GDV
DIE DEUTSCHEN VERSICHERER

Position Paper

of the German Insurance Association (GDV)

on the White Paper on Artificial Intelligence

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

German Insurance Association

Wilhelmstraße 43 / 43 G, 10117 Berlin
P.O. Box 08 02 64, 10002 Berlin
Phone: +49 30 2020-5000
Fax: +49 30 2020-6000

51, rue Montoyer
B - 1000 Brussels
Phone: +32 2 28247-30
Fax: +49 30 2020-6140
ID Number 6437280268-55

Contact:
Legal and Compliance
Consumer Policy/Data Protection

E-mail: recht@gdv.de

Introduction

The German insurance industry endorses the specific European approach taken by the EU-Commission to leverage the enormous potential of data and algorithmic systems for sustainable economic growth and societal wellbeing in Europe while adequately addressing potential risks. This also implies that beneficial applications of the new technologies should not be prevented or slowed down by over-regulation. A thorough, unbiased discussion on the use of algorithmic systems and artificial intelligence is the right approach in this context. A regulatory framework and policies that promote technological innovations are crucial for sustaining and increasing prosperity and quality of life of our society and each individual as well as the international competitiveness of the European Union. The aim should therefore be to **achieve a high level of protection while at the same time promoting digitalisation** and technological progress.

Existing principles of liability for damage caused to third parties, and especially the Product Liability Directive (PLD), are fit for purpose to address the risks posed by AI-applications. Rather than altering existing liability systems, developing appropriate product safety and security legislation and technical standards for AI-applications needs to be prioritised.

I Current regulatory framework

The EU-Commission's approach to first assess the effectiveness of the current regulatory framework with regard to AI is sensible. As the Commission correctly determines, the existing EU-legislation is fully applicable to AI-applications. However, it should not only be assessed whether existing laws can be enforced adequately to address the risks created by AI systems. It should also be reviewed whether the current regulatory framework hinders their beneficial use and thus needs to be adjusted to facilitate AI dissemination. It is commendable that the Commission wishes to create the right incentives for the adoption of AI, but in most cases sufficient business incentives would already be there. The adoption is rather made difficult by legal uncertainty and strict regulation. For instance, Art. 22 GDPR and its strict interpretation by the European Data Protection Board would rarely even allow the use of simple, non-risky AI-systems for automated decision-making involving the processing of personal data unless the data subjects give their consent. Controllers face similar difficulties when their AI-systems require training with personal data since it is unclear which legal basis may apply aside from consent. As consent is rarely a viable solution (e.g. its withdrawal results in the obligation to delete the data and thus render the training at best inaccurate and at worst faulty), this situation contributes to the low investment level in Europe compared to Asia and the USA.

II Risk-based regulatory approach

We welcome the EU-Commission's recommendation to choose a risk-based regulatory approach. What is crucial for the effectiveness of this approach is the correct classification of the algorithmic systems into the different levels of risk.

Our assessment of the EC's recommendation is as follows:

- The approach is based on the correct assumption that the EU has a strict legal framework in place to ensure inter alia consumer protection, to address unfair commercial practices and to protect personal data and privacy.
- As a matter of principle, the new regulatory framework for AI should achieve its objectives effectively and efficiently. In particular, a disproportionate burden on users of AI - e.g. because of excessively prescriptive provisions – should be avoided
- A risk-based approach is important to help ensure that the regulatory intervention is proportionate.
- However, clear criteria are required to differentiate between the different AI applications, in particular in relation to the question whether or not they are 'high-risk'
- A given AI application should generally be considered high-risk in light of what is at stake, considering whether both the sector and the intended use involve significant risks, in particular from the viewpoint of protection of safety, consumer rights and fundamental rights. More specifically, an AI application should be considered high-risk where it meets the two cumulative criteria:

    - First, the AI application is employed in a sector where, given the characteristics of the activities typically undertaken, significant risks can be expected to occur.
    - Second, the AI application in the sector in question is, in addition, used in such a manner that significant risks are likely to arise.

However, we see the approach of the EU Commission to partly abandon the basic classification of high-risk AI applications on the basis of two factors in order to ensure legal certainty critically. According to the white paper, in exceptional cases AI applications should also be subject to the high-risk requirements if the two factors are not given.

The White Paper suggests that "further specific applications affecting consumer rights could be considered". This sounds vague and the scope can potentially be very broad. Nor it is clear how "the application affecting con-

sumer rights" is defined. In our view these exceptional cases should be strictly limited if the EU Commission does not want to weaken its own good approach. If there are exceptions to the two-factor approach, these should be clearly defined. The requirements should also be determined on the basis of the principle of proportionality and in compliance with the risk-based approach.

III Definition of the scope

The scope of future legislation must be precisely defined. The White Paper rightly states that defining the scope is a central issue for the future specific legal framework for AI. The working hypothesis of the White Paper is that the legal framework should apply to products and services involving AI. It is therefore necessary - also according to the ideas of the EU Commission - that AI is clearly defined.

