Acta Univ. Sapientiae, Legal Studies, **10**, 1 (2021) 35–53

DOI: 10.47745/AUSLEG.2021.10.1.03

Certain Issues of Innovations Affecting the Insurance Business in the Light of the GDPR and Hungarian Insurance Law[1]

Mário ČERTICKÝ
LLM Assistant Lecturer
University of Miskolc (Miskolc, Hungary)
Faculty of Law, Department of Commercial Law
E-mail: civmario@uni-miskolc.hu

Abstract. Technological innovations affect many sectors of the economy, including the insurance business. Among these innovations, IoT-based (Internet of Things) solutions can be highlighted, the main feature of which is that real-time and continuous data collection is performed using the Internet, thus optimizing the risk management of the insurer. Given that a significant part of the data thus collected constitutes personal data, the rules of the General Data Protection Regulation (GDPR) should apply. The data protection examination of the technologies affecting the insurance institution raises several issues, which, in my view, significantly impede the application of these technological achievements. The study aims to explore these problems and attempts to make proposals to solve them.

Keywords: insurance, GDPR, insurance and IoT, GDPR and IoT, data protection and insurance

1. Introductory Thoughts

Thanks to the technological development that began explosively at the beginning of the 21st century[2] and has been going on continuously ever since, it is now essential that all actors in the economy apply new technological solutions adequately. These innovations are taking advantage of the almost limitless possibilities of information technology, digitization, and the Internet and take

1 The study was accomplished as part of the EFOP-3.6.1-16-2016-00011 *Younger and Renewing University – Innovative Knowledge City – Institutional Development of the University of Miskolc Aiming at Intelligent Specialisation* project implemented in the framework of the Széchenyi 2020 programme. The realization of this project is supported by the European Union and co-financed by the European Social Fund.

2 Kerényi–Müller 2019. 7 (DOI: 10.25201/HSZ.18.1.533).

a completely different approach to practice in the concerned field. The wave of innovative development has also reached the financial sector, so the actors of that field prefer to use financial technologies (Fintech) which can help in the economic and financial management and operation of the company.[3] Fintech solutions can be used throughout the financial service sectors, including the insurance sector, so insurers are already moving to technologies (Insurtech) that develop this legal institution and benefit both insurers and 'clients'.[4]

This study aims to examine the data protection issues related to the technological means applied in each insurance form in the light of the General Data Protection Regulation of the European Union[5] (hereinafter: Regulation or GDPR). We can distinguish between two levels of innovation affecting the insurance business. One of them has an impact on insurance coverage – for example, the emergence of self-driving vehicles, which pose significant problems for vehicle insurance (such as damage and liability insurance).[6] The other includes innovations that are specifically designed to 'serve' the insurance institution by placing an element of insurance in a different light from the traditional or by changing the usual (meaning: traditional) mechanisms. Each chapter details issues from a data protection point of view, which often comes into sight concerning the use of different technological solutions in each type of insurance.

In the study, in addition to the norms defining the data management rules, I also examine the legislation on insurance contracts both from the private and public law perspective, such as Act V of 2013 on the Hungarian Civil Code (hereinafter: Civil Code) and Act LXXXVIII of 2014 on Insurance Business (hereinafter: Hungarian Insurance Act, or Insurance Act); the latter lays down specific data processing rules, the most important of which I highlight and examine through the lens of the GDPR.

3 Kagan 2019.

4 In this case, I consider using the term 'client' of the Hungarian Insurance Act because these technologies do not exactly affect just a contracting party of the insurer or the insured person but may affect any person involved in the insurance legal relationship.

5 Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

6 Serious questions from the data protection point of view can also arise concerning self-driving vehicles. In particular, it is expected that vehicles may only be started by an authorized person, which requires the utilization of some means of unique identification. Regarding a unique identifier, especially because they are typically biometric data, the dilemma of determining the legal basis for the lawfulness of data processing, the establishment and maintenance of strict data retention requirements, and the possible transfer of data may raise data protection and data security issues. These issues are even more important if the self-driving vehicle is connected to the Internet as well. In connection with the assessment of damages caused to the owner or caused by the user of the motor vehicle within the framework of the insurance contract, all of these also add to the insurer's requirements for data processing, the legality of which must be ensured. In this context, see the Recommendations of the EDPB no. 1/2020. Besides, data

We cannot find extensive literature on the specific topic, so, basically, the problems are explored, and solutions are proposed using a descriptive method. Of course, the Hungarian and foreign literature, the opinions and decisions of the Hungarian Data Protection Authority, the National Data Protection and Freedom of Information Authority (hereinafter: NAIH or Hungarian DPA), and the guidelines of the Article 29 Data Protection Working Party as well as the guidelines of the European Data Protection Board (EDPB) established under the GDPR will help us explore the specific topic.

It can be stated in advance that the basis of all innovations is the Internet-based flow of information (Internet of Things – IoT), which helps these to function.[7] The applicability of the Internet of Things is virtually inexhaustible; with some estimates, the number of devices based on this technology will reach 125 billion by 2030.[8] Connecting to the Internet enables real-time data collection and data flow, which hide as yet untapped opportunities for its user.

