At a glance

Bitkom on the European Commission’s White Paper on AI

A European approach to excellence and trust

The EU’s regulatory framework for AI will take fundamental decisions on the technology and strongly influence the use for European societies as well as future competitiveness of the EU’s economy. The wide reach of the technology means that it touches many areas of the law. Given that the technology is at an early stage key concepts are still in flux and effects can only be anticipated. In order to shape rules, Europe has to leave room for developing the technology for the benefit of the society and economy, which is the basic premise Bitkom’s position is based on.

- **Prepare empirical ground:** Good policy making has to be built on verifiable and evident need for regulation. Given that implementation of AI regulation is going to come with high implementation costs, regulation has to be clear in scope, proportional and implementable for economic operators (developer, deployer, producer etc).
- **Check the existing legislative framework in place:** In principle, Bitkom believes that specific legislation should not be based on one technology (technology neutrality) . AI should be regulated mainly by sector specific regulation in order to avoid unrealistic requirements, overlaps and double structures with existing law. Sector-specific expertise, experience and regulatory framework of data-based innovations (e.g. in the fields of health, transport, etc.) are a better starting point than general horizontal regulation.
- **Leverage investments:** We support the idea of connecting investments by the EU, member states and private actors. In order to achieve this goal, current investment streams should be mapped and public procurement should be used to leverage the technology and achieve wide uptake.
- **Principles must be operationalised:** When drafting legal principles it should be considered to what extent they are already covered and to what extent they can be enforceable by companies of all sizes. Bitkom doubts that the principle obstacle to AI uptake is the lack of trust but rather anticipated costs and legal uncertainty. The prospective enforcement system should be drafted in a way that avoids bottlenecks.
- **Define high risk applications:** To keep strict and burdensome requirements proportional they should be limited to high risk areas based on case by case analysis. When defining these areas the counterfactual needs to be established, namely what are the costs and risks of not using AI

Bitkom’s number of the day

6 percent

of German companies with more than 20 employees use AI technology.

↗ https://www.bitkom.org/Presse/Presseinformation/Unternehmen-tun-sich-noch-schwer-mit-Kuenstlicher-Intelligenz

Comments on the White Paper on AI

Bitkom comments on the White Paper on Artificial Intelligence – A European approach to excellence and trust

I. General Remarks

The White Paper on Artificial Intelligence intends to develop and establish a European approach to excellence and trust in the field of Artifical Intelligence. Bitkom comments on the Commission's considerations in line with the above mentioned objectives of the White paper.

At the outset, we would like to stress that we welcome the objectives of the European Commission in general: Support the EU in becoming leader in AI (chapter 4: ecosystem of excellence) complemented by introducing new safeguards for citizens (chapter 5: ecosystem of trust).

In principle, we do not see the need for a specific AI-regulation throughout Europe. Before such regulation is introduced, it should be examined in detail from a legal point of view where there are blank spots on the EU regulation map and where significant restrictions of the digital single market are imposed by regulations in member states. This applies in particular to potential regulation that is explicitly introduced as a consequence of the increased use and dissemination of artificial intelligence in the economy and society. In our view, it has not yet been proven that the considerations made in the paper give rise to a general need for additional regulation of AI.

In this context, the scope of the white paper's suggestions should be further clarified in terms of whether the proposals refer to AI, machine learning or automated decision making and its impact on humans, which we will elaborate on in later comments.

There must be evident need for regulation, particularly in the context of the goal to establish an attractive ecosystem for innovation and excellence. Regulation is inevitably associated with effort and costs because of the relatively fixed (and thus degressive) cost structure, which is particularly challenging for start-ups and small companies. The need for regulation must therefore be comprehensibly documented and justified, which must be taken into account in all future considerations of regulation, particularly given the EU's goals to create the framework conditions for an ecosystem of excellence.

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.
(Federal Association
for Information Technology,
Telecommunications and
New Media)

Lukas Klingholz
Big Data & Artifical Intelligence
T +49 30 27576 101
l.klingholz@bitkom.org

Benjamin Ledwon
Head of Brussels Office
Office +32 2 60953-21
b.ledwon@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Achim Berg

CEO
Dr. Bernhard Rohleder

Apart from fundamental principles, the application of AI should not be regulated in a dedicated AI directive, but on a sector- or topic-specific basis if necessity emerges. Regulations across various industries already consider and regulate data-driven applications. If new regulation needs to arise in the application of artificial intelligence, it makes most sense to link it with existing rules, standards[1] and regulatory framework within sectors.

