



Axel Voss

Member of the European Parliament

Position Paper on the 2021 'Coordinated Plan on AI'

EU Roadmap for AI: How to become a global leader

15 March 2022

Artificial Intelligence (AI) will shape the current digital transformation as one of its key technologies. At the same time, the term 'AI' has become a buzzword with various - even contradicting - understandings. How can we describe it best? AI is an **umbrella term** that encompasses a wide range of old and new technologies that often have little more in common than being guided by a given set of human-defined objectives and having some degree of autonomy in their actions. While some AI technologies are already in widespread use, others are still under development or are even just speculative concepts that may or may not exist in the future. At this point, it is important to underline that even today's powerful data-driven algorithms can only solve tasks in domain-specific niches. They do not 'understand' the tasks they are performing. Therefore, experts refer to them as '**narrow**' or '**weak**' AI.

At the same time, the impact of AI within the current digital transformation should not be understated. Modern systems are vastly superior to humans when it comes to predicting

outcomes, finding patterns, optimising processes and making recommendations. In fact, AI will revolutionise the way we work, move and communicate. It will transform and improve our societies, our administrations, our industries, our economies as well as our health care and our security systems. AI offers humankind the unique chance to prevent, tackle or even solve global societal challenges such as climate change, pandemics or starvation. Consequently, it is not an overstatement to say that AI will have an impact on every part of our day-to-day life.

An objective assessment shows that the **vast majority of AI systems** that are currently in use - such as automatic translation systems, Eureka machines, gaming applications or robots that execute repetitive manufacturing processes - are almost or even completely **risk-free**. Only a very small number of use cases can be categorised as risky and only those do require regulatory action. It would be desirable if the public debate could shift its focus at least a bit away from the risks and move more towards the enormous potentials of AI technologies.

With its regulatory and market powers, the EU would have **the potential to be a global leader in AI** and to shape the international debate. Together with its allies, the EU could push for common global standards based on an ethics-driven, sustainable and trustworthy development as well as use of AI technology, which is fully in line with European principles and values. **Yet in reality, the EU has severely fallen behind in the global tech race.** Europe does not meet the preconditions that would allow to fully capturing the potential of AI. Other countries, especially the two **frontrunners China** and the **USA** are doing much better.

Significant parts of AI innovation and even more the commercialisation of AI technologies are nowadays taking place outside of Europe. What is holding us back? A lack of legal certainty, access to and sharing of high-quality data, harmonised rules and standards, funding, research, skills and infrastructure for core technologies, as well as high regulatory burdens, have led to a situation in which **the EU's competitiveness is constantly decreasing.** Furthermore, the EU's efforts to strengthen its global AI footprint were severely set back by Brexit, as the UK was one of the leading EU countries in AI with London as one of the EU's most important AI hubs, home to 1.000 AI companies, 35 tech hubs and reputed research centres such as the Alan Turing Institute.

The consequences of falling further behind do not only threaten our economic prosperity but also pose a major threat to our democracy. Over the

past years, AI technologies did increasingly become an **instrument of manipulation in the hands of authoritarian states and their proxies.** As shown by recent events, digital espionage, low-scale warfare, and disinformation campaigns powered by AI are an existential threat to democratic societies. They are able to question the European way of life. To safeguard our political stability, social security and individual liberties of citizens, the EU must 'level up'.

The window of opportunity to tackle the EU's deficiencies in AI and to catch up in the global tech race is closing fast. **The time to act is now!** **The 'Coordinated Plan on AI', updated by the Commission in 2021, is hardly enough.**

What the EU needs is the implementation of a bold and comprehensive *'EU Roadmap for AI'*. Since the EU does not have the legislative power to address all the listed points, a political process such as the EU 2000 Lisbon agenda should be launched in parallel. It would help to pull all Member States in the right direction and drastically improving the performance of those that are lagging furthest behind. The lack of long-term policy goals as well as ongoing pressure on Member States to reform led us to our current situation.

I. Executive Summary

A) Favorable Regulatory Environment

Law making

- Advance the Better Regulation agenda to find overlaps with upcoming files and gaps in existing legislations. Promote in-depth impact assessments to improve foresight in policy-making.
- Opt for reviewing and enforcing existing laws instead of creating new rules. Propose legislative acts only in form of regulations to achieve full harmonization.
- Set up a digital committee with legislative powers in the Parliament to respond to horizontal challenges in all sectors.

Governance and enforcement

- Establish an adequately resourced AI board that incorporates national competent authorities, EDPB, ENISA, etc. to guarantee the effective implementation and enforcement of AI laws across the EU.
- Combine ex ante/ex post approaches to better tackle the 'pacing problem' and complement the legislative toolbox with alternative governance approaches that are quicker and more adaptable.

Legal framework for AI

- Adopt a risk-based legislative framework that addresses certain risks, gives legal certainty and leaves enough leeway for innovation in AI.

- Differentiate between minority of high risk and majority of low risk AI use cases.
- Develop a European approach to AI that is grounded on our ethical standards.

EU data challenge

- Enable the (international) free flow of data and metadata. Open data silos. Foster access for AI researchers and companies to make better use of the large amounts of available but unutilised data.
- Make data protection laws more applicable to autonomous, self-learning AI.
- Fund research on standardising 'privacy by design' approaches and promote cryptographic solutions and privacy-preserving machine learning techniques.

B) Complete the DSM

Market barriers

- Remove barriers, such as country-based discriminations, burdensome market access procedures, high regulatory costs, and the frequent use of derogations resulting in diverging rules across the DSM.

Level playing field

- Increase the funding and technical capacities of competition authorities for enabling the quick and effective enforcement and the better targeting of abuses of market power.

C) Digital green infrastructure

Connectivity and computing power

- Establish a resilient digital infrastructure without major gaps across the EU to guarantee high-speed connectivity.
- Strongly fund and deploy broadband, fibre, edge nodes, 5G, and key emerging technologies such as quantum computing.

Sustainability

- Utilize AI to build up a green digital infrastructure that is climate neutral and energy efficient by 2030.
- Launch competitions and missions to innovate in AI solutions tackling environmental issues. Set up testing facilities to assess the sustainability performance of AI systems.

D) Ecosystem of excellence

Talent

- Use AI applications in education to foster digital literacy and skills while at the same time raising awareness of certain threats such as deep fakes. Cater to the need to train talent in AI at all levels and address the shortage therein.

Research

- Invest in research on AI-related key technologies (e.g. robotics and quantum computing) through a strategic roadmap.
- Expand the existing network of digital hubs and add AI lighthouse projects as well as ambitious missions.

E) Ecosystem of trust

Society and AI

- Promote awareness and build trust in AI, in particular by adjusting the consumer protection laws and by informing individuals when they are subject to algorithmic decision-making processes.
- Establish monitoring mechanisms to analyse, measure and score the social impact of AI. Reconsider those strategies and policies where AI has positive effects.

eGovernance

- Include AI systems in eGovernance services to provide borderless, interoperable, personalised, user friendly, and end-to-end digital public services with standardised, streamlined procedures.

eHealth

- Create health sector specific, harmonized legislation as well as a European health data space in order to adopt AI application in healthcare and seize its full potential.
- Draft lex specialis or include a specific section in the GDPR to process data and ease consent requirements for AI in medical research.
- Focus on patient-oriented and high-quality digital healthcare based on ethical standards, feedback, and development.
- Store data in pseudonymised form in Open Data Trust Centres to protect an individual's information.

F) Industry strategy

Strategic planning and investment

- Strengthen the EU's role by formulating a digital industry strategy that reduces our dependence from hardware, software and services from non-European providers.
- Use big data analysis to increase transparency and to perform stress tests assessing the resilience of value chains, map dependencies or future supply bottlenecks.
- Revise the investments for AI within the InvestEU and Digital Europe Programme.

SMEs & start-Ups

- Develop AI-transition plans through networks, digital hubs, and AI trainers to incentivize investment in AI research and human resources by SMEs and start-ups.
- Promote the use of digital tools, lower administrative burdens and offer better access to public procurement and venture capital.

International stage

- Uphold a strong international core value-based technology alliance to overcome regulatory divergence based on privacy rights, data flows or competition rules while remedying strategic vulnerabilities by building on each other's assets and pooling resources.

