Privacy, software and insurance

Privacy, software and insurance

Sara Landini

Abstract: This paper deals with the use of software in insurance production and distribution considering the privacy issues that can arise. With regards to those uses we will consider on first the use of software in distribution in order to better perform the compliance with the regulations in insurance distribution (submission of information documents, administration of questionnaires on demands and needs to clients, registrations of contracts, payments etc.) and on second the use of software to reduce cyberisk on clients, insured with a cyberisk policy, or the use of software to supervise the activity of the insured person in order to assess the risk over the duration of the contract and possibly regulate the premium. In these cases, specific clauses in the contracts regulate the use of such software in order to obtain premium reductions. New privacy issues arise from the application of software in insurance that we are going to consider.

1 Definitions

What is a software and when we can use properly the term software applied to insurance? Software comprises the entire set of programs, procedures, and routines associated with the operation of a computer system. The term differentiates these instructions from hardware, the physical components of a computer system.

Software is often divided into categories. System software is a computer program designed to run a computer's hardware and application programs. System software coordinates the activities and functions of the hardware and software. In addition, it controls the operations of the computer hardware and provides an environment or platform for all the other types of software to work in.

Application software is a computer software package that performs a specific function for an end user or, in some instances, for another application. An application can be self-contained or a group of programs. The program is a set of operations that runs the application for the user. Applications use the computer's OS and other supporting programs, typically system software, to function. Application software is different than other software that might come pre-bundled with a computer's operating system, such as a utility.

Application software refers to user-downloaded programs that fulfil a want or need. They include office suites, database programs, web browsers, word processors, software development tools, image editors and communication platforms. Another category of software are the utilities, which are small, useful programs with limited capabilities. Additionally, some utilities come with operating systems. Like applications, utilities tend to be separately installable and capable of being used independently from the rest of the operating system.

System software includes operating systems and any program that supports application software. It is also important to distinguish the term software from software engineering. Although the terms computer science and software engineering are often used interchangeably, they are not the same. Computer science is the field of computing that deals with the study, implementation and analysis of algorithms. Software engineering, on the other hand, focuses on applying structured engineering principles to the development of software. In any case, Software engineering is directly related to computer science, where engineers take systematic and disciplined methods to the development, operation and maintenance of software.

We will focus application software used for specific needs of insurance industry.

And now what is an insurance contract and why software is of interest in insurance industry? An insurance contract is the agreement between an insurance company and the insured under which one party (the insurer), in consideration of receipt of a premium, undertakes to pay money to another person (the insured) on the happening of a specified event (as, for example, on death or accident or loss or damage to property). Central to any insurance contract is the insuring agreement, which specifies the risks that are covered, the limits of the policy, and the term of the policy. Additionally, all insurance contracts specify: conditions, which are requirements of the insured, such as respecting of a special conduct code or installing a software; limitations, which specify the limits of the policy, such as the maximum amount that the insurance company will pay; exclusions, which specify what is not covered by the contract.

Insurance contracts have an additional requirement that they be in legal form. Insurance contracts are regulated by state law, so insurance contracts must comply with these requirements. The state may stipulate that only certain forms may be used for certain types of insurance or that the contract must have certain provisions.

If a contract lacks any of these essential elements, then it is a void contract that will not be enforced by any court.

In insurance, the offer is typically initiated by the insurance applicant through the services of an insurance agent, who must have the authority to represent the insurance company, by filling out an application for insurance. Sometimes the application for insurance can be filed directly with the insurance company through its website or indirectly through a broker. A broker is a person or firm who arranges transactions between an insurer and a client for a commission when the deal is executed. Neither role should be confused with that of an agent—one who acts on behalf of a principal party in a deal. How the offer is accepted will depend on whether the insurance is for property, liability, or life insurance. These are the types of insurance contracts.

With regard to insurance distribution we have to recall that on 20 January, 2016, the Council of the European Union issued Directive (EU) 2016/97, the Insurance Distribution Directive (IDD).

The IDD introduced new duties on distributors and reinforced some past duties:

• Expanding the scope from agents and brokers by adding all sellers of insurance products, including insurance manufacturers that sell directly to customers and market participants who sell insurance on an ancillary basis (subject to the proportionality conditions).

• Stricter requirements surrounding conflicts of interest and remuneration disclosures.

• Special disclosure requirements for bundled products and other product oversight requirements similar to those of MiFID II, Directive 65/2014 the legislative framework instituted by the European Union (EU) to regulate financial markets in the bloc and improve protections for investors.