With regard to the „ Ecosystem of Excellence“, the main objectives are on the one hand to develop a European ecosystem in which research results can be applied as best as possible in the public and private sector as well as in the society as a whole. On the other hand, it is important that public and private investments complement each other optimally.

With regard to the „Ecosytem of Trust“, it is important that the private sector is closely involved in the definition of the various requirements. Standards and certificates developed by business. Private sectoral self-government is just as relevant for a proper regulatory framework of the application of AI as the expertise of the regulatory authorities from the different sectors.

In further commentary we focus on the chapters four and five of the White Paper because these chapters deal with the conditions necessary to develop „Ecosystems of Excellence and Trust” in the European Union.

[1] For example ISO/IEC JTC1 SC42 already has a work board programme in place for this purpose.

II. An Ecosystem of Excellence

1. General Remarks

Bitkom welcomes the goal of establishing an ecosystem of excellence along the entire value chain (research & innovation and incentives for AI adoption in the economy).

2. Specific Remarks

A.Working with member States

Action 1: The Commission, taking into account the results of the public consultation on the White Paper, will propose to the member states a revision of the Coordinated Plan to be adopted by end 2020.

Bitkom Assessment

It must be more clearly worked out how, in the view of the Commission, various actors (both public and private) contribute to actually investing 20 billion annually in AI. In this context, a systematic inventory of current investments on the one hand and a realistic growth path of investments on the other hand should be aimed at.

Sustainability and energy effiency is not a new challenge for businesses. Just as with other technologies, companies have a strong self-interest in exploiting the potential of technologies for more sustainability. AI offers much potential for achieving sustainability goals. Bitkom therefore welcomes the Commission's statements and considerations to fully exploit the potential of AI in this context.

B. Focusing on the efforts of the research and innovation community

Action 2: the Commission will facilitate the creation of excellence and testing centres that can combine European, national and private investments, possibly including a new legal instrument. The Commission has proposed an ambitious and dedicated amount to support worldclass testing centres in Europe under the Digital Europe Programme and complemented where appropriate by research and innovation actions of Horizon Europe as part of the Multiannual Financial Framework for 2021 to 2027.

Bitkom Assessment

We fully support the goal to establish a lighthouse centre of research in Europe. We would suggest to establish a structure in which the lighthouse centre has a coordinating role in the european research and innovation community. The lighthouse center must be clearly linked to existing structures of excellence, such as CLAIRE and ELLIS. It also should strive to connect with standardization to foster market development.

Furthermore, we welcome the approach of concentrating on the sectors where Europe has the potential to become a global champion. In addition to excellence in research, a consistent approach on the transfer of knowledge & AI adoption is central regarding this.

It needs to be further clarified which financial instruments and incentives will be used to achieve these objectives.

C. Skills

Action 3: Establish and support through the advanced skills pillar of the Digital Europe Programme networks of leading universities and higher education institutes to attract the best professors and scientists and offer world-leading masters programmes in AI.

Bitkom Assessment

We support the objectives of the section on the creation of academic excellence and upskilling in the workforce. The measures to achieve these objectives need to be further specified.

D. Focus on SMEs

Action 4: the Commission will work with memberstates to ensure that at least one digital innovation hub per member state has a high degree of specialisation on AI. Digital Innovation Hubs can be supported under the Digital Europe Programme. The Commission and the European Investment Fund will launch a pilot scheme of €100 million in Q1 2020 to provide equity financing for innovative developments in AI. Subject to final agreement on the MFF, the Commission's intention is to scale it up significantly from 2021 through InvestEU.

Bitkom Assessment

We support this goal. Existing hub structures and hub-like structures must be taken into account and further developed in a proper way in order to achieve the goals.

E. Partnership with the Private Sector

Action 5: In the context of Horizon Europe, the Commission will set up a new public private partnership in AI, data and robotics to combine efforts, ensure coordination of research and innovation in AI, collaborate with other public-private partnerships in Horizon Europe and work together with the testing facilities and the Digital Innovation Hubs mentioned above.

Bitkom Assessment

We fully support this approach.

F. Promoting the adoption of AI by the Public Sector

Action 6: The Commission will initiate open and transparent sector dialogues giving priority to healthcare, rural administration and public service operators in order to present an action plan to facilitate development, experimentation and adoption. The sector dialogues will be used to prepare a specific 'Adopt AI programme' that will support public procurement of AI systems, and help to transform public procurement processes.

