Engaging contradicting customer needs in a digital world: data based benefits vs. privacy

Claudio Stadelmann

Bartholomäus Konat

David Pankoke

It seems like the insurance industry is facing a dilemma. On the one hand, customized services which rely heavily on individual information have become more important in the digital age. On the other hand, customers become more cautious about the usage of their data and demand more privacy. In this article we discuss this paradox and ideas how to handle it.

Introduction

Digitization means employing new technologies to meet individual customer needs.[1] Subconsciously, people take the better fulfillment of their needs for granted. For example, GPS and smartphones allow all users of Google Maps to receive the necessary directions to arrive anywhere on earth. However, the privacy implications are not always welcome. It is debatable whether Google should be able to compile a movement profile of nearly every user.

This point of conflicting interests between data based benefits and customer's privacy interests is what we discuss in this article. In addition, we provide ideas of how insurers can best deal with this issue, for the sake of the customer and for the sake of the company.

Blessings of data based offerings in insurance

The risk assessment is a core function of insurance and therefore using individual data is as old as the insurance industry. For example, flood insurance has always taken into account where a property is located. Improving the accuracy of the assessment means that the safety margin for technical provisions can be lowered. This benefits not only insurers and current policyholders, but also potential policyholders. If the risk assessment becomes too inaccurate, insurance becomes unavailable. In the aftermath of the attack on the World Trade Center in New York, for example, insurance against terrorism was not offered anymore.

Self-tracking devices combined with Analytics let the insurers walk further down this road by sharing the benefits with their customers in innovative ways. In health insurance, certain devices allow the insurer to track a customer's life style and encourage maintaining a low-risk profile. Discovery Holding, a South African insurer, was one of the first to do so with its Vitality program.[2] In this program, subscribers can earn Vitality points by undertaking health assessments and exercise. The points can afterwards be redeemed for various benefits such as discounts on flights.[3] Dacadoo, a start-up, goes even further and offers individuals a health index based on sport, eating, sleeping and stress habits. The idea is that policyholders of participating health insurers receive premium reductions based on their lifestyle as measured by this index.[4] In Switzerland, for example, CSS is offering such a scheme.

Another insurance related topic, where Big Data and better risk classification offer direct benefits to consumers, is telematics. Young male drivers normally have to pay the highest motor vehicle insurance premiums, since statistically they are the group of most reckless drivers. As a consequence, a young male, who is a responsible and cautious driver, pays too much for insurance. Telematics, however, allows the insurance company to assess his risk profile directly by examining his driving style and to charge him a lower premium. Last but not least, insurance as-you-go is possible if the customer is prepared to share data in real time. For example, an insurer could offer travel insurance which

The authors

Claudio Stadelmann, Senior Manager Insurance, BearingPoint.

Bartholomäus Konat, Business Consultant Insurance, BearingPoint.

Dr. David Pankoke, Business Consultant Insurance, BearingPoint.

Existing regulation (written rules)	Privacy frameworks (implied rules)
• CH: - «Datenschutzgesetz (DSG)» - Further sectoral regulations: «Informationsschutz-verordnung», VAG • EU Data Protection Directive: - Basic framework for proper handling of personal data - Contains adequacy requirements that prevent the transfer of personal data to entities outside the EU that do not comply with EU standards for privacy protection • UK Data Protection Act: - Principle of fairness - Transparency in collection and purpose of usage • US: - Sectoral approach (examples: HIPAA, US-EU Safe Harbor Framework) • Others	• OECD privacy principles: - Collection limitation: imposes limits to the collection of personal data - Data quality: data is accurate, complete and kept up-to-date - Purpose specification: no later than the time of data collection - Use limitation: not to be disclosed, made available or used other than specified - Security safeguards: against such risks as loss, unauthorized access, etc. - Openness: about developments, practices and policies - Individual participation: rights of individuals regarding their data - Accountability: for complying with data privacy principles • APEC privacy framework: - Collection limitation: imposes limits to the collection of personal data - Integrity: data is accurate, complete and kept up-to-date - Notice: provide clear and easily accessible statements about practices and policies - Use of personal information: used only to fulfill the purposes of collection - Security safeguards: prevent misuse of information - Choice, access and correction: rights of individuals regarding their data - Accountability: for complying with data privacy principles

Figure 1: Data privacy regulations

is automatically activated when the policyholder is entering certain countries and deactivated when he leaves. In combination with a country specific pricing, this product would offer tremendous added-value. Insurance coverage would always be there when needed, but never when unnecessary.

