between the different bases, to the systemic risk on the IS etc. Organisations have to analyse this thorny issue carefully and take the time to identify possible strategies. The regulation indeed includes the right to be forgotten, which anonymization (not to be confused with pseudonymization) can help to reach, so does containerisation (or data segregation) at some points etc. As for the right to data portability, it is problematical because the scope of data that could be transferred is not defined yet!

AND WHAT ABOUT DATA PROTECTION AND CYBERSECURITY?

Security measures should be easier to implement... for companies of a certain size. These companies usually have CISOs (Chief Information Security Officer), who are structurally concerned by data protection in general, not only by personal data protection. Some companies also have the status of Outsourced Essential Service Providers and are therefore already well equipped, particularly in terms of fighting cybercrime, among IT risks. Risks assessments will have to be more thorough but that should do it!

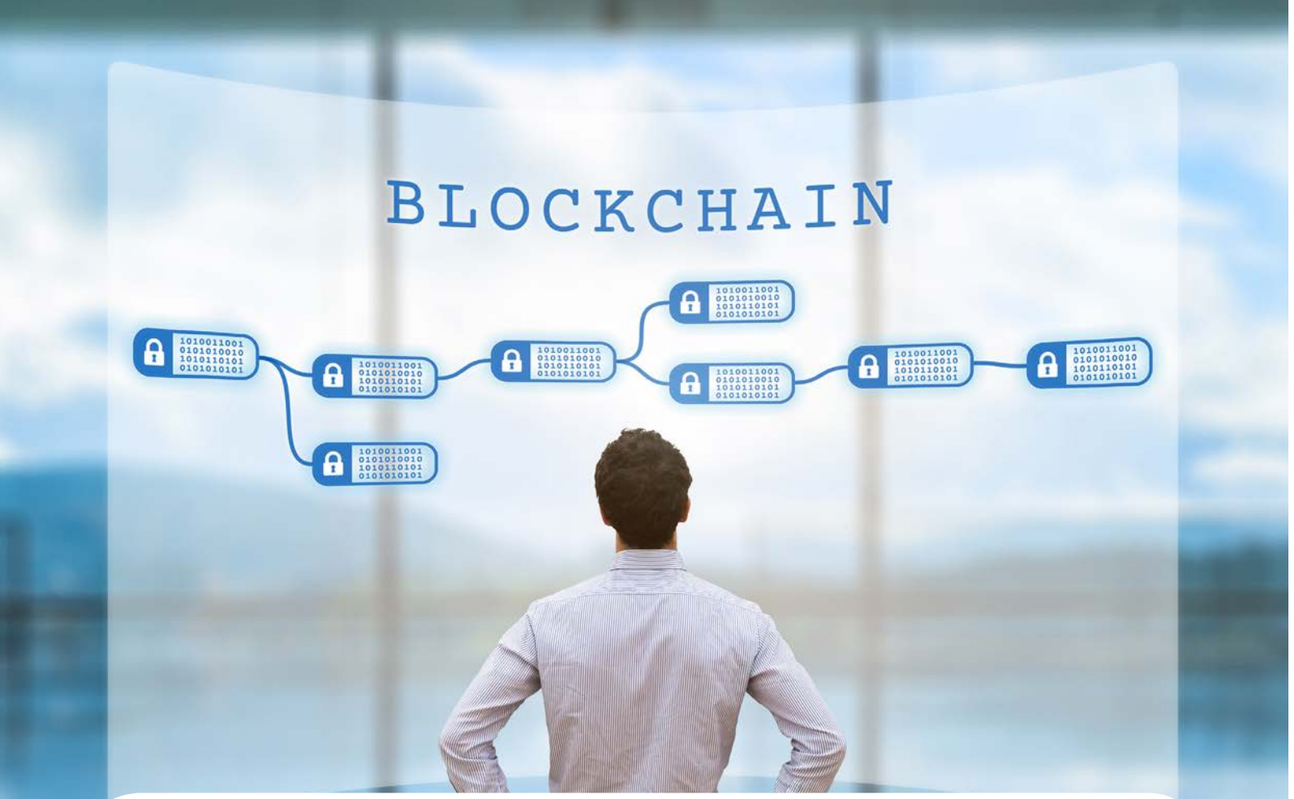
WHAT'S LEFT TO DO?

Finally, companies have to adapt their organisation around the DPO, a task that could include all other requirements of the regulation: GDPR governance; obligation of information; formalisation of privacy by design & by default methodologies; processors risks; update of standards, procedures, control plans and training. Those topics must be developed, but not from scratch: the existing organisation can be enriched to turn GDPR compliant.