Bitkom Assessment

In the scope of funding, we miss the reference to leveraging by public procurement, taking into account that half of EU's GDP is public money. Also, the paper misses a reference to an EU-funded national and transnational lighthouse-project that would facilitate private development and implementation of AI.
In general, we fully support the goal to promote and accelerate the deployment of products and services based on AI by the public sector. In addition to this abstract objective, an analysis is needed of how broad use of AI in the public sector can be promoted in concrete regulatory and organisational terms.

G. Securing Access to data and computing infrastructures

Bitkom Assessment

We fully support the goal to invest in strategic data and computing infrastructures which forms the basis for the digital transformation.

H. International Aspects

Bitkom Assessment

We support these considerations

III. An Ecosystem of Trust: Regulatory Framework for AI

1. General Remarks

Overall we don't see major gaps in EU legislation. The law applies without regard to a certain technology. Consequently it seems not only inadequate, but rather detrimental to create specific law only for AI.

Besides, there is no agreed upon mechanism for classifying AI applications as such.

Chapter 5 is strongly oriented towards the concept of AI. The key questions for different economics operators arising from chapter 5 are the following two.

- Is the relevant data-driven application an „AI application"?
- If the relevant data-driven application is an „AI application": Is this specific AI application a high-risk application?

If a future regulatory framework - as follow up of the White Paper on AI - plans to regulate AI, the concepts of AI and algorithmic systems must be defined in a way which makes them easy to handle for the economic operators involved (developer, deployer, producer etc.) to determine if a specific data-driven application meets the criteria AI/algorithmic system.

It is very important that the regulatory framework under discussion for high-risk AI applications does not create serious burdens that prevent companies and society from developing and using high-risk AI applications in and in the EU.

2. Specific Remarks

Opportunities and risks of AI

Bitkom Assessment

It is to be welcomed to systematically consider the opportunities and risks of new technologies. Therefore, the scenario of not using a new technology should be compared to the scenario of using the specific technology. The use of artificial intelligence offers many advantages in many industries and areas. These advantages and potentials must be weighed against the risks of their use. We believe that the overall potential of artificial intelligence is very high.

Assumption that the lack of trust is main factor holding back AI uptake

Bitkom Assessment

We do not fully agree with this thesis as the empirical basis for this claim is missing. There are multiple other possible reasons, which are responsible for the low uptake of AI such as lack of legal certainty due to GDPR or missing standards etc. Standards can help to increase trustworthiness.

Role of HLEG seven key requirements

Bitkom Assessment

While we welcome the seven requirements in principle, it remains to be noted that further steps need to be taken for their practical application on a broad scale, precisely because a legal implementation of ethical criteria is not directly possible 1:1.

A.Problem Definiton

We strongly recommend the highest possible degree of technology neutrality in a regulatory framework for implementation.

Risks for fundamental rights, including personal data and privacy protection and non-discrimination

Bitkom Assessment

To what extent is the existing legal framework not sufficient to limit these risks in the operational use of AI applications and to ensure compliance with fundamental rights? From our point of view this is not clear enough in this section.

Risks for safety and the effective functioning of the liability regime

Bitkom Assessment

We reject an additional liability regime for the application of AI-based technologies. Liability regimes should be set up in a technology-neutral way.

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

Effective application and enforcement of existing EU and national legislation:

Bitkom Assessment

We agree that transparency is key and thus, provision of clear information needs to be guaranteed. It is however completely unclear where the GDPR's requirements in that regard are considered insufficient – and the White Paper does not provide any indication here. Also, often it remains unclear whether the paper refers to personal or non-personal data. With regard to personal data, GDPR appears as sufficient means to close potential gaps.

Limitations of scope of existing EU legislation:

Bitkom Assessment

The highest possible degree of technological neutrality should be maintained in the regulatory framework. We therefore reject the idea of creating product safety legislation especially for AI based technology.

Changing functionality of AI systems:

Bitkom Assessment

We are of the opinion that the changing functionalities of AI in high-risk applications are already largely covered by regulations. There is no evidence of where specific regulatory gaps exist. These may have to be adapted sector by sector in the respective regulatory frameworks.

