Die Bundesregierung

Comments from the Federal Government of the Federal Republic of Germany

on the White Paper on Artificial Intelligence - A European Concept for Excellence and Trust COM (2020) 65 final

Introduction

The Federal Government would like to thank the European Commission for submitting the White Paper on Artificial Intelligence and the Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, and for providing the opportunity to comment on it.

The White Paper addresses key parameters for unlocking the potential of artificial intelligence (AI) and counteracting potential risks. With its national AI strategy, the Federal Government is pursuing the goal of making Germany and Europe a leading centre for AI and thus helping safeguard Germany's and Europe's competitiveness in future. The Federal Government shares the European Commission's objective of basing an AI ecosystem on European values and rules, which will open up the advantages of this technology to the entirety of European society and economy.

AI systems are already in everyday use in industry and services, such as in the B2B area and research. They are playing an increasing role for use by public authorities. They touch the lives of many people, for example, through virtual assistants, the use of spam filters, selection of human resources, credit scoring or in medical diagnostics. While these constantly growing application possibilities can be accompanied by major economic, social and individual benefits, they may also entail risks. The Federal Government's objective is to promote the responsible, public interest oriented and human-centric development and use of AI, and to promote competitiveness and innovation in the European Union.

For the Federal Government, the ecosystem of excellence means a balance between innovative research, competitive companies, modern administration and people possessing digital competence. We share the view of the EU Commission that the use of AI will make a significant contribution to achieving the goals of the European Green Deal. Aligning climate protection and competitiveness even more closely, ensuring more efficient and citizen-

friendly public administration, supporting efforts to cope with pandemics and promoting overall social and economic well-being are all in line with the UN's sustainability goals. The Federal Government is, therefore, advocating a broad-based, value-creation network in order to make the innovative potential of AI technologies and the excellent European AI expertise available to actors of all sizes and sectors. There are tremendous opportunities for business and the economy, especially if small and medium-sized enterprises are provided special support in the application of AI. Comprehensive development of AI competence is also required. An ecosystem of excellence can ensure that the European Union further strengthens its pioneering role in the field of research and safe and trustworthy technology design and that the opportunities offered by AI systems are put in the service of all humans. The current COVID 19 pandemic, in particular, demonstrates that AI can make an important contribution to crisis management.

The Federal Government would note that, to shape the ecosystem of excellence, appropriate funding is indispensable for the relevant programmes of the Multiannual Financial Framework (especially the Digital Europe Programme).

At the same time, we need a European regulatory policy on AI. All actors need planning and legal certainty and need to be able to trust AI applications. The human-centric and traceable development and deployment of AI systems on the basis of an appropriate legal framework must be an integral part - and thus a trademark of - "AI Made in Europe". As the COVID-19 pandemic has shown, the legal framework must be sufficiently flexible to accelerate innovation when the task at hand is to avert major damage to the Community.

The ecosystem of trust is based on existing law, in particular on the provisions of the General Data Protection Regulation and the Directive on Data Protection in Law Enforcement. In general, security and respect for civil and consumer rights, in particular fundamental rights (such as freedom of action, informational self-determination, freedom to choose an occupation, equal treatment and effective legal protection), must remain guaranteed, even in the case of new types of risk that can be traced back to certain specific characteristics of AI. The different requirements relating to fundamental rights must be taken into account, ranging from the use of AI systems for state intervention to other areas of AI use.

To counter risks effectively, specific requirements must be set for the development and deployment of AI systems. These include, in particular, a risk-adequate level of transparency and traceability (“Nachvollziehbarkeit”) as well as, if necessary, an appropriate control structure and verifiability of AI applications and their results.

At the same time, the question to be answered is whether the existing legal framework of product safety and product liability for AI systems embedded in products is sufficient or whether new regulations also need to be established in order to provide legal certainty.

Finally, standardisation can contribute to the acceleration of development processes, legal certainty for companies, and greater trust and confidence among the population in the technology.

Part 1: An ecosystem of excellence

The Federal Government welcomes the proposed measures to create an ecosystem of excellence in order to maintain Europe's leading position in research, promote innovation, expand the application of AI and achieve the goals of the European Green Deal. Measures need to be closely interlinked with other relevant strategies and initiatives in the overall picture, for instance, with the industrial and SME strategy and the announced mobility strategy. Europe's existing strengths in research, innovation, industry and services need to be further developed, and AI should be more widely used in business and economy, including at SMEs. At the same time, AI can contribute to a CO_2-neutral, resource-efficient economy.

A. Working with the Member States

Close cooperation between Member States is essential. The revision of the Coordinated Plan is necessary and useful in order to adapt it to current developments and in this manner, respond to urgent challenges. The Covid-19 pandemic in particular has presented society and the economy with new major challenges.

The use of artificial intelligence can also support efforts to cope with pandemics. In areas such as diagnostic and therapeutic assistance, telemedicine, protection of certain population groups, and search for a vaccine, AI already offers promising solutions. To this end, a European Health Dataroom is needed to facilitate rapid sharing, use and analysis of data in compliance with data protection. This needs to be further researched and used throughout Europe.

In the view of the Federal Government, the aim of the further development of the Coordinated Plan should be the creation of a responsible, sustainable, public-interest-oriented and human-centric European AI ecosystem as a value-creation network for

innovations. To this end, actors of all shapes and sizes from all sectors should be linked with one another across national borders. This includes not only science, research, business, policy-making and administration, but also civil society, whose instruction and participation in the development and application of AI is important for its acceptance and trust.

With the GAIA-X project, Germany and France have already laid an operational cornerstone for a decentralised European data infrastructure, and Germany intends to further refine and develop this in future together with other Member States.

