CRO FORUM

Big Data & Privacy: unlocking value for consumers

CROs in a changing environment

Table of Contents

Executive Summary

The scale of the collection and sharing of data has increased significantly thanks to digital solutions making new data available in huge quantity. Technology allows both private companies and public authorities to make use of data on an unprecedented scale in order to pursue their activities. As a consequence, a new EU General Data Protection Regulation (GDPR) has been endorsed in June 2016 and companies will have to apply it from May 2018. The GDPR justly provides all personal data[1] processors with a rulebook to harmonise data handling practices and gives more control of personal data back in the hands of European citizens.

Insurers are becoming digital players, although at a slower pace than companies from other sectors. Insurance data mining and analysis have found in Big Data a promising environment to enhance their capacity. Thanks to Big Data & Analytics, data from digital interaction and sensors allow better risk profiling and customer insight during both the marketing and servicing phases. This data can unlock value for consumers and lead to personalized solutions. Insurers are increasingly able to offer customized services to suit customer needs, better personalise premiums, lower costs for low-risk policyholders and improve loss prevention. Consumers, on the other hand, can benefit from insurance products on previously excluded risks. For example, as discussed in a previous Chief Risk Officer Forum paper[2], patients suffering from previously non-insurable behaviour-induced diseases could share data related to daily physical activity and nutrition to enjoy individualized care offers, or the holders of motor policies could digitally communicate the maintenance status of their cars and so receive price incentives. In such contexts, persistently safe or healthy behaviours could be encouraged and rewarded.

In this paper, two case studies on life insurance for diabetes patients and flood insurance for home owners respectively, show how previously excluded risks may be covered by insurance products developed using Big Data. These case studies highlight the challenges of data privacy and protection as it relates to the new provisions of GDPR, identifying a number of key points for further development and discussion. A narrow interpretation of the legitimate interest concept, for example, or an incomplete implementation of data portability may result in constraints limiting opportunities for insurers to use data and offer consumers innovative solutions.

Chief Risk Officers (CROs) can support the transition to the new GDPR while establishing and nurturing relationships with the relevant institutional as well as corporate stakeholders, such as Chief Compliance Officers and Data Protection Officers. On top of managing existing operational risks amplified by the GDPR, like the risk of de-anonymization or decryption of stolen data, CROs can promote the benefits of a considerate and responsible use of Big Data within a strong risk management culture, which in turn builds consumers trust through a clear understanding of how their data is used and protected.

Insurers are becoming digital players, increasingly able to offer customized services and improve loss prevention while covering previously excluded risks.

[1] According to art. 4 GDPR, personal data is defined as “any information relating to an identified or identifiable natural person”.

[2] See The CRO Forum, Big Data & Analytics: the algorithm of modern business, 2015.

1 Overview

Innovation in the insurance sector has typically been propelled by changes in social, industrial and natural environments, which have progressively increased the demand for original insurance products. Today, Big Data is promising to dramatically change the way insurers operate and interact with their customers, exponentially enhancing risk detection, prediction and management capabilities.

Big Data & Analytics represent a powerful tool to improve risk assessment and horizon scanning and is extending the playing field for insurers beyond risk transfer to include risk foresight, human behaviour prediction and customer relationship. Better understanding of risk and lower administration costs could allow insurance to be offered for risks that were previously excluded. Big Data applications can be used to identify completely new insurable risks, to steer underwriting decisions and to tackle changing risk landscapes. Insurers can therefore develop new solutions, allowing customers to enjoy more specific prices as well as customized services and to benefit from improved loss prevention.

By using Big Data technology, insurance firms can collect extensive information about customers and their risk profiles and therefore proceed with a micro-segmentation of risk. Insurers will be able to use detailed information about their customers to offer tailored insurance policies, calculate more personalised premiums and lower the cost of insurance for low-risk policyholders. Usage-based insurance models, for example, have already emerged and will further improve their risk profiling accuracy due to improved technologies.

Data from digital interaction and sensors allows a refined profiling during both marketing and servicing phases for customers who consent to this processing, thus leading to personalized solutions that better suit customer needs. Big Data & Analytics are also introducing tools to make fraud review and detection possible in areas such as underwriting and claims[3]. Insurers can therefore mitigate the costs linked to fraudulent claims and overcompensations, which ultimately are borne by honest policyholders.

