

Steering brief

Scene setter

You are meeting

Microsoft.

AI

Microsoft AI is a robust framework for developing AI solutions in conversational AI, machine learning, data sciences, robotics, Internet of Things (IoT), and more. The company is heavily investing into AI, ranging from their AI-powered assistant Cortana to Azure AI – a portfolio of AI services designed for developers and data scientists.

Microsoft's responsible AI program has established internal processes, including practices and tools to uphold the company's AI principles. As part of this work, Microsoft has long supported the goal of creating a regulatory framework for AI, including in Europe, in particular to set common guardrails for high-risk scenarios.

Microsoft is also a member of the Grand Coalition for Digital Jobs – the initiative of the European Commission to tackle the lack of digital skills in Europe.

TTC

On 15 June 2021, Microsoft posted a blog entry¹ on “Stronger Together: The Case for a Transatlantic Technology Alliance”. They state that a transatlantic technology alliance is vital and that the transatlantic cooperation can serve as a catalyst for cooperation among democratic allies and partners in the face of fundamental global challenges and that real actions will be taken now.

Microsoft see five main areas for cooperation:

- Strengthening the resilience of democratic institutions
- Deepening collaboration on norms for responsible technology development
- Implementing a sustainable solution for transatlantic data flows
- Defining principles for fair treatment
- Fostering the digital transformation of small and medium-sized enterprises

All five are areas that resonate well with the intentions of the Trade and Technology Council (TTC).

NIS2 - Network and Information Security (NIS) Directive:

Microsoft's interest in NIS2 was mainly in relation to supply chain security requirements, the obligations applicable to digital service providers, in particular cloud, as well as the alignment between NIS2 and the proposal for the digital operational resilience for the financial sector ('DORA Regulation proposal').

Reporting obligations of significant incidents and significant cyber threats is also of interest,

Cyber Resilience Act (CRA):

Microsoft is overall supportive of this initiative and engaged very actively and constructively with the Commission in the preparation process of the CRA, with a particular interest in how software, including standalone software, would be covered in the CRA scope.

¹ <https://blogs.microsoft.com/eupolicy/2021/06/15/stronger-together-the-case-for-a-transatlantic-technology-alliance/>

DSA

Microsoft is generally supportive of the aim and approach of the DSA but has suggested several detailed and fundamental amendments to safeguard its interests:

- further differentiation and clarification on services covered and obligations linked (e.g. exclude hosting services obligations, sharpen online platform definition and clarify status of ancillary services);
- clarification of obligations (e.g. simplify transparency reporting, clarify KYBC requirements, clarify data access & auditing requirements for very large platforms).

Key messages

AI

- We welcome the commitment of Microsoft to responsible AI.
- The benefits of AI will only materialise through uptake, but uptake requires trust.
- The AI Act seeks to define the uses of AI technologies that are allowed and the conditions under which they can be deployed on the EU market.
- It will foster trust, legal certainty for businesses, and a well-functioning single market with uniform rules for AI.
- Our goal is to support innovation while making sure that people's legitimate concerns are addressed.
- I believe that this goal will be achieved through a proportionate, risk-based approach.
- That is why the AI Act mainly focuses on high-risk systems. It addresses the real risks of the technology, while shielding systems that do not pose high risks to safety or fundamental rights from diverging national regulations.
- To further support excellence and innovation, the Commission will invest at least EUR 1 billion per year in AI between 2021–2027.
- The objective is to increase public and private investment in AI gradually to a total of EUR 20 billion per year over the course of this decade.