Investments are essential to expanding the potential offered by artificial intelligence. Leveraging effects should be sought after through supporting investments by Member States and enterprises, for example. The corresponding programmes of the EU Commission in the new Multiannual Financial Framework, such as "Digital Europe" and "Horizon Europe", as well as from the European Structural and Investment Funds must therefore, be provided with sufficient financial resources.

The Federal Government endorses that the revised version of the Coordinated Plan will place a focus on social and environmental well-being as an important principle underlying AI. In the development of AI, solutions to social and ecological challenges should be taken into account as early as possible (e.g. through "sustainability by design"). AI applications can make a decisive contribution to achieving the goals for sustainable development laid down in Agenda 2030. Furthermore, the accessibility of AI applications should be guaranteed in all Member States.

B. Focusing the efforts of the research and innovation community

AI research activities should continue to be coordinated between Member States within the framework of the Coordinated Plan. As a key part of the value creation chain, research and development also offer the foundations for sustainable economic success in the field of AI. Fundamental questions in AI research, such as traceability, explainability, robustness and security, have not yet been clarified and require additional research efforts in order to better exploit the full potential of AI.

Existing European AI research centres need to strengthen their collaboration and cooperation with industry and public authorities. The proposed lighthouse centre for research, innovation and expertise should be organised as a decentralised network. It should be dedicated to both basic and application-oriented research, closely integrate users and promote the transfer to business and industry. It should build on existing European AI

networks and develop these further in the direction of specific application sectors. The transfer of knowledge and findings between different sectors, particularly with a view to creating confidence in overarching AI standards, could also play a central role.

The Federal Government supports the promotion of world reference testing centres in Europe, which should pool investments. It is important that test centres can be used by research projects and business enterprises alike, in particular SMEs, and,possibly, by the public administration. Ideally, test centres should also be combined with “Reallabore” (regulatory sandboxes). Regulatory sandboxes can also serve the aim of deregulation, but safety and protection standards must be maintained.

C. Skills

The Federal Government supports the Commission's approach of building up skills and competence in the field of AI on as broad a scale as possible in order to train young scientists in Europe, to further strengthen the broad use of AI in society and industry and to counteract the shortage of skilled workers. The development of digital skills must be promoted from childhood to adulthood. To this end, AI competence must be comprehensively conveyed both in educational systems as well as in continuing education and training, especially at SMEs. This includes ethical, legal, ecological and social skills. When building up skills and competencies, special attention needs to be devoted to diversity and to training and employing more women in this field.

The development of networks of leading universities and institutions of higher education should be pursued within the framework of the Digital Europe Programme. Universities of applied sciences should also be included in this, given their needs-based approach and proximity to SMEs. The development of skills and competencies should be supplemented by additional measures to support young scientists, such as doctoral programmes and further training programmes for users.
The changes that the use of AI in the world of work entails must be taken into account and must be a positive force for works councils and employees. Updating the Digital Education Action Plan is an appropriate means of supporting the Member States in further developing capacities and instruments for digital literacy, including in the field of AI. In order to strengthen AI skills at the European level, it is desirable to connect national AI learning platforms and AI courses and make these accessible to the general public.

D. Focus on SMEs

The Federal Government welcomes the focus on SMEs. The measures described must be

resolutely expanded so that the Digital Innovation Hubs reach as many SMEs as possible. Under no circumstances should the number of supported Digital Innovation Hubs be statically assigned to the Member States and limited to only one centre per country. Larger states need several centres spread over their territory in order to reach regionally-based SMEs.

When using AI in SMEs, process- and data-driven approaches can be helpful. For this purpose, processes in companies are first analysed in detail and this analysis is then used to identify where specific data should be collected and where AI can be applied to optimise the process.

E. Partnership with the private sector

Public-private cooperation is an important element in facilitating developments in the direction of an integrated European Data Space and ultimately, a European AI ecosystem as a value-creation network for innovation. With the GAIA-X project, governments, companies and various organisations in Germany and France, but also in other Member States, have already taken the first steps towards public-private cooperation.

Germany has set itself the goal of establishing a digital quality infrastructure for the development and, wherever appropriate, evaluation of AI systems, and to make this infrastructure available to users from other Member States. This is of great importance for the more rapid approval of products in regulated areas (health, safety or mobility).

F. Promoting the adoption of AI by the public sector

AI has great potential when it comes to sovereign national tasks and public administration and should be used more widely in these areas. The Federal Government, therefore, supports measures that promote the use of AI in the public sector. The point of departure is always respect for fundamental rights. In addition, citizens should be informed and involved in the development and application of AI in an appropriate manner so that their experience and needs can be taken into account. In addition to the proposed dialogues at the sectoral level, a dialogue regarding the opportunities and legal limits of the use of AI for sovereign tasks in the security sector should be initiated.

G. Securing access to data and computing infrastructures

Given the importance of data in the development and deployment of AI, the Federal Government welcomes the link between the White Paper and the European Data Strategy. Interoperability and the high data quality required must be ensured. It is also necessary to ensure the availability of high-quality analytical tools with which to work with data. There are great opportunities, particularly in the areas of health care as well as environmental protection, where the increasing spread of smart devices is generating data with tremendous potential for guaranteeing public services of general interest, even beyond the public sector.

The Federal Government would request the European Commission examine whether a second IPCEI in the field of microelectronics would be expedient. Within the framework of the European AI concept, access to critical hardware and software should be taken into account, and competitive services offered by European suppliers of chip manufacturers, start-ups and technology companies should be established. In addition, computing power is increasingly being provided through cloud models (hardware-as-a-service).

The Digital Europe Programme, as the new sectoral programme of the next Multiannual Financial Framework (MFF), should place a topical focus on supercomputers and AI. If the budget were to be significantly curtailed, the implementation of key initiatives on AI, data and industrial competitiveness would be acutely endangered and would prolong dependence on non-European technology and infrastructure. This could endanger the recovery of European industry in the wake of the COVID-19 pandemic.