Data privacy is a right, not a luxury

The benefits of Big Data and Analytics come at a cost: personal data has to be revealed in an unprecedented scale. As a consequence, people have become more and more suspicious about the side effects of this extraordinary data gathering.

90 percent of Europeans favor harmonized data protection rights. Just recently this demand was met in the European Union by the General Data Protection Regulation which came into force in 2016 and has to be applied by 2018. Basically, the new regulation strengthens the citizen's self-determination with regards to personal data. It follows the trend of evolving privacy regulations on national and supranational level as shown in Figure 1.[5]

We at BearingPoint believe that especially two issues raise concerns for customers: opacity of data handling and data security. According to a survey initiated by Bitkom Research, about 37 percent of (German) citizens who are using fitness trackers on mobile devices are willing to share their data with their health insurance company.[6] Consequently, gathering personal data is not an issue itself, though we believe that if the data is used for purposes which are not expected by the customer, this might be problematic. Stefan Weiss, Global Data Protection Officer at Swiss Re points out: «Clients trust and expect us to handle their personal data with great care. This is one of the most important motivating factors for why compliance with data protection law and regulations is very close to our hearts and our minds all the time. In response, Swiss Re has a comprehensive Data Protection Compliance Framework with policies, guidelines, training and enabling support in place to support its staff in the daily work when processing personal data.»

The same is true in the case of data security. Customers might be willing to provide highly personal data to a trusted health insurer. However, if a data breach occurs, the trust that has been built over a long time can vanish in seconds. To ensure a safe environment for sensitive data, special actions have to be taken. According to Roland Lüthi, Head of Private Clients and member of the board at Visana Health Insurance, «several repetitive actions are needed to sharpen employee's awareness for the topics of compliance, information and data security. Therefore, Visana provides a number of guidelines as for the usage of social media or the handling of sensitive data. Furthermore, each employee is obliged to pass different physical as well as e-learning trainings to be prepared for the correct data handling in terms of security.»

Addressing the paradox

We at BearingPoint believe the following aspects are important for insurers in addressing these contradicting needs for data privacy and service offering.[7]

- Be transparent when handling data: It is important that the customer understands for which purpose and in which way his data is used. Due to the growing awareness of customers regarding this topic, it is necessary for insurers to focus on transparent communication, so that the customer's trust and loyalty are granted.
- Receive affirmation for gathering data: Clearly ask customers for consent to share data and give them the

ability to delete data if necessary. Generally, allow customers to stay in control. This ensures their peace of mind and prevents the feeling of being lured in some murky deal.

- Protect personal data: Data breaches should not be taken lightly. In the time of cloud computing, this can be disastrous both for the customer and the company. Just think of Ashley Madison, an online dating website for married people, which got hacked.[8] An insurer losing sensitive data could have a comparable trust issue.
- Be responsible: Complying with regulation and acting upon the values of the customers is an absolute necessity. For Roland Lüthi this means to «create a culture regarding data privacy and security as a foundation distinguished by good faith, legitimacy, a common purpose and appropriateness.»

Based on these principles, BearingPoint developed an information management approach to effectively handle the challenges of data based benefits vs. data protection as shown in Figure 2.

The first step of the information management approach is to assess the current information landscape. This means identifying the data owner, systems and people having access to the data. The next step is to classify the different information domains and to set up a classification framework. This is followed by a risk assessment of each domain. It takes into account not only the probability and damage for the data owner in case of a data breach or privacy issue, but also the willingness to be exposed to such a risk. In the fourth step goals are set according to every attribute relating to data privacy issues in the information domains, like cost, time, acceptable risk and compliance with guidelines. Last but not least, actions are defined to reach these goals, implemented and monitored.

Conclusion

In the digital age there is an increasing demand for customized services which rely heavily on Big Data and Analytics. The insurance industry is no exception in this regard and the future will bring many services based on policyholders' personal data. We believe that trends such as telematics or insurance as-you-go are only the beginning and that customized insurance products are the future.