Noteworthy – although it will not be explained in detail, as it would go beyond the topic of this paper – is the possibility of using blockchain technology among the increasingly widespread smart contracts. Due to the decentralization of the blockchain (known as 'distributed ledger technologies'), several problems may arise, as we are already experiencing difficulties in examining the first and most important question: who is the data controller?[9] On this issue, prior to the GDPR becoming applicable, the Hungarian DPA also accepted an opinion[10] stating that the identity of the controller is very difficult to ascertain; in fact, all users are data controllers. We can also find an example of the applicability of smart contracts in insurance contracts in practice.[11] The essence of the operation of a smart contract is that the contract 'comes to life independently', and its fulfilment takes place automatically, without the need for any human intervention. Obviously, this can only be achieved in a contractual construction in which human behaviour can truly be avoided.

Furthermore, when using smart contracts, data controllers must comply with data protection standards, as it is emphasized by the European Parliament in its resolution on this subject.[12]

protection issues may arise concerning the processing of environmental data recorded by self-driving vehicles during movement if the vehicle records an image of a natural person.

7 Alföldy–Seregdy 2015. 48.

8 Kounoudes–Kapitsaki 2020. 1.

9 I note that a preliminary question already arises as to whether the GDPR with a centralized approach applies at all to systems based on blockchain technology operating on a decentralized basis. In my view, it does, in which all participants should be considered data controllers. Also, the author of a recent study, given that this issue is not explicitly addressed, believes that the application of the GDPR to blockchain-based technologies is a fundamental proposition. See Eszteri 2020. 9–27.

10 See NAIH 2017.

11 About the applicability of the blockchain system in insurance contracts, see Gatteschi–Lamberti–Demartini–Pranteda–Santamaría 2018. 1–16.

12 See European Parliament 2017.

2. Insurance and Data Processing – Basic Concepts

A legal relationship of insurance is extremely complex because it can have many actors related to each other in different ways. Given this complexity, I use the concept of an insurance relationship here, which opens up a broader framework for examining individual data processing issues.

Due to its complexity, it is extremely difficult to adjust to the maze of data processing in the context of the insurance relationship. In this chapter, I would like to identify the cornerstones of data processing in the context of an insurance relationship. In this context, I define the purpose of data processing in the light of legal provisions as well as the range of persons who may be considered as data subjects in the insurance relationship, and I also define the concept of personal data in the light of the speciality of the topic. Finally, I outline the range of persons who may arise as data controllers and data processors. I will examine the question of possible legal bases for data processing in the light of the application of the technological means concerning each form of insurance in the following chapters.

2.1. The Legal Purpose of Data Processing in the Light of the Hungarian Insurance Act

The 'Alpha and Omega' of data processing is to determine the legitimate purpose of data processing, which is essential to comply with one of the most important[13] data protection principles, i.e. the limitation of purpose,[14] which must be complied with throughout the data processing.[15] Section 135 of the Insurance Act defines exclusively, but at the same time extremely broadly, the possible purposes of data processing in connection with insurance activities, according to which 'processing of such data shall take place only to the extent necessary for the conclusion, amendment, and maintenance of the insurance contract and the evaluation of claims arising from the contract or for any other purpose specified in this Act'.[16] Concerning the topic, the primary goal of data processing is to determine the fulfilment of the obligations arising from the insurance contract, and within this we can identify several sub-goals.[17]

13 It should be emphasized that there is no hierarchical distinction between the principles of data management; however, the very purpose of the limitation principle is to be 'first among equals'. See: Révész 2018. 96.

14 See Article 5(1)(b) of the GDPR.

15 Révész 2018. 96.

16 Translation by the author. Unless otherwise specified in the footnotes, all quotes from non-English source materials are translations by the author.

17 It should be noted that the purpose of data processing can be approached from two directions: (i) the purpose of data processing as a set of personal data; (ii) the purpose for which each personal data item is processed. The first one forms a set of personal data, so the two categories are in a

2.2. Personal Data and the Data Subject in Insurance

From the data protection point of view, the complexity of insurance as a legal relationship is primarily due to the fact that the insurer can process the personal data of several data subjects, who are named by the Insurance Act as a 'client'. The definition of client is set forth by Section 4(101) of the Insurance Act as:

> *'client' shall mean the policyholder,*[18] the insured person,[19] the beneficiary,[20] the injured party,[21] any other person who makes a contractual offer to the insurance company[22] and who is entitled to receive benefits[23] from the insurance company; furthermore, in the case of independent insurance intermediaries, any person who enters into a contract with an independent insurance intermediary for the purpose of brokering.

The GDPR does not explicitly define the concept of data subject, but we can identify these persons from the concept of personal data, according to which personal data means that 'any information relating to an identified or identifiable natural person ("data subject") is considered as a personal data'.[24] If we compare the concept of 'customer' to the concept of 'data subject', we can conclude that

part–whole relationship with each other. The former has a broader purpose, while the processing of individual personal data may have a narrower purpose (possibly several purposes), which is either the same or different from the broader purpose, but should also be in line with it in the event of a discrepancy. However, the GDPR does not require the purpose of data processing but the purpose of the processing of individual personal data.

18 The policyholder is the person who concludes the insurance contract with the insurer. See Sections 6:439(1) and 6:440 of the Civil Code.

19 An insured person is a person 'who, on the basis of a financial or personal relationship, has an interest in avoiding the occurrence of the insured event, or, with respect to life insurance conditional upon reaching a certain age, birth, or conclusion of marriage, has an interest in the occurrence of the insured event'. See Section 6:440 of the Civil Code. I note that the policyholder and the insured are basically the same, but they may also be separated if the policyholder contracts in favour of a person who has an insurable interest.

