MEETING WITH [redacted], Microsoft

Scene setter

You met Mr. [redacted] in May, where he updated you on the announcement of Microsoft that it will create an "EU Data Boundary" for the Microsoft Cloud (https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/), which will enable European customers to both process and store all of their data in the EU. It is foreseen to be implemented by the end of next year. This type of approach may correspond to an increasing demand of certain customers (e.g. as regards the security of their data). However, there is no requirement under US data protection law to process or store personal data in the EU and it is not for the Commission to comment on a choice made by a private company as regard its business model.

For the present meeting, Mr. [redacted] has indicated his interest in discussing the state of play of the negotiations on the successor arrangement to the Privacy Shield.

Meeting with [redacted] Microsoft

Videoconference 3 December 2021 17h30

Line to take

Negotiations on a successor arrangement to the Privacy Shield

- The EU and US have been engaged in intense negotiations in the past months and weeks. Commissioner Reynders was in Washington DC last months to take stock of the talks.
- We have entered into the substance of the issues (proportionality and necessity, judicial redress) and are discussing the details of possible solutions.
- What is at stake here are complex and sensitive issues that relate to the delicate balance between national security and privacy, but we have made progress.
- This remains a top priority in Brussels and in Washington DC.
- At the same time, we will only agree to a new arrangement that is fully compliant with the Schrems II judgment.
- This is also the only way to develop a durable solution, one that ensures the stability and legal certainty that stakeholders expect on both sides of the Atlantic.

Meeting with [redacted] Microsoft

Videoconference 3 December 2021 17h30

Artificial Intelligence

- [redacted]

AI and law enforcement cooperation

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

[1] [redacted]

[redacted]

[redacted]

Meeting with [redacted], Microsoft

Videoconference 3 December 2021 17h30

AI and the EU-US TTC

- [redacted]

Meeting with [redacted], Microsoft

Videoconference 3 December 2021 17h30

DEFENSIVES

Will data flows also be discussed in the TTC?

- The TTC is not a forum for developing a successor arrangement to Privacy Shield.
- There is a specific negotiating setting for that and the progress made in the past months and weeks confirm it's the appropriate one.

We are concerned about the uncertainty created by the Schrems II judgment, which is further fuelled by the very strict guidance of the data protection authorities

- We understand the need for practical guidance and therefore worked closely with the European Data Protection Board, which issued detailed guidance on 18 June.
- In our own work on standard contractual clauses, which are the most used tool for international data transfers, we have operationalised some of the clarifications provided by the Court, which we believe provide a helpful toolbox to assist companies in their compliance efforts.
- While we were finalising the clauses, we also worked closely together with the EDPB to ensure consistency between our approaches.

We are concerned about calls for data localisation

- We have repeatedly confirmed the Commission's commitment to facilitate data flows. This is reflected in our ambitious agenda on facilitating trusted data transfers.
- For instance, we recently concluded adequacy negotiations with South Korea and the UK, two years after having created the world's largest area of free and safe data flows with Japan. We are in talks with several other countries, in particular in Asia and Latin America.
- We actually believe that there are many more opportunities today than even a few years ago to promoted trusted data flows. This is a direct result of the (upward) convergence trend in privacy we are observing in many parts of the world. It's much easier to facilitate data flows between systems that speak a similar (not an identical) language.
- Our commitment to data flows is also reflected in the approach we are taking in our trade negotiations, at both the bilateral (current FTA negotiations with countries such as Australia, New Zealand, Indonesia, Chile, Tunisia etc.) and multilateral (ecommerce negotiations at the WTO) level.
- For example, in the trade agreement with the UK, we included a straightforward prohibition of data localisation requirements and an emphasis on the importance of data flows.
- We want to make very clear that genuine data protection, on the one hand, and digital protectionism, on the other hand, are two very different things.

- Developing strong privacy safeguards and promoting the free flow of data are not opposite objectives but complementary.
- The EU is also actively participating in the multilateral conversation on data flows – in the OECD; the G7 and the G20. The latter in particular under Japan's leadership and under the Osaka track with 'data free flow with trust' as the central underlying concept.
- I believe that these are particularly interesting fora where the EU and the U.S. can cooperate with other like-minded partners – and are already doing so – to create common global standards.

(AI PROPOSAL)

[redacted]

Meeting with [redacted], Microsoft

Videoconference 3 December 2021 17h30

[redacted]

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

Meeting with [redacted], Microsoft

Videoconference 3 December 2021 17h30

[redacted]

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

Meeting with [redacted], Microsoft

Videoconference 3 December 2021 17h30

[redacted]

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

[redacted]

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

Meeting with [redacted], Microsoft

Videoconference 3 December 2021 17h30

[redacted]

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

Meeting with [redacted], Microsoft

Videoconference 3 December 2021 17h30

BACKGROUND

Standard contractual clauses

The Standard Contractual Clauses (SCCs) are **model data protection clauses** that an EU-based exporter of data and a data importer in a third country can decide to incorporate into their contractual arrangements (e.g. a service contract requiring the transfer of personal data) and that set out the requirements related to appropriate safeguards. These SCCs can be used as a **tool for transfer of personal data to countries outside the EU** that are not subject to a Commission adequacy decision. SCCs represent by far the **most widely used data transfer mechanism for EU companies** that rely on them to provide a wide range of services to their clients, suppliers, partners and employees. Their broad use indicates that, through their standardisation and pre-approval, SCCs are an **easy-to-implement tool** for businesses and are of particular benefit to companies, especially SMEs, that do not have the resources to negotiate individual contracts with each of their commercial partners. The SCCs are of general nature and not country specific.