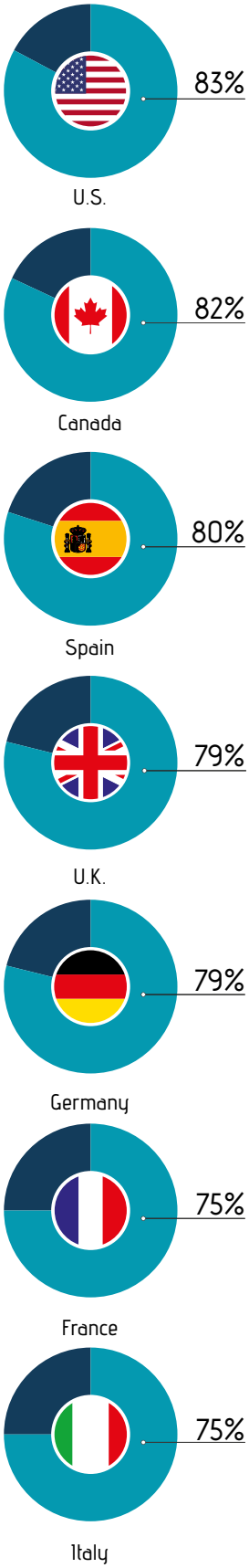
The use of Big Data raises a number of questions related to data privacy, transparency and ethical use of information. Customers should fully understand the processing of their own data.

[3] AI, Machine Learning & Pattern Recognition Help Indict 7 in $98 Million Workers Compensation Case, Ecmconnection.com, 6 June 2016

While providing a number of benefits to the society as a whole[4] , the use of Big Data by insurers also raises a number of difficult questions related to data privacy, transparency, and ethical use of information. As a matter of fact, application of the GDPR will bring some additional challenges. For global insurance groups, possible diverging national regulations on the protection, storage and transfer of data provides yet another challenge.

In order to design insurance contracts to mitigate new risks, such as for example hydrogeological or cybercrime risks consequent to climate change and the digital revolution, insurers have to understand risks nature and occurrence. For this purpose, insurance companies need to collect and process data with the goal of setting fair and competitive prices while timely meeting the demand. At the early stages of data collection though, it might not be known which data is useful and informative and which data is not, making it hard to strike a balance between minimizing data collection and providing room for innovation. Customers should in turn fully understand the processing of their own data and they should be able to give consent to its use. Insurers, accepting their data controller role, must work in a manner that is consistent with legal requirements and cultural expectations, and adopt a strong ethical conduct. Across the EU, insurance firms are expected to demonstrate that they treat customers fairly throughout the product life cycle and the value chain[5].

Compliance with the GDPR will also require strong efforts as regulation evolves alongside the evolution of data processing: use of personal data, in particular sensitive personal data, potentially leads to reputational risks. In addition, customers may be unwilling to disclose relevant data due to concerns about discrimination and unfair treatment such as undiscounted premiums or limited services.



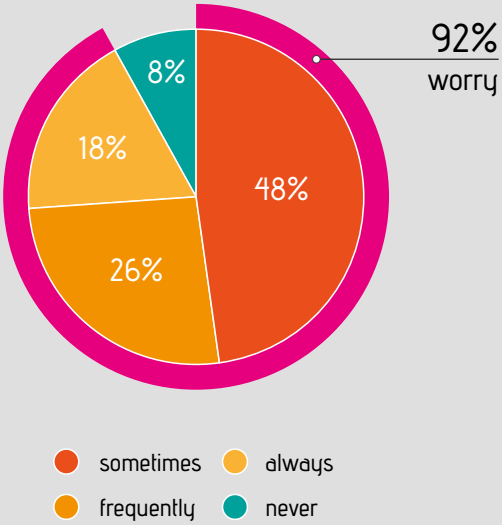
Caution: Data on Board[6]

For consumers in most countries, the privacy of personal data remains a top issue

% WHO AGREE THAT THEY HAVE TO BE CAUTIOUS ABOUT SHARING PERSONAL INFORMATION ONLINE

Consumer Concern is Rising[7]

"How often do you worry about your privacy online?"



[4] Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions, p. 21-35
[5] Regulations in Europe include FCA's guidance on fair treatment of long-standing customers, EU Insurance Distribution Directive, the EU Charter of Fundamental Rights and others
[6] BCG Global Consumer Sentiment Survey 2014
[7] TRUSTe 2015 Consumer Confidence Privacy Index

2 A New Rulebook to Empower Consumers

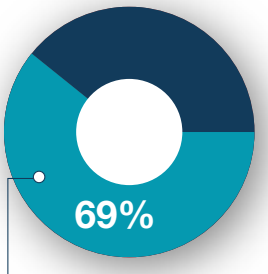
On 15 December 2015, the 28 Member States of the European Union agreed on a renewed European General Data Protection Regulation (GDPR) that will unify data privacy regulation across the European Union. Companies are expected to apply it from 25 May 2018. As a Regulation, it is directly applicable and enforceable, without the need of national legislations.

> **“The GDPR embeds numerous ethical references, from privacy as a “fundamental human right” to emphasis on values such as “fairness” and “transparency”.**

The aim of the GDPR is to have a rulebook for all data subjects and organizations, while the main political objective is to give more control of personal data back in the hands of European consumers and harmonize the practices at European level in doing so. The Regulation has broad jurisdictional reach and will apply to data controllers that are not based in the EU in a number of circumstances. This will be the case if a data controller processes the personal data of individuals residing in the EU and such processing activities relate to offering clients goods or services or are used to monitor clients’ behaviour.