H. International aspects

The Federal Government welcomes the fact that international cooperation is founded on a value-based approach and that the intention is to continue fostering AI development and deployment based on ethical and ecological principles while respecting human dignity and fundamental rights, including participation and protection against discrimination, privacy, personal data and accessibility, and to export this "European" approach in the context of international cooperation. In this context, economically weaker states should also be supported in taking advantage of AI for local innovation, for example, through Open Data. For reasons of European and national security, it may be warranted to deny access to some selected data sets in compliance with WTO rules and the provisions of the EU Dual-use Regulation. International business models based on data use and AI must be afforded planning certainty and protection if they adopt the European approach.

Part 2: An ecosystem of trust: Regulatory Framework for AI

The Federal Government shares the European Commission's assessment that AI entails both opportunities and risks. In the interest of all parties involved, it makes sense to have clear rules that can strengthen trust in AI, reasonably balance the various interests, leave room for further technical and socio-technical developments, and can accelerate their introduction. In order to build up a high level of trust in AI, it is necessary to develop and use AI in a human-centric, responsible and public-interest oriented way. In order to strengthen the Single Market, necessary rules should be adopted at the EU level and should apply throughout the EU.

A. Problem definition

The Federal Government shares the European Commission's analysis that the use of AI can pose risks to the fundamental rights of citizens, through unjustified discrimination, as well as with regard to safety and liability-related issues, for example.

At the same time, it points out that there are areas where the deployment of AI has enormous potential for innovation. Regulation must be carefully designed to encourage innovation, not to inhibit it.

B. Possible adjustments to existing EU legislative framework relating to AI

In Part 2, the European Commission rightly emphasises that EU legislation already applies to the development and deployment of AI, for example, with regard to fundamental rights, consumer protection, and product safety and liability. However, in some cases, these do not yet or do not adequately take into account the specific risks of AI applications mentioned in the White Paper. Thus there may be shortfalls in the application and enforcement of this legislation.

The Federal Government welcomes the proposed approach of reviewing the existing EU legal framework to determine whether current legislation is able to address the risks and requirements of AI applications, can be effectively enforced and, if not, what adaptations are needed or new legislation is needed.

C. Scope of a future EU regulatory framework

In addition to the possible adjustments to existing legislation (e.g. in the area of product safety and product liability law), a new legislation specifically on AI may be needed, depending on the outcome of the review.

In principle, the Federal Government welcomes the approach regarding an EU legal

framework for AI, outlined in the White Paper, which adequately addresses the opportunities and risks of AI, promotes innovation, balances interests in a fair manner and avoids over-regulation. As proposed by the European Commission, this framework should apply to products and services where AI is deployed and cover the use of AI by public authorities as well as by private individuals and businesses.
However, such an approach must take into account the fact that the use of AI by the public sector is subject to different underlying legal conditions than in the private sector. For example, in the area of state intervention, specific fundamental rights questions arise regarding the "whether" and "how" the government should use AI, such as, in the area of remote biometric identification.

The definition of "AI" is of great importance in this context. Here, a wording should be found that covers as many AI applications as possible. The definitional approaches, of the High-Level Expert Group, amongst others, lead in the right direction but to be operationalised as a legal term it must be concretised and defined more precisely while at the same time taking into account the dynamic development taking place in the field of AI.

The Federal Government supports the view of the European Commission that the legal framework should be founded on an opportunity and risk-based approach in order to ensure that regulatory intervention is proportionate. However, the differentiated implementation of a risk-based approach requires further discussion. While the European Commission is considering introducing requirements only for "high risk" AI systems, the Federal Government considers a classification scheme consisting of more than two levels appropriate. As the European Commission itself emphasises that certain aspects are not covered by existing horizontal or sector-specific legislation, it is questionable whether existing EU legislation solely is sufficient for AI applications whose risk level is below "high".

The Federal Government, therefore, requests the European Commission develop a classification scheme for AI systems together with the Member States. A regulatory approach based on opportunities and risks must take into account the different features of AI systems. On the one hand, the classification scheme must take into account the fact that there are applications without any potential to cause damage. On the other hand, the classification scheme must provide for gradations in line with relevant risks and damages, while taking into account the possible scale and probability of damage. Relevant risks may exist to life , health, property, democratic processes, the environment, climate, social, social and economic participation. The classification must, therefore, both accurately ascertain different risks posed by an application in a specific application context and enable a practicable assignment of the AI system in actual legal practice while taking into

consideration public and individual interests and that innovations must not be hindered. For this reason, special exceptions for research and development should be examined. In addition, applications with no potential for harm should not be subject to specific control.

Concerning the definition of a "high risk" AI system, the European Commission proposes specifying this characteristic in such a way that both the "sector" and the "intended use" of an AI system must entail "significant risks". As a consequence, certain uses fraught with risk would not be covered from the outset if they did not fall within certain sectors. The European Commission proposes "exceptional instances" which are to be classified as high-risk regardless of the sector concerned. The AI applications that the European Commission cites as examples in this connection (systems in the context of recruitment processes , consumer-relevant applications, remote biometric identification applications), warrant special attention from the Federal Government's point of view. However, the fact that the European Commission considers it necessary in the White Paper to specify exceptional instances requires reassessment and, if necessary, expansion of the cumulative definition of the "high risk" characteristic.

In addition to considering risks to safety, consumer rights and fundamental rights, it is essential to explicitly recognise other high-level public interest concerns, such as climate and environmental protection, and thus to exploit the great potential of "AI Made in Europe" for the Green Deal.

The Federal Government also suggests that a register and an obligation to report accidents and incidents in the form of a vigilance system be established for high-risk AI systems. Due to the nature of their assignments, security authorities almost exclusively use high-risk AI systems, they would be unduly affected by a vigilance system and a register. The central office for the use of AI by security authorities referred to in Section F should also serve as a central registry agency in charge of all security authorities in this sector.

