ERHVERVSMINISTERIET

NOTAT

Annex: Specific comments from the Danish Government on the white paper on artificial intelligence

Specific comments

An ecosystem of trust: Regulatory framework for AI

The overall aim must be to create a regulatory framework where trustworthy, ethical, safe and secure AI goes hand in hand with the ability to provide innovative solutions. This regulatory exercise must also include stocktaking of existing legislation in order to make sure that existing legislation is up to date and is able to address specific issues related to AI. A stocktaking process should also ensure that potential new legislation does not overlap with existing requirements.

The General Data Protection Regulation (GDPR) has illustrated how the EU has been able to set global standards. However, the subsequent demand for guidance on how to adhere to the new standards showed the importance of legal clarity and user centric guidance. Therefore, clear and operable regulation is a precondition and must be factored in from the outset when establishing a regulatory framework for AI.

The scope for a new EU regulatory framework for AI

Where certain situations related to serious risks to individuals or to society stemming from the use of AI are not best tackled by existing legislation, the Danish Government finds it appropriate to address such risks in a new risk-based regulatory framework at the European level, while taking into consideration Member States' competences in specific sectors. This regulatory framework should address serious risks in relation to transgressions of fundamental rights such as discriminating decision-making as well as risks of infliction of injuries, especially where these may be irreversible.

Certain AI applications can be applied in critical sectors, which may involve serious risks of societal or individual significance, thereby categorising such application as high-risk. At the same time, it is important to consider that AI is also being developed and applied in critical sectors for the benefit of health, welfare and public services. Therefore, it is essential to find the right balance in the risk-based regulatory framework between minimizing risks and facilitating the development and uptake of new solutions for societal challenges.

Defining high-risk AI

It is crucial that the definition of high-risk AI is clearly limited to applications, which can actually cause serious risks, as it is imperative that unproblematic applications of the technology are not unnecessarily limited to the detriment of innovation, the development of new business models as well as the creation of future jobs. Therefore, essential building blocks for this new framework have to be a clear and targeted definition of high-risk AI and provide businesses and public authorities with proper guidance on how high-risk AI is defined in practice.

Firstly, such a definition should entail a clear definition of AI itself. The definition of AI will need to be sufficiently flexible in order to accommodate technical developments, while being precise enough to provide the necessary legal certainty. However, there is a need to elaborate further on the definition set out in the white paper, as it is still uncertain which kinds of AI is covered. The properties of AI as currently defined ranges from statistical models to neural networks, whereas in our view, the former should not be covered by the definition AI.

Secondly, the aim must be to identify the AI applications, which constitute serious risks and determine how serious risks are defined. Such an identification should result in making the category of high-risk AI the exception rather than the rule. With this in mind, the two cumulative criteria set out in the white paper constitutes a good starting point, as an exhaustive list of sectors combined with the application itself could provide the necessary predictability and delimitation. However, this will furthermore depend on the elaboration of the two criteria. The exhaustive list of sectors must cover a limited set of sectors and the definition of application should be clarified. This list should also be accompanied by clear guidance, as the term "application" could cover many different aspects such as the process as well as the end purpose. In order to bring clarity and cover the actual high-risk AI, we would give greater weight to the end purpose of the application, as this would characterize the potential outcome and thereby the risk more precisely.

In continuation hereof, applying the two cumulative criteria could nevertheless bring about different grey zones as well as overlook nuances with respect to serious risk. Therefore, greater emphasis should be put on a-built-in risk assessment, which for example should assess both individual and societal risks as well as assessing the probability of the actual risk. However, such a risk assessment should not in itself create legal uncertainty or bureaucracy.

Furthermore, the role of human oversight already incorporated in the application should be taken into account in the risk assessment. There should be a difference in terms of adhering to a stricter regulatory framework, when an application takes autonomous decisions compared to the situation where the application constitutes a support tool for humans in the decision-making process.

Lastly, we are wary of the exceptional instances, where the use of an AI application for certain purposes is to be considered as high-risk irrespective of the sector, as such an approach could undermine the legal certainty. There could be certain applications with a horizontal nature where such an exceptional category would make sense, but it must be composed of an exhaustive and limited list of specific applications.