Existing regulatory frameworks (e.g. in the health sector or in the transport/automotive sector) already cover the topic of changing functionality of AI systems. In this context, please also note our explanations further down in this section (d) on robustness and accuracy "Requirements ensuring that outcomes are reproducible“). We strongly recommend taking a sectoral look at the advantages and disadvantages of locked algorithms from a user's point of view.

We point out that the wording "software" or "software update" is not clear or misleading in this context. A model can evolve (by adjusting parameters in the course of continuous learning) without the software itself changing. Is this a software update in the literal sense of the word?

Uncertainty as regards the allocation of responsibilities between different economic operators in the supply chain:

Bitkom Assessment

We do not see this uncertainty. Where such ambiguities exist regarding responsibilities they should be addressed in technology neutral regulatory frameworks such as EU product liability legislation and in vertical regulatory frameworks rather than in an AI-specific and non-technology-neutral new framework & special law.

Changes to the concept of safety

Bitkom Assessment

See considerations above. We reject AI or mandatory technology specific regulation. Potential changes should be addressed in technology neutral regulatory frameworks such as safety legislation and in vertical regulatory frameworks rather than in an AI-specific and non-technology-neutral new framework & special law.

However, we welcome the proposal to dock these considerations and plans closely to the considerations and plans of ENISA. To reach a high security-level for AI, technical standards particularly concerning robustness should be developed and approved, possibly based on the certification mechanism foreseen in the Cyber Security Act.

Based on the Security-by-Design Principle, all relevant stakeholders along the value chain should be addressed and the trader or deployer of the AI-system must not be left alone.

Report on the safety and liability implications of AI, the IoT and robotics

Bitkom Assessment

No further comments. Comments regarding „Section B" sufficiently represent our position.

C. Scope of a future EU regulatory framework

Definitions: Data, Algorithms, AI

Bitkom Assessment

There is no agreed mechanism for classifying AI applications as such. If a future regulatory framework plans to regulate AI, the concepts of AI and algorithmic systems must be defined in a way which makes them easy to handle for the economic operators involved (developer, deployer, producer etc., compare p. 22) to determine, if a specific data-driven application meets the criteria AI/algorithmic system.

Two concrete possible definitons are mentioned in the White Paper (Communication on AI for Europe[2] and the defintion from the HLEG[3]). We do not think that one of these defintions is approriate. We would like to emphasize that we find it very difficult to define AI precisely, also relative to data-based innovations and algorithms. When a definition is specified, it is in our view essential to make it as technology-neutral and as possible.

Looking at the definitions in the White Paper, in particular the definition of HLEG, we would like to make the following points about this definition, in the sense of an adapted and completed definition.

Artficial intellience (AI) systems are software (and possibly also hardware[4]) systems designed by humans that, given a complex goal, are taught by their designers or learn[5] from experi-

[2] Compare page 16, footnote 46 in the whitepaper
[3] Compare page 16, footnote 47 in the Whitepaper

[4] Regarding hardware we want to emphasize that this is only true for hardware with embedded software. Not for hardware itself.
[5] We would like to encourage you to speak of "optimize" rather than "learn"

ence how to 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.

High risk, cumulative approach

Bitkom Assessment

We agree that a combination of defining relevant sectors and relevant use-cases within the sector could be a reasonable way to identify high-risk AI-systems, for the purpose of keeping strict and burdensome requirements proportional. While a sector-approach alone could lead to overly extensive regulation, solely looking at specific use-cases across all sectors could lead to a very high level of complexity and bureaucracy.

Potential high-risk sectors are mentioned in the paper (healthcare, transport, energy and parts of public sector)

How is „significant risk“ concretely defined? This must be specified as clearly and practically as possible in order to enable an operationally manageable application and classification.

In this context, is the reference scenario considered enough (not using AI) when declaring a sector high-risk?

It is important to prevent entire sectors from being placed under general suspicion, as each sector involves applications, products and services with different risk requirements. In every sector, risks must be assessed on a case basis. We would like to emphasize once again that we believe that the majority of the applications in the various proposed high-risk sectors are uncritical in the sense of the White Paper (no significant risks in application, see p.17 bullet 2). Even though there are already sector-specific rules, the following is worth considering: a list of “high-risk sectors” is very difficult to manage and could significantly impair the use of AI for non-critical functions/services in all the sectors listed.