D. Types of requirements

The Federal Government shares the view of the European Commission that aspects already covered by existing horizontal or sector-specific legislation should continue to be governed by this legislation. The classification scheme proposed above should include appropriate requirements for the risk in question. A potentially expanded EU legal framework for AI of this kind should be complemented by specific requirements if necessary.

In general, the Federal Government welcomes the catalogue of requirements formulated by

the European Commission with regard to training data, data and record-keeping, information provision, robustness and accuracy, human oversight and remote biometric identification systems. However, the respective specific requirements, the scope and concrete legal form of the requirements still need further elaboration. Furthermore, it should be examined whether and, if so, which additional aspects need to be laid down in laws and regulations as binding requirements (e.g. requirements pertaining to "energy efficiency" and bans on certain AI applications).

In addition to specific requirements, the Federal Government considers it expedient, in the interests of principle-based regulation, that central principles harmonised across the EU be formulated for trustworthy AI (for example, with regard to transparency, traceability, verifiability, non-discrimination, the possibility of final decisions being taken by humans, robustness, security, accountability, impact assessment, barrier-free accessibility). Harmonisation of such principles could facilitate uniform interpretation and application of the rules and regulations. They could also provide a framework for specifying details in the form of standards, as the European Commission rightly emphasises.

When imposing requirements, SMEs in particular, must not be disproportionately burdened.

The legal framework could also lay down basic guidelines for the subjective rights of users/consumers. This includes, in particular, detailed arrangements setting out the rights of stakeholders as well as provisions governing enforcement, for example, in the form of rules on presumption and burden of proof.

Turning to the details regarding the requirements set out in the AI White Paper:

a) Training data

First of all, the Federal Government expressly welcomes the proposal that binding legal requirements for training data for AI systems be considered. It considers this to be the right point of departure, as training data is an essential basis for the development of learning systems in particular. Consistent requirements for test and evaluation data should also be considered.

In the view of the Federal Government, depending on the classification of the AI system, this may also include quality parameters and requirements for training, testing and evaluation data, so that appropriate AI systems can be developed from quantitatively sufficient and high-quality data sets. Important indicators are, for example, the correctness, topicality, representativeness and completeness of data

sets. At the same time, the target context of the system and the application environment must generally always be taken into account in order to decide whether the quantity and quality of data sets meet the requirements. In the area of research and development it must be taken into account that training data sets cannot always meet the aforementioned requirements in terms of completeness and representativeness, the development of a suitable database may itself be part of research and development, and there must be sufficient latitude for the further development of systems.

When using AI systems, risks can arise with regard to unequal treatment relating to fundamental rights, for example, when training data map social inequalities, thereby perpetuating and possibly strengthening them. Non-representative training data sets or those that depict structural inequalities, but also errors in programming or lack of, or insufficient, quality assurance can preserve discriminatory structures and place individuals at a disadvantage. To strengthen trust and confidence, the manner in which AI systems work must be as transparent and traceable as possible.

In principle, the Federal Government supports efforts to optimise the security of AI systems through appropriate requirements applying to training, testing and evaluation data. We, therefore, believe that these overlap with requirements regarding robustness and accuracy. Regarding the consideration forwarded by the European Commission as an example that training, test and evaluation data need to cover all scenarios relevant to the avoidance of dangerous situations, however, the Federal Government would note that people can only act on the basis of recognisable and realistic risks. Therefore, it might be appropriate to formulate the requirement so that only recognisable and realistic scenarios have to be covered.

The Federal Government expressly supports the approach of the European Commission to effectively counter the discriminatory potential of AI systems, if necessary, by imposing binding requirements, amongst others on the representativeness/balance of data sets. The basis for assessing whether these requirements have been taken into account can also be the results produced by the respective AI system, which means that access to the training, test and evaluation data set as such is not always necessary. This requires, however, that suitable procedures be available for the operational scenario to review results in terms of representativeness and balance.

b) Keeping of records and data

In principle, the Federal Government supports the proposals relating to the documentation, recording and storage of data. Binding requirements can make an important contribution to the transparency, traceability and explainability of AI systems. They also facilitate effective monitoring and enforcement by the supervisory authorities in charge.

If an obligation to store data records is even required, this requirement presupposes a high level of data integrity and data security. Effective IT security provisions are required to prevent unauthorised access, unauthorised use or manipulation of data. Access to, and use of, stored data sets must be linked to formally verifiable legal requirements.

The AI White Paper does not yet indicate in which 'certain justified cases' there should be an obligation to store records as such. Particularly with regard to criminal prosecution, storage of training, test and evaluation data is indispensable in order to be able to trace possible biases and omissions. The "limited, reasonable time period" during which data sets must be retained also requires specification in greater detail.

In cases where such is necessary, requirements should be set for the type of documentation. In order to maintain traceability, auditability needs to be implemented to reflect the respective different version statuses of training, test and evaluation data as well as the software itself. Furthermore, organisational and technical measures must be taken to ensure that only authorised persons have access to training data, algorithmic models, protocols and possible evaluations.

c) Information provision

In principle, the Federal Government welcomes the requirement that certain information on AI systems is made available to the group of persons with a legitimate interest - consumers, citizens, operators of AI systems and supervisory authorities, amongst others - which is to be specified in greater detail.

This requirement makes an important contribution to transparency, traceability and verifiability of AI systems. At present, it is often not clearly recognisable whether a product or service uses an AI system in the first place, and if so, according to which criteria the AI system operates.