Requirements for high-risk AI

The key features set out in the white paper are a good basis for identifying the relevant requirements for high-risk AI. An essential element of the future discussion is the operationalization of them. In this context, it is important to build on the existing work concerning the guidelines for trustworthy AI and take into account the experiences stemming from their feedback process. As stated by the Commission, one of the key results of the feedback process is that a number of the requirements are already reflected in existing legal or regulatory regimes. As the requirements should complement, but not overlap with existing legislation, such results must be taken into account, especially as it is likely that high-risk AI applications are also covered by sector-specific legislation.

In order to not unnecessarily hamper innovation and future solutions within the area of high-risk AI, any new requirements imposed must be proportionate, technology neutral and be able to address the specific risks associated with the AI application.

Furthermore, the Commission should incorporate, to the utmost extent possible, technical standards on AI as well as data technology in general, since standards have proven to be a flexible way to regulate a field including rapid technological developments. ISO/IEC and CEN/CENELEC as well as the IEEE are currently working on different aspects of standardization of AI and ethics/trust.

- *Training data*

As AI is only as useful, as the data, which it is trained upon, it is essential to set tangible data requirements for the development and use of high-risk AI. These should be easy to interpret, and therefore it is necessary to elaborate as to what constitutes “sufficiently representative” training data with regards to dimensions of gender, ethnicity and other possible grounds for bias or discrimination as well as those of privacy and safety. Such requirements should not inhibit the innovation of AI, which does not touch upon these dimensions.

- *Data and record-keeping*

An essential part of AI oversight is the ability to review the decisions taken. A complete transparency requirement might not be technically possible and could in some cases be a de facto hindrance for innovation. Instead, it should be required that certain information about the AI model such as records regarding the data used for training as well as the techniques used for developing the system is stored. These obtainable inputs will enable explanation of the output performed by the model and thereby enhance the transparency.

In terms of storing significant characteristics of datasets, it is vital that these characteristics rely on existing standards prevalent in the market in order to avoid imposing potential transition costs on authorities and businesses who are already using common metadata standards when describing data.

As to not create unnecessary burdens, it is important to establish strict retaining limits as well as what specific information is necessary in order to explain the AI's output. At the same time, this requirement should not lead to a situation, where developers and deployers of high-risk AI are required to publish data as well as algorithms. The objective should be to give the competent authorities, if needed, the adequate insight in order to verify whether applicable rules and requirements are complied with.

Furthermore, it is essential to take into account the requirements already set out in the GDPR as well as to specify how developers and deployers of AI are able to collect, store and use data for AI and still be GDPR-compliant. In this aspect, it should be considered, if GDPR is a sufficient legal framework in order to avoid creating new legislative burdens.

- *Information to be provided*

Proactive information related to the AI system's capabilities and limitations is essential, as such information could raise the understanding of the system as well as how it should be deployed. It could furthermore help in cases concerning liability, for example if a system is utilised in a way, which contradicts its capabilities and limitations, which the deployer was made aware of in advance. However, as to not lay unnecessary burdens upon developers, it is important to establish what specific information is needed in order to explain the system's capabilities as well as limitations.

When it comes to a requirement about informing users about the interaction with an AI system, it is unclear whether such a requirement in practice will empower citizens. The GDPR already sets out requirements, when personal data are obtained, concerning the existence of automated decision-making. Furthermore, despite this requirement, the deployer or developer of the AI – including public authorities - will still be responsible for the output and citizens will still be able to challenge the output. Lastly, another potential requirement for high-risk AI involves human oversight, which seems to overlap with this particular requirement. Transparency should be our point of departure in order to promote trust, but the aim should be to enhance transparency by giving citizens a meaningful choice and/or giving the possibility for the output to be put to the test.

- *Robustness and accuracy*

For AI to be trustworthy, it requires both robustness and accuracy of the application. However, in our view, both aspects require further elaboration, also in terms of the specific definitions of robustness and accuracy. One of the most important questions in terms of establishing such new requirements is whether AI must be more precise than humans, for example should autonomous vehicles be more precise than humans driving traditional ones? In order to minimise risks, but without hindering innovation, it is essential to find the proper balance in this question.

The issue of security is partly covered by the requirements on robustness and accuracy. Given the importance of cybersecurity in relation to AI and other data-based technologies, the item should be elaborated. Denmark supports a horizontal approach to cybersecurity, where existing legislation regarding cybersecurity would be updated, if necessary, in order to address potential risks in relation to AI – instead of establishing a sectorial approach for AI in relation to cybersecurity.