The GDPR specifically provides for and encourages the drawing up of codes of conduct, by associations or other bodies representing categories of data controllers or processors. The intention is that a code of conduct will facilitate the implementation of and compliance with the GDPR. The draft code is submitted for approval to the EU Member States’ authorities.

The GDPR is a technical set of standards, but it also embeds numerous ethical references, from privacy as a “fundamental human right” to emphasis on values such as “fairness” and “transparency”, enhancing several key areas, including:



69% of Europeans are concerned that their personal data held by companies may be used for a purpose other than that for which it was collected.[8]

[8] Special Eurobarometer 431, Data Protection, June 2015

2.1 Data protection by design and by default

A culture of data protection will need to be embedded across all business areas to ensure that data protection is considered at the very first step of any new business planning and at every stage thereafter. 'Data protection by design' requires data controllers to implement appropriate technical and organisational measures to protect the rights of the data subject. Pseudonymisation[9] is referred to as a good example of data protection by design. 'Data protection by default' means data controllers must implement appropriate technical and organisational measures to ensure that only personal data that is necessary for processing for a specific purpose is processed.

2.2 Processing of Personal Data

The customer's consent to processing of Personal Data must be freely given, specific, informed and unambiguous. Subject to certain conditions, new provisions on profiling allow the data subject to unsubscribe/opt out from decisions based on profiling. The data subject will also be able to ask for a human being to intervene in the profiling, to contest a decision based on profiling, and to object to profiling for direct marketing purposes. No fee can be charged to data subjects for Data Access Requests and the response must be given within one month, with a possible extension of two months.

2.3 Enhanced Right to Erasure

Individuals will have the right to require companies to erase their Personal Data where the individual withdraws consent or objects to processing on certain grounds. However, data controllers can keep personal data on specific instances, such as compelling legitimate grounds, compliance with a legal obligation and establishment, exercise or defence of legal claims. With the balance of power now shifted from data controller to data subject, the burden of proof is on the data controller to demonstrate the legitimate interest and/or legal and regulatory reason for data retention.

[9] Pseudonymization is the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information. The additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person.

2.4 Data portability

Individuals will have the right to receive details of the personal data that they have provided to a data controller and/or to require the data controller to transmit such data to another controller (e.g. a direct competitor). An issue may arise due to how data is accessed and combined into a structured, commonly used and machine readable format. Many insurers and intermediaries hold personal data on different systems that may not be compatible with newer software. Telematics data may also be problematic, particularly given that a data standard has not yet been developed.

