**VICE PRESIDENT VĚRA JOUROVÁ**

# MEETING WITH [redacted] MICROSOFT

## BRUSSELS

DATE AND TIME: 18 MAY 2022, 17H00-17H30

MEMBER RESPONSIBLE: WOJTEK TALKO

# Steering brief

## Scene setter

You are meeting [redacted] Microsoft.

The main issues for discussion are:

- Actions in relation to war in Ukraine (fight against war propaganda (RT/Sputnik), support journalists, fight disinformation)
- Code of Practice on disinformation
- DSA and political ads
- Privacy Shield
- Microsoft Cloud initiative
- TTC statement

Last time you met [redacted] in Lisbon. Among other things, [redacted]

[redacted] will also meet EVP Vestager on the same day, [redacted]

During [redacted] visit to Brussels now, [redacted] plans to announce concrete steps and outline five broader European cloud principles that will guide all of Microsoft's cloud business in Europe.

### Actions related to War in Ukraine

EU has rolled out sanctions targeting Kremlin's disinformation and war propaganda machine in the EU, namely the RT (Russia Today) channels and Sputnik. As a result, the reach of targeted RT channels and Sputnik in the EU is now extremely limited. All online platforms have quickly suspended the transmission of Russia Today and Sputnik in the EU, and have taken further action. The Commission asked the European Digital Media Observatory to focus its activities on Ukraine. In addition to this Observatory's fact-checking and investigating activities, its Ukraine task-force also supports researchers in the attempt to get access to online platforms' datasets which are essential to understand disinformation spreaders and tactics in the current context.

The Code's signatories are currently heavily involved in taking urgent action related to the aggression of the Russian federation against Ukraine. They indicated that they will need additional time to finalise the Code's revision.

The Commission expects that lessons learned on Ukraine war-related disinformation are reflected in a revised and future proof Code.

The Commission would expect a Code before the summer, ideally in May.

### *Democracy Action Plan, political ads and disinformation and Code of Practice*

Microsoft leads several initiatives to protect electoral processes through its Defending Democracy Program and provides software in that regard such as ElectionGuard (free open-source software developer toolkit (SDK) that, when integrated into a voting system, provides voters and the public with reassurance that votes were counted accurately) and Election Security Advisors (which offers organisations access to reactive cyber incident response services or proactive security assessments of their environments).

On 22 May 2019, Microsoft became the 13[h] signatory of the Code of Practice against Disinformation. One of its technologies combating disinformation, NewsGuard, enables people to learn more about an online news source before consuming its content.

Microsoft does many actions to comply with EU and US sanctions on Russia and you can expect [redacted] to outline them.

***Data transfers***

On 25 March, the EU and US announced an 'agreement in principle' on a new TransAtlantic Data Privacy Framework. Like the previous Privacy Shield, this new framework will take the form of a Commission adequacy decision based on which personal data could flow freely from the EU to participating companies in the US. The two sides will now need to translate this agreement in principle into legal texts. In particular, the U.S. commitments will be included in an Executive Order that will form the basis of the Commission's assessment in its future adequacy decision.

For a US company as Microsoft, the Privacy Shield successor arrangement is of high importance and will, therefore, likely be raised in the discussion.

You may therefore want to:

- Recall that an agreement was reached on the key elements of a new framework, but that the details still need to be finalised and translated into legal texts.
- [redacted]
- [redacted]
- [redacted]
- [redacted]

## Key messages

***War in Ukraine - Disinformation / Code of Practice***

- Russia's unprovoked and unjustified **military aggression against Ukraine** has greatly exacerbated the risk of further efforts to interfere in elections, and further highlighted the need for prompt actions to strengthen the resilience of our democracies and address vulnerabilities and disinformation.
- Disinformation related to the war in Ukraine illustrates the threats and challenges that this phenomenon poses to our societies.
- At the beginning of the year, as the crisis was growing in intensity, the spread of false news about Ukraine detected in the EU was still very small. A growth was detected in the first half of February, even if the qualitative and quantitative levels of the disinformation was not alarmingly high.
- After the military actions against the whole Ukraine started in the morning of 24 February, though, fact-checkers witnessed the situation changing substantially and the disinformation about the events growing both in quantity and gravity.

