I.   INTRODUCTION, BACKGROUND, AND ACTIVITY IN 2019

The EU-US Insurance Dialogue Project's Big Data Working Group (WG) has been focusing on aspects of the relationship between innovation, technology, and insurance, specifically: (1) the increased use of large data sets (Big Data) by insurers; and (2) the use of data analytics in the insurance sector. The penetration of data-driven technologies is seen in almost every segment of the insurance value chain. New technology that relies on the collection and analysis of Big Data is allowing for innovation in the insurance sector in a variety of contexts, including rating, underwriting, marketing, and claim settlement.

The Big Data WG published a paper in 2018 providing the reader with a better understanding of what data is collected, how it is collected, data portability, data quality and how it is made available and used by both insurers and third parties.[1]

Building on the work done in 2018, the Big Data WG spent 2019 discussing third-party vendor issues, including regulatory oversight of insurers' use of third-party vendors, how the regulatory framework addresses big data accuracy concerns and the ability of insurance supervisors to monitor new vendors operating in the insurance marketplace. Further, the Big Data Working Group discussed disclosures to applicants and policyholders about how rating factors and third-party vendor reports are being used and the opportunities for applicants and policyholders to correct potential errors, while at the same time respecting insurer's intellectual property rights, such as in the use of credit score reports. Finally, the Big Data WG discussed insurers' use of artificial intelligence (AI) models. This report provides a summary of the Big Data WG discussions since publication of the 2018 paper and outlines proposed next steps for 2020-2021.

A.   <u>Third Party Vendor Issues</u>

Regulators in the US and EU hold insurers responsible for their use of third-party vendors for operational decisions. Insurers cannot cede their responsibility to the third-party vendors with whom they contract.

In the US there is broad market conduct examination authority in the context of third-party vendors. Contracts between insurers and third-party vendors assuming a business function or acting on behalf of an insurer must comply with applicable licensing requirements, statutes, rules and regulations. Such contracts must also specify the responsibilities of the vendor regarding record keeping. Insurers are responsible for ensuring data sources do not collect or utilize prohibited data and that underwriting or rating guidelines are not unfairly discriminatory. An insurer should not rely on a third-party vendor's assessment that the use of non-traditional insurance data points, such as a

---

[1] EU-U.S. Insurance Dialogue Project, *Big Data Issue Paper* (October 31, 2018), https://www.eiopa.europa.eu/sites/default/files/publications/pdfs/big_data_issue_paper.pdf.

consumer's purchase history or internet activity, is not a proxy for the use of a prohibited factor, such as race, religion, or national origin.

In the EU, in May 2019 EIOPA published a thematic review on the use of Big Data Analytics (BDA) in motor and health insurance.[2] The thematic review showed how the use of data outsourced from third-party data vendors and their corresponding algorithms used to calculate credit scores, driving scores, claims scores, etc. is relatively extended. Insurers ensure the accuracy and lawfulness of this data by performing their own data quality checks and via specific clauses included in the outsourcing contracts. The thematic review also showed how European insurers increasingly make use of third-party service providers to quickly and efficiently gain access to new technologies and business models. It should be noted that the Solvency II Directive clearly establishes that insurers remain fully responsible for all the activities that they outsource. In the particular case of cloud computing service providers—which often offer to their customers not only data storage services but also other services such as machine learning (ML) applications—the outsourcing of such critical services raises a number of challenges, including but not limited to concentration and potential financial stability risks. In this regard, EIOPA published Guidelines on outsourcing to cloud service providers in order to clarify to the market supervisory expectations on issues such as materiality assessments, the need to develop exit/contingency plans, or notification requirements.[3]

B.   Disclosures to Applicants and Policyholders

There are several US and EU regulations and initiatives in place and underway relating to maintaining and enhancing consumer protections relative to consumer disclosures.

In the US, the *NAIC Insurance Information and Privacy Protection Model Act* provides standards for the collection, use and disclosure of information gathered in connection with insurance transactions.[4] This model act requires insurers to alert consumers of the insurer's information practices and gives consumers the right to request that an insurer: (1) give access to recorded personal information; (2) disclose the identity of the third parties to whom the insurer disclosed the information; (3) provide the source of the collected information; (4) correct and amend the collected information; (5) amend the personal information; and (6) delete the collected personal information. Recognizing the need to address current marketplace issues impacting data privacy such as the use of Big Data and AI in insurance, the NAIC has created the Privacy Protections (D) Working Group[5] to review state insurance privacy protections regarding the collection, use and disclosure of information gathered in connection with insurance transactions and to make recommended changes as needed to certain NAIC models including the *NAIC Insurance Information and Privacy Protection Model Act* and the *Privacy of Consumer Financial and Health Information Regulation*. As part of this work, the Working Group is reviewing state data privacy legislation, the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) to understand what broader

---

[2] https://www.eiopa.europa.eu/content/big-data-analytics-motor-and-health-insurance.

[3] https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers_en.

[4] In addition to U.S. state insurance regulatory protections there are federal provisions in place relating to consumer disclosures. The Fair Credit Reporting Act (FCRA) is a federal law passed in 1970 that helps to ensure the accuracy, fairness and privacy of the information from consumer reporting agencies and applies to the use of a credit report or a consumer report in the business of insurance. Under the FCRA consumers have a right to know what is in the file, to ask for a credit score and the right to dispute incomplete or inaccurate information.

