Meeting with [redacted]

30 March 2022, 10:30

MEETING WITH [redacted]

at Meta

Scene setter

Meta Platforms is the parent organisation of, among others, Facebook, Instagram and WhatsApp, and is one of the Big Five American information technology companies, alongside Google, Amazon, Apple, and Microsoft. Meta's products and services include Facebook, Messenger, Facebook Watch, and Facebook Portal. Meta's European Headquarter is based in Ireland, therefore **Ireland's Data Protection Commission is Meta's lead Supervisory Authority** in the EU.

Meta has been very vocal about the ongoing investigation of the Irish data protection authority (see background), including by **claiming that it will no longer be able to offer its services in Europe** if the Irish DPA prohibits data transfers to the US/"threatening" to leave the European market (see also the statements/articles in the annex). For example, in a recent annual report (that Meta is required to publish under US law), Meta mentioned that "If a new transatlantic data transfer framework is not adopted and we are unable to continue to rely on SCCs or rely upon other alternative means of data transfers from Europe to the United States, we will likely be unable to offer a number of our most significant products and services, including Facebook and Instagram, in Europe, which would materially and adversely affect our business, financial condition, and results of operations". While Meta subsequently indicated in public statements (and a letter addressed to the Commission, see attached) that it has no plans to withdraw from Europe, contrary to other US players who took a more cautious position, [redacted]

LTT

Negotiations on a successor arrangement to the Privacy Shield

- The EU and the US have reached an agreement in principle for a new Trans-Atlantic Data Privacy Framework.
- To comply with the requirements set by the Court of Justice in the Schrems II judgment, the future arrangement will provide for:
  - A set of rules granting Europeans whose personal data are transferred to the US binding safeguards limiting access to data by American intelligence authorities to what is necessary and proportionate to protect national security.
  - The establishment of a two-tier redress system to investigate and resolve complaints from Europeans regarding access to their data by US national security authorities.
  - These new safeguards and redress mechanism will complement the strong obligations that will apply to companies processing data transferred from the EU.

- The two sides will now finalize the details of this agreement in principle and translate it 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.

- On the EU side, the adoption process for an adequacy finding involves obtaining an opinion from the European Data Protection Board (EDPB) and the green light from a committee composed of representatives of the EU Member States. Moreover, the European Parliament has a right of scrutiny over adequacy decisions. Once this procedure will have been completed, the Commission will be able to adopt the adequacy decision.

Data protection inter-EU aspects

- There is room for improvement in the cooperation between Data Protection Authorities in cross-border cases and within the European Data Protection Board (the "Board").

- The smooth collaboration between Data Protection Authorities is important. We therefore welcome the recently adopted guidelines of the Board which will streamline the application of the cooperation mechanism.

- Questions concerning effective enforcement of the GDPR are at the core of discussions in various fora, just last week the European Parliament (LIBE) organised a conference in this respect.

- We attach great importance to coherent enforcement of the GDPR across the EU.

- We value the efforts by businesses to ensure compliance with the GDPR and encourage them to use data protection guarantees as a competitive advantage.

- The GDPR rules and principles will be embedded in a series of EU initiatives in the digital field, namely the Data Governance Act, Digital Markets Act, Digital Services Act and the recent Data Act. In the context of the Digital Markets Act the Commission proposed (in Art. 5(a) of the draft regulation) that gatekeepers (i.e. large platforms such as Facebook) can combine data from their various core services and from third parties only if a data subject gave a valid consent for such processing.

BACKGROUND

Data protection (general)

On 24 June 2020, the Commission issued the **first evaluation report of the GDPR**, which looks back at the first two years of its application. As mandated by Article 97 GDPR, the report focuses on the provisions on the international transfer of personal data and on the cooperation and consistency between Data Protection Authorities.

Up until now, the **major fines imposed by Data Protection Authorities affecting Facebook** include the following:

1. On 15 March 2022 the Ireland's DPC adopted a decision, imposing a fine of €17 million on Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) because it failed to have in place appropriate technical and organisational measures which would enable it to readily demonstrate the security measures that it implemented in practice to protect EU users' data. This decision is the result of an inquiry by the DPC into a series of twelve data breach notifications it received in a six month period between June 2018 and December 2018.

As this was a cross-border case, the DPC's decision was subject to the co-decision-making process under Article 60 GDPR and all the other Data Protection Authorities were engaged as co-decision-makers. Although objections to the DPC's draft decision were raised by two Data Protection Authorities, consensus among those authorities and the DPC was achieved.