Response

- The **EU sanctions** target the core of the Kremlin's disinformation and war propaganda machine in the EU, namely the RT (Russia Today) channels and Sputnik. Our priority is the fast and effective implementation of the adopted sanctions on this 'core' of the propaganda machine with EU-wide relevance.
- As a result, the reach of targeted RT channels and Sputnik in the EU is now extremely limited. The most relevant, traditional means of distribution, in particular by EU satellite providers (Eutelsat and Astra), are tackled and the access to related websites has been dramatically reduced. However, the implementation of the sanctions with regard to the Internet has its challenges.
- We remain in close exchanges with Member States and national regulatory authorities to ensure that the sanctions are properly implemented.
- We have proposed further three outlets in our latest 6th package of sanctions – still to be adopted by the Council.
- Due to their role in spreading disinformation, we aim to strengthen the **transparency and accountability obligations of platforms**.
- We are in close contact with you and other main platforms, Google, Meta, Microsoft, TikTok and Twitter, who are signatories of the Code of Practice on Disinformation.
- All online platforms have quickly suspended the transmission of Russia Today and Sputnik in the EU, and have taken further action.
- The information provided to the Commission shows that, in recent weeks, they have strengthened their monitoring and intervention tools related to the situation in Ukraine, including the following:
  - De-prioritising or removing of proven disinformation content and closing of accounts that are persistently disseminating such content.
  - Depriving players who spread disinformation related to the war of funding, and in particular avoiding any 'ad' placements on and by Russian state affiliated media.
  - Increasing the cooperation with fact-checkers and labelling of state affiliated sources.
  - Promoting authoritative content.
- The current extraordinary situation demands extraordinary and decisive action. It shows the importance that platforms deliver a strong revised **Code of Practice on Disinformation** as soon as possible. The Commission is involved in helping this process along.
- I thank you Microsoft for its engagement (*You may ask how [redacted] sees the process going and when [redacted] expects finalisation).*
- We have also asked the **European Digital Media Observatory** to focus its activities on Ukraine. In addition to this Observatory's fact-checking and investigating activities, its Ukraine task-force also supports researchers in the attempt to get access to online platforms' datasets which are essential to understand disinformation spreaders and tactics in the current context.
- They also produce – at our request – weekly insights into disinformation narratives and trends related to Ukraine. The newest one reports 2 new trends: discrediting media reporting on Ukraine and false information on foreign support for Ukraine.
- Finally, I welcomed report by the **INGE Committee**, whose approach and holistic nature is very much aligned with our EDAP that we are rolling out – next with the EMFA.

- Russia's war of aggression also showed that the EU needs to be better equipped to protect its citizens against an ever-growing risk posed by hybrid warfare, including the use of information manipulation and interference.
- As proposed in the EDAP, we have developed a concept of a foreign information manipulation and interference **(FIMI) toolbox**.
- The proposed measures are grouped in four crosscutting dimensions:

  (i) Situational awareness;

  (ii) Resilience;

  (iii) Disruption and regulatory responses; and

  (iv) Diplomatic responses and instruments in the Common Foreign and Security Policy area.
- This is now being discussed with MS to highlight existing measures and possible new ones that could be developed.

***Support to Ukraine's journalists / communication efforts***

- Our first priority is the safety of journalists. This is why the EU has already dedicated more than 6 million euros for emergency support for journalists in Ukraine, including protective equipment, training, and also relocation when necessary.
- We are working with various partners, including Deutsche Welle, Reporters without Borders, the European Endowment for Democracy (EED).
- We also welcome that the European Broadcasting Union is supporting their Ukrainian member, organises a lot of solidarity initiatives and content in Ukrainian for refugees.
- EEAS provides support to Ukraine with shaping and promoting narratives and communication content. [redacted]
- [redacted]

***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.

***Political ads***

- As you know, the framework to our response to threats to democracy is EDAP.
- On 25 November 2021 we adopted a package of legislative and other measures to reinforce democracy and protect the integrity of elections. It includes soft measures to support cooperation on resilient elections and a flagship initiative on political advertising.
- We are grateful for **Microsoft's input** in the preparation of these initiatives, and would kindly invite you to continue to engage with us in this regard.
- **People must know** why they are seeing a political ad, who paid for it, how much and what targeting criteria were used. New technologies should be tools for emancipation, not for manipulation, and the online platforms must help us make this happen.
- Our proposal will introduce **common rules for political advertising services** across all media, to provide legal certainty for service providers, to promote accountability in the use of political ads and discourage bad practices and interference, and to empower citizens. The proposal protects freedom of expression, does not regulate the content of advertising, and is without prejudice to national electoral rules.
- We will work with industry and other stakeholders to ensure that the **labelling requirements and transparency notice** are effective, improving awareness and offering useful information for citizens, supporting the roles of interested entities and authorities in the democratic process. We have included **safeguards** to protect commercial interests, privacy and to minimise administrative burden, in particular for SMEs.
- The proposal complements and is articulated with the **Digital Services Act (DSA)** and the existing data protection acquis. It addresses the specific problems associated with the **processing of personal data** to target and amplify political advertising in a balanced way, which ensure that explicit consent and the targeting necessary to support political participation can continue.
- We have **worked with Microsoft** in the context of our initiatives. The political ads proposal articulates with the DSA, the aims of the code of practice on disinformation, and work should advance on both in tandem.
- There is a **substantial role to be played by Microsoft**, other large platforms and their associations in making our legislating work to provide accessible, usable transparency with political advertising, and to contribute to the success of our policies more broadly, to support free and fair elections and resilient democratic processes in the EU.
- We look to you to go that extra mile to support our world leading legislation and our initiatives combating disinformation.