G) Security and military deterrence

AI and law enforcement

- Promote diligently developed algorithms for crime prevention and investigation, based on qualitative data sets as they may provide a higher level of efficiency, neutrality, and legal certainty than human law enforcement agent may.

Cybersecurity

- Confer competences in cybersecurity to the European level in order to pool resources, coordinate better, and streamline national cybersecurity policies efficiently.
- Formulate mandatory cyber security requirements for all digital and in particular AI applications that cover the entire lifecycle from development.

Cyber defense

- Introduce an active EU cyber diplomacy strategy in order to counterstrike against foreign AI-powered cyberattacks.

Military use of AI

- Exempt the exclusive use of AI for military and national security reasons from the upcoming AI legislation in order to prevent hampering innovation in this field and avoid affecting our security and defence.

II. Roadmap

A) Favorable regulatory environment

Law Making

- Calls on the Commission to propose only legislative acts in the form of regulations for new digital laws in areas such as AI, as the digital single market needs to undergo a process of genuine harmonisation; is convinced that due to rapid technological development, digital legislation should always be swiftly adaptable, principle-based and future-proof, while adopting a risk-based approach; stresses, furthermore, the importance of legal certainty and, consequently, the need for robust, practical and unambiguous applicability criteria, definitions and obligations in all legal texts;
- Highlights the principle of proportionately in the EU Treaties, which determines that any proposed means of intervention must be proportionate to the stated goals, without being overly prescriptive or invasive; states that new digital laws in areas such as AI must therefore find the right balance and prevent unnecessary new administrative burdens for SMEs, start-ups, academia and research; considers that ‘as much as necessary, as little as possible’ should serve as the guiding principle for the regulator;
- Believes that the Better Regulation Agenda is a key element for making the EU AI-strategy a success; calls on the Commission and the co-legislators to commit to drastically reducing the number of new EU legislative acts and to instead shift their focus to the review, adaptation, implementation and enforcement mechanisms for existing laws; proposes that the REFIT platform, together with a comprehensive group of stakeholders such as the European AI Alliance, be used to evaluate the suitability of legislation in the light of changing contexts;
- Urges the Commission to perform more in-depth impact assessments with adequate foresight and risk analysis, prior to issuing any new digital proposals in areas such as AI and across the different DGs; emphasises that, by default, impact assessments should systematically map and evaluate all existing horizontal and sector-specific legislation, as well as all ongoing proposals under negotiation that could be relevant to AI and other digital technologies;
- Underlines the particular relevance for new AI legislation of the New Legislative Framework, the GDPR, the ePrivacy

- Regulation, the Platform-to-Business Regulation, the Data Governance Act, the Open Data Directive, the Cybersecurity Act, the NIS Directive, the Law Enforcement Directive, the Product Liability Directive and the Digital Services Act, as well as the Directives on Unfair Commercial Practices, Unfair Contract Terms, Consumer Rights, the Sale of Consumer Goods and Price Indication;
- Finds that both the Council's general approach and Parliament's first reading position should also undergo rigorous impact assessments before the inter-institutional negotiations start; proposes that the co-legislators institutionalise a structured dialogue on AI with the European AI Alliance and with the EU-level bodies that have a role in the implementation of the law, for instance through the issuance of guidelines or the development of common standards;
 - Calls for the Parliament, the Commission and the Council to reduce internal competence conflicts when it comes to overarching topics such as AI, as such conflicts risk delaying the legislative procedure, with knock-on effects in terms of the entry into force of the legislation in question and its market relevance; requests, in this regard, a review of Annex VI of the Rules of Procedures of the European Parliament and specifies that the entire process of establishing and

attributing the competences of standing committees needs to be revised;

- Is convinced that Parliament should process horizontal files on topics such as AI exclusively in new ad hoc committees with legislative powers; states that each of these ad hoc committees, named in alignment with the political priorities of the Commission, such as 'Europe fit for the digital age', would exist for the whole political term, incorporate MEPs from all standing committees and work on all digital legislative files.

Governance and enforcement

- Calls for the creation of an adequately resourced mechanism to supervise the uniform, EU-wide implementation and enforcement of the upcoming AI laws; prefers a European AI Board over the creation of a costly new EU Agency for AI; suggests, however, that this board should be made up of not only the national AI supervisory authorities and the European Data Protection Board (EDPB), but also a broad range of relevant EU bodies, such as the EU Agency for Fundamental Rights, the High-Level Expert Group on AI, the EU Agency for Cybersecurity, the European Consumer Consultative Group, and standardisation organisations the European Committee for Standardization, the European Committee for Electrotechnical Standardization and the

European Telecommunications Standards Institute;

- Highlights the need to learn from GDPR flaws such as its low-compliance rate by realising that just focusing on ex post controls by courts and regulatory agencies will only scratch the surface of the legal challenges posed by emerging technologies; concludes that the ‘pacing problem’ requires the EU to combine ex ante and ex post approaches by complementing its legislative toolbox with alternative governance approaches that are able to deliver much quicker, more adaptable and more effective solutions; supports, therefore, the increased use of regulatory sandboxes, private-public partnerships, standards and certification;
- Explains that regulatory sandboxes would give AI developers the unique chance to experiment in a fast, agile and controlled manner outside the strict application of regulatory rules, but under the supervision of competent authorities; notes that these regulatory sandboxes would be experimental spaces in which to challenge existing legislation, detect regulatory obstacles to innovation and test, under real-world conditions, new business models that could potentially achieve more significant benefits and higher levels of user protection than those on which the original regulations were based;

- Explains that private-public partnerships such as the European Alliance for Industrial Data, Edge and Cloud are another promising governance approach; elaborates that this approach would enable the EU’s AI ecosystem to operationalise its principles, values, objectives and industrial interests at the level of software code, making compliance binding by design, but at the same time keeping the set of protocols flexible enough for technological advances;
- Explains that any new digital laws in areas such as AI should also go hand in hand with the promotion of consensus-based and industry-led voluntary standards; warns, however, that the EU should avoid the fragmentation of standards, discrepancies with international standards and overlaps with sectoral standards; proposes, therefore, that EU standardisation organisations be used as a platform to translate the essential requirements, determined by digital legislation in areas such as AI, into product-specific and state-of-the-art technical standards and design instructions; notes that these could then be combined with labelling schemes as a way to build consumer trust and develop, for instance, a European AI brand that stands for trustworthy services and products;

- Explains that an open certification platform could also establish an ecosystem of trust that involves governments, civil society, businesses, accounting firms and other stakeholders; explains that such certificates would license AI developers and producers to operate while also validating that they provide secure digital products, technologies and services throughout their entire lifecycle; notes that such an approach would allow for up-to-date and technology-specific minimum standards to be maintained, while facilitating the continuous adaptation of certificates and verification information based on the newest technological developments observed by approved platform subscribers.

Legal framework for AI

- Highlights that the underlying objective of the EU's digital strategy, as well as that of the AI strategy is to create a 'European Way' in a digitalised world; clarifies that this approach should be human-centred, value-oriented and based on the concept of the social market economy; underlines that the individual, with their respective dignity and individual freedoms, should always remain at the centre of all political considerations;
- Agrees with the conclusion drawn by the Commission in its 2020 White Paper on

artificial intelligence that there is a need to establish a risk-based legal framework for AI, covering high-level ethical standards combined with appropriate liability rules and sector-specific provisions, while at the same time providing the private sector with enough flexibility, practicability and legal certainty to develop new business models based on AI technologies;

- States that the co-legislators should aim to align the AI definition in future legislation with the concepts, terminologies and standards developed together with other like-minded democratic countries in the OECD; stresses that doing so would give the EU an advantage in shaping a future international AI governance system;
- Is convinced that it is not AI as a technology that should be regulated, but that the type, intensity and timing of regulatory intervention should solely depend on the type of risk incurred by the use of an AI system; underlines, in this regard, the importance of distinguishing between a minority of 'high-risk' and the vast majority of 'low-risk' AI use cases; concludes that while only the former category indeed demands legislative safeguards, businesses should self-regulate 'low-risk' technologies by choosing measures that deliver the best outcomes;