20 The beneficiary is the person who is primarily entitled to the service of the insurer.

21 The injured party will be the client of the insurer if, under the liability insurance contract, the insured will be entitled to be exempted from compensation for the damage caused by him/her and the payment of restitution. In this case, the insurer generally performs the service for the injured party. To perform this service, the insurer has to determine the conditions of performance (to investigate the circumstances of the insured event); so, before the performance, it is necessary to process the injured party's personal data, often also special data.

22 This person is the potential contracting party if s/he has made an offer to the insurer, but the insurance contract has not yet been concluded or will not be concluded.

23 This person can be, e.g. in the case of a liability insurance contract, the relative of the injured party if the injured party loses his/her life during the insured event. Also, the client status of third parties may arise in several other cases, which I do not intend to outline in full.

24 See Article 4(1) of the GDPR.

only natural persons as an insurer's clients can be considered as data subjects, so legal persons as policyholders are not considered as data subjects.[25]

The processing of data in connection with an insurance relationship covers the personal data of the data subject. It is clear from the definition set out in Article 4(1) of the GDPR that all information relating to the data subject is personal data. Concerning the insurance relationship, it is also a feature that this information is considered not only personal data but also an insurance secret.[26] Because of this, the Insurance Act essentially lays down rules on the treatment of insurance secrecy, which obviously includes personal data. The specific scope of personal data that may be processed in connection with the performance of the insurance contract shall be determined by the insurer under the provisions of Chapter XXII of the Civil Code and must specify, in the light of the law applicable to the contract in its entirety, the purpose of the specific contract and the nature of the risk covered by the insurance.

Special categories of personal data are subject to special consideration.[27] Among the sensitive data, the processing of genetic[28] and biometric data[29] of the data subject as well as the health data[30] of the data subject may arise in the context of the insurance relationship, the most prominent of which may be the processing of the latter. The processing of health data may arise in many forms of insurance, but primarily in fixed-amount insurance, especially in life

25 I note that natural and legal persons are treated by the insurer in the same way for the protection of insurance secrecy, but the application of the GDPR is relevant only to the former. I further note that although they do not qualify as a client, the GDPR covers the personal data of natural persons acting on behalf of a legal person as a client, so the provisions of the Regulation already apply to them.

26 The definition of insurance secrecy is established by Section 3(1)(12) of the Insurance Act as follows: 'insurance secret shall mean all data – other than classified information – in the possession of insurance companies, reinsurance companies, and insurance intermediaries that pertain to the personal circumstances and financial situations (or business affairs) of their clients (including claimants), and the contracts of clients with insurance companies and reinsurance companies'.

27 The scope of specific data can be deducted from Article 9(1) of the GDPR as follows: 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.

28 See Article 4(13) of the GDPR: 'genetic data means personal data relating to the inherited or acquired genetic characteristics of a natural person, which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question'.

29 See Article 4(14) of the GDPR: 'biometric data means personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.'

30 See Article 4(15) of the GDPR: 'data concerning health means personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status'.

and accident insurance contracts. Furthermore, the processing of health data may arise in liability insurance as well, wherein the insurer may process health data of the insured party and the injured party. In this study, I will emphasize the rules of processing sensitive data, especially health data in insurance contracts.

2.3. Data Controller and Data Processor

In the context of an insurance relationship, several persons as data controllers or data processors may come into contact with the personal data of the data subject.[31] Of course, one of the most important data controllers will be the insurer with whom the policyholder concludes the insurance contract, but the data processing of certain contributors (e.g. a person involved in claims settlement) may also arise in connection with the performance of the insurance contract.[32] Also, especially in the case of electronic contracting – if the electronic interface is not provided by the insurance agents or the insurer's own system –, the data processing of individual software providers may also arise. The IT innovations discussed in the study (software, telematics and telemetry systems, individual smart meters) can be said to be operated not by insurers – although this possibility is clearly not ruled out – but by other persons, in the name and on behalf of insurers.

First of all, we need to examine the relationship between the insurer and software providers in the context of data processing. The definition of data controller is in Article 4(7) of the GDPR, which establishes that 'controller means the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data'. The most important aspect of data controller quality is that the purposes and means of data processing are independently determined by the data controller, which covers a number of 'partial decisions'.[33] In contrast, 'data processor means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.'[34] The most important difference between a data processor and a data controller is that the former acts on behalf of the latter,[35] so it does not determine the purpose and means of data management independently.[36] Concerning the data processing performed within the framework of the insurance legal relationship, the definition of the data controller is simple as the purpose of all data processing performed in connection

31 Zavodnyik 2018. 19.
32 Zavodnyik 2018. 19.
33 Osztopáni 2018. 81.
34 See Article 4(8) of the GDPR.
35 Bölcskei 2019. 65.
36 The criteria for the demarcation of the data controller, the data processor, and the joint controller are defined by the EDPB in Guideline no. 7/2020. It is currently in the post-social consultation phase, so its text is not yet final. See EDPB Guideline no. 7/2020.