***Privacy Shield***

- On 25 March, President von der Leyen and President Biden announced an agreement in principle for a transatlantic data transfer framework to replace the Privacy Shield.
- This is an important step, but the work continues.
- We now need to translate the agreement into legal texts.
- As a first step, the US commitments have to be included in a new Executive Order to be adopted by the US President and implementing regulations.

- [redacted]

***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 (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.

**Background and more extensive LTTs on selected issues**

# EDAP and political ads

## Main messages

- Our political ads initiative is based on a **broad definition of political advertising**, to cover messages sponsored by political actors in a traditional sense, but also those sponsored by other actors, which are liable to influence the outcome of a democratic process.
- It is essential that we include such 'issues ads', which are used increasingly inside and outside electoral periods, and to ensure that high **transparency and strengthened personal data protections** apply to them.
- In our proposal, we aim to ensure that this **broad definition is based on objective factors, which** can be determined using information available to service providers. We have provided a process where most political ads will be identified by their sponsors, and we will support compliance, including through standards and codes of practice.
- The focus of the definition is obviously to cover political advertising, and while some commercial adverts **might overlap with this or pursue a dual aim**, where commercial advertisers use advertising which is liable to influence the outcome of democratic processes, they should do so transparently.
- The same goes for **fund-raising and informational advertising**, as used by civil society actors, for instance. They are not the focus of the definition or the obligations, which we impose on service providers. But advertising liable to influence the outcome of an election should be transparent, and individual rights should be protected.
- We will work with industry and other stakeholders to ensure that the **labelling requirements and transparency notice** are effective, improving awareness and offering useful information for citizens, supporting the roles of interested entities and authorities in the democratic process, while being implemented through streamlined and automated processes. We have included **safeguards** to protect commercial interests, privacy and to minimise administrative burden, in particular for SMEs.
- The proposal complements and is articulated with the **Digital Services Act (DSA)** proposal and the existing data protection acquis. It addresses the specific problems associated with the **processing of personal data** to target and amplify political advertising in a balanced way, which ensure that explicit consent and the targeting necessary to support political participation can continue.
- The mechanisms and processes proposed to implement these obligations are compatible with the existing and upcoming acquis, and oversight is ensure through existing frameworks, which will contribute to **certainty for market actors**.
- We are working to support the **European co-legislators in its negotiations**. We have valued your substantive input throughout this process and we welcome your willingness to continue to engage.
- We have **worked with Microsoft** in the context of our initiatives. The political ads proposal articulates with the DSA, the aims of the code of practice on disinformation, and work should advance on both in tandem.

- There is a **substantial role to be played by Microsoft**, other large platforms and their associations in making our legislating work to provide accessible, usable transparency with political advertising, and to contribute to the success of our policies more broadly, to support free and fair elections and resilient democratic processes in the EU.
- The Commission has also adopted on 27 April 2022 a strong package to address strategic lawsuits against journalists and human rights defenders engaged in public participation (SLAPP). It is essential that journalists and human rights defenders are afforded the necessary space including to counter disinformation and other manipulative interference in the democratic debate.
- Delivering on the Commission's European Democracy Action Plan, a joint mechanism on election resilience is offered as of this year to Member States as a capacity-building tool to support the exchange of expertise in areas such as disinformation, cybersecurity, and online forensics. Member States can use the mechanism to build their capacity to fight illegal interference, discover covert political funding or ensure effective implementation of their electoral rules online.
- The Commission also intends to deliver in the coming year a compendium on e-voting practices, as announced in the Democracy Action Plan.
- We look to you to go that extra mile to support our world leading legislation and our initiatives combating disinformation.

## Defensives

***What is the current timeline for the Code?***

- Disinformation related to the war in Ukraine illustrates the threats and challenges that this phenomenon poses to our societies. It reinforces the case for establishing a strong framework to fight disinformation.
- The Code's signatories are currently heavily involved in taking urgent action related to the aggression of the Russian federation against Ukraine. They indicated that they will need additional time to finalise the Code's revision.
- Adjusting the timeline of the Code is therefore not only justified but also useful to strengthen the commitments of the future Code
- The Commission expects that lessons learned on Ukraine war-related disinformation are reflected in a revised and future proof Code.
- The Commission would expect a Code before the summer, ideally in May.