We therefore strongly recommend that clear criteria be defined according to which a sector is "high-risk". The explanations and justifications for this in the White Paper are very vague and not sharp enough. If necessary, the sectoral approach must subsequently be discarded if no clear criteria can be established which classifies a high-risk sector or if this classification leads to hampering general AI use and developments of AI applications (especially low risk applications) in this sector to be included in this list.

In this context problems regarding the differentiation of sectors may arise. Indeed, as digitisation increases, sectors overlap and are no longer distinct.

The complementary criteria to identify high-risk AI-systems, needs further specification to avoid legal uncertainty and over-regulation. This includes e.g. the clear definition of "significant" impact on affected parties or the "exceptional instances" that classify an AI-system as high-risk. Furthermore, as mentioned above, it must be clear and easy to classify if a specific data-driven application is an AI application6.

Also, it remains generally unclear whether the more general definition of high-risk for AI-systems is consistent with the separate proposal of high-risk in the scope of the proposed liability provisions for AI-systems.

Recruitment processes & applications impacting workers rights should always be considered high-risk

Bitkom Assessment

To what extent is the comparison with the reference scenario (no AI deployment) taken into account? To what extent is the existing legal framework not sufficient?

Biometric identification & biometric authentification

Bitkom Assessment

Already now, several security and data protection requirements apply to all applications in the field of remote biometric identification. It must be clearly worked out, which additional requirements are necessary by classifying remote biometric identification as high-risk, given the regulatory status quo.

D. Types of requirements

Bitkom Assessment

[6] Following the spirit of the whitepaper in general and the considerations on page 18 concretely.

In general, a lot of the requirements discussed in this chapter are very costly. This tends to mean that many AI applications can no longer be developed profitably. Therefore, the most unbureaucratic and unobtrusive implementation of the requirements is central to the design of a possible regulatory framework for high-risk AI applications.

a) Training data

- **safety rules**

Bitkom Assessment

In general, our comments regarding „Section B“ sufficiently represent our position. Furthermore, compliance with safety standards must be closely linked to the results and findings of standardization activities.

- **anti-discrimination**

Bitkom Assessment

Authorities need to define clear and easy-to-use requirements and test criteria to identify potentially unlawful discrimination. In this context, sector-specific standardisation activities must be taken into account and encouraged.

We see several and major conflicts with GDPR here. Due to GDPR and data protection regulation, personal data can not be collected in a lot of cases. However, in many cases these would be necessary to meet the anti-discrimination requirements outlined in this section.

The important messages should be: It is not apparent why a new, additional anti-discirmination regulation specifically for data and AI algorithms is necessary. Discrimination is already covered by law. The focus should be on a non biased outcome of the AI system, as potential discrimination only occurs when the trained algorithm is applied, even if the data on which the algorithm is trained play a significant role.

- **privacy**

Bitkom Assessment

It must be made clearer where additional requirements are needed which are not covered by General Data Protection Regulation and the Law Enforcement Directive.

b) Keeping of records and data

- **accurate records regarding the data set used to train and test the AI systems, including a description of the main characteristics and how the data set was selected**

Bitkom Assessment

While a clarification regarding the documentation and retention obligation for development documentation is welcomed, we see the following problems here:

For already applied AI technology, it is very complex and costly. If a third party is auditing the records and data, there a major conflicts with trade secrets and security arising. This leads to the general question of how IT-security issues managed in the new regulatory framework by authorities?
Numerous data sets used in training AI systems could not be recreated and AI systems may be ingesting continuous flows of historic or real-time data over time. It would often be ineffective for companies to be required to keep such records or datasets when AI is frequently developed in a dynamic and iterative manner.
Also the trend of edge computing is not considered here (which is relevant and becoming more and more relevant in several sectors & industries). One characteristic of edge computing is that data is processed at the edge and not a (central) cloud.

Also, the consequences of the rise of federated computing paradigms for the availability of data records and datasets must be taken into account in this context. Especially, when the overall policy framework tries to promote this trend in other areas (see for example the data strategy)

Furthermore, many of the software-development processes and standards that have evolved over time and are used to help build trust in software do not exist for data; there are no common data naming conventions, no formatting standards or concurrent versioning systems used for data which make regulation in this area premature and impractical. Therefore, to require AI developers to keep records and data would be unlikely to lead to anything meaningful that could be garnered for assessment.

We also see various potential problems and legal conflicts with copyright law. Furthermore We see several conflicts regarding this requirement with GDPR in general and also in particular with the GDPR-based right to forget.