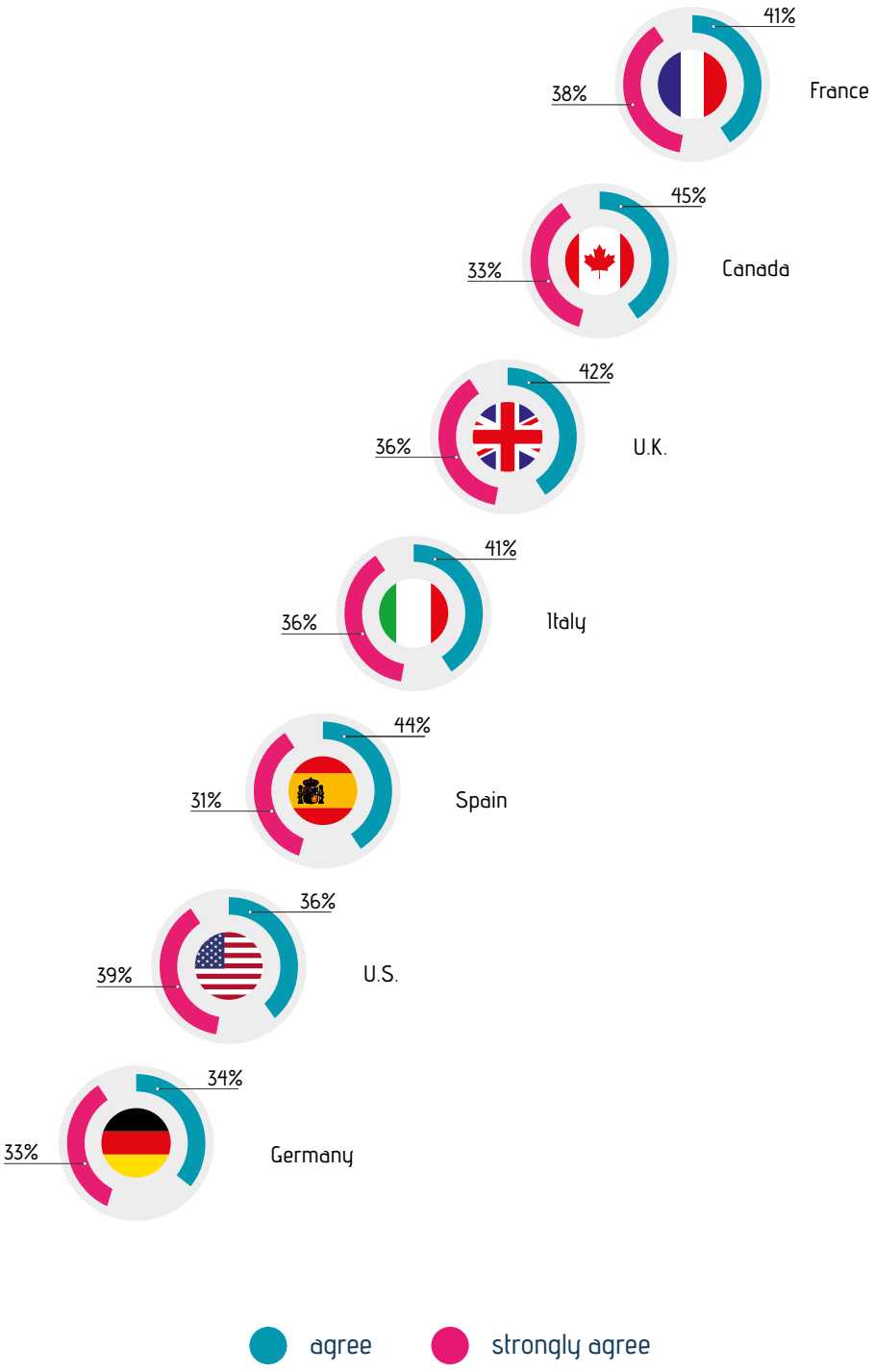
2.5 Accountability

Breaches of the GDPR may lead to significant monetary penalties, as high as 4% of a company's annual worldwide turnover. The GDPR also grants the right for compensation from the data controller or processor to any person who has suffered damages as a result of the infringement of the GDPR, including the possibility to file class action lawsuits. Member States' authorities are empowered to issue warnings, reprimands and orders, for example a ban on processing or an order to suspend data transfer to a third country. While a fine will hurt a company financially, orders could prevent undertakings from doing business and generating income.

Consumers Want Control[10]

In most countries, citizens want easy ways to shape the use of data about them

% WHO WANT SIMPLE TOOLS TO CONTROL HOW PERSONAL DATA IS USED



[10] BCG Global Consumer Sentiment Survey 2014

3 Use Cases

Life Insurance for diabetes patients

Insurance company ABC[11] Life is using existing and new data sources to launch "Diabetes Care", a new life insurance product specifically designed for diabetics. The new product is aimed at customers like John, aged 40, who suffers from type 2 diabetes and who historically has been unable to obtain life insurance.

Product Development

The product development team explored a number of different data sources to support the development of a robust underwriting and pricing model. ABC Life has been selling private medical insurance for many years and its claims experience would allow it to identify customers with diabetes (type 2) and compare their mortality probability against those of the remaining portfolio. The team is unsure if the historic consent of the medical insurance policyholders allows them to use this data for such purpose. As a possible alternative, the team is considering requesting colleagues from their US business to perform the same type of analysis on a similar US portfolio, where limitations on the use of policyholders' data are potentially less onerous.

Certain historical personal data can support product development. Clarity is needed on the admissible use of this data in the context of retrospective insurers' legitimate interest. Consent mechanisms and procedures, when required, must be practical and realistic.

Risk Assessment

Medical underwriting requires the disclosure of sensitive medical information like blood pressure, cholesterol level and smoking history in order to exclude pre-existing complications and to ensure that the risk pool remains sufficiently homogeneous.

To improve its underwriting process, ABC Life wishes to collect and store additional personal data, such as the frequency of doctors/diabetic clinic follow-ups, to include a valuable indicator to customer's diligence in managing the condition. According to the GDPR, though, customers' data should only be captured for the specific purpose for which it is intended.

Insurance firms will have to strike a balance between the data-minimisation requirement and the need to capture data for assessing risk in order to support future product innovation and development.

[11] ABC Life is a fictitious name. No identification with actual persons and companies is intended or should be inferred.

Pricing

Thanks to GDPR's new data portability regulation, the transfer of existing personal data from other sources, like from existing insurances, can be facilitated. ABC Life has decided to offer a 10% discount to any customer who is providing activity tracker data for the last 12 month period, as regular exercise is an important risk factor for diabetes and could serve as an indicator for good control of the condition. The provision of such personal data is offered as an option, in line with GDPR's principle of customers' right to object. The cost of the discount is offset by a small increase in price for other customers.

The stated intent of data portability is to empower data subjects and foster competition, as well as reduce the amount of manual data entry required by the customer. It is important to note that competition, however, does not stem from consumers' mobility only, but also from the insurers' ability to access sources of information for better product development, pricing and servicing.
Insurers should therefore be able to develop products and services that mandate or incentivise the use of data portability.

There are key aspects for the effective data portability to be clarified, such as:

- the scope of the data pertaining to the subject to be made available for transfer
- the mechanism to be used for data transfer (considering format, media and security)
- the mechanism for granting and validating customer consent to data to be transferred
- the validation of the data being transferred (how data integrity/ security is ensured)

Market operators should cooperate among themselves and with supervisors to develop good practices and standards on the exchange of data according to structured, commonly used and machine-readable formats.