with the insurance contract is established by Section 135(1) of the Insurance Act, the addressee of which is the insurer. The data processes related to the performance of the insurance contract, including the manner of risk management mechanisms, are determined by the insurer – of course, in agreement with the policyholder, which is reflected in the contract and its provisions –, thus independently determining the purpose and means of data management. If the insurer outsources[37] certain subtasks required for the performance of the contract (e.g. data collection and even data analysis), for example, when the insurer performs risk management using an IoT-based device operated by an external person, we can conclude that this service provider qualifies as a data processor. It is noteworthy that the content of the legal relationship between the controller and the processor must be governed by a contract defined in Article 28(3) of the GDPR, which specifies the details of the data processing. The relationship between the data controller and the data processor is subordinate, as the data processor is obliged to perform the data processing operations under the instructions of the data controller and only within the framework of a contract. This rule does not mean that the data controller cannot make an independent decision regarding data processing, but this has to be accordant with the contract.[38] It is important to determine the details of the data processing precisely (e.g. data processing specifically) in the contract concluded between them. It is also important to emphasize that the data controller is primarily responsible for the legal compliance of data processing. The data controller is responsible for ensuring the lawfulness of the data processing and for taking the appropriate technical and organizational measures, including the provision of appropriate instructions to the processor.

3. Data Processing Issues related to Innovations in Damage Insurance Contracts

One of the most important parts of individuals' interests is wealth. The protection of property interests is the task of non-life insurance and, as such, it serves a societal interest. There can be many types of external influences on property, the foresight and prevention of which, and handling of adverse events if they

37 Osztopáni 2018. 83.

38 According to Guideline no. 7/2020 of the EDPB, we can distinguish between 'essential' and 'non-essential' decisions. The former is closely related to the purpose and scope of data processing, while the latter involves deciding issues related to the practical implementation of data management. The guideline provides the data processor with the possibility to make the non-essential decisions. I note that the GDPR does not allow a distinction to be made between individual data processing decisions. It is important that decision-making is an option and not a given requirement; in the contract, the parties have the opportunity to regulate even the smallest detail of the data processing.

occur, are important issues in non-life insurance. The risk management methods of the 21st century are constantly changing and are being taken to a new level of complexity by taking advantage of technological achievements. The innovations mentioned below reinforce the preventive purpose of the insurance institution so that effective measures can be taken to avoid damaging events, in the interests of the parties involved in the insurance.

One of the areas of useful innovations may cause significant changes in the field of home insurance. Insurers can offer a number of benefits when using telemetry systems[39] in a home. These include various camera, sensor, and fire protection systems, which are primarily used to prevent damage.[40] The basic function of these systems is to continuously monitor the assets of the data subject,[41] which results in different data processing than usual. In view of the broad definition of personal data, e.g. technical data on the condition of the piping of a house, the fact whether the door of the building is closed or not, etc., may qualify as a personal data as this information is indirectly relevant to the insured as a data subject. The question may arise as to whether an impact assessment[42] is required prior to such data processing. This data processing is not covered by the mandatory impact assessment[43] and should also be considered[44] under Article 35(1) of the GDPR, but, given the content of the impact assessment list published by the Hungarian DPA[45] under Article 35(4), an impact assessment must be carried out.

The number of motor vehicles is gradually increasing, which raises the risk for insurers, so insurers must strive to develop the most accurate risk management methods,[46] to which each technological achievement can make a major contribution. In this context, both forms of motor insurance, such as damage and liability insurance, may come to the fore. I deal with the former here and with the latter in the next chapter. In motor insurance, telematics systems seem to be the most applicable.[47] The telematics system allows for the real-time collection and analysis of personal data concerning policyholders, thus making the insurance conditions, the content of the insurance contract, in particular the payment of premiums,[48] flexible and unique while allowing for more effective risk analysis.[49]

39 Telemetry is a typically wireless communication system that enables long-distance data transmission, remote measurements, and control.
40 Alföldy–Seregdy 2015. 51.
41 Wágner 2017. 61.
42 See Article 35 of the GDPR.
43 See Article 35(3) of the GDPR.
44 In my view, given the nature, circumstances and purpose of the data processing, it is unlikely to pose a high risk to the rights and freedoms of data subjects.
45 See the List of Assessment under Article 35(4) of the GDPR published by the NAIH.
46 Wang 2020. 582.
47 Hauer–Góg–Horváth–Hrabár–Pálinkás–Urbán 2017. 23–24.
48 Sallai 2019. 102.
49 Kadocsa 2018. 85.

Among the telematics systems,[50] the use of a 'black box' in a vehicle, which records information about the operation of a vehicle, is most common.[51] The system works on the basis of GPS, so the risks associated with the operation of the vehicle can be assessed on the basis of a comparison of the positioning data and the data recorded as a result of the use of the vehicle, i.e. driving style.[52] All this can be applied by insurers to the calculation of the insurance premium,[53] which thus becomes essentially usage-based and thus fairer than the methods currently used (age of the vehicle, age and driving experience of the policyholder, history of claims, etc.).[54]

By using the telematics system, the insurer collects data on the condition of the vehicle (i.e. tire pressure, brake status, etc.) and information on the driver's driving style based on which the insurer can send alerts to the driver to prevent damage.[55] The purpose of all this is primarily to avoid events which may cause damage to the insured; furthermore, a more precise assessment and faster settlement of the circumstances (i.e. whether the occurred event is also an insured event) and the extent of the damage. However, for this purpose, the insurer carries out unusual – real-time and continuous – data collection, which monitors and evaluates the use of the vehicle by employing an automated system and which may lead to a more serious debate, for example, concerning the driver's

50 In this context, the European Data Protection Board has adopted Guideline No. 1/2020.

51 In this context and for other telematics system-based solutions, see: Hauer–Góg–Horváth–Hrabár–Pálinkás–Urbán 2017. 33, 24–25.