SO, THEN, IT'S ALL GOOD?

Not even close, but you got to take a documented risk approach. Why documented? In the event of a control by the Supervisory Authority, the company must be able to prove that its compliance roadmap is clearly defined and that the necessary resources are allocated, in order to justify the compliance horizons observed on the market: May 2018, end of 2018 and end of 2019. If you're small, they'll play nice, but if you're big, well… buckle up!

Guillaume Louvet, Senior Manager, Ailancy. Born in 1980, Guillaume holds a Master's Degree in Industrial Economics of the Paris La Sorbonne University. He worked on the financial market as a hedging analyst for corporates financial risks before turning to the consultancy industry. He's specialized on the private and retail banking and expert on data.



BLOCKCHAIN AND ACCOUNTABILITY

7 QUESTIONS TO HUBERT DE VAUPLANE

1. **Would it be reasonable to claim that it is easier to ensure asset protection, and cybersecurity more broadly, in a decentralised system, such as blockchain, than in a centralised system?**

At the present time, I would say no. Blockchain technology is still in its early stages and cannot be considered fully secure. This is also the message given by the ECB; it certainly sees a bright future for this technology, but we must see if it comes up with the goods first, particularly in terms of security. If we take the more specific case of assets, particularly securities "held" in the blockchain (as permitted by the Sapin II Law in France), there is also a distinction to be made: the issue is not as black and white for private blockchains as it is for public blockchains, as the latter's security weaknesses are less about the technology itself than the third parties (market places) with which the assets (e.g. cryptocurrency) are held. We have seen a number of thefts of bitcoins and others owing to a lack of wallet security.

2. **Many private blockchains simply seek to reap the benefits of registered shares by cutting out the middleman between issuers and investors. However, isn't there a risk that we will also have to deal with the disadvantages, notably as regards a lack of external control of the register held by the issuers?**

I am of the opinion that using blockchain for securities amounts to making the registered form of securities more widespread, since the investor is registered directly in the chain in his own name and the issuer has direct access to this information. Now, just as in the case of registered securities, I think that a certain number of issuers will call on third parties, such as financial intermediaries, to act as registrar for their decentralised registers in accordance to their mandate. Indeed, some issuers will prefer to entrust the keeping of their blockchain-based registers to experts, particularly given the complexity involved.

3. **How is or how should the responsibility to protect the assets in a blockchain be shared in your opinion? Is the situation the same in a public blockchain with only one participant profile (such as on the Bitcoin blockchain) as it is in a private blockchain with several participant profiles (e.g. investors and issuers)?**

Obviously, in a public chain, it is difficult to assign responsibility for an event or an act to a specific party without putting in place a governance regime that is accepted by all involved. As we know, the governance of public chains is their Achilles heel; we must therefore look at private chains to find a way of resolving the issue of responsibility through governance. The organisation and operating conditions of this private chain will be addressed in some form of Terms and Conditions. Where the roles of technology provider and users will be defined by the parties, as is currently the case in the Swift system, for example. This goes to show how important the implementation of the 8 December 2017 French decree is since it defines. How authentication can provide adequate safeguards.

4. **Many private blockchains are choosing to make an official role for the operator in charge of the technical platforms that support blockchain. Doesn't this boil down to reintroducing a trusted third party or at least a trusted service provider?**

Yes, indeed. In this case, blockchain is a technology whose applications are offered by a specialised provider acting as the chain organiser. This is similar to in a football match, where a set of rules is applied by the players and it is the referee's job to ensure those rules are adhered to.

5. **If there aren't any trusted third parties in a blockchain, what happens to the obligation to return assets that was previously imposed on custodians? Can it still exist? If so, is it an obligation of means or results?**

You've touched on one of the most important legal (and practical) issues concerning securities. It is indeed difficult to conceive of an obligation to return assets in a public chain; who should it fall on? Even in a private chain, such an obligation cannot easily be imposed on all members of the chain without fostering a certain sense of solidarity among them. It's actually worthwhile considering whether it would technically make sense: the obligation to return assets applies when assets disappear (e.g. in the case of an intermediary or counterparty default). In a blockchain, however, the securities registered in the chain never (or should never) appear in the balance sheets of the participants. The only possible scenario then is assets being stolen from a securities wallet, and this issue has not been addressed (yet).