***What is the Commission's view on the European Parliament's proposed ban on targeted advertising (displayed by online platforms) based on special categories of personal data and personal data of minors to be included in the DSA?***

- GDPR has already limit if not de facto bans using sensitive data, but I think there is a lot of legal creativity in how digital ad sector approaches this. So, I think it is a good idea to try to close this loophole wit the DSA. We tried to do the same with the political ads, but in a way much closer to the GDPR. Let's see the final text of the DSA first, but I believe such sensitive data should not be used for advertising purposes, especially in a political context.

***What does the Commission understand by political advertising?***

- Sponsored political content ('political advertising') is often regulated nationally, and there are a number of definitions which can include issues-based and partisan adverts, and certain other kinds of commercial communication during a defined electoral or campaign period.
- Online platforms have also established their own approaches to such advertising, which do not necessarily align with any relevant national definitions.
- An aim of the political advertising initiative will be to harmonise the definitions, as well as the relevant transparency obligations. Narrower and broader options are envisaged.

***Will the political ads proposal stop Russia and its proxies disseminating political advertising in the EU?***

- The proposed regulation will introduce a high standard of transparency to political advertising circulated in the internal market, including from outside the Union.
- It will also introduce stricter rules about how such advertising is disseminated.
- It is based on a broad definition of political advertising which covers both adverts bought be political actors and those acting on their behalf, as well as many "issues ads" where those are liable to influence a democratic process.
- The proposal does not affect national competence to establish rules on the content of political advertising, and its availability, including prohibitions, but these provisions at EU level will make it easier to monitor and enforce such rules, as well as discouraging manipulative techniques, such as those using sensitive personal data.

***Who is covered by the new rules? Ad companies, like Google Ads, but what about bloggers and newspapers? Does this regulation also cover private persons or only political parties and foundations?***

- The requirements concerning the transparency of political advertising established by the new rules will apply to the providers of political advertising services.
- This includes all services consisting of the preparation, placement, promotion, publication or dissemination, by any means, of a message by, for or on behalf of a political actor, unless it is of a purely private or a purely commercial nature; or which is liable to influence the outcome of an election or referendum, a legislative or regulatory process or voting behaviour.
- This would include newspapers and other traditional media such as radio and television when they are publishing political advertising, but also bloggers and influencers when they are paid to present political messages. It would also cover, for instance, new websites which provide paid-for content which meets the new definition.
- This could also include, for instance, Google when it provides political ads through its search services, or Facebook when it displays political ads to its users.
- However, the rules about the transparency of advertising will not be engaged in the context of online intermediary services which are provided without consideration for the placement, publication or dissemination of a specific message, unless the user has been remunerated by a third party for the political advertisement.
- This means that individual's personal social media posts will not fall under the definition of political advertising, unless they have been paid to make political posts.

- The requirements concerning the targeting and amplification of political advertising apply to anyone who uses personal data to target or amplify political advertising using personal data. This would cover in many instances service providers, but also other actors like European political parties.

***How is this proposal articulated with the DSA proposal and why is it necessary to have additional rules in the field of political advertising?***

- This initiative will complement the proposal for a DSA, which the Commission announced in December 2020.
- While the DSA imposes transparency requirements on online platforms, the political advertising initiative covers the entire spectrum of political advertising publishers, as well as other relevant service providers involved in the preparation, placement, publication and dissemination of political advertising.
- It adds specific requirements for political ads, including for very large platforms, including to make sure that information is provided about the amounts spent on ads.

## SLAPP initiative

***Why is this initiative needed now?***

- It is important to act now at EU level in order to ensure that SLAPP targets can be evenly protected across the EU, that courts have effective tools to identify and deal with SLAPP cases and, ultimately, that we prevent the erosion of democratic values by nipping this growing phenomenon in the bud.
- All available data show that this particular form of harassment against those who speak up to defend the public interest is on the rise in the EU.
- SLAPPs have corrosive effect on freedom of expression and ultimately affect a pluralistic democratic debate and the right of EU citizens to be informed about matters of general interest.
- SLAPPs are also abusing our legal and judicial systems and overburdening courts. Our work shows that Member States and their courts are not well equipped to address them – the safeguards in place are limited and generic and the extent to which they can be effectively employed against SLAPP is not equal and not effective. This is why some Member States have initiated processes to address the problem via national legislation.