- *Human oversight*

When categorised as high-risk AI, there must be a requirement to have an appropriate involvement of human oversight in the specific AI application. One example could be when applying AI to diagnose patients or to choose medical treatment. In such cases, human oversight must be required. For example, a doctor must have the final say in the beforementioned matters, thereby making the AI application a support tool for the doctor in order to qualify the decision-making process.

As the AI applications within the category of high-risk AI may be a diverse group, there will not be one size fits all-model in terms of human oversight, meaning that human oversight could manifest itself in different forms. The appropriate involvement of human oversight - type as well as degree – should be proportionate and take into account the specificities of the AI application in question. In such determination, it would be useful to bring into play the results from the build-in-risk assessment used for establishing whether the AI application in question was high-risk or not.

- *Specific requirements for certain particular AI applications used for remote biometric identification*

Usage of technology for remote biometric identification calls for a very cautious approach, as it must neither result in general surveillance of our citizens nor erode fundamental rights as well as existing EU and national legislation. At the same time, we acknowledge that certain, but strictly limited cases may justify its deployment for example in terms of the prevention, investigation and prosecution of crimes. However, it is important that we strike the right balance between conflicting considerations. We need to find the right balance between fundamental rights and the prevention, investigation and prosecution of crimes. Biometric remote identification must always have a clear purpose, be proportionate, allowed for a strictly limited period as well as subject to adequate safeguards. As to whether further guidelines and regulations are needed in this respect, we will reserve the right to form our position, once such a potential proposal has been presented by the Commission.

Certification and control of high-risk AI

An efficient governance structure must strike the balance between the need for a uniform application of the requirements and the need for avoiding unreasonable burdens for developers and deployers of AI. An overarching European governance structure should play a key role in facilitating the implementation of the regulatory framework, as this is important to ensure a consistent and harmonized application of the requirements related to AI. Especially the responsibility of guidance as well as capacity to assist developers and deployers covered by the regulatory framework should be clearly defined from the beginning.

The specific conformity assessment should be entrusted to notified bodies designated by the Member States. This would increase assessment capacity, as developers and deployers would have access to at least 27 different notified bodies in order to obtain the conformity assessment. Furthermore, sufficient capacity to certify AI products and services needs to be ensured before entry into force of the regulatory framework.

Important considerations for the set-up of a conformity assessment should be to avoid lengthy, burdensome processes as well as duplication with other conformity assessments and tests in other fields such as medical devices. Additionally, some specificities of the requirements are not relevant for all types of AI products and services. The conformity assessment should be able to take into consideration the different aspects of different AI applications, focusing on those, which are relevant for the application in question. Also, it could be considered if a conformity assessment could be divided into different steps or similarly where an AI application in its testing stage would not be obliged to go through a conformity assessment, thereby giving room to innovate as well as minimizing the pressure on the notified bodies.

It should be the responsibility of the developer or deployer of AI to assess whether their applications are required to be certified. As grey areas are unavoidable due to the continuous development of the technology, it is essential to develop practical guidance tools in order to reduce legal uncertainty. A practical tool could for example involve an algorithm assessment tool, where developers and deployers could get immediate guidance on whether they are subject to the requirements or not.

As AI is a fast-evolving technology with an algorithm, which is not always static, recertification must be a requirement, if the AI application has been significantly modified. In order to avoid a situation, where developers and deployers find themselves in continuous conformity assessments, it should be explored how to stipulate benchmarks for when recertification is needed and whether the developer or deployer, which has already been assessed could be able to have specific aspects assessed based on their prior assessment.

Concerning SMEs, a conformity assessment could be a burdensome and lengthy process. However, once a conformity assessment is in place and a SME's AI is categorized as high-risk, the SME would for the most part be requested to deliver a fully-fledged certification from buyers and users who would otherwise turn to other certified providers. Therefore, an outright exception for SMEs would not solve the issue. Instead, SMEs should be given priority at the notified bodies and when establishing the Digital Innovation Hubs, SMEs should be given assistance with their potential conformity assessment.

In order to ensure that the different requirements are complied with over time and ensure consistent application of the requirements, compliance must be monitored and controlled by the existing competent national authorities, part of a market surveillance scheme. In our view, such control does not call for a new enforcement setup, as AI is just one technology out of many and would at the same time be controlled in connection with other areas such as competition, product safety etc. However, there could be a potential competency gap of the existing national authorities, which must be addressed in order to be fully equipped to enforce the new requirements related to high-risk AI.