6. **If an investor's private key is stolen, what can they do (compared with an investor whose bank card is stolen, for example)?**

Nothing, for the time being. And we need to be clear on that point. It's like losing cash or it being stolen.

7. **Does the fact that there are no accounts as such in blockchain mean that it isn't possible to apply the same kind of audit scrutiny?**

Strictly speaking, it isn't possible to apply the same kind of audit scrutiny. But other controls should be used instead. Such as wallet security, for example.

Hubert de Vauplane co-leads the Alternative Investment Management practice in the Paris office of Kramer Levin Naftalis & Frankel LLP, offering a global and integrated vision on regulatory and transactional structuring and operations matters. Hubert advises on EU and French laws on banking and investment services regulatory matters, asset management and funds, insurance investment regulations, and financial/securities litigations, e-money and payment services, and financial institution mergers and acquisitions. He provides legal counsel on fintech, blockchain and cryptocurrency assets, and financial regulatory issues relating to investment advice, asset management, payment services and banking. Hubert de Vauplane is Partner at Kramer Levin Naftalis & Frankel LLP, and admitted to the Paris bar. PhD in Law, Université de Paris 2 Panthéon-Assas, 1991 and a Master in Law, Corporte and Tax, Université de Paris Panthéon-Assas, 1985.

CRYPTO-FUNDS:
A SEA OF OPPORTUNITIES BUT AN OCEAN OF RISK

Absent from our vocabulary until 2008, Bitcoin has now registered in excess of 340 million searches in Google, a figure that compares to the total searches for the word “Luxembourg”. So what is it? Bitcoin was the very first cryptocurrency, created in 2008. Just ten years on and more than 1500 crypto currencies have been launched with a total capitalization of 500 billion USD (1 Feb. 18).

2017 witnessed a strong rise in crypto currencies. The spectrum of new investors ranges broadly, mainly divided into three categories - a tech population known as « Crypto Traders », sophisticated investors seeking exposure (crypto hedge, crypto funds) and a retail population in the quest of the next ‘Gold rush’.

The Asset Management industry, keen to be at the forefront of innovation, is constantly on the lookout for new investment opportunities to attract new clients. And crypto-funds have come on their radar as just such an opportunity.

Crypto currencies could be the next asset class – but could we be opening Pandora’s box? And what are the main risks?

Since 2013, more than 150 crypto-funds have been launched, especially in the US, where hedge funds are the preferred vehicle. According to a research performed by the ALFI (Association Luxembourgeoise des Fonds d’Investissement), the market size could be between 10 and 15 billion USD. The top 3 worldwide funds alone have a value close to one billion dollars. Some of these funds are actively managed, others are passive, while others are a mix of crypto-assets and blockchain investment.

As the old adage says, there is no profit without risk. Several regulators (like AMF in France or SEC in US) or more broadly securities associations (ESMA) have warned investors about the risks associated with crypto currencies. These fall into 5 major categories, having a strong impact in terms of investor protection:

- **Security risk:** the storage of digital assets is done based on cryptographic methods (private / public keys). Private keys are kept private like a computer password. These keys have become a target for hackers via spyware, wifi…. Digital assets should be recorded with a cold wallet to reduce the potential of cybercrime and companies have emerged (eg Ledger) that offer such solutions. The risk should not be underestimated - recently, the Japanese platform Coincheck was hacked and the equivalent of USD 536 M in NEM assets were stolen.
- **The volatility** of the crypto assets, often perceived as a trading opportunity, presents a strong counterparty risk. The basic premise is simple - you can lose all your money. Any cryptocurrency can lose its value overnight and it has been already the case with the Initial Coin Offering Tezos.
- **Furthermore,** a high number of exchanges are not regulated and have no quality commitment, regulatory capital, nor risk management policies. The exchange you keep your coins on can just disappear and you will never see your coins again. There is no investor protection in cryptocurrency trading because it is not a regulated market. This was the experience in December 2017 when the market was going down.
- **The classification of crypto currencies** (assets, other assets …) is a crucial element as it determines how the depository bank should behave in case of default. As this classification is still not defined in several countries, it is difficult for asset servicers to enter the market, taking into account the additional risk. Recently, the Indian government proposed to issue a law deeming that crypto currencies should not be recognised as a currency. Clearly there is a legal risk that jurisdictions could restrict or even outlaw cryptocurrency trading.
- **Finally,** the reputation risk is significant, especially when considering your choice of digital asset & counterparties. Understanding the protocol and strong due diligence can mitigate this risk, but it is nonetheless essential to choose a crypto currency backed by solid fundamentals, cognizant of the risk of scams and false promises.

