Cyber Security Supervision in the Insurance Sector: Smart Contracts and Chosen Issues

Dr. Remy Remigius Zgraggen*
PhD, Attorney at Law
(PhD from EPFL Lausanne, Switzerland) *now: Financial Market Authority, Vaduz, Liechtenstein Militärstrasse 91 8004 Zürich*, Switzerland
+41788018723
remy.zgraggen@fma-li.li

Abstract*— *There are still many open issues and questions concerning the supervision and the legal and regulatory assessment of cyber security issues in the insurance sector, especially regarding smart insurance contracts and similar issues. In the present case the focus shall be on the underlying legal framework in the European Union and in Switzerland, including the most relevant ordinances and circulars as well as public and private guidelines, followed by an outlook and some general ideas how Brexit could potentially have an impact on the general recognition and acceptation of smart contracts within the legal and regulatory framework and the society in general.

Keywords—Insurance Supervision, Smart Contracts, Smart Insurance, Cyber Security Supervision, Solvency II, EEA, EU, Risk Management, GDPR, Switzerland, Liechtenstein, Insurance, Cyber Risks, G7FE, Risk-Based, Proportionality, Operational Risks, Data Carriers, Brexit

I. INTRODUCTION

With this paper an overview will be provided about chosen issues of cyber security supervision in the insurance sector, especially regarding smart (insurance) contracts. In the face of Brexit, the present research shall focus on two specific jurisdictions outside the EU, Switzerland and Liechtenstein, with the aim to provide theoretical and practical findings, which will be also useful and interesting to determine the impact of Brexit on the British insurance sector from a regulatory and legal point of view. More specifically, the present paper shall focus on the supervision and regulation of cyber security issues within the insurance sector as well as on chosen legal and regulatory questions regarding smart insurance contracts. Switzerland and Liechtenstein have been chosen, because they are the only two countries in Central Europe outside the European Union, even though Liechtenstein is member of the European Economic Area (EEA).

There is widespread agreement that smart insurance contracts or blockchain technology in general will have a relevant impact on a variety of application scenarios within the insurance sector in the future, such as example given in the form of pay-per-use insurance models, microinsurance contracts or frauds prevention systems [1]. However, in Europe the insurance market is highly regulated today, which makes it very challenging to establish new products based on a new technology, or to enter the market as an insurance-start-up company in general [See 2]. This might be one reason why the digital transformation process seems to progress more slowly in the insurance sector than in other business sectors.

II. GENERAL REMARKS

It is however important to point out that regulation and supervision of cyber security issues in the insurance sector concerns more sensitive issues than in other economic sectors. Insurance companies have a huge amount of sensitive customer data, such as especially health data or behavior patterns of policyholders. Cyber security incidents can therefore potentially have extensive social and societal impacts, when for example pension funds or health insurance cover is affected. Therefore, smart insurance contracts will only catch on for the general public when related relevant cyber risks can be minimized. Regulatory or supervisory measures are an important means in order to minimize such cyber risks and to build up trust in the functioning and the safety of smart insurance contracts.

**The opinions expressed in this publication are those of the author*

The following outlines shall give an overview about the existing legal and regulatory framework against cyber risks in the insurance sector and how this framework can be applied on smart contracts. With the aim to understand the legal challenges concerning cyber security supervision in the insurance sector, it is useful to outline the most important cornerstones of the relevant legal frameworks in Switzerland and Liechtenstein first.

III. Legal Framework of Supervision of Cyber Security in the Insurance Sector

A. Legal Framework in Switzerland

As Switzerland is neither part of the EEA nor of the European Union (EU) the relevant legal framework is considerably different from all the jurisdictions around. Main legal basis for insurance supervision in Switzerland in general is the Swiss Insurance Supervision Act (ISA)) [3]. Article 22 (1) ISA ("Risk Management") foresees that supervised insurance companies shall be organized in a way that they are able to identify, limit and monitor all main risks. According to Article 22 (2) ISA, the Federal Council enacts provisions on the objective, content documentation of the risk management through an Ordinance ("Verordnung"). The Ordinance on the Supervision of Private Insurance Companies (AVO) [4] contains detailed provisions concerning the risk management of insurance companies in Article 96. According to Article 96 (2) AVO the insurance companies must identify, monitor and quantify all main risks. In addition, according to the *FINMA-Circular 2017/2* [5] ("Corporate governance – insurers; Corporate governance, risk management and internal control system at insurers") the Financial Supervisory Authority in Switzerland (FINMA) expects the insurance companies to have in place an effective framework concerning governance, as well as an appropriate risk and control environment concerning cybersecurity. In this way, FINMA can force insurers to keep an appropriate cybersecurity strategy, which considers internal standards and guidelines as well as the principle of proportionality [6].