## Background

***State of negotiations on political advertising***

**The Presidency** supports the aim of having the elements of the package in place in time for the 2024 European parliamentary elections (i.e. by May 2023). The Presidency aims to achieve a general approach to the political parties' regulation and a partial general approach to the transparency of political advertising regulation.

The Member States are generally supportive of the objectives of the overall package and of the legislative proposals presented. Discussions at technical level began in the General Affairs Group (GAG) on the democracy package on 7 December 2021. At GAG on 8 and 25 February, Member States began considering the proposal article by article.

The General Affairs Group (GAG) has discussed the proposal on the transparency and targeting of political advertising at a technical level at six meetings since then, which has included first reading of the first three chapters, as well as detailed consideration of specific issues. The Commission has also organised detailed technical sessions with national experts from a number of Member States in coordination with the Presidency.

The French Presidency presented on 3 May a compromise text on chapters I-III that was discussed at GAG in 17 May.

As regards the Parliament, a first presentation of the new Regulation on transparency and targeting took place in the IMCO committee on 10 January. Members' comments were generally supportive, though the Left and Greens called for stricter controls for targeting. Questions focused on the scope of definitions, the articulation with the DSA and the extent to which third country actors are addressed. EP has resolved the issue of competence on the file so that IMCO is in lead, LIBE has exclusive competence on some provisions and shared competence for the relevant provisions and CULT has shared competence on some provisions. IMCO rapporteur is MEP Sandro Gozi (Renew, FR).

***Microsoft political advertising policies***

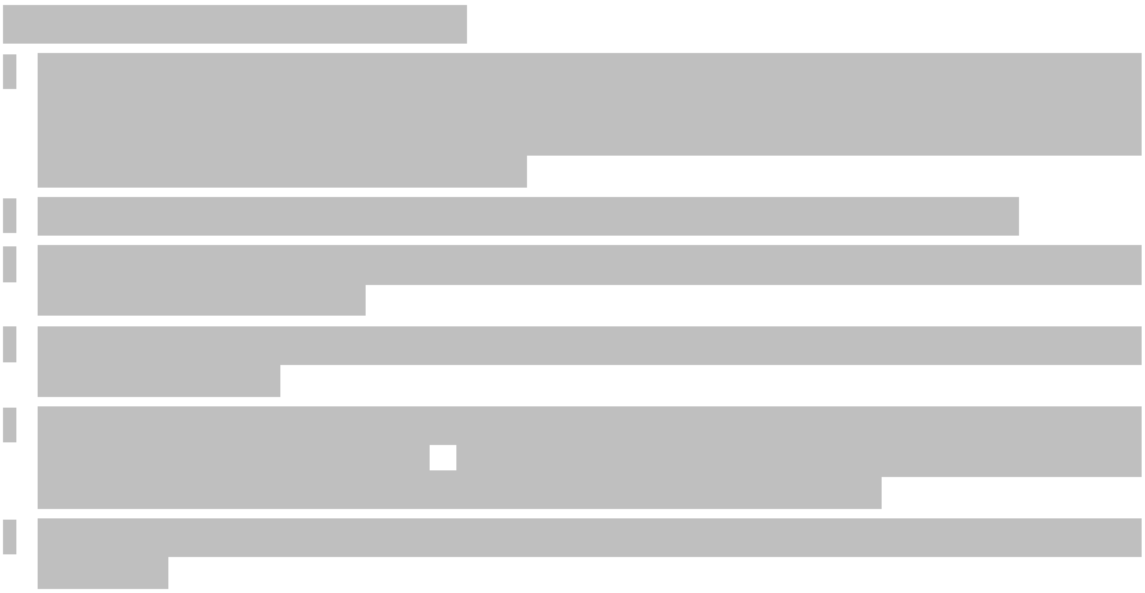
- Advertising for election related content including election canvassing and election polls, political parties, candidates, and ballot measures is not allowed.
- Fundraising for political candidates, parties, PACs, and ballot measures is not allowed.
- Advertising that exploits political agendas, sensitive political issues or uses "hot button" political issues or names of prominent politicians is not allowed regardless of whether the advertiser has a political agenda.
- Use of political figures past or present cannot be linked in text or images to political content, products, sensationalized messaging, hot button issues, or as a way to link historical topics to current issues/events. For example, an ad with the headline "Lowest to Highest Presidential IQs, ranked" with an image of a political figure would not be allowed.
- Use of political figures past or present cannot be linked in text or images to political content, products, sensationalized messaging, hot button issues, or as a way to link historical topics to current issues/events. For example, an ad with the headline "Lowest to Highest Presidential IQs, ranked" with an image of a political figure would not be allowed.
- Use of political figures past or present cannot be linked in text or images to political content, products, sensationalized messaging, hot button issues, or as a way to link historical topics to current issues/events. For example, an ad with the headline "Lowest to Highest Presidential IQs, ranked" with an image of a political figure would not be allowed.
- In 2020 it removed 20 million ads and 10,000 sites over its political advertising policy.