The SCCs that had been adopted under the previous data protection regime (the Data Protection Directive) had to be modernised and on 4 June 2021, the Commission adopted new SCCs. **Compared to the previous ones, the modernised SCCs**:

- Have been updated in line with new GDPR requirements;
- Provide one single entry-point covering a broad range of transfer scenarios, instead of separate sets of clauses;
- Provide more flexibility for complex processing chains, through a 'modular approach' and by offering the possibility for more than two parties to join and use the clauses;
- Contain a practical toolbox to comply with the Schrems II judgment.

For controllers and processors that are currently using previous sets of standard contractual clauses, a transition period of 18 months is provided.

To provide **general guidance** on the use of the new SCCs and respond to the most received questions, we are currently **working on a Q&A that will be published on the Commission's website**. To make sure that this can provide practical guidance, we have sought the input from stakeholders and already received several useful contributions over the summer. In addition, we will have a dedicated discussion on 29 October with the 'Multistakeholder expert group to support the application of the GDPR', which consists of representatives from civil society, consumer organisations, trade associations, legal practitioners and academics.

EDPB Recommendations on supplementary measures

On 18 June, the **EDPB adopted the final version of its 'Recommendations** on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data', which **provide an overview of the steps companies have to take** following the Schrems II ruling when using tools such as standard contractual clauses. This is the version after the public consultation, which ended in December.

The **main change** in the recommendations (compared to the version that was published in the fall) concerns the **approach of the EDPB to the factors that companies can take into account** when assessing whether sufficient protections are in place for their transfers. According to the first version of the recommendations, this assessment would only have to take into account the scope of relevant laws in the third country of destination, i.e. whether the data importer would be subject to those laws. This would have meant that data importers that fall within the scope of third country legislation but in practice never receive government access requests would still need to put in place supplementary measures, or would no longer be able to receive data from the EU. This was heavily criticised by stakeholders, who expressed a preference for the approach of the draft SCCs (as they were published in November), which included the relevant practical experience of companies with prior requests (or the absence thereof) as one of the factors to be taken into account in this assessment. The **final version of the recommendations contains more nuanced wording**, allowing companies to take into account their practical experience with government access requests. The language is overall **aligned with the approach in the final SCCs**.

The language of the recommendations has **also been nuanced on several other aspects**, e.g. on some of the so-called 'use cases', i.e. examples of situations for which the EDPB has identified/has not managed to identify possible supplementary measures. For example, the revised recommendations no longer contain an example that requires companies transferring data to countries benefiting from an adequacy decision to put in place supplementary measures if their data would be 'routed' via a another third country where it may be subject to disproportionate government access.

At the same time, **the two 'negative' use cases**, i.e. examples of situations where the EDPB was not able to identify any solution that would allow companies to continue transferring personal data to a third country where it would be subject to disproportionate government access, **have been maintained**. These examples were heavily criticised by stakeholders, as they concern two scenarios that are very common in the commercial sector. First, the scenario where EU companies use cloud providers (or other service providers) in a third country that need to have access to 'clear', unencrypted data. Second, the scenario where an EU company shares clear, unencrypted data with a commercial partner outside the EU for common business purposes (e.g. within a corporate group). **However**, given that the final recommendations allow companies to take into account their practical experience, **companies in those scenarios will now be provided with more flexibility** and could still transfer data if they conclude that the data importer/the transferred data will in practice not be subject to government access requests (whereas under the first version, such data transfers could never take place as long as the non-EU company fell within the scope of disproportionate surveillance laws, regardless of whether or not access requests are received in practice).

Post-Schrems II actions of data protection authorities

US companies are increasingly putting pressure [redacted] to agree on a successor arrangement to the Privacy Shield as soon as possible. This is fuelled in particular by fear of **upcoming enforcement action by European data protection authorities** (DPAs) after the Schrems II judgment. In the past months, we have started to see the first "post-Schrems II" cases, e.g. the suspension by the Portuguese DPA of the transfer of

census data from a Portuguese public authority to the US, cases before the Belgian and French Council of States (insisting on the importance of specific protections, such as encryption) and ongoing investigations into the use of Google and Facebook services (currently being discussed at EDPB level).

Moreover, while it seems that the investigation of the Irish DPA into Facebook's data transfers (which were the subject of the national proceedings that led to the Schrems II judgment) is taking more time than expected, its decision is expected in the coming weeks.