According to the clarification provided by the HLEG, artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.

As such, algorithms that do not incorporate any form of machine learning or self-improvement should by definition not be subject to AI-regulation. The use of algorithms, for example, to determine insurance premiums, should not be included in the scope. The provision of private insurance cover has always required respective providers to analyse respective data and apply the results accordingly by means of mathematical algorithms. Ever since the insurance industry has emerged, insurance undertakings have therefore made extensive use of data and algorithms.

IV Insurance industry is not a high-risk sector

For the insurance industry there is no need for additional, special regulation as planned for high-risk AI applications.

The insurance industry, as part of the financial services sector, is highly regulated. On the occasion of the consultation of the HLEG our analysis has shown that all high-impact ethical principles are already covered by the existing regulatory framework for the insurance industry. Because leg-

islation is generally technology-neutral, novel technologies or methods such as AI are already captured by the existing regulatory framework and supervisory authorities are continually refining their approaches regarding new technologies.

The German insurance industry is subject to supervision on the european and on the national level (EIOPA and BaFin). Both EIOPA and BaFin have already increased their regulatory efforts in this field, and they have the expertise required for this purpose. Already today the regulations of the analogue world in insurance automatically apply to the digital world as well. Double regulation should be avoided.

V Requirements for high-risk AI-applications sometimes too extensive

1. Training data

Among others the Commission proposes establishing requirements that ensure AI systems being trained on sufficiently broad data sets that cover all relevant scenarios. This proposal appears sensible. With respect to personal data, a specific regulation should explicitly state that the principle of data minimisation pursuant to Art. 5 GDPR does not prohibit such training as long as it is necessary to ensure the safe use of the AI system.

2. Keeping of records and data

The call for a higher level of comprehensibility of algorithmic decisions is understandable, however, it ignores the burden which such a duty to draw up documentation will place on companies. We believe that the potential benefit of such a duty should be proportionate to the burden put on providers. We appreciate the approach, that if a fundamental, comprehensive duty to draw up documentation is actually being implemented, it should only apply to systems which have a significant potential for harm. It should further be taken into account that the GDPR already contains comprehensive obligations concerning the processing of personal data which also apply to AI systems.

3. Human oversight

Any future legislation must by necessity ensure that the requirement of human oversight does not counteract the advantages gained by using AI systems. AI systems are subject to intensive training and analysis during the design phase prior to their use. That is why, it should generally suffice that the customer or data subject is granted the right to request that a human retroactively reviews a decision made by an AI system and corrects

the decision in case he deems it necessary. Prior validation of algorithmic decisions before they become effective or constant monitoring and intervention in real time should only be required for decisions made by AI systems which cannot be reversed.

Even if the insurance sector is not classified as a high-risk sector and no ex-ante compliance check is foreseen for the insurance sector, these considerations should in principle be viewed critically.

VI No conformity assessment

The EU-Commission recommends using an objective, prior conformity assessment to verify and to ensure that certain of the mandatory requirements apply to high-risk applications. These procedures should explicitly be established in addition to already existing regulation.

For the insurance sector, such a conformity assessment is generally not required. Such considerations should take into account how the relationship to the already existing supervisory powers of the Federal Financial Supervisory Authority *(BaFin)* would be. As regards industries that are already subject to regulation and comprehensive oversight, additional regulation seems unjustified in terms of a cost/benefit analysis. Otherwise there would be a strong risk that many innovations benefitting customers and the society might be stifled and that the attractiveness and performance of the insurance market might decline relative to foreign markets due to bureaucratic requirements.

Moreover, the planned conformity assessment is problematic because it can prevent a quick adaptation of algorithms and systems. It is also to be feared that certification will lag behind technical progress and that modern procedures can only be used with delay in the areas of application concerned.

Separate licensing procedures are therefore not required in the insurance sector. The Federal Financial Supervisory Authority *(Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin)* already has the possibility to examine product conditions, calculation bases as well as the underlying algorithms and impose respective measures where considered necessary.

VII Governance

The EU-Commission’s proposal that a governance structure on AI should feature comprehensive cooperation between the national authorities of different EU-member states is agreeable. Special caution should be taken to avoid repeating the situation that persists with regard to the different

national data protection supervisory authorities. Their diverging opinions on the data protection regulation actually promote fragmentation and gold plating.

VIII Liability and Liability Insurance

Existing principles of liability for damage caused to third parties, and especially the PLD, are fit for purpose (adequate and appropriate) to address the risks posed by AI and other emerging digital technologies. The PLD constitutes a well-balanced system by providing a high level of protection to injured persons while at the same time taking into account producers' legitimate interests and thereby encouraging technological innovation and promoting economic growth.