52 Assessing driving style means two things. One of them is that by following the rules of the traffic, which reduces risks arising from participation in transport (e.g. by respecting the speed limits, tracking or overtaking distances, etc.); so, compliant drivers have to pay a lower fee given that they drive less riskily. Another aspect that evaluates driving style is the actual use of the vehicle's equipment (e.g. brakes and steering use), so the risk of the driving is lower when the driver makes smaller and safer brakes or careful and not sudden steering movements.

53 The insurance premium basically consists of two premiums, one of which is the 'basic premium', which must be paid even if the vehicle is not used in traffic. The other fee is a 'variable fee' calculated based on the use of the vehicle, which changes depending on what data are stored about the operation of the vehicle. As the telematics system can provide real-time data on vehicle position, utilization, and driving characteristics related to driving style, the pricing developed in this way makes the insurance conditions much more transparent. See Alföldy–Seregdy 2015. 51–52.

54 I would like to emphasize a view which is one of the primary sources of the reluctance of society to use the telematics system. This is due to the fear that this system will or may provide data to the police on traffic compliance. In my view, this is not a real fear because the data collected using the telematics system cannot be accessed directly by the authority, as there is no legal basis for data processing on the part of the insurer. I do not consider it viable to create a legal provision that makes the provision of data mandatory as this would mean a level of restriction of personal rights that would probably fail the test of proportionality of the restriction of fundamental rights. I note that the exceptions to the obligation of professional secrecy contained in Section 138(1) of the Insurance Act do not apply in this case, as it regulates the provision of information to the authorities acting in a specific case (i.e. the procedure must have already been started) and does not mean a continuous – pre-procedure – provision of information.

55 Alföldy–Seregdy 2015. 55.

driving style. The collected data can also be used by the insurer to develop its products and to make the content of individual insurance contracts (e.g. setting a more favourable premium) and risk management more efficient. The purpose of the data processing is thus clarified and can be considered lawful; however, questions may arise in connection with the determination of the legal basis of the data processing.

The use of new technology may require a prior impact assessment (see above), and the continuous monitoring and evaluation of driving style makes it mandatory in accordance with Article 35(3)(a) of the GDPR.[56] The use of telematics systems can only work effectively if it covers the entire risk pool. So, the first condition for the application of this rule (i.e. it must affect more than one natural person) is fulfilled. As the data processed in this way is a personal characteristic of the insured (driving style as a personal characteristic), which is assessed through an automated system during systematic monitoring, the other two conditions for the application of the provision are also fulfilled. The last condition for the application of the provision, according to which data processing in this form must result in a decision having a legal effect on the data subject or a significant decision on the data subject, is also fulfilled as the purpose of data processing is to determine the insurance premium to be paid by the insured, which is a decision affecting the insured.

It is also necessary to define the legal basis of data processing, in which we must first examine whether the data processing constitutes automated decision-making.[57] As the data processing performed by the system – from data collection to decision-making – is free from human intervention, it can be concluded that data processing based on an IoT system is considered to be automated decision-making, including profiling.[58] Article 22(2) of the GDPR allows for the lawfulness of automated individual data processing in the presence of three legal bases, one of which is the applicability in the present case of the provision in point (a) that the use of automated decision-making is lawful if 'the decision is necessary for entering into or for the performance of a contract between

56 On this basis, a preliminary impact assessment must be carried out if the data processing is 'a systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person'.

57 I note that the notion of automated decision-making is not defined in the GDPR. Article 22(1) establishes only the right of the data subject to be excluded from the scope of automated decision-making.

58 I note that it constitutes automated decision-making if a decision which affects the data subject is made. If no decision is taken but the data is collected, we can talk about profiling according to Article 4(4) of the GDPR (without a decision), which can later be used by the data controller to make a decision, but this can only be done by human intervention. If the whole process is automated, then we are talking about automated decision-making that includes profiling.

the data subject and a data controller'. Based on this, therefore, if the parties expressly agree on the use of telematics systems, this provision can be applied, and the data processing will be lawful.

Spiced up with a measure of utopian naivety, but with even greater data protection awareness, I consider it conceivable to apply Article 22(2)(b) of the GPDR, which prescribes that the automated individual decision-making is lawful 'if the decision is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests'. Thus, if the Member State legislator regulates at the national level or the EU legislator at supranational level certain data protection issues regarding automated individual decision-making related to the insurance contract, or, rather with sufficient abstraction, to the use of IoT systems, this provision could become applicable. If this happens, I would primarily consider as appropriate the adoption of directly applicable norms at the EU level (meaning a European Union regulation-level norm) to ensure that all insurers treat the issue in the same way.

4. Data Processing Issues related to Innovations in Liability Insurance

The telematics system can also be used in liability insurance, under which motor liability insurance can be highlighted. This will or may put this insurance product on a new basis, resulting in a much fairer premium system and a more sensitive risk pool for users. However, it has a positive effect on insurers as it can lead to a more prudent and accurate assessment and continuous monitoring of financial risks, thus reducing their financial losses. In connection with the issues related to the legal basis of the data processing and impact assessment in this context, I consider the explanations expressed in the case of non-life insurance.[59]

Nevertheless, serious data protection issues may arise if the policyholder and the insured are different. Moreover, according to Section 3(4) of the Hungarian motor liability insurance Act,[60] the person driving the motor vehicle – who is not necessarily the same as the former – is also considered an insured person. These issues arise in the context of the legal basis of data processing since if the policyholder is not the insured – so, the data processing cannot be based on the insurance contract [on the Article 6(1)(b) of the GDPR], as in this case –, then the insured does not appear as a party to the contract. In this case, the question arises as to whether or not the insurer processes personal data. This

59 I note that the opinion expressed on the applicability of Article 22(1)(b) of the GDPR could be the most feasible in the case of motor liability insurance.