• Additional requirements for insurance-based investment products (IBIPs) and the introduction of an Insurance Product Information Document (IPID) for non-life insurance products.

• New provisions regarding cross-border activity (freedom to provide services and freedom of establishment).

• Stricter administrative sanctions and other measures, including pecuniary sanctions.

IDD also introduces product oversight and governance requirements similar to MiFID II for all insurance products. The approval process for each insurance product should be defined as proportionate to the nature and function of the insurance products that are about to be sold to customers. The process should incorporate the identification of the target market, the risk assessment and assure that the distribution strategy is aligned with the identified market. Regular reviews are expected to check that products remain effectively distributed and consistent with the objective of the respective target markets. There are exemptions for insurance of large risks.

As we have seen, insurance production and distribution are characterized by moments of risk assessment, which can be facilitated by the presence of software, and by a strong process and compliance with formal rules that can be facilitated by software.

2. Software in distribution: profiling clients, check list and compliance

The insurance industry is charged with protecting and supporting its customers in their most challenging of times. Any breach of insurance industry regulation is compounded not only by regulatory consequences (administrative sanctions), but also by the damage inflicted onto the individual customer or corporate client. Regulatory compliance and risk management for insurance companies requires organizations to abide by comprehensive “know your customers rule” standard, impeccable privacy, anti-money laundering and anti-corruption practices.

Transparency is key to all businesses, but especially insurance providers. Strict adherence to insurance industry compliance needs to be woven into daily business practices. Operating above board on issues like data security and privacy, case and complaint management, and all forms of fraud management are essential to building and keeping customers as well as aligning with insurance industry regulatory compliance.

Insurance compliance software enables insurance companies and insurance intermediaries to meet compliance regulations efficiently and effectively. They use these solutions to reduce noncompliance events, establish effective compliance processes, and maintain strict, auditable records for compliance officers.

Insurance compliance solutions typically contain policy and procedure management, tools to manage compliance policies and procedures, insurance-specific regulatory intelligence capabilities, incident management, complaint management, task management, audit trails for compliance officers, workflow management, reporting, and regulatory intelligence features. These provide a comprehensive set of tools for insurance intermediaries to use to govern all of their compliance-related tasks.

And like any other large business, insurers face all the usual requirements to protect personal information under rules such the GDPR and state consumer protection laws. In all these cases the application of software deals with clients' personal data processing.

As said it is important to meet customer's needs, and in insurance contracts it is difficult to assess risk and customers' needs (capability of the customer to retain the risk on his/her own)

Generally speaking, there are different reasons why a company opts for a customer profiling tool. But the main reason is so that companies can focus their sales and marketing efforts on generating high-quality sales leads.

This is why creating customer profiles is so important. Customer profiling tool is the means to create a portrait of customers to help companies make design decisions concerning their service.

Nowadays there is a comprehensive range of good data profiling software solutions (even free for download)

Data profiling is an assessment of data values within a given data set for uniqueness, consistency, and logic – the key data quality metrics.

Data profiling is the first step of data quality assessment that identifies business rules violations and anomalies. It involves activities of analysing your data contents and structure.

Data profiling software and techniques provide companies with the ability to analyse large amounts of data fastly, in no time.

Additionally, Big data can enable big changes in the way claims are handled. If claims handlers have access to the data and can use it in a meaningful way, they are able to paint a much clearer picture and investigate more accurately. Drawing back on the example of the black box in cars, insurers can see when the accident occurred, where, what speed the insured was moving therefore giving them a much clearer indication on the validity of the claim.

3. Software to reduce risk and monitor claims

Software can also be used to help insured to reduce the risk and insurer can introduce into the general conditions of the contract clauses on the mandatory installation/application of software to reduce the risk.

With regard to cyber-risk insurance coverages (business interruption due to cyberattack, liability for damage to customers' data due to cyberattack), this solution can reduce the risk.

Cybersecurity remains a challenge for businesses across industries. Cyberattacks such as malware, ransomware, and phishing can breach enterprise systems and networks to steal confidential client and business data. Also, cybercriminals are continuously coming up with new attacking tools and techniques, making cybersecurity the need of the hour for all businesses.

Cybersecurity software can help protect computer systems, IT networks, software platforms, and mobile applications from hacking attempts. It uses security technologies such as encryption, endpoint protection, and multi-factor authentication to protect your enterprise data in real time from cyberattacks.

A wide range of cybersecurity software tools are available on the market. Cybersecurity software is a software solution that identifies vulnerabilities and potential threats to protect business systems, applications, and networks from cyber threats, including viruses, ransomware, and phishing attempts. It uses a combination of technologies such as firewall protection, data encryption and backup, incident response, and website scanning to prevent unauthorized access and ensure real-time enterprise security.