Rather than altering the existing liability systems, developing appropriate product safety and product security legislation, technical norms and standards (rules on design, production and operation) for innovative digital technologies should be prioritised. These act as a filter for liability and help to define whether a product does not provide the safety which a person is entitled to expect and is therefore defective under the PLD.

The concept of a product defect as trigger for producer liability is indispensable. It provides the justification for imposing the economic burden for damage on the producer. Abandoning it would shift liability to the producer even for a product that *does* provide the safety which a person is legitimately entitled to expect, as well as in cases where persons other than the producer have caused the damage (e. g. the operator choosing an inappropriate product or using it incorrectly, or persons performing maintenance, repair or overhaul of the product).

Software should be considered a product under the PLD.

Products and services should continue to be distinguished from each other. In case of “embedded software”, potential difficulties in determining whether a product or a service has caused damage will be mitigated by recognizing software as a product. Refurbishers, i. e. entities that go beyond maintenance, repair and overhaul by altering an existing product in such a way as to turn it into a new product which they market themselves should be classed as producers.

A risk-based approach is highly appropriate for determining product safety and security for AI applications as the term encompasses a multitude of uses and devices that will require specific solutions.

But at the liability level, an additional risk-based differentiation prescribing more stringent levels of liability within the PLD for certain products deemed especially dangerous is not required.

The PLD's technology-neutral approach is one of its biggest advantages. Its imposition of strict liability on all producers is in itself a risk-based decision. Strict, as opposed to fault-based, liability is traditionally only imposed on activities that are deemed inherently particularly dangerous.

Defining and identifying those products that are deemed so dangerous as to mandate inclusion in a special "high risk liability" category would be highly contentious and difficult. Frequent amendments to the catalogue would jeopardise legal certainty for producers.

The defences available to producers – with reversed burden of proof - under the PLD must be conserved. They are a necessary correlation of producer's strict liability.

The 'development risk defence' (e.g. the product's defect was objectively not discoverable according to the state of science and technology - the strictest test known to technology law - at the time of marketing) is vital to enable technological innovation. Innovation would be discouraged if producers could be held liable for defects that were objectively undiscoverable when brought to market.

The 'later defect defence' promotes legal certainty by clarifying that a producer is only liable for defects that existed when the product was put into circulation as the producer ceases to have control over the product at that time. In the case of products requiring continuous software updates provided by the producer or by others on his behalf, such updates should be considered to have been put into circulation when made available for download or automatically downloaded and installed in devices. That cannot, however, mean that the product in its entirety is put into circulation anew every time its software is updated. Where damage is caused by defects unrelated to software updates, the relevant time would continue to be when the product as such was originally put into circulation. Otherwise producers would be eternally liable for such products, which would contravene the basic principle that all liability must be time-barred at some point.

The burden of proof on the injured party for the damage, the defect and the causal link between them should not be altered. This is, again, a correlation to producers' strict liability.

Automated and connected devices are controlled by software. Access to data stored by these systems will be key to allocating responsibility for

damage either to the producer (if caused by a product defect) or to the user (if caused by the circumstances of use). Questions of data recording, storage and access should be addressed by regulations outside of liability legislation (e. g. on product safety and security), and not within the PLD's rules on the burden of proof.

Infringements of basic rights (data protection, discrimination, privacy) should continue to be dealt with exclusively in existing dedicated EU legislation such as the GDPR. Basic rights infringements are alien to the PLD's concept and adding related provisions to the PLD could only provoke a conflict of statutes. Consistency and coherence between the various legislative instruments at EU level must be preserved.

Introducing compulsory insurance requirements for producers would be unnecessary and would not work in practice.

A free voluntary insurance market is best able to provide tailored insurance solutions that are designed to cover the individual insured's risks and liabilities.

Compulsory insurance only works where a large pool of identical or sufficiently similar risks exists, allowing insurers to draw on sufficient data to quantify and price these risks. This is not the case for AI applications at this time.

'AI applications' covers a wide range of different systems and uses, and effective insurance protection must be geared towards individual risk exposure. But compulsory insurance of necessity introduces a "one size fits all" approach when defining minimum requirements. These tend to be orientated towards higher risks. Insureds with a lower risk profile are forced to buy an excessive level of insurance that is uneconomical (higher premiums). Particularly exposed insureds, on the other hand, may be deterred from purchasing the (higher) level of insurance that would be appropriate for their individual risk profile, as a lower level of protection would come cheaper and still meet legal requirements.

Insurance solutions are readily available to cover the liabilities of producers of AI applications. Introducing obligatory liability insurance would be unnecessary as product liability insurance on a voluntary basis is already standard for companies from all sectors of the economy, to include AI applications and other emerging technologies. Subjecting producers of AI applications to compulsory insurance would cause this cover to be removed from existing product liability policies and require producers to buy additional and separate insurance.

Berlin, May, 2020