Voluntary labelling for AI applications outside the high-risk category

As the general objective should be to enhance trustworthy AI - not only for the AI which poses serious risks – the Danish Government strongly supports a European voluntary labelling scheme. In this regard, the Danish Government will bring concrete experiences from the recent work with developing a Danish prototype of a data ethics seal as well as from the privately established Danish labelling scheme for IT security and data ethics which is planned to launch by the end of 2020.

A European labelling scheme should promote human-centric and ethical AI and data use in Europe by making it visible for consumers which companies, products and services to trust and thus empower consumers to make the ethical choice. A Danish study from 2019 showed that over 80 percent of citizens would avoid shopping at places, if they suspected that their data was not being processed responsible. At the same time, 65 percent of citizens stated that their choice would be influenced by a labeling scheme. A labelling scheme would therefore be a practical way of enhancing trustworthy AI for citizens as well as creating a push for making this a competitive advantage for companies.

Scope of a European labelling scheme

The Danish Government supports the idea for a European labelling scheme to target AI specifically. At the same time, we would underline the need for the labelling scheme to cover broader issues in the digital economy which citizens are concerned about in order to secure the relevance of the labelling scheme, which should be demand-driven. Such issues would encompass for example the usage and storage of data, tackling cybersecurity as well as ensuring unbiased decision-making processes, all of which are essential parts of AI. The Danish study from 2019 also showed that citizens do not differentiate between IT security and data ethics when using online services. Based on these insights, we would advocate for a European labelling scheme, which both incorporates IT security as well as data ethics into the scheme's criteria, in order to make the scheme relevant for citizens and to avoid confusion.

Furthermore, it must be ensured that the scheme is not inconsistence with corresponding regulation and requirements, for example the GDPR. However, the scheme should not be limited to the processing of personal data or guaranteeing GDPR compliance and the scheme should therefore be an addition to these.

Criteria for the scheme

The European labelling scheme should be rooted in a set of common criteria based on the ethical guidelines for trustworthy AI. As a successful labelling scheme is based on a broad market uptake, there should be a difference between the very strict requirements for high-risk AI and the requirements in the labelling scheme, which would cover all other AI, even though the requirements should be based on the same foundation. Such differentiation should aim at not requiring all developers and deployers of AI to adhere de facto to the regulatory framework of high-risk AI.

The criteria could require that data ethics are anchored at the managerial level of an organization, for example by requiring that businesses' internal policies for data ethics are included in their annual non-financial reporting. The criteria should also address and be anchored at the technical level such as fulfilling certain cybersecurity standards and ensuring that the use of algorithms is explainable, transparent and unbiased.

As the category of AI outside the high-risk category would cover a diverse group of developers and deployers of AI, it could be worth to consider a differentiation of criteria, depending on a risk profiling. In the Danish prototype, companies are categorized into four groups based on their organizational complexity and data complexity. In order to obtain the data ethics seal, each group is required to adhere to a set of different criteria, which also vary in strictness. We would recommend for the European labelling scheme to follow a similar approach.

Furthermore, it will be challenging for many developers and deployers in the target group such as SMEs to comply with all the criteria. For this reason, it could be considered to use a progressive disclosure model when rolling out the labelling scheme, meaning that the applicants will not be asked to comply with all the criteria at once. This strategy has multiple purposes such as reducing complexity for the applicants, making it easier to get started and thus increases the chance of buy-in, and giving the feeling of progression by providing the applicants with the most relevant criteria for its risk profile first and then increase the complexity-level progressively.

Furthermore, the model and criteria should be flexible to reflect future technological development and be revised continuously. In order to secure trust in the labelling scheme, it should be voluntary to apply for the label, but when first awarded, the criteria should be legally binding.

Governance of the scheme

An efficient governance structure for the scheme could be based on the set-up for the EU cybersecurity certification framework. This entails giving an EU agency the responsibility to provide the common criteria and certification scheme for the label. An advisory group, which could be the high-level expert group on AI could provide recommendations for drafting the common criteria and the Member States, should be responsible for appointing national conformity assessment bodies. An alternative model could be to anchor the governance of the labelling scheme in an advisory board and a secretariat constructed by industry bodies.

Adjustments to existing EU legislation related to AI

The Danish Government supports a horizontal approach towards AI and thus supports that the Commission also focuses on adjusting existing legislation to address specific issues in relation to AI.

