Meeting with [redacted] Ref. Ares(2022)4935753 - 06/07/2022 /2022

18 May 2022

Steering brief

Scene setter

You are meeting [redacted] Microsoft.

The meeting is a follow up to your meeting on 17 March 2022 (notes attached). On that meeting, [redacted] expressed Microsoft's commitment to take action to address the concerns of European cloud providers. During his visit to Brussels, he plans to announce concrete steps and outline five broader European cloud principles that will guide all of Microsoft's cloud business in Europe. He will also be joined in Brussels by [redacted]

Key messages

Data Act

- The Data Act introduces minimum regulatory requirements of contractual and commercial nature to enable cloud switching and improved open interoperability standards.
- One of the aim is to unlock the potential of data and cloud technologies.
- Secondly, it is essential that European data can be stored and processed securely in Europe. This principle is in line with our rules and values.
- Finally, by embracing the edge revolution and the green transition, Europe has an unprecedented opportunity to reverse this market trend. This will require a fundamentally new architecture and processing capabilities.

Cloud Alliance

- The Alliance aims to foster the development and deployment of advanced and next generation cloud technologies. Members come together in three dedicated groups: Edge and Cloud, Aeronautics and Defence, Member States.
- The Alliance aims to create a roadmap for investments in the cloud sector in Europe. It does not aim to duplicate the activities of Gaia-X who aims to develop technical standards. The Alliance represents a complementary instrument to the Important Project of Common European Interest (IPCEI) to implement the European data strategy.
- [redacted]

[redacted]

- [redacted]
- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]

[redacted]

EU Cloud Certification Scheme

- [redacted]
- The Commission facilitates discussions on the certification scheme for cloud services in the European Cybersecurity Certification Group (ECCG), in close cooperation with ENISA.

AI

- One of the key points being negotiated in the AI Act right now is the obligation of the providers and the users of high-risk AI systems.
- Microsoft rightly points out that these should be calibrated, but the starting point should indeed be the provider and at the stage of design and development of the AI system.
- Another important point is regulatory sandboxes, which will provide an environment for businesses and regulators to cooperate on ensuring the development of compliant AI.
- This is part of our overall approach to create innovation-friendly rules, which will encourage demand for AI solutions, create legal certainty in the single market and lay out support measures for providers.
- Harmonised standards operationalising the requirements for high-risk systems will play a key role in facilitating the implementation of the Regulation by economic players. We are working on this with European standardisation organisations and will provide guidance as appropriate.

NIS2 – revised Network and Information Security (NIS) Directive:

- Legislative deliberation started in January 2022 and has concluded with the last trilogue on 12 May 2022.
- EU legislators have paid 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).

Digital Services Act (DSA)

- The DSA will include a single set of horizontal rules on the content moderation practices of online platforms, in particular the removal of illegal content, and their interaction with freedom of speech and a healthy, well-informed public debate.
- The Digital Services Act takes an asymmetric approach, to ensure that very large online platforms and search engines (45 million EU users) which have become ‘public spaces’ of expression are open and fair. The Digital Services Act requires more from these platforms concerning the organisation and design of their systems: they will need to assess, and address risks their systems pose to freedom of expression and other fundamental rights.
- The DSA also includes specific obligations for marketplaces to ensure a better traceability and accountability of their sellers (e.g. Know Your Business Customers (KYBC) rules) as well as the products sold on their platforms (compliance-by-design, random checks, notices of the illegality of former purchases).

- The Commission will have the exclusive competence for the designation of very large online platforms (VLOPs) and the enforcement of systemic obligations against them. The Commission will be able to charge VLOPs an annual supervisory fee, its amount will be capped to 0.05% of the worldwide net income of platforms.

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.
- So far, Member States not only met, but most of the time exceeded their **20% digital target,** and about 26% (i.e. about EUR 120 billion) is spent on digital.
- 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 RRPs, 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.
- To **speed up** the **digital transformation** and **strengthen our resilience**, we need to build on our **strengths**, pool resources to create critical mass and **weight internationally**. We count on the **support of the Member States**, but as well the **industries**, to make the digital transformation happen. This is even more important in view of the Digital Decade Policy Programme, which provides an EU level framework to guide and accelerate Europe's digital transformation by 2030 and is an ambition that can only be reached with the cooperation of all Member States.

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 TTC working groups, made up of key staff, addressing a wide range of topics, as defined in the Joint Statement from Pittsburgh.

- We strive for new ambitious global norms, **AI-related** international standardisation initiatives and cooperation frameworks, in line with the rules-based multilateral system and the values it upholds.
- More generally, 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. This topic falls under TTC Working Group 4 on ICT Security & Competitiveness.
- Discussions are currently ongoing with the US on potential areas of cooperation [redacted]
- 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.

Child sexual abuse

- On 11 May we adopted a proposal for a Regulation on preventing and combating child sexual abuse. It is an important step in the fight against CSA in the EU and globally.
- It could be a game changer by
  - ensuring that companies do their part to improve child protection and create a hostile environment for the sharing of child sexual abuse materials;
  - where necessary, mandating companies to detect, report and remove child sexual abuse online, and
  - establish an EU centre to prevent and combat child sexual abuse.
- The proposal focuses on prevention first and foremost.
- The proposal requires relevant providers to detect and, if needed, remove online child sexual abuse on their services, be they encrypted or not. However, this must be done without creating vulnerabilities on such services that might be exploited for purposes other than online child sexual abuse.
- We will continue to work with industry on solutions to technological challenges, such as end-to-end encryption, and to support the EU Internet Forum expert process on encryption, by funding further research in this area. We want to foster the development of tools that can operate at scale.
- I welcome Microsoft's leadership on combating child sexual abuse, and request your support for the proposed legislation.

Contact – briefing coordination: [redacted]