Distribution

ABC Life considers traditional distribution channels less suited for identifying and acquiring customers who have historically been excluded from life insurance. A dedicated distribution strategy is considered necessary and support from the national diabetic's society is explored. ABC Life will support society campaigns with its own doctors and the society will endorse a mailing campaign to its members to promote Diabetes Care.

The obligation to ensure members' consent for the sharing of their contact details to ABC Life lies with the diabetic's society. As all members are diabetics, the personal information is considered to be sensitive. ABC Life is also working in partnership with a reinsurer to share the risk and obtain support in medical underwriting. For the policy acceptance process, ABC Life is ensuring that the policyholder's consent is provided to share all relevant data with its partner for the purpose of reinsurance.

The sharing of data with third parties under GDPR requires specific considerations for the sharing of sensitive customer information (such as medical and health information). If this sharing is strictly limited to cases of legal obligation, public interest or exercise of official authority, the impact on insurance offering can be significant. Case by case consideration and a constructive debate with regulators are needed, while the gold plating left open by the GDPR should be kept to a minimum.

Customer Service

People with good management of their diet and blood sugar level are at significantly lower risk of developing complications. Other lifestyle factors, like physical exercise and cessation of smoking play an equally important role. The Product Development team therefore designed the product to include several additional services as part of a diabetes management program, including free consulting and medical monitoring, premium discounts to customers who attend yearly medical check-ups and meet certain targets to average blood sugar level, and a personal online portal providing access to a knowledge base where customers can upload information from their activity trackers.
To incentivise the sharing of personal data and building a solid relationship, apart from providing a financial incentive at underwriting stage, ABC Life is providing tailored health advice to customers based on their individual health situations. While some customers will obtain support in increasing physical activity, others receive recipes tailored to their diets.

Clarity is needed on to what extent the customer can object to data processing. In particular, whether any objections are valid to data processing performed as public interest or legitimate interest.

Experience Analysis

Diabetes Care is the first product of its kind for ABC Life and the on-going analysis of its experience is considered crucial. The detailed analysis of customer behaviour will provide a valuable basis for the design of other new products with similar features. ABC Life has included within its consent process a statement that allows the use of customer data for statistical/ analytical purposes. Additionally, it makes reference to the future deletion and/or anonymization of that data once the policy has lapsed to support future use in experience analysis.

Anonymization and de-anonymization algorithms are not yet mature from a scientific point of view. Supervisors should consider that the Regulation relies on difficult concepts and that dialogue is needed with stakeholders to define workable interpretations and rules[12].

[12] Data anonymization is a type of information sanitization whose intent is privacy protection. It is the process of removing personally identifiable information from data sets, so that the people whom the data describes remain anonymous.

Flood insurance for home owners

Insurance company DEF RE[13] is using historical and Big Data sources to launch “Home Safe”, a new insurance for real estate homes built in areas exposed to flood risk. The new product is designed for home owners who historically have been unable to obtain flood insurance as the risk was previously uninsurable at affordable prices.

Product Development

DEF RE is using Big Data technologies to allow for more granular data/models in risk assessment. In this context, for example, satellite images offer more reliable information than postcodes to assess the actual location of real estate properties and their exposure to flooding. In getting more data to gain the necessary knowledge, some issues arise in relation to sharing customer data with third parties, especially reinsurers. According to the principle of data minimization, personal data must be adequate, relevant and limited to what is necessary to fulfil the purposes for which data is processed. Should the forwarding of personal data not be necessary for the creation, execution or termination of the contract with third parties, information should be rendered anonymous beforehand or at least pseudonymised.

Anonymised data falls out of the scope of the GDPR, whereas pseudonymised personal data is not exempt from the Regulation.

Risk assessment

The use of Big Data & Analytics may allow the inclusion of data from individual risk prevention measures, leading to a more accurate risk assessment at a lower rate and to an extended range of insurable risks. Granular segmentation modelling requires the handling of a large amount of data, potentially conflicting with data minimization, an important principle in the new GDPR. Data processing should only use as much data as is required to successfully accomplish a given task. Additionally, data collected for one purpose can only be processed for other purposes if compatible with the purpose for which data was originally collected or consent is given by the data subject. More importantly, there would not be a level playing field if non-EU insurers with non-EU customers were allowed to develop such kind of models abroad and then deploy them in Europe.

[13] DEF RE is a fictitious name. No identification with actual persons and companies is intended or should be inferred.

As of May 2018, all data processing must be in line with the GDPR new provisions and there are some uncertainties about how these provisions will be implemented for existing contracts.

Normally, the legal basis for processing personal data is the fulfilment of the insurance contract. However, the extent to which a more accurate risk assessment leading to a possible lower rate falls under the legitimate interest provisions is not obvious to determine. The insurer would need to evaluate whether a data subject could reasonably expect, at the time and in the context of the collection of the personal data, that processing for that purpose may take place. Insurers are required to strike a balance between granular modelling and data minimisation and perform impact assessments to evaluate the origin, nature, particularity and severity of risks.