2. On 31 December 2021 France's CNIL fined Facebook Ireland Limited €60 million because the users of the social network facebook.com residing in France can't refuse cookies as easily as to accept them.

The one-stop shop mechanism under Article 60 GDPR did not apply to this case and consequently, the role of the Ireland's DPC as Lead Supervisory Authority was not triggered because the operations related to the use of cookies fall within the scope of the ePrivacy directive, transposed in article 82 of the French Data Protection Act. Therefore, the CNIL issued the fine on the basis of its competence pursuant to the ePrivacy directive to verify and sanction operations related to cookies deposited on the terminals of Internet users located in France.

3. On 2 August 2021 Ireland's DPC has fined WhatsApp €225 million. This was the largest GDPR fine that has been imposed concerning Facebook and the second highest under the GDPR. The case goes back to 2018 when the DPC received many complaints concerning the data processing activities of WhatsApp Ireland, especially regarding transparency. The DPC, in its draft decision, proposed a fine in the range of €30-50 million. Eight Data Protection Authorities raised objections on this and other aspects, saying that the fine was not high enough given the seriousness of the matter and the number of data subjects involved. The issue was solved within the consistency mechanism (Article 65 GDPR), during which the Board requested in a decision that the DPC amends the WhatsApp decision with clarifications on transparency and on the calculation of the amount of the fine due to multiple infringements.

On 15 September 2021 WhatsApp has challenged this decision in front of the national court.

On 1 November 2021 WhatsApp lodged a direct action against the Board's decision addressed to the DPC in this case (T-709/21). [redacted]

On 17 March 2022 DG JUST Director-General Ana Gallego participated in a **public hearing in the European Parliament organised by LIBE** on the "GDPR implementation, enforcement and lessons learned". She underlined that for the GDPR enforcement system to work all Data Protection Authorities have to ramp up their efforts in enforcing the GDPR – and the GDPR provides for a variety of tools for them to cooperate efficiently and effectively. She also welcomed the recently adopted Board's guidelines which will streamline the application of the cooperation mechanism as well as the strong willingness of the Data Protection Authorities to further improve their cooperation.

Article 5(a) of the draft regulation on the **Digital Markets Act** stipulates that "In respect of each of its core platform services identified pursuant to Article 3(7), a gatekeeper shall:

refrain from combining personal data sourced from these core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data, unless the end user has been presented with the specific choice and provided consent in the sense of Regulation (EU) 2016/679."

The exact formulation of this article is now at the core of the discussions during the trilogues.

<u>Ongoing procedures in Ireland following the Schrems II judgment</u>

The **Schrems II case** was based on a complaint of Austrian privacy activist Max Schrems before the Irish data protection authority (Data Protection Commission, or DPC) about **data transfers by Facebook Ireland to its headquarters in the US on the basis of Standard Contractual Clauses** (SCCs). Now that the Court of Justice has issued its judgment, it is **for the DPC to apply the clarifications provided by the Court** in this specific case. This means that the DPC will have to decide whether Facebook can continue to transfer data to the US on the basis of SCCs, in light of the Court's assessment of the relevant US surveillance laws, to which Facebook US is subject.

Following the judgment, the **DPC decided to open a so-called 'own volition' inquiry** (i.e. an ex officio investigation), which means that it will carry out this general investigation (which concerns the data transfers by Facebook more generally), instead of first finalising its specific investigation of the complaint lodged by Max Schrems. The DPC explained that it has taken this approach, which has been criticised by civil society (including Max Schrems) and other data protection authorities, because it wants to address Facebook's transfers with respect to all users, instead of focusing only on one complainant.

Max Schrems initiated a judicial review procedure against the DPC, arguing that his complaint should be resolved independently of the 'own volition' investigation. Before the case was heard before the Irish courts, the DPC reached a settlement with Mr. Schrems in January 2021, indicating that it would finalise his complaint procedure swiftly.

In the context of the own volition investigation, **Facebook also initiated legal proceedings against the DPC** before the Irish High Court on procedural grounds, after the DPC issued a preliminary order to Facebook in fall 2020 to suspend its data transfers to the US. While this was only an intermediary step as part of the ongoing investigation, on which Facebook was requested to provide its views (the investigation was therefore not yet finalised and no decision had been taken), Facebook claimed, in particular, that it did not receive sufficient time to present its views. In May 2021, the Irish High Court dismissed Facebook's claim. Following that decision, the DPC pursued its investigation in the context of which it received numerous submissions (by the parties by also by third parties such as the US etc.). Several parties that have intervened before the DPC have asked to wait until the conclusion of the negotiations between the Commission and the US before taking a final decision.