***IAB contribution to the European democracy action plan***

IAB Europe to which Microsoft is a member provided responses in the consultation process when preparing the European democracy action plan and then when preparing the proposal on political advertising. IAB Europe has also contributed a position paper in the post-adoption process, which asks for changes in the scope & definitions proposed (incl. of 'political advertising' and 'political actor'), the transparency requirements, targeting provisions (incl. alignment with the GDPR) and enforcement.

IAB Europe is the European-level association for the digital marketing and advertising ecosystem. Through its membership of national IABs and media, technology and marketing companies, its mission is to lead political representation and promote industry collaboration to deliver frameworks, standards and industry programmes that enable business to thrive in the European market.

***Background on media:***



***Overview of measures taken by national regulators against Russian channels (beyond EU sanctions)***

- Several national regulators have taken restrictive measures targeting Russian TV channels that are not covered by the EU sanctions:
- **Latvia**: On 24 February, the Latvian regulator suspended the retransmission of Rossiya RTR, Rossiya 24 and TVCI for 5, 4 and 3 years respectively, referring to threats to state security. On 27 and 28 February, the regulator took further measures against MIR 24, RTVi and RBC. Moreover, the regulator withdrew the broadcasting licenses of PBK Estonia and PBK Lithuania.
- **Poland**: On 24 February, the Polish media regulator adopted a resolution to stop the distribution and retransmission in cable networks, via satellite and ICT systems of RT, RT Documentary, RTR Planeta, Soyuz TV, Russija 24. On 4 March, this was extended to Belarus 24 (TV Belarus) and Pervyj Channel (also known as Channel 1 Russia, ORT1).
- **Estonia**: On 25 February, the Estonian regulator issued an injunction to communications companies to stop broadcasting five TV channels on its territory: RTR Planeta, NTV Mir (NTV Mir Baltic), Belarus 24, Rossiya 24 and TVCI. On 9 March, the regulator suspended the retransmission of RBC-TV.
- **Lithuania**: On 25 February, the Lithuanian regulator suspended the retransmission of six TV channels (Primais Baltijas Kanals Lietuva (PBK), TVCI, Planeta RTR, Rossija 24, NTV Mir and Belarus 24) for 3 to 5 years, as potential threats to national security. On 28 February 2022, the Lithuanian regulator suspended the reception of television channels MIR24 and RBK-TV in the territory of Lithuania for 5 years (referring to instigation and propaganda of war).

# Digital Services Act

## Main messages

- The Digital Services Act 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.
- In this way, the Digital Services Act will be a gold standard that ensures transparency and accountability of the online space, enforced by effective democratic oversight across Member States, and by the Commission.
- 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.
- This includes equipping citizens to understand and interact with the information they see online, and giving them rights where currently they are at the discretion of private actors – in particular the large online platforms. This includes measures related to online advertising, recommender systems, but also core content moderation processes and ensuring users are appropriately informed.
- The DSA aims at facilitating cross-border enforcement of the specific DSA obligations through a structured system of public supervision, based on independent authorities in the country-of-origin principle and tools for cooperation cross-border and at EU level.
- 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 DSA prohibits online platforms from presenting advertisements to children based on profiling, as well as advertisements to any user based on profiling using special categories of personal data (e.g. personal data revealing racial or ethnic origin, data concerning health, etc.).
- We are monitoring the situation in Ukraine very closely. We have the dual objective of effectively limiting Russian war propaganda in the EU, while allowing access to trustworthy information to reach Ukrainian and Russidan audiences.
- The DSA contains a range of measures that are useful in a crisis like the one we are in today. It contains a dedicated risk management framework to counter, among others, also risks related to intentional manipulation of the service, supported by comprehensive transparency and accountability tools that will shed greater light on the dynamics of information operations and allow the design of adequate response and mitigation measures.
  - The DSA's crisis response mechanisms can essentially be seen as a faster trigger for the risk assessment and risk mitigation protocols previously included in the DSA, to make sure that these protocols are conducted in an ad hoc manner during specific crises.
  - Having a clear mechanism in place will ensure that the crisis response is balanced, proportionate and efficient. It will also allow platforms to hold the Commission accountable for the measures that it might require from them.

- 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.