TTC

- Digital topics are an important part of the EU-US transatlantic dialogue. The Russian aggression against Ukraine acutely demonstrates the need, or even obligation, for democratic countries to provide an alternative vision of the world, based on our values.
- Creating strategic partnerships with likeminded nations provides a positive narrative and shows that digital can be to the service of people, not used to control them.
- We have regular dialogues within the ten working groups, made up of key staff, addressing a wide range of topics, as defined in the Joint Statement from Pittsburgh.
- Through bilateral and multilateral efforts the EU aims to ensure a global level playing field for trustworthy and ethical use of AI. It seeks to be an active player in promoting good governance of AI globally.
- The protection of supply chains, notably ICT, is key, for both the EU and the US. We share the objective of making them (cyber)secure and resilient.
- Discussions are currently ongoing with the US on potential areas of cooperation (e.g. security and resilience of key ICT supply chains, including network infrastructures, cloud and data centres, development financing, and cooperation on 6G).
- It is important to look into ways to ensure security and resilience of critical digital, telecoms and ICT supply chains (including cloud, undersea cables, etc.), beyond 5G.
-

NIS2 – revised Network and Information Security (NIS) Directive

- Legislative deliberation started in January 2022.
- We are confident that they will go smoothly and can be finalised by mid-2022, with EU legislators aware of the importance of keeping the momentum and of ensuring that an effective and ambitious European cybersecurity framework is in place.
- EU legislators pay particular attention to the alignment between the NIS2 and the Digital Operation Resilience Act (DORA) proposals.

Cyber Resilience Act (CRA)

- In the second half of this year, the Commission will propose legislation on common standards for digital products under a new European Cyber Resilience Act.
- The Act will set out horizontal cybersecurity requirements for digital products and ancillary services (hardware, but also ‘intangible’, like non-embedded software).

DSA

- The DSA sets rules on content moderation practices of online platforms, and its interaction with freedom of speech and healthy and well-informed public debate.
- It follows three objectives:
 - protect users from illegal goods or content online;
 - better secure their freedom of expression online; and
 - allow companies to emerge and scale in a borderless Internal Market.
- Platforms would have to apply effective measures against misuse of their systems and transparency mechanisms. Users will have the right to be informed about moderation policies and decisions by the platform, to contest them and seek redress.
- These rules should not create a disadvantage to smaller companies. The obligations are proportionate to size and societal reach. Very large platforms need to ensure that those ‘public spaces’ are open and fair: they will need to assess and address risks their systems pose to freedom of expression and other fundamental rights.
- Enforcement is primarily a task of national competent authorities, but for very large online platforms, often with significant cross-border impact, the rules provide for enhanced supervision and enforcement, involving the Commission.

RRF

- The RRF supports Member States to overcome the crisis, and **re-build the economy in a resilient, sustainable and forward looking way.**
- It finances **structural reforms** with lasting impact on the green and digital transitions, with an unprecedented **EUR 724 billion in loans and grants.**
- **Payments are made against performance.**
- Together with **strong monitoring and control**, this will ensure effective delivery of reforms and investments.
- Each national plan must include **at least 20% for digital objectives.** With almost EUR 130 billion in the adopted plans allocated to the digital transformation.
- Several measures aim specifically at **supporting digital transformation** through the deployment of very high capacity and 5G network, the development of digital skills for the population and the workforce and the digitalisation of public services.

- This presents **significant opportunities for the business sector**. This is the case for the large investments in advanced digital technologies (cloud, artificial intelligence), cybersecurity, digitalisation of agriculture, sustainable mobility, digitalisation of businesses and several calls for research and development (R&D) projects.
- In addition, there are multi-country projects that will support the development of EU key digital capabilities, including microelectronics, cloud and edge solutions, **enhancing coordination for critical investments** in strategic sectors.
- The two potential IPCEIs on microelectronics and cloud technologies are amongst the multi-country projects with the highest take-up in RRP, followed by projects in Digital Innovation Hubs, 5G corridors and quantum communication.
- Small and large firms alike will benefit from reforms improving the business environment and reducing red tape.
- These reforms are present in many national recovery and resilience plans and aim to simplify the procedures for starting up businesses, obtaining permits and licenses, or by introducing public administrations' one-stop shops and electronic registries.
- Other key reforms are foreseen in the area of insolvency procedures, access to finance, or for the promotion of private investments, venture capital, and other innovative forms of financing.

Contact – briefing coordination: [REDACTED]