All the these additional requirements lead to processing costs and have a strong impact on the marginal/break-even decision of applying AI-based applications. Furtheremore, these requirements lead to additional energy/environmental costs.

- **in certain justified cases, the datasets themselves;**

Bitkom Assessment

The term justified case must be defined more concretely. Furthermore, there are special challenges in different AI technologies such as federated machine learning where data sets themselves are never collected. The role of anonymised and pseudonymised data in these cases needs to be worked out. Finally, we see several conflicts with GDPR.

- **Documentation on the programming and training methodologies, processes and techniques used to build, test and validate the AI systems, including where relevant in respect of safety and avoiding bias that could lead to prohibited discrimination.**

Bitkom Assessment

High administrative costs must be taken into account. Clear, operationally manageable rules and standards are necessary for implementation. Industry must be closely involved.

c) Informations provision

- **AI system's capabilities and limitations. This information is important especially for deployers of the systems, but it may also be relevant to competent authorities and affected parties.**

Bitkom Assessment

From our point of view, these questions are already sufficiently addressed in a large amount of cases, especially in B2B relations.

- **Discussion on information and labelling requirements**

Bitkom Assessment

Which specific additional informations, in addition to informations induced by EU data protection legislation should be provided?

We would like to stress that the objective of "avoiding unnecessary burden" is to be welcomed.

d) Robustness and accuracy

- **Requirements ensuring that the AI systems are robust and accurate, or at least correctly reflect their level of accuracy, during all life cycle phases;**

Bitkom Assessment

Precise definition of accuracy is necessary, especially when compared to processes and situatiuons without AI applications usage.

- **Requirements ensuring that outcomes are reproducible;**

Bitkom Assessment

From our point of view, this is not always appropriate and in the interest of the user. In several applications, new versions of AI systems come at short intervals. In this case, all intermediate versions must be kept available following this requirement. Therefore, we would argue to look in detail where this requirement is neccessary given the trade-off of insights into reproducibility on the one hand and the additional administrative and processing costs on the other hand.

This requirement is also problematic as it is not always possible to achieve this. AI systems change over time and outcomes are not reliably reproducible, therefore compliance with requirements of this nature would be impossible for many AI applications. Reproducibility of outcomes may require exactly reproducing the entire dynamic environment and the entirety of the data flows used to train the model and this would simply not be possible in practice in several cases.

Requirements ensuring that AI systems can adequately deal with errors or inconsistencies during all life cycle phases.

Bitkom Assessment

How is this exactly defined and how is monitoring to be ensured in practice?

e) Human oversight

Bitkom Assessment

Generally, we support to have human oversight. However, the degree of this possible oversight might vary from one case to another and should be limited to high-risk applications. Again, legal certainty for businesses is key and therefore, clear criteria need to be established that allow companies to determine what rules have to apply in specific situations.

In principle, the different gradations below are to be evaluated positively, since it shows that there is no "one size fits all“ solution for human oversight.

The interaction between the four different non-exhaustive manifestations and their respective fields of application[7] should be considered and clearly defined.

- **Output of the AI system does not become effective unless it has been previously reviewed and validated by a human (e.g. the rejection of an application for social security benefits may be taken by a human only);**

Bitkom Assessment

Clear criteria, for example based on standards, must be defined when the human is applying the „review & validation“ process. Otherwise, partial automation through the use of AI is taken ad absurdum.

- **Output of the AI system becomes immediately effective, but human intervention is ensured afterwards (e.g. the rejection of an application for a credit card may be processed by an AI system, but human review must be possible afterwards);**

Bitkom Assessment

This objective has to be compared with the regulatory status quo in the relevant vertical regulatory frameworks. For the most part, these rights of human intervention are already legally secured and no further regulation is needed. This leads to the question for which of the six high-risk areas this requirement should apply.
There must be clear and easily manageable rules and limits regarding the explainability of AI systems. Standards and certificates developed from business must play a central role here. Criteria for reversibility and unwinding as legal consequences must also be clearly defined.

[7] for which high-risk sector is the application of the respective manifestation appropriate, but for which area is it not?

- **monitoring of the AI system while in operation and the ability to intervene in real time and deactivate (e.g. a stop button or procedure is available in a driverless car when a human determines that car operation is not safe);**

Bitkom Assessment

Standards and certificates developed from businesses must play a central role here regarding the question of safety. In addition, it must be made clear how human oversight in the sense of the economic operators in Section E „Adresses" is to be implemented here with regard to responsibility/the distribution of obligation.