In conclusion, crypto-funds offer the opportunity of significant returns for investors. However, regulatory uncertainty and high risk are proving to be a significant hindrance to the development of such vehicles in a regulated framework. Crypto-Funds ; a sea of opportunities but at the same time, an ocean of risk.

Laurent Marochini is Head of Innovation & Quality at Societe Generale Securities Services in Luxembourg. Prior to joigning SGSS, Laurent worked at BNP Securities Services in Luxembourg as a Middle Office Derivative Products. He joined in 2000 the Credit Suisse Private Banking as Head of Settlement Operations & Client Service and entered the Societe Generale in 2006 as a Risk Manager, and then became Head of Innovation & Quality. Laurent was twice 2nd Worldwide Best Innovation Maker of Societe Generale, he is also Co Chairman of the Working Group Blockchain & Crypto Currencies at ALFI and Member of the Fintech & Digital Executive Committee.

DIGITAL ASSETS:

IS IT A REVOLUTION FOR INVESTORS' PROTECTION AND DO CURRENT REGULATIONS PROTECT APPROPRIATELY OR NOT?

All the relevant EU pieces of legislation (MIFID II, MAR, Prospectus Directive, UCITS, AIFMD, AML) target the investors' protection and the integrity of the financial market as the cornerstone of the EU single market.

ESMA clarified that "financial services have a significant impact on investors. It is important that investors make informed decisions and feel confident they are adequately protected if something goes wrong ".

Nowadays, there is a huge debate around the nature, the utility and the risks associated with digital assets, such as coins, tokens, smart contracts or, more in general, the use of the Blockchain associated with the Distributed Ledger technology in the financial industry.

Legal uncertainty is usually paired with a wrong perception of the new technologies as such; we should point out that, besides the conceivable frauds, the Blockchain technology associated with the Distributed Ledger technology could enhance the quality and safety of the services provided.

In this new scenario, investors' protection could be better assured via an operation performed using different nodes provided by an indefinite number of users (miners). This open architecture makes the transaction (almost) irreversible and identifiable in terms of date and time.

In this context, we should try to clarify why current market operators and regulators are so worried about the use of digital assets and if the available legal toolbox is sufficient to protect both the investors and the market.

This new business model is based on the disintermediation of the offer, allowing direct, usually less costly, investments through the issue of coins or tokens; the role of such process is still developing and some major "traditional" financial players (banks, insurances, services providers and even central banks) are trying to better understand the market to be part of it.

Therefore, legislators around the globe are taking initiatives, both to foster and encourage the development of these new technologies in the financial sector, or to prevent the use of these technologies, while waiting for other countries to take a full position on the matter.

In Luxembourg, the CSSF is still analyzing the different pros and cons of the implementation of these new technologies in the financial sector and since now, to the best of our knowledge, it merely issued a press release on February 14, 2014 on virtual currencies.

We do believe a normalization in the use of this FinTechs will be inevitable in the next years and that the advantages linked to these instruments, once the technologies will be stable, could lead to a better environment for the financial industry as such in terms of transparency, reduction of costs and investors' participation.

Lastly, current regulations are potentially applicable to several aspects of these new technologies and we do believe, at least in the European Union, that we already possess an existing legal toolbox to cope with most of the challenges of the implementation of ICOs, issuance of virtual currencies and/or exchange platforms linked to tokens or coins.

Indeed, these new operations could fall under the scope of some existing package or not; what is important to bear in mind is the nature of the operation and not the instrument through which the operation is carried out.

For example, the risk associated with an ICO, depending on the structure of the token and the rights attached, could be equal or lower than the risk associated with a bond issuance or a listing of some standard company.

Beyond the qualification and the necessary development to standardize FinTech operations, we do believe that these new opportunities are boundless and could incentivize a capital release to the advantage of both SMEs/start-up companies and market players able to shape their businesses towards the new digital era. It will always be vital to impose transparency to allow investors to make their choices.

(1) See, ESMA on MIFID II protection: https://www.esma.europa.eu/regulation/mifid-ii-and-investor-protection, accessed on the 5 February 2018. **(2)** See, for example, the Swiss financial authority, FINMA, that adopted a liberal approach towards blockchain technology while granting protection to any investor that reports a breach of regulatory law, taking its supervisory role in an ex post logic. Canadian CSA provided for an express regulatory sandbox to help FinTech companies using the new technologies in the course of their businesses. **(3)** This is the case of China, that banned all possibility to launch an ICO in China.