In this respect, the Danish Government welcomes a revision of the General Product Safety Directive (GPSD) in order to ensure a set of minimum standards for product safety in regard to AI embedded into consumer products. These should be complemented by updates to the existing sector specific legislation to address the specific needs pertaining to different categories of products. However, it is important that the sector specific regulation is aligned with the general requirements in the GPSD in order to avoid conflicting demands.

The Danish Government also supports the Commission's proposed provisions in relation to product safety in order to support responsible innovation in AI technology, including a focus on the life cycle of products, quality of data, transparency and cooperation among economic operators and public authorities. Additionally, the regulatory framework for product safety should also address possible changes in consumer behaviour, when interacting with products embedded with AI technology and ensure that existing safety requirements - such as physical or mechanical means to deactivate a product - is not compromised. Finally, updates to the regulation must also address resilience towards external threats and be aligned with existing legislation concerning cybersecurity.

Furthermore, it is essential to analyse whether and to what extent the current legal framework on liability is still fitting in order to protect users in the area of AI. The Danish Government supports that individuals having suffered harm caused with the involvement of AI systems need to enjoy the same level of protection as individuals having suffered harm caused by other technologies, whilst technological innovation should be allowed to continue to develop. In this respect, the Danish Government welcomes that all options to ensure this objective should be carefully assessed, including possible amendments to the Product Liability Directive and possible further specific targeted rules in the specific area of AI.

Overall, it is important that the adjustments of existing legislation are drafted as clear as possible – both regarding the scope, definitions and allocation of responsibilities, but also that they take other Union or national legislation into consideration. A common and clear European regulatory framework will increase consumer protection and benefit European companies.

An ecosystem of excellence

The Danish Government supports the Commission's ambitious focus on research concerning AI and recognizes the importance of international cooperation among research centres with expertise in AI. For research initiatives to accelerate the innovation of AI, these must be coupled by adjusting our framework conditions at the European level. Therefore, the Danish Government further supports initiatives to make data, investment and testing facilities available across the EU with the aim of making the technology accessible for both the private as well as the public sector. In this respect, effective coordination across fields, programmes, the Commission and the Member States is essential in order to achieve the common objectives in terms of AI.

Revising the Coordinated Plan

As AI is undergoing rapid development – both in terms of the technology itself, but also due to initiatives set out in the Digital package as well as the context with COVID-19 - the Danish Government looks positively at revisiting the Coordinated Plan with an aim to review the impact of its initiatives and based on such a review, adapt where necessary. The overall objective of the Coordinated Plan must still be to foster closer cooperation and coordinating common priorities and initiatives within AI.

If Europe truly wants to be a front-runner in the global digital economy, we need to be ambitious in our priorities as well as maximizing efforts through closer cooperation which the Coordinated Plan caters for. At the same time, the Coordinated Plan should utilize and build upon existing well-functioning structures, institutions and clusters of expertise and capacities in order to improve the impact of the plan. This must be taken into account when revisiting the plan.

With regards to the energy sector, the Danish Government strongly supports the focus on how digitalization, access to data and emerging technologies can support our efforts to meet the EU's climate neutrality targets by 2050. In our view, the Coordinated Plan could to a greater extent become an enabler of accelerating the twin transition towards a green and digital economy which must be the backbone of the EU's recovery plan for a more sustainable and resilient Europe. For instance, by establishing testing and experimentation facilities that focus on developing and using solutions that paves the way towards a carbon-neutral and circular economy.

Furthermore, the Danish Government suggests that a review of the Coordinated Plan builds on the experiences obtained from the existing plan with respect to the security implications related to AI. The review should also include considerations on the security implications of AI in other critical functions in society beyond transport, security and energy.

Focusing efforts on the research and innovation community

The proposed creation of reference testing centres for AI under the Digital Europe programme should focus on providing a competitive advantage for Europe by ensuring that the testing centres are relevant for a variety of public and private sectors, applications and initiatives. It is important that the selection of testing centres follows an open, transparent and inclusive process and that the test centres commit to involve both SMEs as well as start-ups in order to foster the entire ecosystem.

Testing centres should have a flexible set-up and not apply a one-size fits all model, as AI can be used in many different settings. It is important that the testing centres build upon and strengthen existing capabilities in Member States and have a strong connection to existing AI ecosystems in order to avoid duplication. Furthermore, the testing centres should be obliged to develop and support responsible and trustworthy AI as well as having a strong focus on promoting carbon-neutral and circular solutions across sectors. We further believe that Denmark has several well-suited candidates that could participate in the set-up of testing centres for the benefit of all of Europe.