- Specifies that the classification of technologies as ‘high-risk’ should be based on the concrete use and context, complexity and autonomy of the AI system, the probability and likelihood of the worst-case scenario, the severity of the harm and its irreversibility, the techniques used and the governance arrangements adopted; stresses that this classification should be introduced together with best practices and guidance for AI developers and should also recognise that AI technologies can significantly reduce certain risks;
- Notes that the requirements that AI systems need to fulfil differ significantly in a business-to-business (B2B) environment compared to a business-to-consumer (B2C) environment; points out that while consumer rights need to be legally protected through consumer protection legislation, companies can solve liability and other legal challenges more quickly and cost-effectively by contractual means with business partners directly; concludes that, in particular, SMEs and start-ups investing in AI technologies would benefit from a B2B exclusion as they are disproportionately affected by new legal obligations, which also harms their ability to attract investments;
- Underlines the need to address open ethical questions raised by new technological possibilities, but clarifies

that new AI ethical guidelines should not set up stricter rules than those already existing for human or automated actions; proposes that on these grounds the EU should introduce ethical guidelines that consist of three categories of core values and principles;

- Explains that the first category could list fundamental, mandatory principles such as the non-maleficence principle, the principle of respecting human dignity or the protection of the democratic process; states that the second category could include good practices in AI development such as human-centric AI, responsible governance and the principles of transparency and explainability; concludes that the last category could include principles of sustainable AI that would be fully aligned with the UN 2030 Agenda for Sustainable Development;
- Highlights, with regard to the third category, the gap in leadership on AI global governance, which gives the EU the chance to become the leading voice in aligning AI with the UN SDGs and using AI technologies to push worldwide for their achievement; stresses, however, that not all AI technologies developed or applied in the EU should need to comply with all three categories; suggests, for example, that sustainable AI could only be mandated for AI implemented or procured by public tender or in specific

sectors, while the majority of AI developers and companies would only be encouraged to align with the second and third categories through soft law;

- Is convinced that efforts to completely ‘de-bias’ AI algorithms are frequently misguided, because this strategy wrongly suggests that bias-free data sets exist; notes that in this regard the requirement that data used to train AI systems is ‘complete and free of errors’ needs to be revisited; stresses, however, that the EU should at the same time cooperate very closely with AI developers to counterbalance structural biases in our societies and daily life;
- Elaborates that transparency or explainability obligations for AI systems, while helpful in certain cases, may not be possible to implement in every instance; notes that both concepts also need to be balanced against other factors, including the interests of businesses in maintaining trade secrets or the potential value of exposed data to potential competitors; stresses, however, that a mandatory self-identification of AI systems or accessible machine logs seem to be very useful for many AI use cases that interfere with the fundamental rights of individuals or affect consumers;
- States that the legislative framework on intellectual property must continue to incentivise and protect AI innovators by

granting them patents as a reward for developing and publishing their creations; finds that existing laws are mostly future-proof, but proposes certain adjustments, including the integration of open source elements and new forms of patent licensing to ensure that tools are available to regions and initiatives that could not otherwise afford them; recognises that it will also be necessary to clarify whether AI will be able to hold intellectual property rights in itself;

- Elaborates that obligatory ex ante risk self-assessments, comparable with CE markings or data protection impact assessments, combined with market surveillance based on clear rules and standards, and complemented with ex post enforcement for high-risk AI systems, seem to be a sufficiently robust governance approach for AI; warns that overly burdensome conformity assessment obligations could create significant burdens that make the business models of AI developers and companies economically unviable;
- Notes that in order to increase product safety and improve the identification of faults, the developers of high-risk AI should at least be obliged to ensure that accessible logs of algorithmic activity are maintained securely; considers that developers should also design high-risk AI systems with embedded mechanisms –

‘kill switches’ – for human intervention to immediately halt automated activities at any moment;

- Is convinced that despite the legal challenges caused by AI systems, there is no need for a complete revision of the existing liability rules; stresses that the Product Liability Directive and the national fault-based liability regimes can in principle remain the centrepiece legislation for countering most harm caused by AI; underlines that only in some cases could there be inappropriate outcomes, but warns that any revision should take the existing product safety legislation into account and should solely be based on clearly identified gaps;
- Notes that certain changes to the legal definitions of ‘product’, including integrated software applications, digital services and inter-product dependency, and ‘producer’, including backend operator, service provider and data supplier, do however seem necessary to ensure that compensation is available for harm caused by emerging technologies; stresses, however, that an overly broad approach to the definition of ‘product’ should be avoided, as this may make it difficult to differentiate between AI and other algorithms;
- Points out that, due to the characteristics of AI systems, such as their autonomy and opacity, there could also be cases where

neither an updated Product Liability Directive nor national fault-based liability regimes apply and where persons who suffer harm or whose property is damaged would end up without compensation; suggests, therefore, the introduction of a limited new liability mechanism for legal claims against the operator, who controls the risks associated with the AI system and who also often is the cheapest cost avoider; specifies that while high-risk AI systems should fall under strict liability, combined with mandatory insurance cover, victims of low-risk AI systems should only benefit from a presumption of fault against the operator.

EU data challenge

- Agrees with the conclusion drawn by the Commission in its 2020 communication entitled ‘A European strategy for data’ that the creation of a single European data space is key to ensuring the EU’s global competitiveness in AI, as well as its strategic sovereignty and economic prosperity; recalls the essential link between the availability of high-quality data and the development of AI;
- Highlights, however, that EU data governance is currently highly uncoordinated; asks the Commission, therefore, to streamline its various policy and funding streams, to rectify existing

- overlaps and to present a consistent overall system that ensures seamless data flows as well as the protection of user rights; proposes that solutions that leverage decentralised data analytics and edge architectures also be prioritised, as these could be more cost-efficient, resilient and sustainable alternatives to the structures currently in place;
- Stresses the key importance of opening data silos and fostering access to data for AI researchers and companies; underlines the need to establish the required legal certainty and technical infrastructure, while also motivating the European industry to make better use of the large amounts of available but unutilised data, and ceasing to cede most of the value generated to dominant platforms; considers that voluntary data sharing between businesses based on fair contractual arrangements and triggered by incentives such as subsidies or tax breaks would help to achieve this goal;
 - Recommends interoperability be further strengthened and consensus-based, industry-led common standards be established in order to guarantee that the free movement of data between different machines and entities can take place in an innovative manner; notes that besides open standards, open source software, creative commons licenses, open codes and open application programming interfaces (APIs) can also play a key role in accelerating data sharing;
 - Calls on Member States to guarantee that fair contractual conditions are more strongly enforced within the scope of competition rules, with the aim of addressing imbalances in market power without interfering with contractual freedom; underlines that a single European data space will require companies to be allowed to closely cooperate with each other, and therefore considers that safe harbours and block exemptions on cooperation for data sharing and pooling, as well as more guidance for businesses on competition law matters from the Commission, are needed;
 - Calls on Member States, with regard to government-held data, to quickly implement the Open Data Directive, making high value datasets available free of charge and supplying them in machine readable formats and APIs; stresses that this initiative would reduce the costs for public bodies to disseminate and re-use their data and would help EU researchers and companies enormously in improving their digital technologies in areas such as AI;
 - Calls on the Commission to ensure that GAIA-X is scaled up into the European Alliance for Industrial Data, Cloud and Edge'; stresses that a GAIA-X, which is coherently linked to the mechanisms in the alliance and which establishes a 'compliance by design' mechanism based on EU legislation, could become the blueprint for setting up common European

data spaces; notes that an updated EU Cloud Rulebook would also help to translate common EU principles and values into actionable processes and checks for technical practitioners;

- Emphasises the importance of clarifying the contractual rights of AI developers and companies which contribute to the creation of data through the use of algorithms or internet of things (IoT) machines, and in particular the rights to access to data, to data portability, to urge another party to stop using data, and to correct or delete data;
- Takes note of the Commission's 2019 practical guidance on how to process mixed datasets; underlines, however, that in practice further specifications concerning the distinction between personal and non-personal data, as well as the definition of 'inextricably linked', seem necessary; points out that not sharing any commercial datasets continues to often be the best option for AI researchers and companies due to the complexity of the existing rules and significant legal uncertainty as to whether data is sufficiently anonymised;
- Considers WP 216 on Anonymisation Techniques of the Article 29 Working Party to be insufficient in practice; proposes instead the introduction of a clear legal basis, guidelines based on specific use cases and relevant situations for different types of data processors, and a checklist with all the requirements that have to be fulfilled to

make data sufficiently anonymous; notes, however, that anonymisation techniques are currently not able to guarantee full and complete protection of privacy, as modern AI systems show in experiments that they nevertheless manage to re-identify a person;