There are many types of cybersecurity software solutions: data encryption tools, web vulnerability scanning tools, network defence tools, penetration testing tools, antivirus software, and firewall software. Application security, information security, network security, operational security, and disaster recovery are some common business applications of these tools.

There are different features offered by cybersecurity software solutions:

-Vulnerability scanning scans your systems, software, and networks at regular intervals to detect and report on any new or existing security vulnerabilities, such as viruses and malware.

-Threat mitigation employs security techniques to detect existing threats, reduce the impact of the detected threats, and prevent the occurrence of new threats. All identified security threats are quarantined to prevent contamination of other files and data.

-Incident management sets up a plan of action to follow in case a security incident is identified. Log incidents by priority, and diagnose the issue to reduce downtime.

-Data encryption encrypts business data, so it can be accessed or decrypted only by users that have the encryption key (i.e., a password or passcode).

-Single sign-on uses a single set of login credentials (e.g., a username and password) to access multiple software applications or platforms.

-Two-factor authentication sets up a dual authentication mechanism to allow user access to business data and applications. All users have to verify their identity using two sets of credentials (e.g., mobile push authentication along with the standard username and password).

Among of the benefits of cybersecurity tools in terms of cyber-risk reduction, we can recall:

-Protection of sensitive business data: Cybersecurity software encrypts enterprise data to protect it from hacking attempts by unauthorized users. With encryption, data is converted into an unrecognizable, coded format, which can be unlocked only by users who have the encryption key—i.e., a password or passcode.
-To keep secure computer networks: In the majority of cases, cyberattacks are launched through an organization's computer network. Cybersecurity solutions identify malicious network activities and immediately send a notification, so appropriate action can be taken. They use various security techniques, such as vulnerability scanning, threat detection, and firewalls, to monitor your networks in real time and prevent attackers from stealing sensitive data.
About recent trend in the cybersecurity software market, it is important to underline the Increasing use of artificial intelligence (AI) and machine learning (ML) to detect cyberattacks in real time: Manual and semi automated threat detection techniques aren't able to keep up with today's constantly evolving cyberattack landscape. In such scenarios, AI and ML technologies are being used to bring the incident response time down to a few seconds via real-time threat intelligence and data security. AI and ML capabilities are being directly deployed at network endpoints, such as mobile phones, laptops, desktops, tablets, and servers, to detect and combat threats in real time.
It is also possible to use software, installed on a car, to monitor the driving habits of the driver. It is the case of PAHD Pay how you drive insurance. Pay how you drive insurance is a special type of motor vehicle insurance that take into consideration how you drive. This simply means your driving habits dictate your premiums i.e. speeding, braking, parking, positioning, stops etc. If you happen to be a rough driver who speeds, breaks suddenly and positions themselves near obstacles/objects, you will obviously pay higher premiums compared to the careful driver who breaks gradually and leaves enough space between the car and objects. Pay how you drive insurance is simply aimed at charging premiums according individual driving habits. Pay how you drive insurance considers all possible factors to ensure car owners are charged fair premiums.
There are many advantages of pay how you drive insurance:
1. it provides useful information: one of the main benefits of pay how you drive insurance is the information collected. Telematics tracking devices collect a lot of vital information i.e. speed, car performance, concentration, braking etc. which helps drivers evaluate their driving skills and take necessary measures;

2. it permits fair premiums: the fact that a driver pays premium based on reasonable parameters i.e. their driving skills and time makes the amount of premiums charged justified. You pay premiums according to experience which is fair;

3. it makes motor insurance cheaper for safer drivers;

4. it makes driving environmentally sustainable. It is possible, for instance, to use eco-driving as model of risk discrimination in case of motor insurance and on some related legal constraints. Several studies done at an international level indicate a direct connection between efficient drivers and those drivers with fewer preventable accidents. The word Eco driving commonly indicates the combination of some driving techniques: a- Maintenance. Key parameters to maintain are: proper tire pressure, wheel alignment, engine oil with low kinematic viscosity. b- Driving lighter and/or lower-drag vehicles and minimizing the amount of people, cargo, tools, and equipment carried in the vehicle (removing common unnecessary accessories such as roof racks, brush guards, wind deflectors, etc., driving with the fuel tank mostly empty and tanking more frequently). c- Maintaining an efficient speed. Optimal efficiency can be expected while cruising with no stops, at minimal throttle and with the transmission in the highest gear. d- Optimal choice of gear (in case of manual transmission). e- Experts recommend accelerating quickly and smoothly. f- A driver may further improve economy by anticipating the movement of other traffic users. For example, a driver who stops quickly, or turns without signalling, reduces the options another driver has for maximizing his performance. g- Using air conditioning as required by the occupants and not continuously.