B. Legal Framework in Liechtenstein

In contrast to Switzerland Liechtenstein is part of the EEA, even though Liechtenstein is not part of the EU. As an EEA-jurisdiction Liechtenstein is however obliged to implement all the European directives, such as for example the *Solvency-II-Directive* (Directive 2009/138/EC) [7]. In addition, European implementing or delegated regulations are directly applicable in EEA-jurisdictions. Article 258 (1) lit. j of the Delegated Regulation (EU) 2015/35 – which is directly applicable in Liechtenstein – foresees that insurance undertakings must *safeguard the security, integrity and confidentiality of information*, considering the nature of the information concerned. In addition, there is the so-called NIS-Directive (Directive on the Security of Network and Information Systems) [8], which includes provisions for the insurance sector, especially concerning risk management culture between economically connected companies and concerning the enhancing of national cyber security. Finally, there is also the General Data Protection Regulation (GDPR) [9] with extensive provisions concerning the handling of data and information in general and concerning reporting measures in the event of data loss due to cyber security issues. Beside the European legal acts, the relevant national legal acts within insurance supervision law must be considered, such as especially the national Insurance Supervision Act (L-ISA) [10], which implements the Solvency-II-Directive on a national level. According to Article 35 of the Insurance Supervision Act, an insurance undertaking must be organized in such a way that it is able to assess, report, quantify, limit and monitor all significant risks. In short, insurance companies must have in place an effective risk management system, including an effective system against cyber risks.

IV. Smart Insurance Contracts and Supervision of Cyber Security

A. About Smart Contracts in General

The concept of smart contracts was already defined in 1996 by [11] as a "set of promises, specified in digital form, including protocols within which the parties perform on these promises". The general objective of a smart contract can be defined as the satisfaction of common contractual conditions (e.g. payment terms, periods, confidentiality, or even enforcement clauses), minimize exceptions, with malice or accidental, and minimize the need for intermediaries, such as for example insurance brokers. In short, smart contracts can be defined as computer programs regulating the rights and obligations between two or more parties [12]. Smart contracts are often (but not necessarily) linked to blockchain. The legal classification of smart contracts is however still disputed and inconsistent. In general, smart contracts *cannot be considered as contracts in the legal sense*, as a legal contract must necessarily be based on two corresponding declarations of intent [12]. The legal uncertainty concerning the classification of smart contracts may be one main reason why insurance products based on smart contracts are still very rare within the insurance industry. One of a few blockchain-based insurance products for the general public is for example "Fizzy", the smart insurance product of AXA against flight delays, which has probably been the first blockchain-based insurance product on the market [10]; even though "Fizzy" must be considered as a kind of hybrid solution between a purely blockchain-based insurance and a traditional insurance product, as it is based on a classic written insurance contract between AXA and the policyholder. Regarding smart insurance contracts it remains to mention that there is especially also the question for the supervisory authorities if and to what extent smart insurance contracts can or must be supervised under a given legal framework.

B. Cyber Security Supervision Guidelines and Frameworks

As a smart contract is just a computer program that implements certain rules with blockchain at the occurrence of a certain event requiring a software client, there is

vulnerability related to every smart contract. Consequently, there is an inherent risk related to all smart insurance contracts and a growing challenge, which must be addressed by insurance supervisors.

As we have seen, the relevant legal framework in Switzerland or in the EU do not clearly mention, how cyber security must be supervised in practice. The supervisory authorities must define their inspection and examination practices on guidelines or frameworks from multiple sources, such as for example the G7 Fundamental Elements of Cyber Security for the Financial Sector (G7FE) [14], the related G7 Fundamental Elements for Effective Assessment of Cybersecurity for the Financial Sector (G7FEA) [15] or the CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures (CPMI-IOSCO Guidance) [16]. There are various other private or public sets of guidance or frameworks, which have been published in order to assist supervisors in their approach to an efficient supervision of cybersecurity[1]. Many of these frameworks explicitly states that financial supervisors within and across jurisdictions can use its elements to guide their regulatory and supervisory efforts[2]. In general, G7FE – which can be divided in seven different subsections (elements) – can be considered as a useful and generally accepted framework for insurance supervisors to organize their management and their assessment of insurance sector cyber security standards. In the following we will especially focus on Element 1 of G7FE as one of the key elements of G7FE.