- Suggests, therefore, the funding of more research on standardising 'privacy by design' approaches, as well as promoting cryptographic solutions and privacy-preserving machine learning, as it is crucial to ensure that high-quality data can be used to train algorithms and perform AI tasks without breaching privacy; notes that data trusts, certifications for truly high risk applications, personal information management systems, and the use of synthetic data also show promise;
- Calls for a limited revision of the GDPR to replace or reinterpret some of its key concepts, such as purpose limitation, data minimisation, the obligation to provide information or processing records, restrictions on secondary use and informed consent, as a way to make data protection laws more applicable to autonomous and self-learning AI; proposes in this regard the replacement of the concept of data minimisation with the concept of data sovereignty, which would allow users to make sovereign decisions about the use of their data; underlines that the ePrivacy proposal discussed does not include any reference to the current legislative efforts

on AI and focuses solely on consent and data minimisation; stresses, in this regard, that a new impact assessment should be conducted with a focus on the proposed changes to the current regime and on technologies that had not yet been developed during the previous legislative term in 2016;

- Calls for a push for a uniform implementation of the GDPR across the EU by making the consistency mechanism compulsory and by streamlining the diverse national interpretations of the law; finds that there is also a need to reduce the frequent use of opening clauses in the GDPR, to better equip data protection authorities, and to clarify unambiguously in the law that data protection is not an absolute fundamental right but should instead be balanced with other fundamental rights and interests, such as the right to life, liberty and security, the freedom to conduct a business and the freedom of the press;
- Encourages the EU and its Member States to leverage the recently established OECD project on trusted government access to personal data held by the private sector as a reference point for policymakers globally to work towards an international solution and regulatory convergence of best practices in this area;
- Stresses, in this regard, that the free flow of data and metadata across international borders is a crucial enabler for digital

innovation in Europe; calls on the Commission to therefore refrain from imposing data localisation requirements, except in limited, proportionate and well-justified cases where such a policy is in the interest of the EU or necessary to uphold our high European standards;

- Calls on the Commission to decisively respond to the ruling of the Court of Justice of the European Union that the EU-US Privacy Shield is invalid by creating an alternative workable system that respects the requisite safeguards, but also simplifies EU-US data flows again; calls on the Commission to continue pursuing data adequacy talks with other third countries, as this is the best way to promote privacy policies of the EU and allow the international exchange of data;
- Asks the Commission to honour the risk-based approach to security measures set out in Articles 25(1) and 32(1) of the GDPR and thus to not require standard contractual clauses to ensure advanced encryption and full unreadability of personal data at every stage of the processing of data outside the EU; notes that researchers and companies in areas such as AI should not be obliged to undertake 'mini-adequacy' assessments for each of their data transfers; stresses that requiring researchers and companies to assess the laws of the country of destination themselves and, on that basis, to decide

which safeguards would be the most appropriate, is not feasible in practice;

- Encourages, furthermore, the stronger use of codes of conduct, binding corporate rules and certification mechanisms as potential alternatives to adequacy decisions and standard contractual clauses; asks the EDPB to issue more guidance for researchers and companies in areas such as AI on how to use those mechanisms to effectively process personal data outside the EU in a GDPR-compliant way.

B) Completing the DSM

National AI strategies

- Calls on the Member States to review their national AI strategies that they developed in accordance with the 'coordinated plan on AI', as the vast majority of them remain vague and lack clear goals; recommends that they formulate more concrete, quantifiable and specific actions, while trying to create synergies between them;
- Calls upon the Commission to help Member States to set priorities and strongly align their national AI strategies in order to ensure coherence and consistency across the EU; points out that, while a diversity of national approaches is a good way to establish best practices, AI developers and companies would face major obstacles if they are subject to different operating parameters and regulatory obligations in each of the 27 Member States.

Market barriers

- Urges the Commission to continue its work on removing key barriers for developers and companies in areas such as country-based discrimination, burdensome market access procedures and high regulatory costs, as well as to address the frequent use of derogations which results in diverging rules among different Member State jurisdictions;
- Underlines the need to swiftly conclude the legislative negotiations on all pending legislative files that aim to complete the Digital Single Market; proposes to focus in particular on telecom networks and the logistic aspects of cross-border e-commerce;
- Calls upon the Commission to strictly enforce the rules of the Single Market as the number of infringements by Member States is constantly on the rise; believes that the enforcement of these rules should not depend on political considerations but instead solely on legal grounds; finds that the focus of the EU institutions should in general shift from creating new obligations to the effective enforcement of the existing rules;
- Notes that the New Legislative Framework (NLF) should be carefully updated and aligned with digital products and services; proposes to focus on modernising and simplifying compliance procedures by introducing digital alternatives to paper-based procedures;

- Supports the introduction of a Digital Euro in the form of tokenised central bank money issued by private sector intermediaries, as a complementary payment instrument, supervised by the European Central Bank and the national central banks, as well as an integrated European payment platform, with high security standards to support pan-European digital payment services and solutions, pre-empt unfavourable initiatives from third countries or large platforms, and to avoid becoming dependent on foreign services;
- Encourages the Commission to tackle barriers faced by offline businesses wishing to go online; underlines, however, that those barriers are not only policy-related but also related to demand-side issues such as language and cultural differences; proposes information campaigns and better market surveillance as a means to increase the trust as well as knowledge of European consumers.

Level playing field

- Is convinced that the current national and European competition and antitrust frameworks need to be reformed in order to better target abuses of market power and algorithmic collusion in the digital economy, as well as to better address the risks of new emerging monopolies without compromising innovation;
- Notes that such a reform should strengthen an evidence-based approach and take the

value of data and the implications of network effects more into account, while also improving the practical and actual control over data, introducing clear rules of conduct for market-dominant platforms and increasing legal certainty for cooperation in the digital economy;

- States in this regard that the Commission should adapt its market definition practices and merger rules to define markets more accurately and in line with modern market realities in the digital sector, taking account of global market conditions and adopting a dynamic analysis and long-term view to assess the existence of competitive pressures; stresses that allowing mergers and other deals between EU companies more often could be a key element in boosting European AI companies' growth and scale up;
- Calls upon the Commission and national competition authorities to increase their efforts of monitoring digital markets on an ongoing basis, identifying competitive constraints and competition bottlenecks, and subsequently imposing more frequently remedies on companies that abuse their dominant position or that engage in anti-competitive behaviour; notes that it is crucial that the principle of "same activities, same risks, same rules" is respected by all market players;
- Calls upon Member States to substantially increase the funding and the technical capacity of competition authorities in order

to ensure the effective and swift enforcement of competition rules in the fast-paced and complex digital economy; underlines that competition authorities ought to speed up abuse proceedings and, where necessary, apply interim measures to prevent the negative impact of infringements and to avoid markets from tipping while at the same time guaranteeing the procedural defence rights of companies;

- Welcomes the new OECD tax deal as it is a balanced instrument that will establish a fair and more effective taxation approach towards globally active digital companies; calls upon Member States to swiftly sign the multilateral convention and implement it.