Pricing

As an undesired effect of such granular risk modelling, worst risks would remain difficult to insure at affordable conditions. Accurate data allow insurers to detect risks that are in fact often affected by flood risks.

Fine risk selection can jeopardize the solidarity principle and potentially lead to negative public opinion.

Progressively, pricing is being driven less by demographic data, and more by the risk factors themselves, so segmentation becomes more granular, pricing more risk-based, and risk selection more effective. In combining existing and new data sets, there would be the chance that sub-standard risks would receive higher rates. In a worst-case scenario, this could result in preventing some consumers from being offered acceptable conditions for a corresponding insurance cover. However, this would conflict with the principle of solidarity in the insurance sector. Insurers nevertheless need to differentiate between different levels of risk, otherwise the principle of insurance/risk pooling will not work anymore. Only “bad” risks will opt for insurance and attractive risks will not, leading to ever increasing premiums and risk pools getting smaller.

Distribution

DEF RE may choose to carry out targeted advertising activities to support the efficient deployment of sales resources. In targeting mainly the non-high risk properties, proposing special offers for preferred risks, the company may be exposed to discrimination and subsequent reputational risks. On the other end, the company may alternatively approach high-risk properties with customized products including prevention measures such as higher deductibles, special exclusions, usage of sensors/drones for individual risk assessment and monitoring. The data generated would certainly entail issues regarding data minimization and explicit consent.

The data subject has to be informed about the processing for new purposes and has the right to object to the processing.

Customer relations and claims handling

DEF RE is adopting post-event estimation techniques using drones, sensors and satellite images for quick and easy claims handling. The company is including a service to support catastrophe management in high-risk zones, while collecting data from the monitoring of the impact of recovery and restoration actions to improve risk models and product development. Sharing data with third parties and explicit consent issues may also arise from the early warning system that the company is offering to the customers.

After taking preventive and privacy-preserving measures, the right for customers to restrict data transfer by early warning systems should not hamper the benefits deriving from sharing collected data. The processing of data for safety reasons in the context of public interest or legitimate interest should be carefully considered.

4 The Role of CROs

Using accurate and relevant data has always been crucial for risk-based calculations, but the emergence and adoption of Big Data tools and platforms represents a revolution in the way the insurance industry has approached risk-based calculations so far.

Artificial intelligence can analyse far larger amounts of new types of data much more quickly and accurately than individuals. From this vantage point, algorithms have an enormous potential to significantly improve the efficiency of operational and decision-making processes while providing tailored solutions to customers. As illustrated by the case study on diabetes, the use of Big Data could render historically uninsurable risks insurable, thereby improving financial inclusion. The use of Big Data could also support the society's efforts in becoming more resilient to risks, as showed by the case study on flood risk.

Insurers should approach the use of Big Data from a holistic view encompassing people, processes, technology and data. Chief Risk Officers (CROs) play a key role in ensuring that the (re) insurance strategy is designed in a sustainable way. The CROs should promote the benefits of a considerate and responsible use of Big Data in the context of a strong risk management culture, which ensures that customers understand how their data is used and protected.

Ensuring that internal policies, processes and systems are appropriate for the use of Big Data and address privacy concerns

The way Big Data is used may introduce new requirements for the governance and control of data-related risks, such as compliance, legal, and operational risk. The responsibility for oversight will need to be shared and clearly defined among relevant internal stakeholders, including Chief Compliance Officers and Data Protection Officers. The CROs should represent the second line of defence with regards to management of risks. One of the key responsibilities of the CRO should be to challenge whether internal policies, processes and systems are suitable for the use of Big Data across the entire insurance value chain. The specific properties of Big Data (volume, variety, velocity, veracity) create new types of risks that require a comprehensive strategy to enable a company to utilise Big Data while avoiding the pitfalls, such as ensuring that the data used does not include errors and is used in a responsible and transparent manner.[14] The CROs should therefore encourage business lines to assess how current data collection tools and processes address the properties of Big Data and whether these can be improved. This is particularly relevant to cloud based storage and processing solutions that an increasing number of insurers is looking to use. Other significant challenges are ensuring that the implementation of anonymization and encryption algorithms is robust and that there is data quality and accuracy through methods that need to be specified (e.g. validation) and assessed (e.g. data quality rating criteria).

Insurers have traditionally used various methods of de-identification to distance the data from individuals while undertaking a privacy-sensitive process of data analysis. Big Data enables the ability to gather and analyse data from multiple locations and sources. However, for international players it also brings the challenge of meeting different privacy regulations around the globe. It is, therefore, of utmost importance that there is collaboration among different functions to ensure that appropriate processes are in place to meet the requirements of local privacy regulations.

One of the biggest challenges to be addressed by the Risk Management function is finding the right balance between ensuring that business is sufficiently protected while at the same time not over restricted in its ability to develop innovative solutions. There is a need for the firm's management to ensure that the company has the right skill set and approach to adapting to the change and identifying new risks. Risk management needs to remain flexible and responsive as there may be unintended consequences with the use of Big Data.