Once the DPC will have reached a conclusion on the lawfulness of Facebook's data transfers on the basis of SCCs its **draft decision will be submitted to the EDPB** for its opinion. The timeline is unclear at the moment, but it seems that the draft decision is to be expected in the coming months.

Post-Schrems II actions of other 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).

In November, the **EDPB endorsed a template decision on the use of Google Analytics by European companies**. These cases were triggered by complaints from None of Your Business, the non-profit organisation headed by Max Schrems. On the basis of the Google Analytics template, the **Austrian DPA issued the first enforcement decision** in January, concluding that the transfers to the US operated in the context of the use of Google Analytics are unlawful. This decision was **followed by a similar one from the French DPA** in February and it is expected that others will follow in the coming weeks/months. [redacted]

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.

Meeting with [redacted]

30 March 2022, 10:30

CURRICULUM VITAE

[redacted]

ANNEX I

Top Facebook exec pushes back on talk of Europe withdrawal

Politico – 24 September 2020

Facebook's Vice President for Global Affairs Nick Clegg poured cold water on the notion that the social media giant plans to withdraw from Europe due to legal concerns about transatlantic data transfers.

The former British deputy prime minister made the remarks late Tuesday after court submissions by Facebook in a legal battle with the Irish privacy regulator over its data transfers to the U.S. led to suggestions the social media giant would quit Europe.

"We absolutely have no desire, no wish, no plans to withdraw. Why would we? ... However, we are clearly not able to operate as we do and nor will many, many other companies if from one moment to the next, the existing legal provisions which govern data transfers from the European Union to the U.S. and other jurisdictions are suddenly removed," Clegg said.

Earlier this month Facebook launched legal proceedings against a pending ruling by the Irish Data Protection Commission (DPC) that would have forced the social media giant to stop sending data from the EU to the U.S. Following Facebook's filing of its appeal, an Irish court ordered a halt to the DPC's investigation.

In submissions to the Irish court, Facebook said the DPC's proposal to turn off its transatlantic data taps meant it was "not clear … how, in those circumstances, it could continue to provide the Facebook and Instagram services in the EU."

Clegg said that not being able to transfer data out of Europe would be "disastrous for the economy as a whole."

The Dublin-based regulator — which oversees Facebook's European data protection practices — issued its preliminary ruling after the EU's top court nixed the transatlantic Privacy Shield data flows deal in July because of fears over the U.S. surveillance regime.

Other companies are keeping a close eye on what happens with the social network's data transfers because many are also reliant on so-called standard contractual clauses — legal tools that underpin transatlantic data transfers — at the center of Facebook's Irish dispute.

If Dublin's preliminary decision against Facebook eventually goes ahead it will set a precedent and force tech giants like Google and smaller firms across the region to reconsider how they move digital information to the U.S.

Previously, companies could have used the Privacy Shield regime. If standard contractual clauses are also taken off the table that means there will be few, if any, legal means to move data from Europe to the U.S.

Speaking at an online event from his California home Tuesday night, Clegg said that not being able to transfer data out of Europe would be "disastrous for the economy as a whole" and that small businesses would bear the brunt.

"A small startup in Germany would no longer be able to use a U.S. cloud-based server or a Spanish product development company would no longer be able to run an operation across multiple time zones," he said

The former leader of the British Liberal Democrats said that legal action against the Irish data regulator's plans to suspend Facebook's data transfers was aimed at buying time for international data flows before a political solution can be found.

"We need the time and the space for the political process between the EU and the U.S. to work out so that companies can have confidence going forward that they're able to transfer data," the College of Europe-educated Brit said.

The European Commission and the U.S. government issued a joint statement shortly after Privacy Shield was struck down saying that they were working on an "enhanced" data flows agreement, though negotiations will only be able to start in earnest after the November election.

Clegg also aimed a jibe at the EU by saying that though the bloc had been unsparing with the U.S.'s snooping regime, "there's actually a carve-out for EU member state surveillance practices" in EU data protection rules.

Source – Politico (https://www.politico.eu/article/nick-clegg-top-facebook-executive-pushes-back-on-talk-of-europe-withdrawal/)

ANNEX II

Securing the Long Term Stability of Cross-Border Data Flows

Statement by Nick Clegg, 9 September 2020

Thousands of European and US businesses rely on the safe and legal transfer of data between jurisdictions. International data transfers underpin the global economy and support many of the services that are fundamental to our daily lives.

