Article from

International News

September 2018
Issue 75

GDPR Implications in Actuarial Work

By Petra Wildemann

Get your organisation ready! Key takeaways for the implementation of the General Data Protection Regulation (GDPR)! Is your organisation compliant and prepared?

Most articles about GDPR start with remarks about readiness and preparedness for the day when the GDPR terms are in place. However, GDPR is not new; it didn't come about from one day to the next. In 1995, the EU released the Data Protection Directive for the EU countries and Switzerland enacted the Swiss Data Protection Act. The law to protect personal data was based on the already-existing social media and big data regulations. With the increasing use of private information in a variety of social media platforms, it is becoming more and more difficult to know what and where data can be used, whether for business or other purposes, in a changing world.

The right to be removed from data and newsletter lists and the right to be "forgotten" are new elements in the new GDPR regulations. But can we be sure that the data and information have really been removed, and will not be sold from one company to another or used for marketing purposes within automated processes?

The implementation of new laws is always a hot topic for insurers, who need to identify new risks for certain groups as well as the mitigation of existing risks for other groups.

There are already cyber policies in the market. They were introduced when the insurance industry became aware of risks associated with data breaches, in particular cybercrime. Now, the insurance industry will have to think about expanding data breach coverage.

The value chain, which an insurer has in place from product design and pricing up to claims management and forensic analytics, requires the handling of personal data of the insurer's clients. Insurers know a lot about their customers' situations and—depending on the coverages of one or many policies—they even know a lot about their clients' specific patterns of behaviour.

Actuaries handle the calculation of personal data for pricing a portfolio in the life, health, pension and property and casualty (P&C) areas. Although the portfolios normally do not include the names of the clients, they do include the date of birth (DOB), gender, age, postal code and other information that is required to price the product the customer would like to buy for coverages. And here starts the dilemma: It is a common trend that actuaries use their own devices to model the portfolios in order to be faster and more secure than would be the case if large IT systems were used. But this practice entails that actuaries have access to personal data on their own devices, and that is no longer allowed under GDPR.

Consider an example of a common practice with respect to outsourcing actuarial services around the world by using different systems and environments. Most actuarial work is done via Excel sheets. This practice is common in particular when data needs to be exchanged. In order to add other risk factors to a portfolio, external service providers offer valuation and modelling whereby Excel sheets including portfolio data such as DOB, national identity, postal codes and other personal information, are downloaded and sent via email or other transfer applications to the external provider. The insurance client is not aware that his/her data has been sent to another country and has no control over who (and even what) might use the data in the future. In most cases, the portfolio, which includes additional risks after the valuation, will be sent back to the actuaries at the insurance company for additional analysis. Both transfers breach the GDPR terms

should the owner of the data and information not have given consent prior to the data transfer. Every insurer has to be compliant with GDPR and has to make sure that their employers and third-party service providers can work with the GDPR terms.

Cybersecurity and GDPR are essentially one and the same topic—the common denominator is data management. Data is essential, and so is proper management of the data. Otherwise, the insurance industry is blocked from modelling the pricing of their products.

Health care is another topic where data breaches and cyberattacks are high risks. Health data is very attractive to cybercriminals because of the high price it can command in the dark web. In addition, data breaches and cybercrime or cyberattacks in the health care business attract an inordinate amount of media and public attention. And even more: Besides health data, genetic data and biometric data are also recorded for the same people in a number, sometimes a large number, of portfolios. In addition, the transfer of information includes health care providers, insurers, the pharma industry, biotech and digital tech. Often doctors or patients require a second opinion from specialists, who may not be in the same city, country or even continent. These experts—who are often called cyberdocs—must obtain the patient data, often with all information included, to do their work. Under the GDPR terms, this practice requires detailed, specific consent, as does—in most cases—the exchange of a patient's blood for an examination.

There are steps to take to profile activities in anonymizing data wherever possible, or to take data outside of the scope of GDPR, reduce profiling and refine algorithms in the actuarial and underwriting models. Interestingly, the intervention of humans in this decision-making process is also increasingly being seen, seeming to swim against the prevailing current of automatization.

Ensuring compliance requires a review of common practices to manage data, handle data and obtain consent for any new product plan for renewals. These steps are important for readiness and preparedness of the insurers to be compliant with GDPR. ■

Petra Wildemann, SAV, DAV, IFoA (Affiliate) is a qualified actuary at Arocha & Associates, a senior associate at Swift Academy and the founder and chair of the Swiss Cyber Think Tank. She is based in Zurich, Switzerland and can be reached at *pw@ArochaAndAssociates.ch*.