In the view of the Federal Government, however, there is a need for further review of how the information proposed by the European Commission on the capabilities and limits of certain AI systems can be put into concrete terms. Those actors obligated to provide information should not be subject to unreasonably high compliance costs and their legal positions, in particular the disproportionate encroachment upon trade and business secrets. For entitled parties, it must be ensured that information is comprehensible and accessible at low thresholds.

The Federal Government agrees with the European Commission that, above and beyond the labels and markings already required under data protection law, additional obligations to state that people are interacting with an AI system and not with a human being may be necessary.

d) Robustness and accuracy

The European Commission agrees that AI systems need to be technically robust and accurate in order to be trustworthy. This will be ensured through the observance of standards and principles in the architecture of AI systems and the continuous quality assurance of AI systems.

The Federal Government considers requirements pertaining to the robustness and accuracy of certain AI systems to make sense in principle. The concrete design of such requirements is crucial, however. In any case, it must be ensured that security and protection standards do not unduly hinder the development of innovative AI systems.

In the opinion of the Federal Government, realistic application scenarios should be used to evaluate the robustness of AI systems. However, it should be possible to consider theoretically conceivable scenarios which could lead to an AI not being used.

The Federal Government also believes that greater attention needs to be devoted to the aspect of information security - understood as protection against both accidental errors, e.g. through unexpected information being provided by users, as well as targeted manipulation by attackers - than the White Paper has pursued to date.

The Federal Government considers an obligatory high IT security standard for high-risk AI systems to be indispensable. Otherwise, there is a threat of considerable risks

in the fields described by the Commission (including harm to life and limb, violation of fundamental rights, discrimination).

The key issue is to ensure the confidentiality, integrity and availability of the AI system over its entire life cycle as such. AI systems often classify data on the basis of other features in a different way than a human being would, thereby creating possibilities for attacks that are difficult for humans to recognise. When developing AI systems, the detection of attacks should, therefore, be included as part of a risk assessment. For classes of algorithms, for which an explanation is only possible to a limited extent or not at all, corresponding legal and technical precautions are required, and these must additionally meet IT security requirements. In particular, the complexity of today's AI models must be taken into account, which cannot be controlled due to the millions of trainable parameters and just as many possible inputs with classical IT security procedures. This means new procedures to ensure the information security of AI systems have to be developed as required. Finally, AI systems must be protected against attacks aimed at extracting data or injecting corrupting data.

e) Human oversight

The Federal Government supports in principle the European Commission's plan to develop requirements for the human oversight of AI systems, including the possibility of humans to make final decisions, provided that this cannot potentially be dispensed with due to sector-specific needs and requirements (e.g. for autonomous driving in future).

The Federal Government acknowledges and approves of the description of ways to perform human oversight. The White Paper on AI does not contain any specifics as to under what circumstances which form of human oversight should be bindingly prescribed as a requirement. Consequently, the proposals pertaining to requirements for human oversight of AI systems need to be further refined and developed.

At the same time, it will be important to make sure that humans can challenge the results of the AI system. This means the possibilities of intervention in usage processes have to be explicitly mapped. This can help ensure that at any time a human being is able to disable the system or change its functionality if necessary.

f) Specific requirements for remote biometric identification

The Federal Government welcomes systems for remote biometric identification receiving special attention because of the particular risks they pose to citizens' civil liberties. The discussion about whether such systems should be used in principle and hence possible prohibitions against their use is still ongoing; to the extent that these systems are to be used, clear legal requirements need to be formulated beforehand.

The Federal Government would also note that the fundamental legal prohibition of the processing of biometric data only limits the use of such systems. Due to the profound nature of possible encroachments on goods protected by fundamental rights, a graduated regulation should also be considered when placing systems on the market that can be used by consumers through their own mobile devices.

E. Addressees

The European Commission identifies the various actors involved in the life cycle of an AI system and who may be considered as parties obligated by the requirements. The Federal Government welcomes the proposal that individual requirements should first be imposed on those actors who are best able to counter the potential risks. This also appears warranted for reasons of proportionality.

F. Compliance and enforcement

The Federal Government supports the proposal to make it mandatory for high-risk AI systems to undergo an objective conformity assessment procedure. This should be carried out before products or services using high-risk AI systems are placed on the EU internal market or if such products or services on the market undergo significant changes. The European Commission rightly points to the need for repeated assessments of learning AI systems as they continue to develop and evolve.

The Federal Government also shares the view that in the case of products and services for which conformity assessment mechanisms already exist under current law and in terms of the quality infrastructure, existing mechanisms can be used. Only substantive requirements would then have to be adapted. For other products or services new assessment mechanisms may need to be introduced. It is important to ensure that actors can obtain the necessary approvals and authorisations at one place ("one-stop shop"). For sovereign tasks in the security sector, it should be considered whether to establish a central body for certification or conformity assessment of any AI systems used by security authorities.

In the view of the Federal Government, the requirements formulated in Section D are suitable as a benchmark for a conformity assessment; none of them would have to be excluded from the conformity assessment from the outset; the requirement for information to be provided also appears to be suitable for a conformity assessment procedure.

For businesses, conformity assessment procedures are a tried-and-proven mechanism to obtain legal certainty regarding the compatibility of a product or service with EU law. At the same time, such procedures are time-consuming and costly. The Federal Government therefore shares the view of the European Commission that appropriate resources (support structures, online tools) should be made available, especially for SMEs and the third sector, in order to limit the administrative burden. At the same time, the equal participation of SMEs in standardisation bodies should be supported. The latter also applies to organised civil society.

It will also be necessary to reflect on the possible exceptions to a conformity assessment, which is generally mandatory. In order to strengthen innovative capacity in the field of AI, suitable opening clauses for research and science (regulatory sandboxes) could be considered. Furthermore, it might be appropriate for the pure evaluation of AI systems (e.g. in the context of applicability studies, market surveys or laboratory research) to either not be subject to any or only subject to limited testing. In addition, an opening clause could be considered for situations where a timely, possibly limited, market introduction appears warranted for reasons of public welfare (e.g. in extraordinary crisis situations such as a pandemic), provided that the risks appear manageable.