- **in the design phase, by imposing operational constraints on the AI system (e.g. a driverless car shall stop operating in certain conditions of low visibility when sensors may become less reliable or shall maintain a certain distance in any given condition from the preceding vehicle).**

Standards and certificates developed from businesses must play a central role regarding the question of safety. In addition, it must be made clear how human oversight in the sense of the economic operators in section E „Adresses" is to be implemented here with regard to responsibility/the distribution of obligation.

f) Specific requirements for remote biometric identification

- **Biometric identification & biometric authentification**

Bitkom Assessment

Already now, several security and data protection requirements apply to all applications in the field of remote biometric identification. It must be clearly worked out which additional requirements are necessary by classifying remote biometric identification as high-risk, given the regulatory status quo.

E. Adresses

Bitkom Assessment

The general statement that each obligation should address those actors who are best placed to address any potential risk is worrying. Those undertakings that are actually most responsible for causing a risk must not be left of the hook and should always be in the first place regarding obligations to mitigate risks ("**polluter pays principle**").

Roles of different economics operators

- **Developer**
- **Deployer**
- **Producer**
- **Distributor**
- **Importer**
- **Service provider**
- **Professional or private user**

Bitkom Assessment

Are the boundaries of roles of the different economic operators and responsibilities clear? In general the Commission's objective to assign clear responsibilities to each of the different economic operators is to be welcomed.

We also recommend adding to the roles under „E. Roles of different economics operators“ the "data provider", since the private sector is increasingly involved in a division of labour in data collection/processing.

Second, there is the question about the geographic scope of the legislative intervention. In the view of the Commission, it is paramount that the requirements are applicable to all relevant economic operators providing AI-enabled products or services in the EU, regardless of whether they are established in the EU or not. Otherwise, the objectives of the legislative intervention, mentioned earlier, could not fully be achieved.

Bitkom Assessment

If new regulations are created, they must be based on the existing legal framework and must not create additional and protectionist barriers for data and AI-based products from outside the EU.
It is very important that competent authorities are able to verify quickly and with legal certainty if the relevant requirements are met by economic operators offering AI-enabled products or services from outside the EU. The mentioned mutual recognition agreements

with third countries are central at this point. Experiences and best practices from other sectors[8] must be taken into account.

Furthermore it is important that appropriate transition periods or cut-off date regulations are created for applications that are already in use.

F. Compliance and Enforcement

Bitkom Assessment

Central to these considerations is the competence of the relevant competent authorities who are to carry out these assessments. The assessments have the potential to mutate into massive bottlenecks in the market launch and therefore in the speed of innovation uptake of the EU economies and societies.

- **prior conformity assessment would be necessary to verify and ensure that certain of the above mentioned mandatory requirements applicable to high-risk applications (see section D above) are complied with.**

Bitkom Assessment

We recommend, besides mandatory conformity assessements for high-risk AI applications to additionaly consider the potential of self-regulation.

Furthermore, it must be clearly worked out which requirements and related standards really have to be fulfilled within the framework of a prior conformity assessment. This varies from field of application to field of application and must be considered sector-specifically. This in turn makes it clear again how important it is that the assement framworks discussed are linked with existing vertical framework.

- **The prior conformity assessment could include procedures for testing, inspection or certification. It could include checks of the algorithms and of the datasets used in the development phase.**

Bitkom Assessment

[8] For example: Healthcare mutual recognition (Link). Additionally the European Commission declared the data protecion rules of 13 countries as adequate to the european framework (see European strategy for data, p.5/35; Link)

We would like to emphasize again how important a cost-benefit analysis and simple practical implementation is in this context. With regard to testing, inspection and certification procedures, the relevance of self-regulation and the standards set by companies must be reaffirmed again. We welcome that the EU-Comission wants to use input of stakeholders and the European standards organisations in this context.

We also welcome that the conformity assessements should be part of the conformity assessement mechanisms that already exist and should be closely linked to them.

When designing and implementing a system relying on prior conformity assessments, particular account should be taken of the following:

- **Not all requirements outlined above may be suitable to be verified through a prior conformity assessment. For instance, the requirement about information to be provided generally does not lend itself well for verification through such an assessment.**

Bitkom Assessment

It must be clearly worked out which requirements have to be fulfilled within the framework of a prior conformity assessment. This varies from field of application to field of application and must therefore be considered sector-specifically. This in turn makes it clear again how important it is that the assement framworks discussed are linked with existing vertical framework.