Certain DPAs have also started to issue specific guidance on the Schrems II judgment. Companies have for instance criticised recent guidance from the Berlin DPA, where it advises companies to switch to providers (referring in particular to cloud service providers) in the EU or countries benefiting from an adequacy decision, and to move personal data stored in the US back to the EU.

EDPS investigation of the use of Microsoft Office 365 and Microsoft cloud services by the Commission

The Commission's current license agreement with Microsoft was signed in April 2018 and reviewed thoroughly in 2019-2020 to bring it in line with Regulation (EU) 2018/1725 ("the EUDPR"). In parallel, the EDPS started a "consultation process" on the data protection terms of the license agreement in April 2019, which became a formal investigation in May 2019. The procedure ended with the EDPS issuing "Findings and Recommendations" in March 2020. DIGIT took those findings and recommendations into account when negotiating a possible revision with Microsoft. The negotiations resulted in a comprehensive amendment of the license agreement, signed in April 2020. In the aftermath of judgment C-311/18 of the European Court of Justice ("Schrems-II"), the data protection terms of the agreement were reviewed once more to reflect the requirements set by the CJEU.

In May 2021, the EDPS launched two investigations: one of the Commission's use of the Microsoft Office 365 and one into compliance with the Schrems II judgment under the Commission's Cloud II contracts with Microsoft and Amazon Web Services. After providing first information on the contractual relationship with Microsoft, the Commission provided a detailed reply to the EDPS' questions in October 2021.

COM work on AI

[redacted]

EU-US Trade and Technology Council (TTC)

[redacted]

Meeting with [redacted] **Microsoft**

Videoconference 3 December 2021 17h30

[redacted]

Statement on AI that was agreed upon on 29 September by the TTC:

1. The European Union and the United States believe that artificial intelligence (AI) technologies have the potential to bring substantial benefit to our citizens, societies and economies. AI can

help tackle significant challenges societies face, transform industries, and improve the quality of our lives.

2. The European Union and the United States acknowledge that AI-enabled technologies have risks associated with them if they are not developed and deployed responsibly or if they are misused.

3. The European Union and the United States affirm their willingness and intention to develop and implement trustworthy AI and their commitment to a human-centred approach that reinforces shared democratic values and respects universal human rights, which they have already demonstrated by endorsing the OECD Recommendation on AI. Moreover, the European Union and the United States are founding members of the Global Partnership on Artificial Intelligence, which brings together a coalition of like-minded partners seeking to support and guide the responsible development of AI that is grounded in human rights, inclusion, diversity, innovation, economic growth, and societal benefit.

4. The European Union and the United States are committed to working together to ensure that AI serves our societies and economies and that it is used in ways consistent with our common democratic values and human rights. Accordingly, the European Union and the United States are opposed to uses of AI that do not respect this requirement, such as rights-violating systems of social scoring.
5. The European Union and the United States have significant concerns that authoritarian governments are piloting social scoring systems with an aim to implement social control at scale. These systems pose threats to fundamental freedoms and the rule of law, including through silencing speech, punishing peaceful assembly and other expressive activities, and reinforcing arbitrary or unlawful surveillance systems.

6. The European Union and the United States underline that policy and regulatory measures should be based on, and proportionate to the risks posed by the different uses of AI.

7. The United States notes the European Commission's proposal for a risk-based regulatory framework for AI. The framework defines high-risk uses of AI, which are to be subject to a number of requirements. The EU also supports a number of research, innovation and testing projects on trustworthy AI as part of its AI strategy.

8. The European Union notes the US government's development of an AI Risk Management Framework, as well as ongoing projects on trustworthy AI as part of the US National AI Initiative.

9. We are committed to working together to foster responsible stewardship of trustworthy AI that reflects our shared values and commitment to protecting the rights and dignity of all our citizens. We seek to provide scalable, research-based methods to advance trustworthy approaches to AI that serve all people in responsible, equitable, and beneficial ways.

Areas of cooperation
The European Union and the United States want to translate our common values into tangible action and cooperation for mutual benefit.

- The European Union and the United States are committed to the responsible stewardship of trustworthy AI and intend to continue to uphold and implement the OECD Recommendation on Artificial Intelligence. The European Union and the United States seek to develop a mutual understanding on the principles underlining trustworthy and responsible AI.

- The European Union and the United States intend to discuss **measurement and evaluation tools** and activities to assess the technical requirements for trustworthy AI, concerning, for example, accuracy and bias mitigation.

- The European Union and the United States intend to collaborate on projects furthering the development of trustworthy and responsible AI to explore better use of machine learning and other AI techniques towards desirable impacts. We intend to explore cooperation on AI technologies designed to enhance privacy protections, in full compliance with our respective rules, as well as additional areas of cooperation to be defined through dedicated exchanges.

- The European Union and the United States intend to jointly undertake an **economic study examining the impact of AI on the future of our workforces**, with attention to outcomes in employment, wages, and the dispersion of labour market opportunities. Through this collaborative effort, we intend to inform approaches to AI consistent with an inclusive economic policy that ensures the benefits of technological gains are broadly shared by workers across the wage scale.