[5] https://content.naic.org/cmte_d_ppwg.htm.

privacy requirements and consumer rights might be appropriate for the collection, use and disclosure of information gathered in connection with insurance transactions and whether these are appropriately addressed in NAIC models.

In the EU, the GDPR entered into force in May 2018. The GDPR establishes strong disclosure requirements for insurance undertakings vis-à-vis consumers, including among other things the need to inform consumers about the types of personal data that they are processing, the purposes of such processing, and the right that consumers have regarding this processing (e.g., right to object to the processing or the right to erasure of their personal data). European insurers often need to obtain explicit consent from consumers to use their personal data; this consent is commonly done via terms and conditions of their insurance policy or via dedicated privacy notices (which can be several pages). In addition, some national jurisdictions such as Belgium ask insurance undertakings to disclose on their websites the segmentation criteria used for certain insurance lines of business.

C.   Insurer Use of AI Models

AI is being used in insurance for marketing and sales (e.g., better identification of consumer behavior and instant quotes), underwriting (e.g., traditional loss data and new data sources), risk mitigation (e.g., use of IoT data evolving from detection to prevention), and claims (e.g., use of images and chatbots). These new uses for AI in insurance bring accompanying potential benefits (e.g., speed of decisions, accuracy of decisions and consistency of decisions) but also potential concerns (e.g., inaccurate incomplete or biased data, consumer privacy issues and lack of transparency and disclosure).

In the US, while insurers using AI are subject to existing regulatory frameworks preventing unfair trade practices and prohibiting unfair discrimination (e.g., rates produced by AI systems must not be excessive, inadequate or unfairly discriminatory), as well as data retention laws, state regulators recognize the benefit of developing high level principles for the use of AI in insurance. Therefore, the NAIC has created the NAIC Artificial Intelligence (EX) Working Group to study the development of AI, its use in the insurance sector, and its impact on consumer protection and privacy, market-place dynamics, and the state-based insurance regulatory framework.[6] The Working Group is developing AI principles specific to insurance and is referencing the OECD AI Principles already adopted by 42 countries as a starting point. In addition, the NAIC's Producer Licensing (D) Task Force[7] is developing a white paper discussing the role of chatbots and AI in the distribution of insurance and the regulatory supervision of these technologies. The white paper will provide some examples of the use of chatbots and AI in the US market and how the regulatory framework for the licensing of insurance intermediaries applies to these activities. In addition, the Federal Insurance Office discussed AI and complex models at length in its 2019 *Annual Report on the Insurance Industry*.[8]

In the EU, European insurers are quickly adopting AI/ML technologies across the insurance value chain, mainly in pricing and underwriting, claims management (including fraud prevention) and

---

[6] https://content.naic.org/cmte_ex_ai_wg.htm.

[7] https://content.naic.org/cmte_d_pltf.htm?tab_3.

[8] https://home.treasury.gov/system/files/311/2019_FIO_Annual_Report.pdf.

sales/marketing.[9] The increasing use of ML in insurance offers many opportunities, both for the insurance industry as well as for consumers. However, even though insurance firms generally already have in place or are developing sound data governance arrangements, there are some risks that need to be further addressed in practice. This is particularly the case regarding fairness/ethical issues of ML, often related to biases in the data used to train the ML model, as well as regarding the accuracy, transparency, auditability, and explainability of certain BDA tools such as AI and ML. To address these issues EIOPA has created a stakeholder Expert Group on Digital Ethics in insurance[10], which will use as a starting point the cross-sectoral AI ethical principles developed by the European Commission's High Level Expert Group on AI (HLEG)[11] and assess how they can be made operational in concrete use cases in insurance. EIOPA is also assessing how ML algorithms can be best supervised in practice, in order to promote supervisory convergence in this area amongst European national supervisory authorities. Moreover, as a follow up of the work of the HLEG, the European Commission is continuing its cross-sectorial work in this area and has recently published a White Paper on AI[12]. This paper outlines the European Commission's plans to increase investment and create an 'ecosystem of excellence' to foster the uptake of AI solutions, while at the same time creating an "ecosystem of trust" with a set of standards that users of AI will need to comply with. The European Commission new Data Strategy[13] also aims to facilitate better access and sharing of data with the creation of sector-specific data spaces (including in financial services).

II.   CONCLUSION AND NEXT STEPS

After discussion, the Working Group has outlined below some areas for potential discussion in 2020/2021.

- The further development of AI principles in the US and EU respectively including ethical aspects.

- Regulatory review of predictive models, including but not limited to assessing transparency and explainability issues arising from the use of ML algorithms.

- Industry use of Big Data for fraud detection and claims settlement.

- Continue monitoring developments on third party vendors and consumer disclosure issues.

---

[9] Based on EIOPA's Big Data Analytics thematic review, BDA tools such as AI and ML are already actively used by 31% of firms, and another 24% are at a proof of concept stage.

[10] https://www.eiopa.europa.eu/content/eiopa-establishes-consultative-expert-group-digital-ethics-insurance_en?source=search.

[11] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[12] https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

[13] https://ec.europa.eu/info/publications/communication-european-strategy-data_en