bpv GRIGORESCU ȘTEFĂNICĂ

Can InsureTech survive in the GDPR era?

December 12, 2017

Nowadays, technology has become an important and essential part of every day's life. The field of insurance makes no difference in this respect. Although such a vast and complex field is usually resilient to major changes, technology has made its way into the insurance market, more and more insurers being mesmerized by the significant benefits brought by the technological developments.

It is undisputable that technology has improved the overall quality of the services rendered by the insurers, by reducing cost and maximizing efficiency. The most common trends in the insurance market are the implementation of artificial intelligence, the use of telematics (and other smart devices) and the use of the blockchain technology.

However, insurers must be cautious in using such technology, as GDPR introduces a series of obligations for the controllers, aimed at safeguarding the rights and freedoms of data subject. In the following paragraphs, we will address the most significant risks that the use of such technologies pose from the perspective of data protection.

Prohibition of automated decision making

The implementation of artificial intelligence, the use of chat bots and other AI technologies has made the insurance sector highly efficient in assessing individuals, concluding insurance contracts and even paying indemnities to the relevant parties. The most common practice of automated decision making is the "scoring" of individuals, in which, based on a certain algorithm, a computer program decides if a specific individual presents a high risk and whether an insurance policy may be concluded with him or her.

The same concept of "scoring" individuals is also used by the telematics devices. Telematics are similar to a plane's "black box" and are installed in the car of an individual, in order to assess their driving skills and determine the likeliness of the insured risk to occur.

Although no one can argue against the benefits of providing tailored solutions to the individuals, in respect to the insurance policies concluded, the lack of human intervention in the assessment process can pose significant risks for the rights and freedoms of the data subjects.

In accordance with article 22 of GDPR, the data subject "shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her". Working Party 29 ("WP 29") has stated, in the draft guidelines regarding automated decision making, that article 22 must be interpreted as a general prohibition of automated decisions making. As a consequence, any exceptions must be interpreted narrowly, and must provide sufficient safeguards for the rights and freedoms of the individuals concerned.

Paragraph 2 of article 22 of GDPR contains 3 exceptions to the general prohibition of automated decision making, provided that suitable measures to safeguard the rights and freedoms of data subjects are also implemented (i.e. at least the right to obtain human intervention):

a) explicit consent of the data subject;
b) authorization of Union or national law, provided that adequate safeguards are implemented;
c) the automated decisions making is necessary for entering into, or performance of a contract between the data subject and the controller.

The remedies at letter a) and c) are the most common in the insurance sector. Although consent may be considered the "strongest" justification for automated decision making, considering the precise circumstances in which the consent is obtained from the individuals may affects its validity.

Specifically, considering the privileged positions of the insurer and the fact that,

in most cases, the conclusion of the insurance policy will be dependent of the consent of the data subject, it may be argued that such consent is not freely given. Moreover, conditioning the service provided from the consent of the data subject also renders such consent invalid (e.g. if insurers would only concluded car insurance policies on the basis of telematics devices).

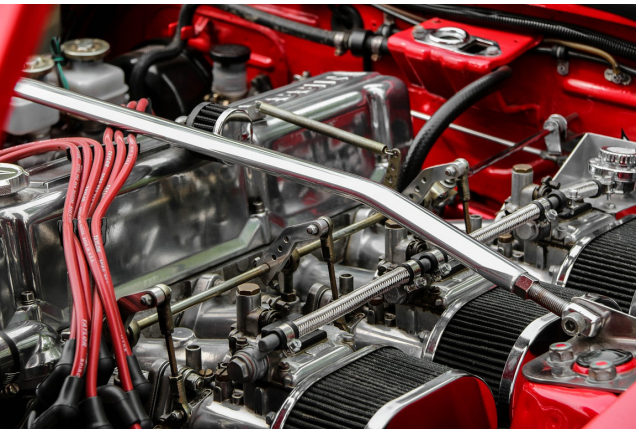
Therefore, the most likely exception to apply in the insurance sector remains the necessity of entering into, or performance of a contract. However, WP29 emphasizes the fact that "necessity" should be narrowly interpreted. In most cases, insurers will have to conduct a DPIA, in accordance with article 35 paragraph 3 letter a) of GDPR, in which other less intrusive methods must be taken into account. If other methods exist, and do not pose a significant financial burden on the insurer, the "necessity" criteria is not fulfilled. As such, the economic interest of the insurers, the efficiency and consistency arguments are not, in principle, sufficient in order to justify automated decision making.