The European Commission rightly points out that the launch of a preliminary conformity assessment procedure for 'high risk' AI systems does not affect the monitoring of compliance with all existing legal requirements and their enforcement by national authorities.

Existing national supervisory authorities should be in charge of regulatory monitoring. Where no state supervision exists, Member States should be obligated to establish authorities or to assign responsibilities to existing authorities.

Regarding the introduction of effective legal remedies, please see Part 3 of the Federal Government's comments.

G. Voluntary labelling for no-high-risk AI applications

The Federal Government welcomes the proposal for a voluntary certification system for low-risk AI applications. However, participation should not only be open to companies, but also

to public organisations, authorities and associations. The Federal Government considers a time limit to be necessary to ensure that participants renew their quality label on a regular basis. The quality label should be awarded by bodies recognised throughout Europe and checked and controlled by the authorities of the Member States and mutually recognised in the internal market.
There is also a need for effective, legally enforceable sanctions if participants fail to meet requirements or misuse the quality label.

H. Governance

The Federal Government supports in principle the considerations on the establishment of a European governance structure on AI in the form of a framework for cooperation of competent national authorities. Close cooperation is an important supplement in the enforcement of the legal framework in cross-border cases, a regular exchange of information and best practices, the provision of advice on standardisation and certification, and the promotion of the implementation of the legal framework, for example by issuing guidelines, opinions and providing expertise.

From the Federal Government's point of view, it should be ensured that the Member States can each appoint a coordinating institution to coordinate the measures of the European network at a national level, involving respective national authorities and supporting them in their tasks.

Part 3: Safety and liability

A. Introduction

The Federal Government welcomes the comprehensive analysis of product safety and civil liability law with regard to AI, IoT and robotics. It shares the assessment that "liability frameworks in the Union [...] work well so far"[1] and that, "in principle, the existing liability regulations of the Union and the Member States are also suitable for new technologies"[2]. Nevertheless, the Federal Government shares the assessment that the emergence of new digital technologies may pose new challenges in terms of product safety and liability. Actors harmed by these technologies must be guaranteed the same level of legal protection as actors harmed by traditional technologies. As the report rightly notes in the view of the Federal Government, digital technologies may pose challenges, in particular due to the

[1] Report, p. 14 (Note: The page numbers refer to the German language version of the report).
[2] Report, p. 20.

current and increasing connectedness of products (connectivity), their autonomy and data dependency, their technical opacity and complexity as well as increasingly complex value chains.[3] In particular, all this produces new challenges for data protection, quality, safety, security and trustworthiness of AI and the promise of "AI Made in Europe", and associated challenges on the one hand for a quality infrastructure - consisting of metrology, standardisation, accreditation, conformity assessment and market surveillance - and on the other hand for the functional security of AI-based products and applications. To the extent that the report considers reforms or sees a need for reform, selective adjustments in the area of liability law - wherever they are required - appear, in principle, appropriate.

B. Comment on the area of safety

In its report, the European Commission emphasises in its overall objective of a legal safety and liability framework that products with new technologies must function safely, reliably and consistently.

Safety is an indispensable basis for trust in and acceptance of new technologies and thus contributes to competitiveness. The question is whether the current legal framework is suitable for ensuring a sufficient level of safety.

Current product safety rules, including sector-specific rules complemented by national legislation and pertinent standards, are also applicable to AI applications. The approach to safety established by current Union product safety legislation is consistent with an expanded approach to safety to protect consumers and users. It covers all risks posed by the product, including not only mechanical, chemical and electrical risks but also cyber risks and risks related to the loss of connectivity of products. It needs to be assessed in the ongoing process whether safeguards can be adequately enforced to counter the risks posed by AI-based products and services.

Regarding the issue of safety and security of AI systems, the COM correctly identifies the following features to be considered: complexity, autonomy, large amounts of data, algorithms, opacity, connectivity/openness (security). The following should be noted in particular:

I. Connectivity/openness (security)

Today's product safety concept also includes cyber risks and risks from the loss of connectivity. Product safety legislation is geared towards the manufacturers of products and covers design and construction, but not the operation of products. Especially in the case of

3

cyber risks, however, intensive coordination between all actors [(component) manufacturers and integrators on the one hand and operators on the other hand] is required. Since these are two separate areas of law (product safety law / internal market on the one hand, and occupational health and safety on the other), there are doubts as to whether this coordination needed in the area of cyber security can succeed solely based on product safety law.

The statement in the report to the effect that explicit provisions should be added to the areas of application does not appear to be consistent. It is not the respective areas of application, but the respective basic requirements (requirements for construction, design and programming) that should be changed/supplemented wherever necessary.

The operation of an AI system, an IoT device or a robotic system is only possible in the long term if security updates are created and installed promptly in case of newly identified security gaps. To ensure a secure integration of products at the user's end, manufacturers need to specify minimum requirements for IT systems. Furthermore, products should always be developed in line with state of the art technology, taking into account the life cycle of the product, including information security. To ensure secure integration of products with users, manufacturers need to specify minimum requirements for IT systems. This would considerably improve the safety and security of consumers.

II. Autonomy

Risk assessment currently already addresses foreseeable use, but AI systems are not always predictable and may still change their features and properties after they are placed on the market.

Within the framework of a risk assessment during the development/design process, the framework conditions, e.g. control parameters, data protection requirements and the necessary safety-related measures, need to be defined. This also applies to AI systems. Situations in which the assessment/categorisation of results (definition of a permissible range of results) for AI systems cannot be completely specified in advance are still *terra incognita*, with this applying even to systems already in use that are based on the use of machine-learning methods. A distinction must be made, however, between fully trained models and machine-learning methods that continue learning during operation.