Improving overall understanding of and resilience to risk both internally and externally

While new technologies could substantially increase the ability to detect emerging risks and improve risk mitigation, the use of Big Data could also lead to a number of new risks. As a second line of defence, it is important that the Risk Management function oversees that the following challenges are managed by the business:

- Address the risk that data used may be incomplete, inaccurate or insufficiently structured. If such information is used in underwriting practises, it could lead to wrong conclusions being drawn from flawed analyses. Therefore, the use of Big Data in the context of automated algorithms should be done with an understanding of the outcome, while all innovative solutions must be checked by a human employee for "soundness".

- Address risks stemming from partnerships with third-parties on Big Data related issues, such as new players in the market who are not as concerned about reputational damage as insurers. In addition, these partnerships may raise questions about the quality of data collected by third-parties and the insurers' ability to comply with the General Data Protection Regulation. As a result, if the data provided is not accurate, this may lead to both technical issues and reputation damage to insurance companies.

- Another barrier to applying Big Data analytics is the potential lack of trust between consumers and corporations, because consumers might fear losing control of what insights could be gained from their own personal information. The CROs can help promote the advantages of providing consumers with clear and transparent information, for example, on how customers will benefit from allowing their data to be used, for what purpose data is being used and how they are protected. The CROs should promote the benefits and costs of fair Big Data use to allow customers to make informed decisions.

- Mitigate the risk that, due to regulatory and non-regulatory barriers, third-parties (including customers) may have a better understanding of risk than the insurance company, which could lead to under-pricing or anti-selection. If certain customers had either more information about their risk profiles or chose not to share this information with insurers, the end result would be that other customers would have to subsidise these risks beyond a justifiable level.

[14] EY's report on "Big Data: Changing the way businesses compete and operate," April 2014

Assisting companies in defining and monitoring a stronger governance around the responsible use of data

Compliance with legal frameworks is essential for the usage of digital tools but it is often not enough. Considerations can go beyond legal and regulatory concerns, and could lead to significant reputational risks for the firm if data is not managed responsibly. Hence, insurers need to be aware of the public debate on the issues beyond regulatory matters and should develop policies that would address the concerns of different stakeholders. Such policies can also be used to reflect to what extent insurers should incentivise good practises (or punish bad behaviours) through dynamic premiums and other mechanisms. However, an open question remains whether insurance firms should incentivise behaviour changes based on correlations observed in data but where causality is not fully understood.

Some new forms of data may provide quick insights, but may not be representative of the whole population. For example, insights produced by social media may not reflect the sentiments and risks faced by certain categories of the society. In addition, data mining can inherit the prejudices of prior decision-makers or reflect the widespread biases that persist in society at large.

The patterns it discovers may simply be a reflection of pre-existing societal patterns of inequality and exclusion. Hence, it is of great importance that insurers have robust processes in place to avoid using spurious correlations discovered by Big Data in decision making.

There is also a risk that even if prohibited pricing variables such as gender are removed, other factors may act as proxies. As a result, when developing internal policies for responsible data management, CROs should take the following considerations into account:

• Data collection and use is done in a transparent way while being compliant with laws and regulations and internal intellectual property regimes;

• Business lines respect the legal requirement to get customers' consent to have their data processed for insurance purposes;

• Clearly defined and consistently applied criteria are used to strike an appropriate balance between industry or company interests and the interests and rights of individuals (e.g. how fair costing should be defined).

A clear governance structure can help ensure that a firm manages Big Data responsibly and transparently, thus avoiding the aforementioned risks. It can also guarantee that the use of Big Data is checked against norms to prevent any potential negative impact on society.

5 Looking to the Future

In so far the economy becomes more and more digitalised, the availability of data is likely to continue to increase. Indeed, technical developments such as intelligent cars, wearable devices and connected houses are still in their infancy. As they gradually develop over time, data is expected to increasingly become a key feature for the business processes of insurance institutions, and hence the value of data and its competitive relevance will increase.

Big Data may have an impact on people's personal lives and environment. Consumers are increasingly becoming aware that data about their behaviour and consumption profile may be used and influence insurance policy premiums. Consequently, consumers could modify their behaviour for the better in order to receive incentives (monetary or of a different nature) to avoid unhealthy habits, exercise more, or drive more cautiously. Big Data processes would allow segmenting consumers based on their personal characteristics, preferences, and so on, but some consumers could be left out of these clusters, for example if they refuse to share their personal information. This may result in such consumers not being offered certain products/ services or being offered products not suited to them. In addition, consumers' access to certain insurance services, and in particular their ability to switch providers, may be impaired if their data is not transferrable.

Analytical models will require adjustments to incorporate new data from evolving technologies, making data quality and governance frameworks key to avoid errors.