C) Digital green infrastructure

Connectivity and computing power

- Calls on the Commission to follow up on its ambition of incentivising 75 % of European enterprises to take up cloud computing services, big data and AI by 2030 in order to remain globally competitive and reach climate neutrality; finds that the allocation of EUR 2.07 billion in funding for digital infrastructure under the Connecting Europe Facility (CEF) is insufficient;
- Stresses that the shift in the volume and processing of data for AI requires the development and deployment of new data processing technologies encompassing the edge, thereby moving away from centralised cloud-based infrastructure models towards increasing decentralisation

of data processing capacities; urges the strengthening of European intense-computing AI architectures as a key strategic priority to maximise investment and research, including distributed clusters, the deployment of edge nodes, digital microcontroller initiatives, and the capacity to enable faster data collection and processing in all aspects of society;

- Stresses that AI requires powerful hardware to make sophisticated algorithms useable, including high-performance and quantum computing and the IoT; urges the maximisation of funding and research for such AI-enabled emerging technologies; finds that, similarly, nano-technologies and chips are essential to enabling AI to be embedded in, for example, medical devices, which also requires priority funding;
- Highlights that a functioning and fast infrastructure for AI must be based on a fair, safe and high-quality foundation by avoiding gaps in digital high-speed connectivity, which requires 5G roll-out in all urban areas by 2030, as well as ultra-fast broadband networks and spectrum policy with licence conditions that do not distort competition; urges Member States to continue to implement the 5G toolbox, specifically enabling legislation related to the risk assessment of suppliers and service providers; calls for the Broadband Cost Reduction Directive to be put into practice to facilitate network deployment;

- Calls on the Commission to establish timetables and financial incentives for Member states, cities, regions and industry, and to accelerate the administrative approval processes for 5G; supports incentivising private investment in 5G roll-out; requests that in regions where roll-out is not carried out by the private sector, more funds are made available; calls for funding for broadband and connectivity projects under the multiannual financial framework, with easier access for local authorities to avoid the underutilisation of public funds;
- Calls on the Commission to establish a precise strategy with a clear timetable for 6G roll-out to better prepare for the next wave of digital infrastructure, enabling Europe to take the lead;
- Finds that it will not be possible to achieve the necessary deployment of dense edge-node connectivity for 5G in rural areas, where half of European households are not even connected through fibre; calls for a clear strategy on fibre-optic network deployment and broadband roll-out in rural areas, which is also key for data intensive technologies such as AI; recommends that European Investment Bank support for connectivity projects in rural areas be enhanced;
- Stresses that the significant investment required for network deployment, coupled with the ambitious expectations of public authorities and consumers regarding roll-

out timing and coverage, will be impossible to achieve without infrastructure-sharing agreements, which are also key to promoting sustainability and reducing energy consumption.

Sustainability

- Urges the EU to take the lead in making green digital infrastructure climate neutral and energy efficient by 2030; calls for coordinated global multilateral action to use AI in the fight against climate change and environmental degradation;
- Highlights the need for clear rules and guidelines for environmental impact assessments for AI; calls for a circular economy plan for digital technologies and AI in particular to incentivise companies to reduce the carbon footprint of data centres and devices; stresses the need to ensure that the processes associated with AI products and services do not have undue sustainability impacts; recommends fostering the use of AI-based solutions such as digital twins in all sectors, to coordinate sustainable standards for businesses and to enable the monitoring of energy efficiency, collecting information on emissions and product lifecycles;
- Calls on the Commission to launch competitions and missions for AI solutions tackling specific environmental problems and to strengthen this component in Horizon Europe;

- Believes that supporting and fostering the application of codes of conduct to enable the integration of sustainability data sets into already existing data space activities or upcoming data spaces at local, cross-sectoral or cross-country level should become a guiding principle; stresses the need to define principles to ensure that relevant climate and sustainability data can be integrated when setting up new sustainability data spaces;
- Calls on the Commission to set up and support testing facilities where AI applications can be tested on their sustainability performance and to offer experience on how to improve the environmental footprint of these applications, including autonomous vehicles; encourages the adaptation of existing testing facilities to focus on use cases in circular production;
- Calls on the Commission to invest in and cooperate closely with the private sector in order to create lighthouse projects in volunteering smart cities, where all available state-of-the-art technologies including AI are combined and where real-life tests are constantly conducted, covering smart buildings, smart grids, connected cars, mobility platforms, public services and logistics; supports the development of an 'EU Smart City App Store' as a common collection of projects and applications that other cities can adopt; urges the effective mobilisation of cohesion policy and for AI in

an urban context to be addressed specifically;

- Calls on the Commission to promote and invest in coherent sustainable transport infrastructure that uses AI built on best practices in order to optimise transport systems to increase efficiency, decrease pollution and promote adaptability to user needs;
- Urges the use of AI to monitor energy consumption in municipalities and develop energy efficiency measures; calls on the Commission to incentivise the outsourcing of data to energy efficient data centres.

D) Ecosystem of excellence

Talent

- Calls on the Commission to create an AI competence framework for individuals that builds on the digital competence framework for citizens, which helps individuals and SMEs to find relevant AI training and learning opportunities and to improve the sharing of knowledge, best practices, digital skills initiatives and funding between organisations and companies, at both EU and national level; recommends the establishment of a central body for the European AI skills data space to coordinate European skills training on sectoral and regional levels in all Member States; urges the Commission and the Member States to support free online courses that enhance digital literacy such as basic training in AI;

- Calls on the Commission, in cooperation with the Member States, to develop policies for the re-skilling and up-skilling of the workforce in AI for all generations and all forms of employment by drawing on existing public-private cooperation initiatives to provide for a regular solutions-oriented policy dialogue; calls on the Commission to incentivise and invest in multi-stakeholder skills partnerships to test best practices; highlights the need for digital and AI skills to be included in life-long learning initiatives; is of the opinion that Member States need to give up legislative competences in this area and consequently calls for a comprehensive and consistent legislative initiative from the Commission on AI skills and education at EU level;
- Urges engagement in horizon scanning to gain an understanding of which skills will become less relevant and which will be in higher demand or at risk of shortage in the future; believes that this will enable a more targeted policy to help workers transition between jobs or acquire necessary new skills, to anticipate the new skills that workers may need and to foster the development of those skills in a timely manner;
- Calls for a high-performing AI education system that fosters digital literacy, skills and digital resilience from an early stage, starting with primary education; calls on the Commission to promote the introduction of mandatory AI and computational competence courses in all European schools, universities and educational institutions; stresses that digital resilience, including awareness of deep fakes, requires additional media education that helps to contextualise new digital and AI competences;
- Is convinced that in order to help raise awareness of and skills related to AI, the use of AI tools for (off- and online) services directed towards EU citizens should be announced and explained in full transparency, with short communication material adapted to the target audience, especially children; calls for a European strategy for better and safer AI for children, in line with the European strategy for a better internet for children, designed to empower children while also protecting them from risks and potential harm;
- Calls for action to ensure that every education facility has broadband access as well as strong digital learning infrastructure; stresses the need to ensure that teachers have the necessary AI skills and tools to provide a digital learning environment; calls on the Commission to support technical training for teachers and the development of innovative teaching and learning tools;
- Draws attention to the need to have multidisciplinary university curriculums that focus on digital and AI skills, including in health, and cross-disciplinary research centres; believes that pathways towards further education to specialise in AI (e.g.

master's and PhD degrees, part-time study) should also be emphasised;

- Calls on the Commission to support the development of innovative solutions such as AI-based intelligent tutorial systems; asks that universities be provided with grants to develop AI concepts and programme them together with education technology (EdTech) companies;
- Requests investment in youth coding skill initiatives to foster AI skills and high-level qualifications, including coding academies, summer school programmes and AI-specific scholarships; is of the opinion that the EU's Digital Opportunity Traineeships (DOT), further expanded to vocational training, could provide cross-border opportunities to get hands-on working experience in AI jobs;
- Calls on the Commission to promote and increase the funding for STEM (academic disciplines to increase the number of students in these fields; underlines that women and minorities should be encouraged to pursue STEM-related educational and professional opportunities such as vocational training; stresses that other disciplines that interact with the STEM disciplines will also be crucial for promoting digital skills;
- Stresses the need to train talent in AI at all levels and to address the talent shortage by ensuring growth, attraction and retention of top talent; urges the Commission to follow up on its goal of having 20 million ICT specialists employed in the EU, and to close

the gender gap in this sector; stresses that AI skills and talent need to be fostered in all sectors including health, transport, energy and agriculture; stresses that in order to retain top AI talent and prevent brain drain, the EU needs to enable competitive salaries, working conditions, cross-border cooperation and a competitive innovation infrastructure;

- Stresses that the acquisition and teaching of digital and AI skills needs to be accessible to all; stresses further that EU policies must strive to remove obstacles to the participation of women and other discriminated groups in the digital economy and empower them to take the lead as tech investors and entrepreneurs; requests an incentive system to encourage companies to ensure their teams of developers and engineers include gender balance and minority inclusion;
- Stresses that within the EU, most AI talent is located in Western Europe with fewer resources in other regions; emphasises, therefore, the need to strengthen innovation cohesion among EU regions and Member States.