Ingrid Dubourdieu – Avocat à la Cour - Partner at d.law - member of several working groups within: The Luxembourg House of Financial Technology (LHoFT), the Association of the Luxembourg Fund Industry (ALFI) and of the Association des Professionnels de la Société de l'Information (APSI). Ingrid takes care i.a. of the use of financial technology and innovation in the legal environment, concerning ICOs, cryptocurrencies funds and legal application of the Blockchain technology. As part of her role, she has several ongoing projects launched and to be launched in Luxembourg in the FinTech space.

SGSS IS SOCIETE GENERALE'S BUSINESS UNIT DEDICATED TO SECURITIES SERVICES

Established in 27 locations worldwide with 4,000 employees,
SGSS provides a full range of securities services that are adapted to the latest financial markets and regulatory trends: clearing services, custody and trustee services, retail custody services, liquidity management, fund administration and asset servicing, fund distribution and global issuer services.

SGSS is among the top ten global custodians and the 2nd largest European custodian with EUR 3,904 billion of assets under custody*.
SGSS provides custody & trustee services for 3,415* funds and the valuation of 4,113* funds, representing assets under administration of EUR 651* billion.
SGSS ranks among the European leaders in stock option management.

*At December 31 2017

CONTACT US

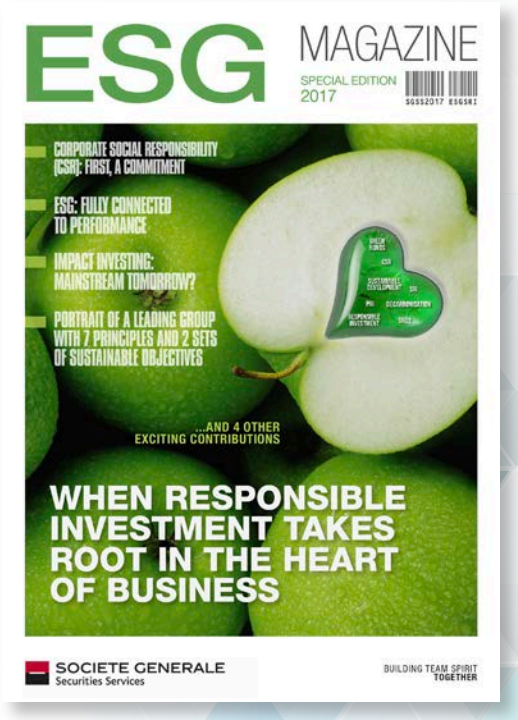
email: sgss.com@socgen.com
web: securities-services.societegenerale.com

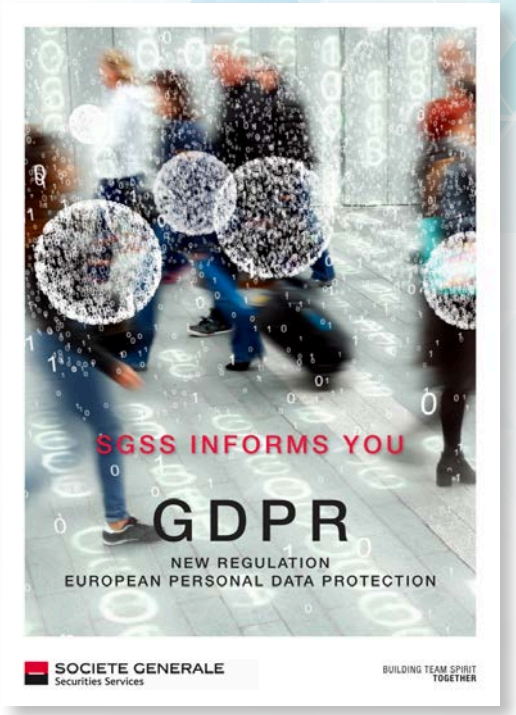
twitter.com/sg_ss

www.youtube.com/user/societegenerale/search?query=sgss

/societe-generale-securities-services

SGSS AT THE HEART OF AWARENESS





SOCIETE GENERALE
SOCIETE ANONYME (PUBLIC LIMITED COMPANY) WITH A CAPITAL OF EUR 1 009 897 173, 75.
B 552 120 222 RCS PARIS - APE 651C - N° SIREN : 552 120 222 000 13
REGISTERED OFFICE : 29 BOULEVARD HAUSSMANN, 75009 PARIS

SOCIETE GENERALE
Securities Services

BUILDING TEAM SPIRIT
TOGETHER