C. *Element 1 of G7FE*

According to Element 1 of the G7FE all insurance undertakings must establish and maintain *a cybersecurity strategy and framework* with the aim to define how to identify, assess, manage and reduce cyber risks in an integrated and efficient manner. Insurance supervisors should especially examine in a risk-based and proportionate way if the cybersecurity strategy of the insurance company clearly articulates principles regarding how the insurer intends to address cyber risks. In other words, the insurance company should be able to anticipate, to detect and to recover from cyber security incidents and to limit in this way the likelihood or impact of such an incident, which could damage the operations of the insurer and the data privacy of its stakeholders [6]. Regarding smart contracts, this means that the insurance undertaking must be able to identify and manage the relevant risks related to smart insurance contracts. Risks related to smart contracts can be divided in *operational risks*, *technical risks* and *cyber security risks* in the narrow sense. When using a broad definition of cyber risks, *all operational risks originating in information stored on data carriers or in networks*, can be considered as cyber risks [17]. In this way, also legal risks or regulatory issues, such as for example legal disputes or liability issues related to the smart contract, can be classified as cyber risks. Consequently, cyber security framework documentation must define how the insurance company identifies and quantifies these potential risks related to the smart contract and how they can be mitigated and managed.

1 For an overview of the most relevant frameworks and sets of guidance, see e.g. [6].

2 See e.g. [14, p. 1].

More concretely, this means for example that an insurer must be able to quantify the probability that a smart insurance contract cannot be executed as planned (e.g. due to technological or oracle failures) and will therefore result in a legal dispute creating procedural costs and attorney fees. At the same time, the insurer must foresee mitigation measures, such as for example the introduction of specific clauses within the smart contract or an underlying contractual agreement.

In Switzerland and in Liechtenstein the financial supervisory authority (CH: FINMA/LI: FMA) has the possibility to urge insurers to have in place an efficient and proportionate cyber security strategy and framework. The financial supervisory authority (or appointed third parties) can also undertake *in-depth on-site cyber risk reviews*. Depending on the results of these on-site reviews, the insurance company can be obliged to elaborate an action plan in order to eliminate deficiencies detected at the occasion of the in-depth on-site review by the authorities or the appointed third parties. In future, such cyber risk on-site reviews will become more important – especially because the scope and the quantity of insurance business based on smart contracts (or other blockchain applications) will certainly grow in future. Especially regarding Element 5 of G7FE (Response) the insurance companies must elaborate strategies and measures in order to assess and mitigate the impact of a cyber incident in a given jurisdiction concerning external stakeholders, including policyholders and customers in general [6].

V. Potential Socio-Political Impacts in the Face of Brexit and Conclusion

As a result of UK's potential withdrawal from the European Union, the underlying legal framework for insurance companies in UK will probably radically change. The Solvency-II Directive and all relevant European regulations, especially Delegated Regulation (EU) 2015/35, will not be applicable anymore in UK. On the one hand the result will be a certain loss of legal certainty – at least in the short and medium term; on the other Brexit gives the opportunity to adopt legal frameworks and guidelines, which are more favorable and less rigid concerning the development of smart insurance contracts (and other applications of insurtech) without compromising the cyber security framework. As a first step, it would be therefore important to reduce legal barriers and uncertainty concerning the implementation of smart (insurance) contracts and to aim at *the recognition of smart contracts as generally accepted legal contracts*. At the same time, private law, especially contractual law, needs to be linked with public law, especially financial supervision law, in order to minimize cyber risks related to smart contracts. Such an approach would help to build up *trust* for the general public in smart contracts – as a precondition for the breakthrough of smart contracts within the insurance market. Concerning the implementation of the legal framework, UK can be inspired to some extent by Swiss insurance supervision regulation. The Swiss insurance supervision system is considered as equivalent with the Solvency II-Directive [18], containing at the same time a

certain flexibility and regulatory adaptability due to the specific legal and political structures in Switzerland.