## Defensives

***What measures do search engines need to take?***

- The political agreement confirms that search engines are online intermediaries. They will continue to benefit from liability exemptions, with a case-by-case assessment.
- A particular attention is given to very large search engines, those reaching more than 10% of the EU population. They will bear similar obligations as very large online platforms, for example in conducting risk assessments, adopting appropriate risk mitigation measures and being subject to independent auditing.

***How will the Commission finance costs associated with the new supervisory and enforcement competences?***

- In order to ensure effective compliance with the DSA, it is important that the Commission has at its disposal necessary resources, in terms of staffing, expertise, and financial means, for the performance of its tasks under this Regulation. To this end, the Commission will charge supervisory fees on such providers, level of which will be established on an annual basis. The overall amount of annual supervisory fees charged will be established on the basis of the overall amount of the costs incurred by the Commission to exercise its supervisory tasks under this Regulation, as reasonably estimated beforehand.
- The annual supervisory fee to be charged on providers of very large online platforms and very large online search engines should be proportionate to the size of the service as reflected by the number of its recipients in the Union. To this end, the individual annual supervisory fee should not exceed an overall ceiling for each provider of very large online platforms and very large online search engine taking into account the economic capacity of the provider of the designated service or services. Such ceiling is set at 0,05% of the annual worldwide net income of the provider concerned.

***When will the DSA start applying?***

- The precise time-table depends on the legal finalisations and subsequent translations, as well as the timing of the final approval in the European Parliament and Council.
- After this, the rules will start applying in two steps: the rules for very large online platforms and search engines supervised by the Commission will kick-in earlier – approximately the second half of 2023, while Member States will have a maximum of 15 months or 1 January 2024 (whichever is later) to empower their national authorities for the rules on smaller platforms.
- Specifically, the Commission is expected to designate providers some six months after the publication of the rules in the Official Journal *[expected for Q3/2022 but ther is still some uncertainty regarding this timeline]* and providers of large platforms and search engines will then have four months to comply.

## Background

[redacted]

# Trade and technology council

## Main messages

- In January 2022, we presented the Digital Decade Principles defining our vision of how the digital economy should abide by values such as democracy, privacy, solidarity, freedom of choice, and security.
- Our digital ambitions are high, from setting rules for online platforms, to upholding the highest standards of data protection and ensuring a fair taxation of the digital economy.
- 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.
- After a period of difficult relations with US, setting up the TTC is an achievement in itself, a closer trans-Atlantic cooperation is re-established.
- 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.
- As you know, on Monday there was a second TTC meeting at ministerial level, where there were a number of good results.

***TTC discussions on Standards***

- In the meeting there was agreement to establish a Strategic Standardisation Information (SSI) mechanism to defend common interests in international standardisation activities. And we will continue work to foster the development of aligned and interoperable technical standards in areas such as AI or Internet of Things.

***TTC discussions on AI***

- 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.
- As digitalisation spreads through the globe, a closer transatlantic cooperation can provide the foundation for a new set of global digital rules aimed at balancing free markets and personal liberties.
- Yesterday, there was agreement with the US to develop a joint roadmap on evaluation and measurement tools for trustworthy AI and risk management

***TTC discussions on cybersecurity***

- 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 (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.

## Background

[redacted]

***The TTC discussions on artificial intelligence***

In the Pittsburgh Declaration after the TTC summit in September 2021, the EU and the US stated their commitment to ensuring that AI serves our societies and economies and is used in ways consistent with our democratic values and human rights.

The EU and the US also expressed their opposition to uses of AI that do not meet this requirement, such as rights-violating systems of social scoring.

Furthermore, the EU and the US underlined that policy and regulatory measures should be based on, and proportionate to, the risks posed by the different uses of AI. This is a significant similarity in the approach between the two.

Since the autumn, discussions have been ongoing in varying constellations to scope the agreed deliverables. The spirit of cooperation has been very good and both sides are keen to achieve progress towards the shared goals.

[redacted]

[redacted]

***The TTC discussions on cybersecurity***

On 5G security, where both the EU and the US share the same objective of making 5G networks (cyber)secure and resilient, we have developed in the EU a comprehensive approach to 5G security over the past two years. This joint approach by all EU Member States is based on a coordinated risk assessment and a joint Toolbox of measures to mitigate such risks.

It is in our common interest to continue to promote the use of trusted suppliers and maintain and support established models, while facilitating market-led and technology neutral innovation.

The report on the cybersecurity of Open RAN developed by Member States within the NIS Cooperation Group, with the support of the Commission and ENISA, has been published on 11 May 2022. The report follows the EU Toolbox methodology and builds on its findings.