In July, the Court of Justice of the European Union (CJEU) invalidated Privacy Shield, a legal framework regulating transfers of personal data from the EU to the US. At the same time, the CJEU stated that Standard Contractual Clauses, (SCCs), an alternative legal mechanism for transferring data from the EU to a third country, continue to be valid. But the rationale in invalidating Privacy Shield has nonetheless created significant uncertainty – not just for US tech companies, or even for all the European businesses who rely on online services to reach new customers, but for all European businesses with transatlantic data flows.

With the establishment of a European Data Protection Board taskforce to consider how to apply the CJEU ruling, as well as a joint statement from the EU Commission and US Department of Commerce that they have initiated discussions for an "enhanced" EU-US Privacy Shield, we are setting out our position on how to secure the long term stability of international data transfers. We support global rules that can ensure consistent treatment of data around the world.

A Safe, Secure Transfer Mechanism Upheld by the Courts

In its recent decision, the CJEU invalidated the Privacy Shield mechanism for transferring data between the EU and US, due to concerns over US national security laws. Before the ruling, more than 5,000 companies relied on Privacy Shield.

Although the court also ruled that Standard Contractual Clauses (SCCs) remain valid (providing the data exporter puts in place appropriate safeguards to ensure a high level of protection for data subjects), its rationale in invalidating Privacy Shield has prompted a discussion around businesses' reliance on SCCs.

Like many other businesses, Facebook relies on SCCs to transfer data to countries outside the EU, including to the United States. Since the CJEU's ruling in July, Facebook has been working hard to follow the steps set out by the Court to ensure that we can continue to transfer data in a safe and secure way. This includes ensuring that we have robust safeguards in place, such as industry standard encryption and security measures, and comprehensive policies governing how we respond to legal requests for data.

The Irish Data Protection Commission (IDPC) has commenced an inquiry into Facebook controlled EU-US data transfers, and has suggested that SCCs cannot in practice be used for EU-US data transfers. While this approach is subject to further process, if followed, it could have a far reaching effect on businesses that rely on SCCs and on the online services many people and businesses rely on.

A lack of safe, secure and legal international data transfers would damage the economy and hamper the growth of data-driven businesses in the EU, just as we seek a recovery from COVID-19. The impact would be felt by businesses large and small, across multiple sectors. In the worst case scenario, this could mean that a small tech start up in Germany would no longer be able to use a US-based cloud provider. A Spanish product development company could no longer be able to run an operation across multiple time zones. A French retailer may find they can no longer maintain a call centre in Morocco.

The effects would reach beyond the business world, and could impact critical public services such as health and education. Ireland's Covid Tracking App states, in its terms, that it relies on SCCs as one of a number of mechanisms to transfer data to one of its processors in the US. International cloud providers and email platforms provide services to schools, Universities and hospitals across Europe. Millions of people use video conferencing software every day, to keep in touch with friends and family who live in different countries.

Clear Global Rules to Protect Consumers

Businesses need clear, global rules, underpinned by the strong rule of law, to protect transatlantic data flows over the long term.

The EU has led the way in establishing a framework for data protection that protects and empowers users. Privacy rules will continue to evolve, and global rules can ensure the consistent treatment of data wherever it is stored. Facebook therefore welcomes the efforts already underway between EU and US lawmakers to evaluate the potential for an "enhanced" EU-US framework – a Privacy Shield Plus. These efforts will need to recognise that EU Member States and the US are both democracies that share common values and the rule of law, are deeply culturally, socially and commercially interconnected, and have very similar data surveillance powers and practices

We recognize that building a sustainable framework that supports frictionless data flows to other countries and legal systems, while at the same time ensuring that the fundamental rights of EU users are respected, is not an easy task and will take time. While policymakers are working towards a sustainable, long-term solution, we urge regulators to adopt a proportionate and pragmatic approach to minimise disruption to the many thousands of businesses who, like Facebook, have been relying on these mechanisms in good faith to transfer data in a safe and secure way.

Our priority is to ensure that our users, advertisers, customers and partners can continue to enjoy Facebook services while keeping their data safe and secure. We will continue to transfer data in compliance with the recent CJEU ruling and until we receive further guidance.

(Source: Facebook, https://about.fb.com/news/2020/09/securing-the-long-term-stability-of-cross-border-data-flows/?utm_source=POLITICO.EU&utm_campaign=4480add956-EMAIL_CAMPAIGN_2020_09_09_07_04&utm_medium=email&utm_term=0_10959edeb5-4480add956-189034885)