60 Act LXII of 2009 on Motor Liability Insurance.

may arise because the natural person about whom the data are collected is not known, and thus the condition of the concept of personal data that it refers to an 'identified or identifiable natural person' is not met. Such a person cannot be considered identified in any way as his/her identity is not known to the insurer, but it can be identified indirectly if the insured event occurs. Until it becomes clear to the insurer that the recorded data do not relate to the policyholder, it will link it to the policyholder (considered as information about the policyholder), as it determines the primary obligation of the policyholder (i.e. the payment of premiums). If the insured event never occurs, the insurer may process these data in such a way that the data subject will not be identifiable.[61]

5. Data Processing Issues related to Innovations in Fixed-Amount Insurance Contracts

Fixed-amount contracts, such as life and accident insurance contracts, are based on risks related to the person, health, and life of the insured, some of which qualify as health data. In the field of traditional data collection, the policyholder typically provides answers to questions related to the health condition, so the insurer determines the extent of the risk according to the health condition at the time of contracting. The insurer may make it compulsory to use the services of a health professional designated by them to assess the contractual risks and will determine the extent of the risk based on the expert opinion.[62]

Technological achievements applicable to life and accident insurance contracts – e.g. smartwatches, smart bracelets, various sensory patches, etc. – are used for continuous monitoring of the client's health; so, the insurer uses real-time data collection. The purpose of this is to enable the insurer to continuously monitor the development of insurance risk and even to become immediately aware of the increase in insurance risk. All this can also result in a fairer and more equitable calculation of premiums, so the amount of the insurance premium increases or decreases depending on the risk borne by the insured. In this case, the insurer may also take preventive measures (e.g. it can draw the client's attention to the need to contact a medical professional or proceed to some form of medical analysis), and it can even provide a partial diagnosis of the client's condition or ascertain its possible deterioration.

61 This data processing falls within the scope of Article 11 of the GDPR, according to which the insurer does not have to request additional information to identify the data subject to comply with the Regulation. The purpose of data processing can be achieved without the data subject being identified by the insurer. The identification of the data subject will be necessary in case the purpose of the data processing expands with the occurrence of the insured event.

62 In this case, the legal basis for the processing will be Article 6(1)(b) of the GDPR, and the lawfulness of the processing of specific data will be based on Article 9(2)(h).

Real-time, continuous data recording is considered to be a form of automated individual decision-making concerning the insured as a data subject as the amount of the insurance premium is determined in an automated manner, depending on the health risk. Because of this, the decision-making clearly has an impact on the insured as it affects, reduces, or increases the extent of the insured person's obligation. It has been stated above that the lawfulness of data processing as automated decision-making may be based on Article 22(2) of the GDPR. However, Article 22(4) of the GDPR limits the lawfulness of processing the special category of personal data in the course of automated individual decision-making to the expressed consent[63] of the data subject.[64] In this context, I would like to highlight a significant problem, which also reveals two possible issues at once. In this context, the processing of special data is necessary for the performance of a contract concluded between the data controller and the data subject. There can be no dispute about the need as the parties have agreed in their contract to use these technologies (meaning a risk management mechanism). Under Article 22(4) of the GDPR, given that automated data processing is carried out on specific data, in addition to the legal basis in Article 6(1)(b) of the GDPR, only Article 9(2)(a) shall apply.[65] Here I would like to draw attention to Section 136 of the Insurance Act: 'According to the relevant Act,[66] insurance companies shall be authorized to process any data pertaining to the medical condition of clients only for the reasons set out in Section 135(1) and only in possession of the express consent of the data subject.' This provision is seemingly in line with the cited provision of the GDPR as it does not regulate the requirement to process health data in the same way but, incorrectly, for the following reasons.[67] According to Article 7(4) of the GDPR, consent cannot be interpreted in contractual data processing because one of the conditions for the validity of the consent, its voluntary nature, cannot be ascertained. The assessment of volunteering should also take into

63 See Article 9(2)(a) of the GDPR.

64 For the sake of completeness, I note that under Article 22(4) of the GDPR, automated individual decision-making on specific data is lawful even if it is justified by the condition in Article 9(2)(g), but in my view this provision does not apply.

65 Although there is no complete agreement in the literature on the relationship between Article 6(1) and Article 9(2) of the GDPR, in my view, the provisions of the latter do not constitute a separate legal basis, but they shall be considered as a standard supplementing the legal bases set out in Article 6(1), needing an additional requirement given the specific quality of the personal data. Because of this, the lawfulness of the processing of special data requires one of the legal bases provided for in Article 6(1) and the existence of one of the conditions laid down in Article 9(2).