From a technical point of view, it is already possible today to conceive and design various kind of smart insurance contracts, not only non-life insurance products (such as for example products against flight delays as mentioned above), but also life insurance products with third-party beneficiaries or liability insurance contracts [See 19]. However, the challenge today is the practical implementation of these contracts in practice for the general public under the current legal framework within the insurance sector – an economic sector, which is in general highly regulated and where the legal barriers for new insurance undertakings or new products are high, especially in the EU. Brexit provides the opportunity to undertake fundamental changes of the legal and regulatory framework in the UK with the aim to facilitate the breakthrough of smart insurance contracts (and other insurance blockchain applications) while maintaining a high level of cyber security in the insurance sector. It is important to mention, that such a new regulatory or legal approach toward the classification of smart contracts must not be detrimental to the interests of the consumers and other stakeholders. However, it can be expected that *a specific legal and regulatory framework* for smart insurance contracts and other blockchain applications would increase legal certainty on the one hand and provide several benefits for the consumers on the other. As mentioned above, smart insurance contracts define for example more transparently whether and under what conditions a claims payment will be made to the insured persons.

Even though some insurance products are more suitable for blockchain-solutions than others, there is a huge potential long-term socio-political impact of smart insurance contracts: they allow for example the automatic transfer of assets to the policyholder without an intermediary (such as an insurance company or an insurance broker), which improves transparency and reduces considerably administrative costs for the policyholder. These cost savings can make certain insurance coverages affordable for a wide public (such as for example smart crop insurance [20]). In this way smart insurance products can help to *promote social equality*, as the insurance premium will be mainly used in general to cover the insured risk (instead of administrative costs).

REFERENCES

[1] Gatteschi V. et al. 2018. Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?, *in* Future Internet, 10(2):20, DOI: 10.3390/fi0020020.

[2] Wilson Reavis III, M. 2012. Concepts and Coverage, Property, Liablity, Life and Risk Management, FriesenPress, Victoria, Canada.

[3] Versicherungsaufsichsgesetz (VAG) vom 17. Dezember 2014 (SR 961.01), https://www.admin.ch/ch/d/sr/c961_01.html.

[4] Aufsichtsverordnung (AVO) vom 9. November 2005 (SR 961.011), https://www.admin.ch/opc/de/classified-compilation/20051132/index.html.

[5] FINMA-Circular 2017/2 [5] (Corporate governance – insurers), https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2017-02.pdf?la=en.

[6] International Association of Insurance Supervisors (IAIS), Application Paper on Supervision of Insurer Cybersecurity, November 2018, Basel, Switzerland.

[7] Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32009L0138.

[8] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS-Directive), http://data.europa.eu/eli/dir/2016/1148/oj.

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), http://data.europa.eu/eli/reg/2016/679/oj.

[10] Versicherungsaufsichtsgesetz (VersAG) vom 12. Juni 2015

[11] Szabo, N. 1996. Smart Contracts: Building Blocks for Digital markets, *in* Extropy Magazine #16, 1996.

[12] Trüeb, H.-R. 2018. Smart Contracts *in* Grolimund, P. et al. (Ed.) Festschrift für Anton K. Schnyder 2018. p. 723-734, Schulthess, Zurich, Switzerland.

[13] Fizzy by AXA, https://fizzy.axa/en-gb/, 2019.

[14] G7 Fundamental Elements of Cybersecurity for the Financial Sector. https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf?69e99441d6f2f131719a9cada3ca56a5.

[15] G7 Fundamental Elements for Effective Assessment of Cybersecurity for the Financial Sector, http://www.g7italy.it//sites/default/files/documents/G7%20Fundamental%20Elements%20for%20Effective%20Assessment%20of%20cybersecurity%20in%20the%20financial%20sector.pdf.

[16] CPMI-IOSCO, Guidance on Cyber Resilience for Financial Market Infrastructures, https://www.bis.org/cpmi/publ/d146.pdf.

[17] Biener, C./Eling, M./Matt, A./Wirfs, J. H. 2015. Cyber Risk: Risikomanagement und Versicherbarkeit, Institut für Versicherungswirtschaft, Universität St. Gallen, Switzerland.

[18] FINMA, EU recognises Swiss insurance supervision as equivalent, 5 June 2015, Press Release, Berne, Switzerland https://www.finma.ch/en/news/2015/06/20150605-eu-recognises-swiss-insurance-supervision-as-equivalent/.

[19] Wendling, L. A. 2019. Contracts: Legal Principles and Practical Applications for Paralegals, Kluwers Law, Alphen aan den Rijn, Netherlands.

[20] Financial Times, Bird, J. 2018. "Smart" insurance helps poor farmers to cut risks – Blockchain will enable cheaper and simpler cover, 5 December 2018, https://www.ft.com/content/3a8c7746-d886-11e8-aa22-36538487e3d0.