At the same time, there is a growing concern of data privacy issues and customers yearn for more self-determination with regard to their personal data. This seems to be a paradox, because some services are only possible if highly personal data is shared. For example, granting a cautious driver belonging to a high risk group premium reductions is barely possible without monitoring his driving behavior.

We at BearingPoint believe that insurers can best deal with this situation by respecting the customer's self-determination with regard to personal data and taking the matter seriously. This means that the insurer should not act in the shadows but in the bright sun light and focus on two aspects: First, making sure that the policyholder understands and agrees with the personal data which is gathered. This includes the possibility to erase data when requested by the customer. Second, being trustful and protecting policyholder's data is key. The customer needs to feel confident that his data is safe and his concerns are taken seriously. This implies that the insurer is not only complying with all data regulations, but also takes into consideration what is deemed legitimate. In this way, we believe, insurers can meet both the needs for customized services and enhanced privacy.

Notes

1 See: Berger, Daniel; Broer Patrick and Pankoke, David «Digitization in life insurance: a prerequisite for success in spite of low interest rates», in: Institut für Versicherungswirtschaft der Universität St.Gallen (Hrsg.), I·VW Management-Information – St.Galler Trendmonitor für Risiko- und Finanzmärkte, I/2016, pp.15–19.

2 See: https://www.discovery.co.za/portal/individual/vitality-how-it-works-overview

3 For a detailed discussion of the benefits and risks of Big Data in health insurance see Markus Franke and Marcel Nickler, «Digitalisierung: Big Data in der Krankenversicherung», in: «Handbuch Consulting 2016», pp. 108–111, Jonas Lünendonk and Hans-Peter Canibol (ed.), 2016, Fakten & Köpfe Verlagsgesellschaft mbH, Kelsterbach.

4 See: https://www.dacadoo.com/?lang=de

5 For more information about the General Data Protection Regulation see http://ec.europa.eu/justice/data-protection/reform/index_en.htm and about other privacy regulations ISACA, Data Privacy and Big Data – Compliance Issues and Considerations, Volume 3, 2014.

6 https://www.bitkom.org/Presse/Presseinformation/Gesundheits-Apps-Jeder-dritte-Smartphone-Nutzer-wuerde-Daten-an-die-Krankenkasse-weiterleiten.html

7 See also Falque, Eric and Williams, Sarah-Jayne, «Adressing Customer Paradoxes in the Digital World», p. 30, 2011, Pearson Education France.

8 See https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/

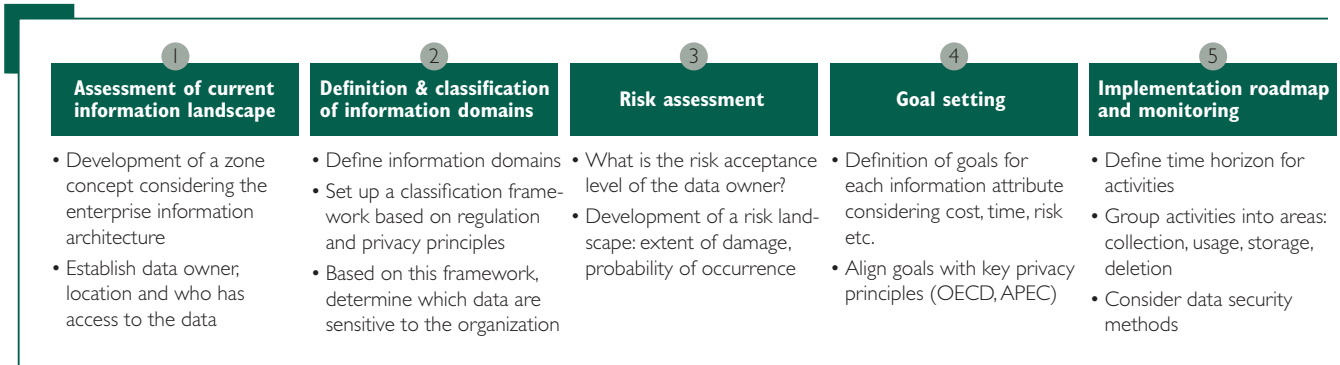

Figure 2: Information management approach for effectively handling data privacy issues