66 See Act XLVII of 1997 on the Processing and Protection of Personal Data in the Field of Medicine.

67 The primary source of the problem, in my view, is that the provisions of the Insurance Act have not been properly adapted after the applicability of the GDPR; it follows the old (pre-GDPR) view of the Hungarian Privacy Act (hereinafter HPA), which regulated data processing based solely on the law and the consent of the data subject. In contrast, the GDPR mentions six legal bases for data processing and provides for the examination of the existence of ten additional conditions for the lawfulness of the processing of the special category of personal data.

account the need for the data subject to be able to withdraw the consent at any time without restriction, all this without disadvantage to the data subject. It is difficult to judge the legal consequences of the withdrawal of consent in the context of a contractual relationship, and it is hardly conceivable that a consent withdrawn in the context of a contractual relationship would not adversely affect the data subject. Therefore, the consent given in the framework of the contractual relationship cannot be valid for the personal data related to the performance of the contract, so it cannot be interpreted.

As I have explained, processing of special categories of personal data is necessary for the performance of the insurance contract; thus, the lawfulness of the data processing is ensured by the contract concluded between the parties. Provisions of the GDPR for processing special data and cited rules of the Insurance Act for health data limit the additional condition to consent, which cannot be valid because of Article 7(4) of the GDPR; so, the processing of special data cannot be lawful. Given this, automated individual decision-making on specific data, which is linked to a contract, cannot be lawful as the data subject cannot give his/her consent validly. Concerning the examined topic, this problem results in the fact that data processing based on automated individual decision-making related to the insurance contract, which is performed on special data, is not feasible; so, this rule hinders such technological efforts and the development of insurance in this direction. We cannot ignore the fact that insurance contracts under which an insurer processes any special category of personal data are specifically contracts that require the processing of these data. However, we cannot find in Article 9(2) of the GDPR a condition that would allow the processing of special data on a contractual basis, and – given the nature of the data – it is not sufficient to process data regarding Article 6(1)(b); the condition laid down in Article 9(2) for the lawfulness of the processing must also be met.

As I explained above, the insurer may process health data in connection with the insurance contract only with the consent of the data subject, and the lawfulness of data processing through automated decision-making based on the GDPR may only be ensured with the data subject's consent. Does the question arise as to whether the expression of the will required for the conclusion of the contract can constitute the consent of the data subject? In the light of the rules set out above, we must give a clear negative answer, but, hopefully, the status will change in virtue of Guideline no. 6/2020 of the EDPB.[68] The EDPB commented on the requirement for explicit consent in Article 94(2) of the PSD2 Directive in the Guidelines.[69] Accordingly, the provisions on consent in Article 94(2) of the PSD2 Directive

68 EDPB Guideline no. 6/2020.

69 According to this provision: 'Payment service providers shall only access, process, and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user.'

and Article 6(1)(a) of the GDPR are not the same – the latter must be regarded as a 'contractual consent'. This opinion is based on a view that the processing of personal data is an essential condition for the provision of this service, in particular because the processing of personal data of the person using the service is always to perform the contract; so, it has a contractual nature, which embodies the will necessary for the contracting.[70] As the processing of specific data is not a priority for services provided under the PSD2 Directive, the content of the 'contractual consent' does not cover these data, i.e. the additional conditions set out in Article 9(2) of the GDPR. The questions arise as to whether the processing of specific data is a condition of the performance of the contract and whether the 'contractual consent' can be regarded as a consent within the meaning of Article 9(2)(a) of the GDPR. If the express consent provided for in Article 136 of the Insurance Act and Article 22(4) of the GDPR could be considered as having been given at the time of the contracting, we would find a solution to the problems expressed above concerning the consent. The adoption of this is only one step away from the provisions of this EDPB guideline, which does not harm the interests of the data subject in the protection of the special category of personal data.

6. Conclusion and Proposal for the Improvement of Legislation

I believe that innovation in insurance will increase significantly in the future as the use of IT-based tools increases daily, and the societal utility of these tools is indisputable for insurers in order to 'serve humanity'. The most important goal of the innovations affecting each insurance type is to optimize the risk management mechanism by continuous and real-time data collection and analysis, which can lead to more flexible contract structures. From the customer's point of view, this means primarily a use-based or risk-based fee calculation, and thus the fair distribution of the risk to the risk pool. From the insurer's point of view, the determination of the real and actual extent of the risk requires a more precise definition of the capital requirements, including the amount of disposable income, which results in a more stable business for the insurer and a more reassuring capital coverage for customers.

The most important and common feature of insurance innovations is that they perform real-time data collection and data analysis, most of which is personal data about the customer. It may therefore be a challenge for insurers to suit the use

70 I agree with Zsolt Bártfai's comments on Guideline no. 6/2020 of the EDPB that 'a contract may not be concluded without the parties agreeing on the terms of the contract'. Because of this, its essential element is the expression of the contractual will, and thus of the consent to data processing. See Bártfai 2020.

of these innovations to the data protection requirements, in particular provisions of the GDPR. The technological solutions used in insurance automatically collect personal data about the customer, thus automatically performing a risk analysis according to a predefined algorithm and, as a result, determining the consideration for the insurers' risk taking. From a data protection point of view, this constitutes automated individual decision-making based on profiling, which is generally prohibited by Article 22(1) of the GDPR.

Article 22(2) of the GDPR sets out the exceptions for which automated individual decision-making is considered legitimate. The biggest challenge in the insurance business is the processing of specific data, especially health data. The source of the problem is the rule in Article 22(4) of the GDPR that the processing of specific data by automated individual decision-making can only be lawful with the consent of the data subject. However, the study explained that the validity of the consent given in the context of a contractual relationship cannot be established for several reasons, thus not ensuring the lawfulness of such data processing. As a result, it may become impossible to apply innovations related to the insurance business based on automated individual decision-making concerning the processing of sensitive data.