Furthermore, research and innovation actions under Horizon Europe will be an important element in Europe's approach to AI. Denmark fully supports the proposed AI and Robotics intervention area of cluster 4 (Digital and Industry) and notes that it is of particular importance to ensure efficient, cross-cutting coordination with other clusters in Horizon Europe, as well as with efforts from other relevant EU programmes.

Skills

The Danish Government recognizes that there is a great need for a larger digitally qualified workforce, while emphasizing Member States' competences in this area. Fully harnessing the potential of AI requires investing in people's digital competences and skills. The Danish Government recognizes the importance of a continuous focus on the intake of students in higher education programmes in information technology, including AI. Here, the Digital Europe Programme will be an important element, as it aims to develop world-leading masters programmes in AI. As the focus in the Digital Europe Programme is based on the broad uptake of digital technologies in the economy, the activities should have a sufficiently broad scope in order to meet the demand from businesses and public sectors.

Furthermore, there is a need for safe and secure use and handling of data on all levels with a specific focus on cyber and information security skills as part of the overall effort to empower individuals and investing in digital skills for citizens and SMEs.

Focus on SMEs

It is important that the European Digital Innovation Hubs under the Digital Europe Programme ensure broad uptake of digital technologies by businesses and especially SMEs. The Danish Government is currently taking steps to integrate the Digital Innovation Hubs in the existing Danish structures for decentralized business promotion. Modalities and framework for the hubs must be drafted in such a way that the hubs can contribute effectively to accelerate the digital transformation and have a real added value for European businesses and public authorities. Therefore, no hindrance should be introduced for the utilization of existing structures which already meet the needs of businesses and public authorities and which can carry out the tasks.

As AI is a technology of horizontal nature with importance for a wide range of sectors, the Danish Government supports the initiative that at least one European Digital Innovation Hub under the Digital Europe Programme has a degree of specialization in AI. Such a specialization requirement will still cater for a flexible framework, which enables Member States to build upon existing national structure and institutions, as the hubs should build on local strengths available as well as the future needs of the local economy.

Partnership with the private sector

The Danish Government supports the Commission's ambition to establish a public-private partnership in AI, data and robotics and acknowledges the importance of building strong ties between public and private institutions in the research and development of AI solutions.

To this end and based on national experiences within data ethics and AI, the Danish Government has established a national cluster organization for digital technologies in accordance with the national smart specialization strategy 2020-2023. The cluster organization aims at promoting innovation in companies developing AI solutions by strengthening collaboration between the private and public sector.

Promoting the adoption of AI by the public sector

The Danish Government supports the proposal to initiate sector dialogues, giving priority to healthcare, rural administrations and public service operators as set out in the white paper, which seems to resonate with the areas incorporated in the existing Coordinated Plan, thereby strengthening existing efforts. However, we suggest that AI systems intended for green, climate-positive purposes are also added to the priority list.

It is important that a new action plan on AI aimed at the public sector allows for both a top-down approach to identify critical functions in society that must be given priority to ensure the strategic autonomy of EU member states, as well as a bottom-up approach, for example an explorative approach that presents local authorities, such as municipalities and regions with a high degree of self-determination to experiment with AI solutions within the realm of the law.

Regarding the “Adopt AI programme”, Denmark proposes that the programme not only focuses on the aspect of the public sector procuring AI systems, but also includes the aspect of the public sector developing AI systems.

A programme focusing on public development and testing of AI solutions could support the “Adopt AI programme” by incentivising local authorities to develop AI solutions for application in prioritised areas holding a potential to heighten the quality and capacity of the public sector through upscaling of the technology, but where experience is needed before a wider uptake is possible. Such a programme could draw inspiration from the Danish “signature projects”, a joint public sector effort to test AI within the prioritised areas of healthcare, public administration and employment.

Securing access to data and computing infrastructures

Ensuring access to computing infrastructure as well as high-quality data across different sectors should be highly prioritized, as access to data is a precondition for the development and wider uptake of AI. Therefore, it is of utmost importance that the initiatives set out in the Commission’s Data Strategy complement the initiatives set out in the white paper on AI. This especially revolves around the development of data spaces, where standardisation is a key driver in establishing useful and well-functioning data spaces, cf. the Danish Government’s response to the Data Strategy.

International aspects

Alongside the EU’s priorities to develop and deploy trustworthy AI, the Danish Government supports the Commission’s continuous efforts to promote the ethical use of AI through international cooperation in order to make this the international norm.