The proposal for a new risk assessment procedure for autonomous behaviour that is not foreseeable for manufacturers, in addition to rules on human oversight go beyond the current scope of product safety law. However, the proposal seems necessary and useful. In this respect, consideration must be given to a stronger link between the legal areas of product provision and operation. In this context, the necessary quality infrastructure should

also be developed and made available from the outset, and the competences for government authorities should be built up. Here too, sector-specific concerns must be taken into account, for example, in the case of autonomous driving.

III. Data dependency

A comprehensive consideration of existing requirements for functional safety, along with information security, is necessary in risk assessment. The accuracy and relevance of data are what matter. In addition, it is necessary to make possible the provision of reference data, benchmark tests and the verification of algorithms on the basis of quality-assured, trustworthy reference data. In principle, the Federal Government supports the statement that data quality must be guaranteed during the entire service life. However, it should be noted that this can only be achieved by the operator, who is once again not deemed to be an economic operator in the meaning of product safety law.

IV. Opacity

The learning, working, and decision-making processes of AI systems are sometimes difficult to understand. Transparency is a central component for trust in AI systems, however. The proposal to disclose algorithms and training data to the authorities in case of accidents is, therefore, welcomed. However, this should not be limited to accidents: in principle, it should also be possible in "justified individual cases". The transparency requirements for AI systems should also allow for human oversight wherever necessary. To achieve these goals, basic research on the explainability of AI methods is necessary.

V. Complexity

Product safety law already takes into account the interactions between different devices. Software is an essential component of AI systems. In this respect, product safety law addresses integrated software, but usually not stand-alone software. If stand-alone software influences the safety of a product, this must also be addressed in product safety law.

The statement that if the intended use originally planned by the manufacturer is changed due to autonomous behaviour and compliance with the safety requirements is impaired, and as a result, the whole product should be considered to be a new product, must be viewed critically. In the event that a new product has been created as a result of a software change, this product must fully comply with all state of the art technology as a new product being placed on the market. This must be taken into account when considering a software change.

The call for explicit provisions to govern cooperation between economic operators and operators once again runs up against the problem that product safety law today ends when

the product is put into operation, i.e. the operator cannot be the addressee of such provisions.

C. Interactions between product safety and product liability

The Federal Government first of all shares the view that AI systems should have conceptually integrated protection and safety measures so that at each phase they can be verified as safe. At the same time, a gradual approach differentiated according to practical risk classes is needed. Product safety regulations that establish specific and binding basic requirements and conformity assessment procedures, in which compliance with these requirements is reviewed, are important steering mechanisms to limit the risks of AI to a socially accepted level from the outset.

In connection with putting AI systems into circulation, the Federal Government therefore believes that it should be a priority to define generally applicable binding requirements for their safety and approval. Particular care should be taken to the examination of how to deal with AI systems, which, as a result of their self-learning function, are able to adjust their "behaviour" independently. In the view of the Federal Government, the process of self-learning must not be uncontrolled or lead to uncontrollable results. Safety and security precautions that are to be tested in a conformity assessment procedure, and in certain cases, continuous human supervision as well, must ensure that the learning process is traceable. It must also be ensured that a machine does not perform any other actions that deviate from those originally intended by the manufacturer and which users therefore legitimately expect.

In this respect, there is also an interplay between product safety or approval requirements and liability law. On the one hand, the more stringent requirements regarding safety, security and approval of AI systems are, the fewer liability cases will occur. On the other hand, binding safety requirements are essential in determining safety and security expectations that are justifiably directed at AI systems, which in turn serve as a benchmark in determining whether an AI system is defective in terms of the Product Liability Directive.

D. Product Liability Directive

I. Definition of a product (Article 2 of the Product Liability Directive)

The definition of a product laid down in Article 2 (1) of the Product Liability Directive is, in principle, drafted in a comprehensive manner. The Federal Government can understand the thoughts and considerations of the European Commission, to the effect that the definition of a product needs to be spelled out in more detail. However, the Federal Government

considers it to be crucial that software - by means of a clause clearly laid down in the Product Liability Directive - can be qualified as a product in the meaning of the Directive, irrespective of any connection it may have with embodied objects. It would also appear correct that manufacturers of defective products should be held liable for damage caused by such products, without it mattering whether the specific product is embodied.

Even if the integration of software could blur what have for the most part been clear boundaries between "product" and "service", it should be clear that the regulatory system of the Product Liability Directive will continue to apply only to products, but not to services.

II. Definition of "put into circulation" (Article 6 (1) (c) and (2), Article 7 (b) and (e) of the Product Liability Directive)

From the point of view of the Federal Government, it should first be stated that any changes in liability law concerning self-learning AI systems should only be undertaken when market maturity and the technical design for such systems are foreseeable. This is to avoid any insufficiencies or inappropriateness of liability law at the time when respective products are launched into the market. In the view of the Federal Government, this point in time has not yet been reached for self-learning AI systems.

Against the background that products equipped with AI could, in future under certain circumstances, independently change their features and properties during their typical product lifecycle by virtue of so-called self-learning properties and that products are already changing their properties at present even after they have been put in circulation by means of software updates, the Federal Government supports the idea of the European Commission to review the notion of "put in circulation " and, if necessary, to submit a proposal to adapt this concept to present-day conditions. In this context it should also be discussed to what extent a product defect already exists at the time when the product is put into circulation, if a product equipped with an AI can change by virtue of self-learning properties in such a way that enable it to perform actions other than those originally intended by the producer and therefore legitimately expected by users.