Finally, with respect to the human intervention, this has to be more than a simple oversight of the automated decision making process. The persons involved must significantly influence the process and give meaningful insights with respect to the results of the profiling process (e.g. a person correlates the scoring results with its own assessment and decides on the basis of the aggregate result, whether a policy may be concluded with that individual).

Data minimization, accuracy and storage limitations with respect to the use of telematics

Although the use of telematics is not new to the global market, certain geographic regions have only just began to adopt telematics for car insurance policies. The telematics devices collect a high volume of personal data regarding the driver such as: location, driving speed, acceleration, cornering, braking and in certain cases even event occurrence (e.g. when an accident occurs, based on the assessed gravity, the relevant authorities are immediately notified). Based on the data collected, a special algorithm assesses the likeliness of the insured risk to occur, and adapts the premium of the insurance policy accordingly (in certain cases the scoring process may also result in a refusal to conclude new or renewed insurance contract).

Certain categories of drivers were considered to present a "high risk" without being subject to any individual assessment (e.g. young drivers). Telematics devices will enable insurers to assess the concrete risk, thus adapting the insurance policies to the actual driving skills of the insured persons, irrespective of their age or other immaterial criteria. However, certain concerns must be raised with respect to the compatibility of such devices with the provisions regarding data protection.



Specifically, the principle of data minimization must be strictly observed by the insurers. The telematics devices collect a huge amount of personal data, in an indiscriminate manner. However, not all data may be relevant for the intended purpose of the insurer. For example, the insurers must assess whether all types of collected data are strictly necessary for the scoring process, whether the duration of collection does not exceed the intended purpose and whether the appropriate technical and organization measures have been implemented in order to safeguard the rights and freedoms of the data subjects.

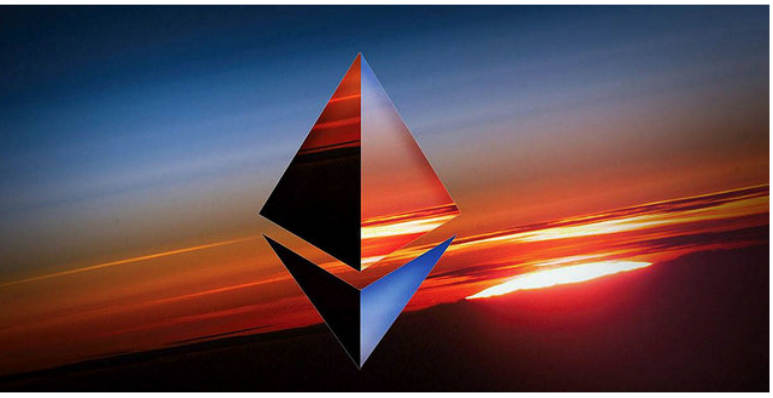
In the light of the above mentioned principles, the purpose of a telematics device is to assess the likelihood of the insured event and to adapt the insurance policy accordingly (e.g. higher premiums, risk exclusions etc.). Consequently, keeping the device active for the entire duration of the insurance policy (permanently monitoring the driver) would exceed this purpose and would be in violation of the above mentioned principles.

Moreover, a relevant aspect, often not addressed by the insurer is the accuracy and storage limitations of the profiling data collected. The human individual is highly dynamic, and their driving style and abilities are, likewise, constantly changing. Therefore, could there be any reason for keeping the data after the conclusion of the insurance contract? Most insurers would argue that such data is necessary for the renewal of the insurance policy, but it is highly unlikely that such data would be accurate after a significant period of time. Moreover, since the relationship between the insurer and insured person is mainly of contractual nature, it is doubtful that the pre-contractual circumstances

have to be stored after the conclusion of the contract, as the understanding of the parties will be the contract itself and all pre-contractual elements would already be included in the contract (implicitly or explicitly).