- **Particular account should be taken of the possibility that certain AI systems evolve and learn from experience, which may require repeated assessments over the life-time of the AI systems in question.**

Bitkom Assessment

Similiar answer as for D. „Requirements“ /d. „Robustness and accuracy“: Requirements ensuring that outcomes are reproducible: In several applications new versions of AI systems are updated at short intervals. Therefore, there must be clear standards and rules which define when an additional assessement is actually necessary. If a repeated assessment is applied it is very important to design it in a way which minimises the additional administrative costs.

- **The need to verify the data used for training and the relevant programming and training methodologies, processes and techniques used to build, test and validate AI systems.**

Bitkom Assessment

As these considerations are a direct consquenence of D. „Requirements"/a. „Training data" & b „Keeping of records and data" we refer to our assessements from this part.

- **In case the conformity assessment shows that an AI system does not meet the requirements for example relating to the data used to train it, the identified shortcomings will need to be remedied, for instance by re-training the system in the EU in such a way as to ensure that all applicable requirements are met.**

Bitkom Assessment

In general, there must be operationally easy to handle criteria, which can be used to decide whether AI applications and systems meet the relevant requirements. AI applications trained with non-European data must be treated in the same way as systems trained with European data in this context. Disproportionate protectionist restrictions on non-European data must be prevented.

Furthermore, the recent developments of the Covid-19 crisis showed how important high-quality data and AI applications are for society as a whole to get necessary insights in the development and fight against Covid-19. Debates about restrictions of the use of non-European datasets and AI applications must always keep in mind the overall trade-off between risks and potentials.

- **Ex-ante and ex-post controls**

Bitkom Assessment

The role of a potential life cycle scheme for product security must be taken into account. The role of ex-post controls in general needs to be specified more specifically and based on standards: when are they necessary? How do they relate to ex ante conformity assessments and to the discussed repeated assessments? Overall, from a life cycle compliance and enforcement perspective, the entire administrative burden must be kept in mind and must be minimized given an aspired level of safety.

G. Voluntary labeling for no high-risk AI applications

- **For applications which are not high risk the possiblity of voluntary labelling is discussed**

Bitkom Assessment

We support the goal of voluntary labelling. However, we have different views and risks as to whether voluntary labeling can achieve these goals. Provisions linked to such labels for low-risk AI must, on the one hand, support trust while, on the other hand, must not be overly burdensome. Otherwise such labels will not be used on a voluntary basis. Applicable provisions falling under the label could relate to transparency, robustness and human oversight. Rules such around enforcement and legal remedies for users should not apply in the same manner as under high-risk applications, which couold result is more severe harm.

In our opinion, the proposed approach oversimplifies the concept of trustworthiness which will be more effectively built by brands and determined by the alignment of incentives and whether the performance of AI systems is meeting consumers' expectations.

We also see the potential for additional uncertainty and confusion through voluntary labelling and a variety of different certificates and labels.

- **Once the developer or the deployer opted to use the label the requirements would be binding**

Bitkom Assessment

We agree with this approach in principle. But if the developer/deployer decides to not use the voluntary label anymore it must be possible to opt-out again from the framework.

H. Governance

- **Given already existing structures such as in finance, pharmaceuticals, aviation, medical devices, consumer protection, data protection, the proposed governance**

structure should not duplicate existing functions. It should instead establish close links with other EU and national competent authorities in the various sectors to complement existing expertise and help existing authorities in monitoring and the oversight of the activities of economic operators involving AI systems and AI-enabled products and services.

Bitkom Assessment

Agreement in principle- If additional regulation is necessary in certain areas, it should always be linked to existing sectoral regulation with the corresponding existing structures. The sectoral structures contain the historical regulatory expertise. Regulatory approaches, if necessary, should build on these vertical regulatory frameworks.

- **The EU enjoys excellent testing and assessment centres and should develop its capacity also in the area of AI. Economic operators established in third countries wanting to enter the internal market could either make use of designated bodies established in the EU or, subject to mutual recognition agreements with third countries, have recourse to third-country bodies designated to carry out such assessment.**

Bitkom Assessment

These observations should not lead to additional and protectionist barriers for data and AI-based products from outside the EU.

Bitkom represents more than 2,700 companies of the digital economy, including 1,900 direct members. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.