Finally, any change in the law should aim to strike a fair balance between the legitimate interests of potentially injured parties and producers. In order to ensure an appropriate balance between the legitimate interests of potentially injured parties and producers, it will also be necessary to take into account the extent to which, for example, producers have provided safety and security updates to ensure that functions are preserved, have informed injured parties thereof, and injured parties may, as a result, have obligations themselves.

III. Modification of the burden of proof (Article 4 of the Product Liability Directive)

In the view of the Federal Government, the existing assignment of the burden of proof under Article 4 of the Product Liability Directive can also, in principle, bring about appropriate and reasonable solutions with regard to AI systems.

In this context, the Federal Government would note that, as a matter of principle, the existing substantive assignment of the burden of proof should only be changed wherever practical difficulties with regard to proof have clearly emerged. If there are indications of such difficulties with regard to the new technologies mentioned in the report, this would first have to be investigated empirically. If these indications are not confirmed, the Federal Government has doubts as to the need for respective modifications.

If the European Commission should decide to advocate for a modification of the assignment of the burden of proof along the lines of the proposal forwarded by the New Technologies Formation (NTF) of the Expert Group on Liability and New Technologies, it must first be noted that the determination of the standard of legitimate safety and security expectations is a legal question which the parties do not have to demonstrate or prove anyway under German law governing evidence. As far as compliance with the standard of legitimate safety and security expectations is concerned, a reversal of the burden of proof in could be problematic a *non liquet* case, since producers would then have to bear liability without the basis for such liability - defectiveness of the product - ever having been established in the first place. Linking assignment of the burden of proof to the difficulties or costs involved in producing evidence would be a novelty that is incompatible with the system of law on evidence. After all, the establishment of proof can also be difficult in non-digital cases. Experts commissioned by the courts can help in complex cases. These mechanisms are facing new challenges due to the opacity of some digital systems.

E. Further harmonisation of national liability law

The Federal Government shares the view of the Commission regarding the important principle that victims of accidents involving new digital technologies must not have less protection under liability law than victims of accidents involving comparable conventional technologies. Furthermore, the liability laws of Member States already pursue this aim at present. From the Federal Government's point of view, special care must also be taken to ensure that issues involving competencies are not ignored when harmonising measures regarding independent national liability law are considered. It must also be taken into account that such measures can disturb the coherence of national liability laws.

I. Introduction of strict liability for operators of "AI applications with a specific risk profile”

At first glance, the introduction of operator's liability for dangerous objects is, from the perspective of the Federal Government, an understandable idea. German law already provides for such liability for certain objects, for example in Section 7 (1) of the German Road Traffic Act (StVG) - including motor vehicles with automated or autonomous driving functions - or in Section 33 (1) of the German Air Traffic Act (LuftVG) - for drones, for example. There are also corresponding provisions governing third-party damage caused by drones in certain treaties to which some Member States have acceded.

Strict liability on the part of operators should, in principle, only be considered if the object in question poses a particular danger, if there is insufficient manufacturer's liability and if persons typically come into contact with the object who have involuntarily exposed themselves to the danger. The danger posed by an object will, however, continue to depend on its type (e.g. a motor vehicle). For this reason, the Federal Government is reluctant to harmonise laws in a horizontal manner that does not focus on the dangerous object itself, but rather on the mode of its operation. If this approach were adopted, there would also be a danger that different liability arrangements would apply to the same object - e.g. conventional and autonomous motor vehicles - for decades to come.

In addition, the Federal Government also has - in contrast to the harmonised product liability of manufacturers under the Product Liability Directive - its doubts regarding the promotion of the internal market through a Union-wide uniform liability on the part of the operators. Furthermore, there is probably no threat of any innovation-inhibiting fragmentation of the internal market due to the further development of national laws governing operators' liability, as this fragmentation already affects traditional technologies today and no significant obstacles to innovation have become evident in this area to date.

II. Modification of the assignment of the burden of proof for operators of "all other AI applications”

In the view of the Federal Government, questions involving the burden of proof in national operator liability law should, in principle, remain in the domain of national lawmakers. According to German legal understanding, the burden of proof is linked to the respective liability claim, so harmonisation of the substantive burden of proof alone is likely to lead to inconsistencies.

F. Summarising assessment of safety, security and liability

Since products today usually fall within the scope of several product safety regulations, it is

essential to define uniform requirements that are directed both at AI applications and at cybersecurity for all connectable products (hardware and software).

These uniform requirements should preferably be laid down for the area of product safety in a horizontal legal instrument with the possibility of sector-specific exemptions. This would avoid divergent rules in basic legislation. Spelling out legislation along sector-specific lines may be necessary for the health sector to meet the specific requirements, for instance (especially with regard to personal data). These requirements could then be underpinned by harmonised standards in line with the existing internal market approach.

Overall, in the area of safety and security, we advocate a differentiated risk classification being made an essential prerequisite for the effective implementation of approvals and controls wherever this is appropriate for the respective risk.

The characteristics and features of AI, IoT and robotics should distinguish between personal and non-personal applications and be extended to cover the aspects of fairness/non-discrimination and data protection. Furthermore, the Federal Government proposes adding additional overarching elements such as sustainability, reliability and impact (system relevance).

Proposals by additional experts can also be included in the discussion regarding the concrete design for future governance of AI applications.

Civil liability law is already able to deal adequately with damage caused by AI, IoT and robotics at present. If these technologies create new legal challenges, however, modifications must be examined in order to respond to the increasing connectivity and complexity of digital systems in an appropriate legal manner. A revision of specific elements of the Product Liability Directive would appear to be warranted in this respect. However, no harmonisation of national liability laws is necessary at present. As is the case in many other Member States, German liability law is highly developed and provides comprehensive protection for injured parties even if the dangerous objects causing damage is operated digitally. Encroachment of EU law into this domain could lead to inconsistencies with the non-harmonised national law of Member States, a development that needs to be avoided.