The problem would be solved if all the legal provisions related to the insurance contract which require consent to the processing of any special category of personal data necessary for the performance of the contract in the given legal relationship would be interpreted as 'contractual consent', an expression of the contractual will. I believe that the general acceptance of this view, in addition to the controversy that has been mentioned, could also eliminate a lot of the problems affecting the contracts.

We have a similar problem if we examine Section 136 of the Insurance Act, as this provision makes the consent of the data subject mandatory for the lawfulness of the processing of health data, regardless of the use of technological means. This provision is contrary to the requirements of the GDPR, which can be resolved by legislative intervention, repealing the provision. Until that happens, insurers will find themselves 'between Scylla and Charybdis' to comply jointly with the provisions of the rules of the Regulation and the Insurance Act.

References

ALFÖLDY, K.–SEREGDY, T 2015. A jövő biztosítása, avagy a technológia szerepe a lakossági ügyfelek biztosításában. *Biztosítás és Kockázat* 2: 48–63.

BÁRTFAI, Zsolt. 2020. Comments on the Draft Guidelines 6/2020 of the European Data Protection Board. https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/comments_to_6-2020_guidelines_final.pdf (accessed on: 10.11.2020).

BÖLCSKEI, K. 2019. *GDPR kézikönyv. 2.0. Új EU-s Adatvédelmi rendelet, Info tv., GDPR Salátatörvény*. Budapest.

ESZTERI, Dániel. 2020. Elosztott mesterséges-intelligencia-fejlesztés blokklánc alapon az adatvédelem érvényesülése érdekében. *Pro Futuro* 1: 9–27. (https://doi.org/10.26521/Profuturo/2020/1/7554).

EUROPEAN DATA PROTECTION BOARD. 2020. Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data – Version for Public Consultation. See: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf (accessed on: 06.01.2021).

EUROPEAN DATA PROTECTION BOARD. 2020. Guidelines 1/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf (accessed on: 06.11.2020).

EUROPEAN DATA PROTECTION BOARD. 2020. Guidelines no. 6/2020 on the Interplay of the Second Payment Services Directive and the GDPR. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202006_interplaypsd2andgdpr.pdf (accessed on: 10.11.2020).

EUROPEAN DATA PROTECTION BOARD. 2020. Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (accessed on: 20.11.2020).

EUROPEAN PARLIAMENT. 2017. Resolution on Distributed Ledger Technologies and Blockchains: Building Trust with Disintermediation (2017/2772(RSP)). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018IP0373&from=HU (accessed on: 16.11.2020).

GATTESCHI, V.–LAMBERTI, F.–DEMARTINI, C.–PRANTEDA, Ch.–SANTAMARÍA, V. 2018. Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? *Future Internet* 2: 1–16. DOI: 10.3390/fi10020020.

HAUER, J.–GÓG, E.–HORVÁTH, A.–HRABÁR, Á.–PÁLINKÁS K.–URBÁN, D. 2017. A használatalapú biztosítás múltja, jelene és jövője. *Biztosítás és Kockázat* 2: 22–41. DOI: 10.18530/BK.2017.2.22.

KADOCSA, F. 2018. A blockchain technológia hatása a biztosítási piacra. *Biztosítás és Kockázat* 2: 82–93. (DOI: 10.18530/BK.2018.2.82).

KAGAN, J. 2019. *Fintech*. https://www.investopedia.com/terms/f/fintech.asp (accessed on: 22.07.2019).

KERÉNYI, Á.–MÜLLER, J. 2019. Szép új digitális világ? – A pénzügyi technológia és az információ hatalma. *Hitelintézeti szemle* 18(1): 5–33. DOI: 10.25201/HSZ.18.1.533.

KOUNOUDES, A. D.–KAPITSAKI, G. M. 2020. A Mapping of IoT User-Centric Privacy Preserving Approaches to the GDPR. *Internet of Things* 11: 1–18. DOI: 10.1016/j.iot.2020.100179.

NAIH. 2017. Commitment of the Hungarian DPA from 18 June 2017. https://www.naih.hu/files/Adatved_allasfoglalas_naih-2017-3495-2-V.pdf (accessed on: 04.01.2021).

2018. List of Assessment under Article 35(4) of the GDPR. https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf (accessed on: 04.01.2021).

OSZTOPÁNI, K. 2018. Alapfogalmak. In: *Magyarázat a GDPR-ról*. Budapest. 63–94.

RÉVÉSZ, B. 2018. Az adatkezelés alapelvei. In: *Magyarázat a GDPR-ról*. Budapest. 95–109.

SALLAI, L. 2019. Insurtech: körkép és trendek. *Biztosítás és Kockázat* 4: 98–109. DOI: 10.18530/BK.2019.4.98.

ZAVODNYIK, J. 2018. Az általános adatvédelmi rendelet biztosítók általi alkalmazásának egyes kérdései. *Biztosítás és Kockázat* 2: 14–39. DOI: 10.18530/BK.2018.2.14.

WÁGNER, M. 2017. Insurtech – lehetőség a piacon vagy veszély az üzletre? *Biztosítás és Kockázat* 4: 60–67. DOI: 10.18530/BK.2017.4.60.

WANG, H. D. 2020. Research on the Features of Car Insurance Data Based on Machine Learning. *Procedia Computer Science* 166: 582–587. DOI: 10.1016/j.procs.2020.02.016.