4. Key points on GDPR and insurance

All the above mentioned applications of software in insurance industry concern personal data processing.

The GDPR General Data Protection Regulation, European regulation on personal data protection no. 2016/679, enforced on May 24th 2016, directly applicable in all Member States, covers insurance and insures in two ways: business and compliance.

The GDPR is applicable to personal data processing carried out by a data controller or a data processor based in the European Union, as well as to personal data processing carried out by a data controller or data processor outside the European Union, where such processing involves the supply of goods or services or the monitoring of the conduct of data subjects located in the European Union. Therefore, insurance brokers or non-EU companies selling policies to EU citizens will be subject to the application of the GDPR as well.

As we have seen, Insurance has always been based on data collection, which today is either intrinsically digital or dematerialised (i.e. digitalised). Personal data, often sensitive, increasingly abundant thanks to new technologies for collection (such as smartphones or wearable, for example) and to the need of structuring and making them a leverage to keep up with today's market, which requires new products, slimmer and more personalized, on-demand policies, micro policies, etc.

GDPR concerns companies of all sizes, in fact, there are no exclusions by sector or corporate dimension from the applicability of the European Regulation apart from the processing register (art. 30 of the GDPR), what matters is whether the company, as data controller or data processor, deals with personal data of data subjects located in the EU. Therefore, any requirement involving a large Company is applicable to the emerging insurtech.

Respect to the past privacy protection systems, some novelties have been introduced by GDPR. First of all, the approach to the regulation that is no longer prescribed, i.e. does not set what must (or must not) be done to be compliant, rather it defines specific targets to be achieved to guarantee the protection of personal data, on which the regulation has been construed, through a series of steps and provisions driving the company through the adjustment process.

It is then important to determine who is the controller and who is the processor in the new GDPR terminology. The GDPR defines a controller as: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The GDPR defines a processor as: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Moreover, the GDPR introduced the concept of accountability of the data controller, which must be able to prove that the principles set out in Article 5 of the GDPR (lawfulness, correctness and transparency in data processing; limitation of the purposes of processing; minimisation and accuracy of the data processed; integrity and confidentiality as well as limitation about data retention), applied to all relevant fulfilments and obligations, have been complied with. This approach is consistent with the introduction of the concept of "Privacy by Design and by default" ", pursuant to art. 25 of the GDPR.

Additionally, the concept of 'Privacy by default' has been introduced, which means that data controllers must implement appropriate technical and organisational measures to ensure that only personal data necessary for a specific purpose will be processed.

Another novelties and one of the biggest challenges that the insurance industry has to face in the new system is the concept of data portability introduced under Article 20 of the GDPR. Data subjects will now have the right to receive any personal data concerning them, which they have previously provided or has been observed, in a 'commonly used and machine readable format' and have the right to transmit that data to another controller. This only applies to automatic processing, and when personal data is being processed under the lawful basis of consent or performance of a contract.

Furth more, new consent form is another big task for insurers in the context of GDPR. Special duties relating to the processing of personal data and particularly of sensitive data (i.e. in case of health insurance).

Problems in case of joint-controlling of data can emerge. Article 26 of the GDPR introduces the concept of joint-controllers where there are two or more controllers that jointly determine the purposes and means of processing. As we have seen, Insurers have relationships with numerous third parties such as agents and brokers. In this case Insurers need to look at arrangements they have with third parties to determine if this is controller-to controller or controller-to-processor relationship.

Many new requirements have been introduced in regard with Transparency that is another Key concept in GDPR. One of the major challenges emerging in the insurance industry is the requirement under Article 14 to provide information where personal data has not been obtained from the data subject.

GDPR poses to insurers and to insurance intermediaries also problems regarding the necessity to appoint a DPO (Data Protection Officer). Data protection officers are responsible for overseeing a company's data protection strategy and its implementation to ensure compliance with GDPR requirements.

According to Article 37(1) of the GDPR, DPO must be appointed if:

- ✓ the relevant data processing activity is carried out by a public authority or body;
- ✓ the *core activities of the relevant business involve regular and systematic monitoring of individuals*, on a large scale; or
- ✓ the core activities of the relevant business involve processing of sensitive personal data, or data relating to criminal convictions and offences, on a large scale.