Research

- Calls for the EU to increase investment in research into key technologies such as AI, robotics, quantum computing, microelectronics, batteries, the Internet of Things, nano-technology, distributed ledger technology and 3D printing; calls on the

- Commission to develop and maintain a European strategic research roadmap for AI which includes major interdisciplinary challenges where AI can be a part of the solution;
- Encourages all Member States to spend a significant proportion of their GDP on research into digital technologies, and for annual combined public and private investments in the EU to reach at least EUR 20-25 billion; urges the continued strengthening of the Horizon Europe programme, notably its AI, data and robotics partnership and the European Innovation Council, and to expand the digital Europe programme, whose allocated funding of EUR 7.6 billion is insufficient to remain competitive;
 - Calls on the Commission to simplify and streamline the structure of research funding instruments by reducing the effort and time needed to obtain decisions when applying for grants; stresses the need to improve the quality and consistency of proposal reviews and to increase the predictability of funding instruments and their timing to support long-term planning, using the European AI research roadmap;
 - Encourages the creation of more chairs on AI at European universities as well as competitive salaries for AI research and the provision of more funding in order to properly train and retain the next generation of researchers and entrepreneurs and prevent brain drain to locations outside the EU; stresses the need to reduce the bureaucratic burden for university researchers in accessing funds and calls on the Commission to provide tools to increase digital interconnectivity between universities; urges the development of cross-cutting networks for AI across European universities and research institutions;
 - Calls on the Commission to improve knowledge transfer between AI research and the business world by setting up business networks, regulatory sandboxes and contact points with legal personnel and business consultants in universities;
 - Stresses the need to accelerate knowledge transfer in the EU from research and science to AI applications in industry and the public sector; recommends the creation of a dedicated public-private partnership (PPP) on AI; calls on the Commission to establish European AI data centres, jointly developed by government and industry and using strong encryption to protect the stored data in an appropriate manner; stresses the need to support the development of large-scale testing sites for AI; calls on the Commission to provide financial incentives at EU level to launch pilot projects in Member States;
 - Supports strongly the establishment of an AI lighthouse under the Horizon Europe framework, which would be the continent's pioneering centre of excellence for AI research and development; notes, however, that the EU and the Member

States should commit to a long-term and much more substantial investment plan in the region of EUR 1 billion per year over the next 10 years; adds that the AI lighthouse would be an excellent place to create regulatory sandboxes, meaning time- and space-limited areas for experimenting with, testing and finessing specific AI applications that carry some risk but also have high potential for public good;

- Points out that the designation of European Digital Innovation Hubs (EDIHs) under the digital Europe programme is another important step in building up an AI ecosystem of excellence based on university-industry clusters; criticises, however, the fact that the hubs are dotted across the continent and that the interplay with other digital hubs designated by the European Institute of Innovation & Technology (EIT) and under the Horizon Europe framework remains unclear; suggests, consequently, that more coordination is needed, as is the establishment of a cooperating overall cluster of decentralised AI hubs based on an EU-wide framework for legal expertise, data, funding, and incentives;
- Proposes to scale up and align existing mission such as ELLIS, platforms such as CLAIRE and flagship projects such as HumanE AI and AI4EU with the goal of promoting ambitious, collaborative and EU-wide research and development goals as well as projects; explains that a single AI

mission with clear milestones and regular evaluation would attract the most talented researchers, bringing them together to address the biggest scientific questions in AI.

E) Ecosystem of trust

Society and AI

- Proposes that on top of the suggested AI training, the EU and its Member States should create awareness raising campaigns, including public discussions at local level, as an additional means to reach, inform and empower citizens to understand better the capabilities, limitations and impacts of AI;
- Underlines the added value of establishing monitoring mechanisms at national and EU level to continuously analyse, measure and score the social impact of AI; explains that those mechanisms could help us to keep track of the positive and negative impacts that AI has on our society and allow us to adapt or redirect our AI strategies and policies; suggests that Eurostat and other EU agencies be involved in order to guarantee high quality outcomes;
- Highlights that this monitoring mechanism might illustrate that the transformation initiated by AI technologies will lead to such radical changes to our lives and habits that the EU might in turn need to rethink further elements of our normative framework, adapt certain social and environmental principles or even establish a fully-fledged European transition fund, helping to

manage, for example, new social gaps or temporary job losses in vulnerable sectors; underlines, however, that potential additional costs during this area of adjustments do not 'kill the case' for AI as the positive effects of AI will strongly outweigh the costs in the medium to long term;

- Supports adjustments to consumer protection laws as another way to build trust in AI, for instance by giving consumers at least in some cases the right to know whether they are subject to algorithmic decision-making or if they are interacting with an AI agent, allowing them to insist upon human review of AI decisions or giving them means to counter commercial surveillance or personal pricing.

eGovernance

- Calls on Member States to deliver on the Tallinn Declaration on eGovernment and put mechanisms in place to provide borderless, interoperable, personalised, user-friendly, and end-to-end digital public services based on AI to all individuals and businesses at all levels of public administration; is of the opinion that the objective should be to increase the number of people that use eGovernment services, with a focus on AI, to up to 80 % of all EU citizens over the next five years;
- Calls for collaborative ecosystems for developing AI eGovernment tools that include both suppliers and local

governments; supports efforts to harmonise eGovernance structures and calls for standardised, streamlined public administration procedures for more efficient exchange across EU Member States and all levels of administration; calls on the Commission and Member States to further promote the use of AI in support of evidence-based and reliable legislation;

- Calls on the Commission to renew the eGovernment action plan and use it together with the digital Europe programme as a common legal framework to support all central public administrations and as many local administrations as possible in fully adopting AI wherever it is beneficial and feasible and in line with the European open-source strategy;
- Calls for a common platform for eGovernance where AI solutions and best practices can be offered and exchanged within and among EU administrations; stresses that platforms enable fast and economical sharing of open-source software within administrations down to the local level that can be shared across the EU in a user friendly way;
- Stresses the need to focus government recruitment and training policies on bringing digitally skilled people with deep knowledge of AI into administrations as well as the judicial sector;
- Calls for the implementation of the digital single gateway to be sped up and for the

development of interoperable platforms that offer cross-border services in the European Union to be promoted, while meeting common security standards for all services in all Member States; supports expansion beyond the limited set of services currently involved in the single digital gateway act;

- Stresses that governments and businesses should only deploy and procure trustworthy AI systems that are designed to be respectful of the law and fundamental rights, are aligned with ethical principles, are socio-technically robust and are able to counter surveillance;
- Calls on the Commission and the Member States to strengthen online connectivity to political decision-making processes, as well as user engagement and analysis, in order to strengthen political participation based on AI; urges for the public consultation platforms of EU and Member State institutions to increase digital information and engagement; recommends investing in improvements to usability and accessibility such as the provision of summaries and information in multiple languages, as well as in dedicated marketing and targeted outreach for digital public engagement platforms;
- Recommends intensifying the interactive and personal dialogue with EU citizens through AI tools via online citizens' consultations, stakeholder dialogue formats or digital functions for

commenting on EU legislation and initiatives;

- Supports the development of digital voting systems based on AI to make elections more accessible, auditable, efficient, secure and transparent, while still providing analogue voting options and preserving analogue voting result backups.

eHealth

- Calls for human-centred design and an evidence-based approach to AI in health that focuses on patient-oriented and high-quality digital healthcare and that seeks consumer and user feedback throughout the development process; calls on the Commission to set the global tone on cutting-edge healthcare and well-being, placing the benefits of AI at the centre of policy-making; urges the prioritisation of funding, the setting of strategic goals, the fostering of cooperation and the adoption of AI applications in healthcare as a critical sector;
- Considers that equitable access to healthcare as a principle should be extended to health-related AI applications, including systems for the detection of diseases, management of chronic conditions, delivery of health services, and drug discovery; emphasizes the adoption of appropriate measures to tackle the risks concerning the digital divide, discrimination, marginalisation of

vulnerable persons or cultural minorities, which have limited access to healthcare;