Insurance institutions' growing interest in the use of Big Data may also be partially attributable to the potential threat posed by (non-financial) technology companies, which have considerable amounts of data that offer valuable insights into their users. It is plausible that tech firms would expand into financial services, leveraging their own technical expertise, innovative and integrated platforms, extensive customers data or loyalty among millennials and digital natives. It is also possible that tech firms would develop more and more effective risk prevention solutions that will eventually result in unregulated insurance substitutes.

Segmentation based on datasets with missing information about certain categories of consumers or on algorithms where potential customers are statistical outliers from the expected behavioural norm, could also lead to certain groups being disadvantaged in terms of access to insurance products. Furthermore, any flaws in the veracity of data could lead to detriment for consumers and could lead to reputational and litigation costs. This risk would be accentuated in case of widespread use of Big Data, in particular where business models are based on similar flawed underlying datasets and algorithms.

Reputational risks and issues around consumer confidence in the use of personal information could also emerge if insurance institutions do not develop suitable controls around Big Data technologies or carry out the monitoring to an extent regarded as invasive or a breach of privacy. In general, failing to observe data protection requirements can lead to supervisory sanctions as well as expensive lawsuits and damage consumer confidence. Insurance institutions should therefore be paying attention to employing and training staff in the field of risk management, compliance, IT and specifically data protection.

Insurance institutions' collaboration with external tech companies, with different business models, regulatory cultures and risk appetites could also entail risks. Furthermore, analytical models will require adjustments to incorporate new data from evolving technologies, making data quality and governance frameworks key to avoid errors. Data quality checks should also cover external data. The reliability on and quality of external data will be a very important element at stake.

Conclusions

Big Data & Analytics allow insurers to (a) better evaluate risks and therefore insure previously uninsurable risks, (b) prevent, rather than financially cover, certain risks and (c) develop more personalised products and services to suit hitherto unmet consumer needs. Such benefits, however, could be hindered by certain new provisions on the processing of personal data introduced by the GDPR.

The new regulation appropriately strengthens the rights of data subjects and harmonises the rulebook, but the emphasis given to concepts like consent as a clear affirmative act, right to object, right to erasure and data minimisation can hinder innovation. Just as well, some dangers can be detected in likely market distortions. Non-EU companies that may process non-EU customers' data will enjoy far greater freedom in analysing data to devise innovative products and services; these companies would therefore transfer innovation to Europe where local companies compete at a disadvantage.

In order to mitigate the risks posed by the GDPR to the competitiveness and operations of insurers as well as to the full realization of benefits for consumers, developing new products and services based on personal data of European citizens should be recognized as a legitimate interest of insurers. In this context, cooperation between supervisors and (re-)insurance undertakings is key to unlock the full value of Big Data for insurance customers while ensuring the highest standards in data use.

Data portability should also be made viable through the adoption of good practices and standards on data exchange according to structured, commonly used and machine-readable formats, so that no market player could lock-in customers by holding their data.[15] Trade associations across the relevant sectors should therefore engage and deliver the requirements of the right to data portability.

On the other hand, insurance companies are called to act on internal policies, processes, systems and, above all, their own corporate culture to embed the principles of protection of persons with regard to the processing of their personal data. In this context, CROs play a key role in helping companies strike the right balance between operational risks and innovation opportunities, facilitating a cultural shift to help organisations implement the new concepts introduced by the GDPR (e.g. data minimisation), and actively promoting an ethical and transparent use of Big Data.

> **Developing new products and services based on personal data of European citizens should be recognized as a legitmate interest of insurers.**

[15] According to one interpretation, portability is only a palliative measure since controllers can still extract insight from personal data and then delete the data, so that portability becomes not applicable in practice.

References

ABI (Association of British Insurers) – ABI response to ICO consultation on GDPR consent guidance, 2017

ABI (Association of British Insurers) – ABI response to DCMS call for views on GDPR, 2017

BCG Global Consumer Sentiment Survey 2014

DAC Beachcroft – The European GDPR, a guide for the insurance industry, 2017

ECM Connection.com - AI, Machine Learning & Pattern Recognition Help Indict 7 in $98 Million Workers Compensation Case, 6 June 2016

Ernst & Young - Big Data: Changing the way businesses compete and operate, April 2014

ESMA (European Securities and Markets Authority) – Joint committee discussion paper on the use of Big Data by financial institutions, 2016

European Commission – Art.29 data protection working party, guidelines on the right to data portability, April 2017

European Commission – Special Eurobarometer 431, Data Protection, June 2015

Insurance Europe – Position paper, comments on profiling, 2017

Marsh & McLennan – Adviser: new data protection law in Europe, May 2016

The CRO Forum – Big Data & Analytics: the algorithm of modern business, 2015

The Insurance Institute – The Insider, issue n.2, June 2017

TRUSTe - Consumer Confidence Privacy Index, 2015

Disclaimer

The CRO Forum is supported by a Secretariat that is run by
KPMG Advisory N.V.

Laan van Langerhuize 1, 1186 DS Amstelveen, or
PO Box 74500, 1070 DB Amsterdam
The Netherlands
www.thecroforum.org