The statement “the core activities of the relevant business involve regular and systematic monitoring of individuals” is of interest for insurers and insurance intermediaries.

The Guidelines (WP29 [working party on art. 29] guidelines on the Data Protection Officer requirement in the GDPR) clarify that the term "core activities" refers to the key operations necessary to achieve the main objectives of the relevant business.

The processing of personal data in the context of internal IT services or payroll processing (which are ancillary activities, rather than inextricably linked to the main objectives of the relevant business) do not trigger the obligation to appoint a DPO, according to the Guidelines.

The terms "large scale" are not defined, but the Guidelines note that there are some cases that are clearly large scale (e.g., processing at a regional, national or international level) and some cases that are clearly not large scale (e.g., processing of personal data of an individual patient by a doctor). But most business activities will fall somewhere between these two extremes. The Guidelines recommend that businesses should consider the following factors in determining whether a given processing activity is "large scale" or not:

- ✓ the number of individuals affected (either in abstract, or as a percentage of the relevant population);
- ✓ the volume of data, and/or the number of categories of data, being processed;
- ✓ the duration or permanence of the processing activities; and
- ✓ the geographic scope of the processing activities.

The concept of “Regular and systematic” includes, among other things, tracking and profiling on the internet (e.g., the use of cookies for behavioural marketing purposes). The Guidelines make clear that "regular and systematic" means any activity that is: (i) repeated (with any degree of frequency); and (ii) is planned or strategic (i.e., more than an accident or a coincidence).

It is clear that insurance intermediaries, as well as insurance companies, can be included among the subjects who process personal data according to regular and systematic monitoring. The WP art. 29 also intervened to point out that it may be useful to proceed with the designation of the DPO even where not mandatory as this helps to improve the "privacy image" of the Owner and / or Manager for accountability purposes.

GDPR represents a burden for insurers, in terms new tools to be compliant with the new rules, but also a challenge, considering the innovative forms of insurance coverage.

References.

Brendan McGurk (2019) Data Profiling and Insurance Law, Bloomsbury Publishing PLC, London

Antonella Cappiello (2018) Technology and the Insurance Industry Re-configuring the Competitive Landscape, Springer, New York

William M. Clarke (2009) The law of insurance contract, Informalaw, London

Nikolaus Forgó, Stefanie HänoldBenjamin Schütze (2017), The Principle of Purpose Limitation and Big Data, pp. 17-42, 39-40, in M. Corales, M. Fenwick, N. Forgo, (Eds), New Technology, Big Data and the Law, Perspectives in Law, Business and Innovation Series, Springer, New York

Dorothy J. Glancy (2012) Privacy in autonomous vehicles, 52 Santa Clara Law Review,

Natali Helberger (2016) Profiling and Targeting Consumers in the Internet of Things, in R. Schultze , D. Staudenmayer (Eds), Digital Revolution: Challenges for Contract Law in Practice, Hart Publishing , 135.

Thomas Hoeren and Barbara Kolany-Raiser (Eds.) (2018), Big Data in Context, Springer, New York.

Stefan Kulk and Frederik. Zuiderveen Borgesius (2015) Freedom of expression and 'right to be forgotten' cases in the Netherlands after Google Spain, 2 European Data Protection Law Review, 113-125.

Samantha Mahmood and Saba Sayers (2015) Privacy and Data Protection, P. & D.P. 2015, 15(8), 3-5.

Pierpaolo Marano , Kyriaki Noussia (Eds.) (2020) InsurTech: A Legal and Regulatory View, Springer, New York

Markus Maurer, J.Chris Gerdes, Barbara. Lenz, Herman Winner (Eds.) (2017) Autonomous Driving: Technical, Legal and Social Aspects, Springer, New York

Anna Carla Nazzaro; Sara Landini (2020) Blockchain e assicurazioni, Daniela Valentino (eds.) Dei singoli Contratti, leggi collegate, codice civile commentato Gabrielli, Utet, Torino, pp. 361-424.

Patrick Pype, Gerardo Daalderop, Eva Schulz-Kamm, Eckhard Walters, Maximilian von Grafenstein (2017) Privacy and Security in Autonomous Vehicles, 17-27,21-23 in D. Watzenig, M. Horn (Eds.), Automated Driving, Springer, New York

Reiner Schultze and Dick Staudenmayer (Eds) (2016), Digital Revolution: Challenges for Contract Law in Practice, Hart Publishing, Baden Baden

Paul M. Schwartz (1999), Privacy and Democracy in Cyberspace, 52 Vanderbilt L.R. 1609.