The report found that Open RAN could bring potential security opportunities, provided certain conditions are met, but also a significant number of security challenges. To mitigate these risks and leverage potential opportunities of Open RAN, the report recommends a number of actions based on the EU Toolbox and a cautious approach towards moving to this new architecture.

We are also interested in discussing possible cooperation on the next generation of communication technologies towards 6G. In Europe, we are currently setting up an EU institutionalised partnership on Smart Networks and Services towards 6G (under our research programme Horizon Europe), in partnership with industry and coordination with Member States to complete the deployment of 5G and mainly to prepare for 6G.

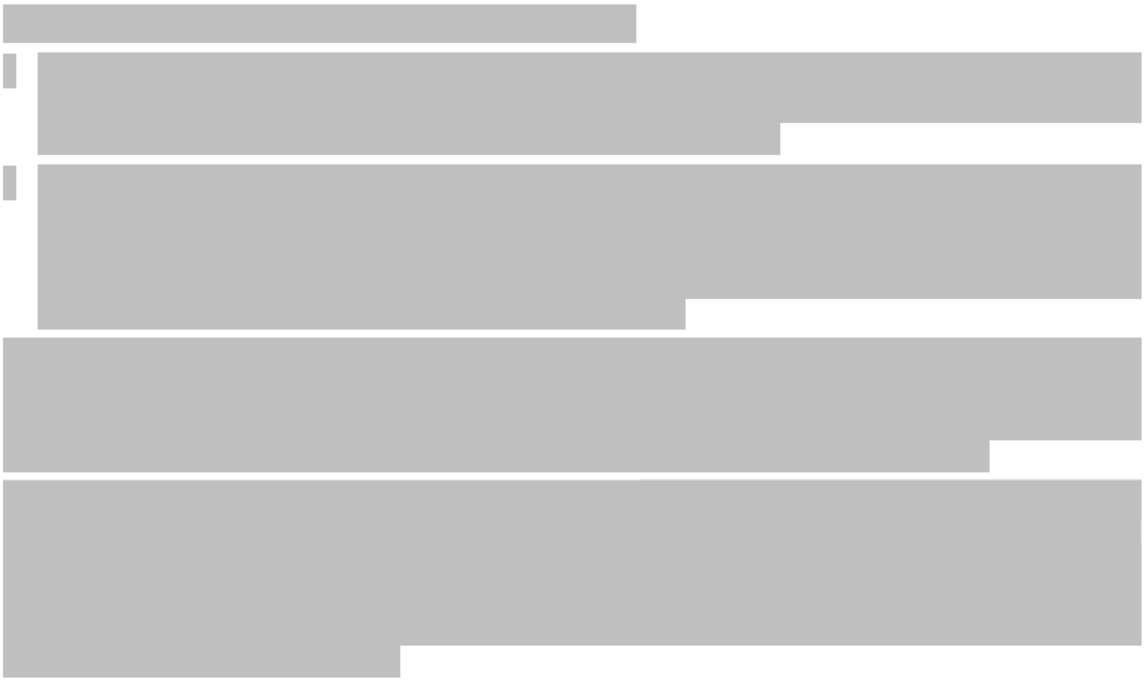
# Successor arrangement to the Privacy Shield

## Background

***State of play***

The agreement in principle represents an important step towards the development of a successor arrangement to the Privacy Shield. It reflects the **outcome of intense negotiations** which were **launched one year ago** after the new Biden Administration entered into office. The future framework will **address the concerns** raised by the Court of Justice in the ***Schrems II*** **judgment**.

In that judgment, the Court concluded that several aspects of the US legal framework in the area of national security did not meet the standard of "essential equivalence" that is required for an adequacy finding[1]. To address this, the **negotiations focused on** (1) putting in place **limitations to the collection** of personal data for national security purposes that reflect the key EU law principles of necessity and proportionality and (2) ensuring that EU individuals have access to **effective redress** in this area.



***Next steps***

The details of this agreement in principle need now to be finalised with the US and translated into legal texts. In particular, as part of the agreement in principle, the **US commitments will need to be reflected in a new Executive Order** to be adopted by the US President. That Executive Order will have to be further implemented through **regulations** to be adopted by the US Administration (Department of Justice, intelligence agencies etc.).

Once this new Executive Order and other relevant acts are in place, the **Commission will be able to propose a draft adequacy decision** and **launch the adoption procedure** for the final adequacy decision, which is composed of different steps.

[1] The GDPR, as interpreted by the CJEU, requires that, when adopting an adequacy decision, the Commission has to assess not only the level of protection applicable to the processing of data by commercial operators in the foreign country but also the conditions and safeguards which public authorities can access data once it has been transferred to that country.