In cases where the third party liability insurance is vehicle anchored (i.e. there are multiple drivers), additional aspects must be taken into consideration. If all the potential drivers are assessed by the telematics devices and their scores are used in aggregated form, such data would not constitute personal data and would be excepted from the GDPR. On the contrary, if not all drivers are assessed, the necessity of the telematics may be challenged, and therefore, may be in violation with the provisions of the GDPR. Such situations will have to be assessed on a case by case basis.

The dawn of blockchain



Finally, one of the most discussed and controversial technology topic at this moment remains the blockchain technology together with smart contracts. More and more companies from various sectors are drawn by the benefits that this technology offers, such as impenetrable security (at least at this point) and transparency.

Indeed, the fact that no operation can ever be deleted or removed from the block chain offers tremendous security and trust in such technology, especially in the highly sensitive sectors such as banking and insurance. However, its most recognized quality may also be its greatest threat, as it is difficult to anticipate how this technology will reconcile with the right to be forgotten, introduced by the GDPR, but also with the principle of accuracy.

Article 18 of the GDPR states that data subjects may request the erasure of the personal data concerning them. No straight forward exception applies to the blockchain technology, so if data subjects exercise their right to be forgotten, what should the controller which is faced with this impossible task do? But what if the records are false or erroneous?

These questions do not have a specific answer at this point. In practice, one of the solutions proposed in order to overcome such conflict was the encryption of personal data uploaded in the blockchain. Indeed, if only the data subject holds the key to such data, enforcing the right to be forgotten on other controllers would not be necessary. However, whereas uploading encrypted information over block chain has the role of ensuring safety of such information (like an indestructible vault), it neglects many of the other functions of such technology (such as transparency).

What remains certain is that block chain technology is here to stay, especially considering the benefits of such a technology. Therefore, it is the task of the European legislator, as well as of the developers, to implement, agree and develop adequate measures in order to reconcile the block chain networks with the relevant provisions regarding data protection (perhaps by introducing relevant legal exception or creating alterable block chains).

So what now?

The pace with which technology takes hold of our lives is overwhelming, and it is highly unlikely that this progress can be stopped (would we even want that?). So, how can controllers minimize the risk of heavy fines? The only reasonable answer is: balance. Given the high risk that technology poses to the rights and freedoms of individuals, a balance must be struck between the benefits of tech and its risks.

In this respect, it is foreseeable that in the near future DPIA's will become a frequently used mechanism to address and mitigate the risk from the constantly developing field of technology. Although most companies will be reluctant, they will eventually have to allocate significant resources to carrying out DPIA's, especially if their internal business processes are keeping the pace with the development of new technologies. The only question that remains is: what is worth spending for a company to avoid a 20 million Euros fine?

Radu Zmaranda
CIPP/E, Associate
radu.zmaranda@bpv-grigorescu.com

bpv GRIGORESCU ȘTEFĂNICĂ
33 Dionisie Lupu Street
RO-020021 Bucharest
Phone: +40 21 264 16 50
Fax: +40 21 264 16 60
office@bpv-grigorescu.com
www.bpv-grigorescu.com

bpv LEGAL Alliance

bpv BRAUN PARTNERS
Europeum Business Center
Suché mýto 1 SK-811 03 Bratislava
Phone: +421 233 888 880
Fax: +421 257 200 170
Email: bratislava@bpv-bp.com
Web: ww.bpv-bp.com

bpv HÜGEL RECHTSANWÄLTE
Rond Point Schuman 9, Postbox 14,
B - 1040 Brussels
Phone: +32 2 286 81 10
Fax: +32 2 286 81 18
Email: brussels@bpv-huegel.com
Web: www.bpv-huegel.com

bpv JÁDI NÉMETH
Vörösmarty tér 4.
H-1051 Budapest
Phone: +36 1 429 4000
Fax: +36 1 429 4001
Email: budapest@bpv-jadi.com
Web: www.bpv-jadi.com

bpv BRAUN PARTNERS
Ovocný trh 8
CZ-110 00 Prague 1
Phone: +420 224 490 000
Fax: +420 224 490 033
Email: prague@bpv-bp.com
Web: www.bpv-bp.com

bpv HÜGEL RECHTSANWÄLTE
Donau-City-Str. 11, ARES-Tower
A 1220 Vienna
Phone: +43 1 260 50 0
Fax: +43 1 260 50 133
Email: vienna@bpv-huegel.com
Web: www.bpv-huegel.com