- Stresses the need for sector-specific legislation for health data in order to seize the full potential of AI; calls on the Commission to harmonize governing rules across Member states for the sharing, processing, standardising, curating, anonymising, interoperability and collaborative use of health data; finds that the objective should be to provide all involved actors (e.g. doctors, hospitals, health companies) with all necessary personal health data without identifying a specific patient;
- Stresses the need for measures and incentives that enhance health care providers' potential to scale up the uptake of AI solutions and share them with others; calls on the Commission to provide interoperable data architectures adapted to local needs for countries to adapt to digital solutions and AI;
- Calls on the Commission to support the setup and operation of a European health data space in order to foster the sharing of health data; supports the establishment of a central health data entity at EU level to select standards and profiles for interoperability, as well as a health data entity in each Member State to implement those standards;
- Call on the Commission to promote the integration of ethical rules at a very early stage in the development and design of AI

applications; stresses the need to promote further research on the methods and bias embedded in a trained AI system so as to avoid unethical and discriminatory conclusions when applied to human health data; recommends to create an EU Code of Conduct for processing health data;

- Urges to create the legal and technological basis for a European Digital Health Ledger as a system to protect individual information by not identifying the respective person, while at the same time improving the quality of available data for each European citizen by allowing digital tools to work properly (e.g. based on self-learning algorithms or big data analysis); recommends that the data of this system should be stored in pseudonymised form in Open Data Trust Centres and should be available for further research as well as the development of new drugs and treatments;
- Finds that it is necessary to determine which health care services can be ethically and responsibly automated; stresses that it must be ensured that automated decisions cannot be influenced, altered or modified by malicious parties;
- Calls for a clear liability framework and harmonised approval regimes for AI-based medical applications and medicines developed or tested via AI and machine-learning; urges that practical best practice regulation, standards and criteria are needed to certify and approve health care application in line with liability risks;

- Calls on the Commission to create a sector-specific chapter on health in the GDPR to ensure the processing of data for scientific purposes in healthcare; stresses the need to reduce the obligation for additional consent, when using AI in medical research; calls on the Commission to update data protection rules so that an “opt-out” alternative is considered sufficient when personal data is used by public bodies or in public-private partnerships to train and develop AI applications for purposes of public good;
- Calls on the Commission to provide and make use of people-centric predictive models of pandemics with diverse data sets coming together in real time to inform decision-making;
- Requests a legal framework for online medical consultation and promote the interconnectivity between European health entities by using international accepted standards (e.g. FHIR, SNOMED) in order to facilitate best practices and evidence-based treatments;
- Underlines that digital and AI skills, need to be included in the education of health care professionals, as well as skills in applying data protection legislation and dealing with sensitive data, including the promotion of data anonymisation.
- Is convinced that the EU should implement an ambitious AI industrial strategy, that attempts to reduce the EU’s dependence on non-European hardware, software and services while establishing sound ethical, technological and security standards for those elements that are not produced in the EU or where the purchasing of imports makes more sense from an economic point of view; declares that this approach does not aim to make the EU protectionist, but to strengthen its role as a champion of international cooperation and trade;
- Encourages the Commission to use big data AI analysis to increase transparency, perform stress tests to assess the resilience of value chains, map dependencies, warn about future supply bottlenecks, diversify suppliers and reshoring some aspects of production back to the EU; warns however that the EU should not nationalize or territorialize supply chains or endorse types of AI sovereignty as these approaches regularly lead to major economic setbacks;
- Urges the Commission to conduct a comprehensive strength-weakness-analysis to determine the EU’s vulnerabilities and high-risk dependencies, establish realistic technical-economic expectations with regard to AI and assess the effects across all sectors of the European industry; underlines that the Commission should thereby cooperate closely with business alliances and multi-stakeholder initiatives;

F) Industrial strategy

Strategic planning and investments

- Continues that the EU should, on the basis of this analysis, formulate and adopt a fully-fledged AI industry strategy combined with a 10-year vision and a concrete rolling action plan; explains that this strategy should be complemented by bold missions, clear timetables, adequate governance and a monitoring system with key performance indicators and yearly updates;
- Stresses the need to firstly consolidate and streamline the vast number of individual initiatives that were launched by the Commission to support EU industry, before secondly, incorporating them into the new AI industry strategy; warns that so far there is a chaotic system of overlapping sector-specific as well as horizontal policies whereas many of them feature contradicting timelines, indicators, definitions or targets;
- Calls on the Commission to add a genuine investment strategy to the overall digital industry strategy, aiming at achieving an optimal balance between public and private investments; suggests to establish new mechanisms that facilitate access to finance, more risk-tolerant investment strategies in new ideas (early-stage financing) and the creation of a specific AI investment fund, which is managed by leading investors and overseen by a multidisciplinary advisory board comprising of both scientists and business leaders;
- Holds that the proportion of resources devoted to AI within the InvestEU and

Digital Europe Programme should be reviewed and strongly increased;

- Stresses to strongly support the recently adopted common framework for the screening of foreign investments but underlines that sensitive technologies with potential dual-use applications must be better protected; states that AI should be considered a critical sector that deserves protection through the investment-screening mechanism; continues that the protection of intellectual property rights as well as the outflow of critical technologies, in particular in partnerships with Chinese firms and research bodies, should become subject of much higher scrutiny.

SMEs and start-ups

- Proposes to offer an alternative to the buy-out vision of many AI start-ups by ensuring that government support is provided at all stages of their development; underlines in this regard that the EU should amplify its efforts at offering SMEs and start-ups development paths and services, especially by promoting the use of digital tools, developing AI transition plans and further expanding the exchange of best practices; urges the Commission and the Member States to provide better counselling and more concrete support through networks, digital hubs, AI trainers, business mentoring and site visits;
- Stresses that it needs to be worth for SMEs and start-ups to invest in AI research as well

as in human resources; notes that tax breaks for doing research, better access to computer capacities and datasets, an EU-Visa scheme for tech-talents, temporary support in technology scouting or in paying the salaries of AI specialists, and state aid exemptions in the area of AI education, training and reskilling of employees are potential ways of how the EU and Member States can help;

- Suggests to ease the administrative burden for SMEs and start-ups in AI, for instance by reducing extensive reporting, information or documentation obligations, and by harmonising the civil procedure law; proposes also the establishment of a single EU online portal in different languages concerning all necessary procedures and formalities to operate in another EU country, of a single point of contact in the home country that can certify the company's eligibility to provide services in another EU country as well as of a standardized EU-wide VAT declaration in the respective native language;
- Underlines that SMEs and start-ups in AI need better access to public procurement and venture capital; notes in this regard that, similar to the USA, the EU should establish a new mind-set by promoting the continuous search for the 'next big thing' on AI; stresses that stock option schemes for AI start-ups across Europe should also be promoted as they would allow European founders to compete with their non-EU

counterparts by selling a share of their idea to high-skilled employees;

- Calls for the creation of a dedicated EU stock exchange that is sought along the lines of NASDAQ as this would allow fast-growing technology companies to finance themselves in Europe instead of migrating to the USA for scaling up;

International stage

- Points out that the EU should forge a strong international core value-based AI technology alliance, working together with like-minded partners in order to overcome regulatory divergence in the fields of privacy rights, data flows or competition rules and to remedy strategic vulnerabilities by building on each other's assets and pooling resources in areas where it is mutually beneficial to do so;
- Welcomes the EU-US Trade and Technology Council (TTC) as a platform to deepen the partnership and collaboration, to develop compatible standards and to ensure the security of critical supply chains; suggests to establish in addition a specific transatlantic working group on AI, including representatives from government, the private sector and civil society to work on common standards and ethical guidelines for AI; wishes in this regard also to continue a close EU-UK cooperation on AI;
- Stresses that the EU should leverage its regulatory power as well as industrial and technological capabilities to advance the European approach on AI in multilateral fora

and international bodies such as the United Nations, the OECD, the WTO, the WEF and the G20;

- Supports the WTO's eCommerce initiative to develop an inclusive, high-standard, commercially meaningful, evidence-based and targeted policy to better tackle barriers to digital trade including AI; underlines that the agreement should also reflect principles of good governance, and provide governments with the ability to counter digital protectionism while protecting and promoting consumer trust and creating real value for the global economy;
- Points out that the EU should act as first-mover with regard to ethical guidelines and standards on AI and identify respective gaps in international standards in order to prevent countries like China or Russia to push for international standards that are not compatible with European standards and values;
- Calls on the Commission and the Member States to increase their participation in international standardisation forums; proposes to provide better incentives and support to academics, civil-society and SMEs for participating in standardization forums as the related costs and travel expenses are often high, while recognition is rather low;
- Encourages the uptake of recent standardisation initiatives from actors such as the Institute of Electrical and Electronics Engineers (IEEE) and the Joint Technical Committee (JTC) of the International

Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), which are both aiming to globally harmonise divergent AI codes;

- Suggests that the European Commission continues to address unjustified trade, in particular non-tariff barriers, or market access restrictions for European AI companies in third countries as well as infringements with regard to intellectual property rights; stresses that trade, neighbourhood and development policy should also be actively used to shape the international debate on AI and to promote European ethical principles on AI.

G) Security and military deterrence

AI and law enforcement

- Considers it to be of paramount importance for the safety and security of citizens that law enforcement agencies are well advanced in AI development, making full use of the potential of digital technologies to prevent and investigate serious crimes through real-time facial recognition in select locations; underlines that diligently developed algorithms for crime prevention and investigation, based on highly qualitative data, may provide a higher level of efficiency, neutrality and legal certainty than human law enforcement agents, and should thus be promoted;
- Warns of the grave consequences of limiting law enforcement agencies' use of state-of-the-art technology in a time when organised

crime increasingly has access to sophisticated technology, becomes increasingly violent, and operates across borders; asks instead for the inclusion of AI applications for law enforcement purposes in the category of high-risk AI systems, ensuring that sufficient safeguards are put in place;

- Suggests that the EU should furthermore participate in the soft law approaches established by the United Nations Interregional Crime and Justice Research Institute (UNICRI), which has developed operational AI toolkits and started a partnership with Interpol, serving as a unique platform for dialogue and cooperation on AI between law enforcement agencies, industry, academia and civil society.

Cybersecurity

- Asks Member States to confer competences in the field of cybersecurity to the European level in order to enable the EU to better pool resources, more efficiently coordinate and streamline national cybersecurity policies, further increase cybersecurity capacity building and awareness raising, and swiftly provide cybersecurity knowledge and technical assistance to SMEs as well as to other more traditional sectors; suggest enhancing AI security in Europe by investing in AI security research
- Proposes to Member States to enforce cybersecurity requirements for AI systems

through public procurement policies by making certain ethical and safety principles mandatory for the procurement of AI applications in certain critical sectors;

- Requests to enable ENISA to perform sectorial security risk assessments, starting with industries engaged in the most high-risk and sensitive uses of AI, and with the highest potential of negative impacts on human health, safety, security and fundamental rights; stresses that ENISA, together with the European Cyber-security Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, should also be instructed to assess cybersecurity incidents as well as to review the latest AI-cybersecurity research with the objective to identify gaps and new vulnerabilities and timely advise the EU-institutions on adequate corrective actions;
- Encourages every AI company that is active in the Digital Single Market to develop a clear and independently evaluated cybersecurity strategy, based on its individual risk situation; encourages furthermore to include AI systems into threat modelling and security risk management; suggests that the Commission, ENISA and national authorities support this process by establishing a common interactive platform that shares best practices, lists the latest vulnerabilities, provides legal advice and facilitates the sharing of cybersecurity relevant data between AI companies;

- Proposes the introduction of horizontal, product-centred and mandatory cybersecurity requirements based on the principles of the New Legislative Framework (NLF) as only a new horizontal legislative act can avoid fragmentation of cybersecurity requirements, while at the same time, guaranteeing a consistent cybersecurity approach across all product groups; notes that AI products on the Digital Single Market that carry the CE marking would as a result stand for both a high level of physical safety as well as a risk-adequate level of cyber-resilience;
- States that mandatory cyber security requirements for all digital and in particular AI products should cover the entire lifecycle from development, e.g. code testing and verification, to maintenance, e.g. patching and updates, until the end of its lifetime; highlights that it has to be also clear that each company in the supply chain has to play its role in contributing to the creation of resilient AI products; points out that the new requirements should be based on the associated risk in the specific product group and the degree of influence on the risk level in order to avoid disproportionate burdens for SMEs and start-ups; suggests that there should be a close corporation with the private sector in order to make the requirements relevant to the market and keep them up-to-date with the pace of technological change as well as the evolution of threats;
- Continues that the certification schemes developed under the EU Cybersecurity Act could complement the mandatory requirements of the new horizontal legislation; proposes to take also the existing initiatives of certain Member States for an EU wide certification schemes for trustworthy AI, such as the German AI Cloud Service Compliance Criteria Catalogue (AIC4) or the Maltese AI certification program, into account;
- Encourage the use of strong, globally accepted and deployed cryptography and other security standards that enable trust and interoperability in AI systems; highlights that to create international convergence of ICT risk oversight, the alignment of all cybersecurity legislation with existing international standards and industry best practices is of utmost importance.

Cyber defence

- Urges Member States to pursue an active policy of European cyber diplomacy by denouncing and attributing foreign-supported AI-powered cyberattacks, while leveraging the full toolbox of EU diplomacy; advises that this should include diplomatic responses, the termination of financial aid and sanctions against those countries or proxies that engage in malicious cyber activities or that sponsor cybercrimes; believes that the EU, in close cooperation with NATO,

should consider using AI to execute cyber counter-strikes against repeat offenders;

- Suggests furthermore the creation of an EU Cyber Defence Agency with executive powers as a way to establish a centralised EU body that has the competences to develop and implement clear EU-wide procedures based on AI for a coordinated and quick reaction to cyber-attacks, covering measures in the political, economic, diplomatic and military domain; notes that this new agency should also monitor the implementation of cyber defence policies in each Member State, have the oversight of the entire EU cyber defence architecture and assess the allocation of relevant resources within the EU;
- Proposes that the EU should also establish a European Security Commission on AI incorporating representatives from Member States, the private sector, and civil society; explains that this Security Commission should analyse the impact of AI on European security and develop recommendations on how to address the new security challenges;
- Encourages to use white hats, meaning hackers that seek to identify vulnerabilities so they can be fixed, while also using hackers to form 'red teams' that are deployed to attack the

systems; notes that such teams could test various AI tools that are already in use for malicious purposes and by doing so, providing constructive insights on existing AI systems and applications.

Military use of AI

- Notes that exclusive military uses of AI should be exempt from civilian AI legislation, since overregulation in the field of security and defence could preemptively restrict the EU's capacity to innovate and deploy AI technologies, placing it at a disadvantage to its adversaries that do not have such constraints;
- Continues that the EU should therefore consider AI as a crucial component of European strategic autonomy, which could significantly enhance the detection, protection, and preparation capabilities against security and defence threats; underlines that not using AI systems for military aspects means to decrease the EU's security level and also hamper the ability of EU militaries to remain interoperable with US forces;
- Concludes that Member States should train their military staff to ensure that they have the necessary digital skills to use AI in control, operational and communication systems as well as to use AI in lethal defensive AI weapons with a human in the loop or on the loop;

highlights the importance of the European Defence Fund to support cross-border cooperation between EU countries in military AI research, to develop state-of-the-art defence technologies and to build up the necessary infrastructures, namely data centres with strong cyber capabilities

- Calls upon the EU institutions to push for a combination of dynamic soft law mechanisms and a legally binding international treaty to address the concerns in relation to lethal offensive AI weapons with no human oversight; states that within the international agreement, it should be determined that all lethal AI weapons must be subject to meaningful human oversight and control, meaning that human beings remain either in the loop or on the loop, and are therefore ultimately responsible for the decisions to select a target and to take lethal action;
- Underlines that the NATO alliance should be used to deter other countries from using lethal offensive AI weapons with no human oversight and to develop a multilateral strategy to effectively sanction those countries that do not join the international treaty but instead further advance the development, production and use of lethal offensive AI weapons with no human oversight.