Uber B.V.

Data Protection Office
Mr. Treublaan 7, 1097 DP,
Amsterdam, The Netherlands
Registration No. 56317441

Amsterdam, 25 January 2022,

L.S.,

In my capacity as Data Protection Officer of Uber B.V. and Uber Technologies Incorporated, I would like to thank the EDPB for providing the opportunity to comment on the Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

Attached I have provided my comments and raised some questions in order to be able to better understand the guidelines and contribute to further improvements. Comments and questions below are mine only, based on multiple years of experience in multinational communications service providers and various data driven companies, and do not necessarily contain the views or opinions of Uber or any organisation I am or have been associated with.

In general the comments and questions are reflective of the “geographical” interpretation of the notion of transfers which seems to be prefered in the draft guidance, instead of the “jurisdictional” or rather “accountability based” approach which is the basis of article 3 of GDPR.

This approach, in my view, leads to a lack of logic and several likely unintended consequences when applied in practice, in particular when taking the factual, practical and physical realities of 21st century data flows into consideration. I also take the view this “geographical” reading may not be required to provide for a non-undermined protection in those cases where the third country controller or processor is directly subject to GDPR for the data it receives and subsequently processes, provided the controller or processor is able to demonstrate compliance with the provisions in GDPR outside Chapter V in accordance with article 24(1), including an “enhanced” risk assessment and “enhanced” mitigations related to applying GDPR in (the legal context of) a third country and considering Chapter IV, section 4 on Data Protection Officers.

Should there be any questions, please do not hesitate to reach out and I will make myself available.

Yours sincerely,

Simon Hania

Uber B.V.

Data Protection Office
Mr. Treublaan 7, 1097 DP,
Amsterdam, The Netherlands
Registration No. 56317441

The topics covered below are:

- The relation between article 3(1) and Chapter V;
- A GDPR undermining effect apparently is introduced by an intermediary EEA entity;
- Elements to include in a transfer instrument in case GDPR applies;
- Transmission of data from a third country to the Union by third country controllers;
- The interpretation of the last sentence of article 44;
- The role of communication service providers factually conducting the transfers;
- The role of Data Protection Officers.

The relation between Article 3(1) and Chapter V.

Could EDPB please elaborate more, for instance by including example scenarios, on the notion of a transfer in relation to controllers and processors in third countries subject to article 3(1), by virtue of meeting the criteria related to having an establishment in the Union as highlighted in EDPB opinion 3/2018, rather than largely focussing the guidelines on article 3(2) only?

I would in particular be interested in a scenario in which a data controller in the EU exports data regarding people in the EU to a separate data controller in a third country, where this data controller engages in solely automated decisions making, including profiling with a legal or similarly significant effect and where only the decision itself is transmitted back to the data controller in the EU. In this scenario I would like the EDPB to consider two sub scenarios and to consider to what extent these differ in terms of non-undermined protections offered by GDPR: one scenario in which the EU data controller is an establishment of the third country controller (and hence subject to GDPR, including article 22) and another scenario in which this is not the case and in which the third country data controller also does not fulfil the criteria under article 3(2) (and hence article 22 GDPR would not apply to the automated decision making in the third country). How would in the later sub scenario the provisions in Chapter V ensure the protections of GDPR related to automated decision making are not undermined?

A GDPR undermining effect apparently is introduced by an intermediary EEA entity.

A direct transmission from a data subject in the Union of their personal data to a controller in e.g. the US subject to article 3(2) is not considered a transfer according to paragraph 12. Yet based on paragraph 3, a transmission of the same data from the same data subject via an establishment in the Union to the same US controller, who, based on EDPB opinion 3/2018 is subject to GDPR by virtue of art 3(1), would have to be considered a transfer and subject to conditions in Chapter V. From a perspective of comparative levels of protection or “essential equivalence” the logic in this seems absent to me.

Uber B.V.

Data Protection Office
Mr. Treublaan 7, 1097 DP,
Amsterdam, The Netherlands
Registration No. 56317441

Could the EDPB please elaborate how the protection of GDPR apparently is considered to be undermined by involving the establishment in the Union, resulting in the requirement to engage in appropriate and/or even additional safeguards, in contrast to the scenario of direct transmissions where the controller in the US is required to demonstrably adhere to all other relevant provisions of GDPR as mentioned in paragraph 5?
Could EDPB consider transmissions to third country controllers and processors already subject to GDPR not as a transfer but subject to “enhanced” risk assessment and “enhanced” mitigations in both cases?

Elements to include in a transfer instrument in case GDPR applies.
In paragraph 23 it is mentioned that tailored safeguards are required in case data is transferred from a controller or processor in the Union to a controller or processor in a third country subject to GDPR. It is highlighted that aside from EC decided Standard Contractual Clauses, alternative options are available, of which the middle four in the enumeration in the draft are available to private enterprises to develop and propose.

To support controllers and processors to render this into a practical possibility, rather than leaving it a theoretical one, could EDPB please elude to which provisions in the EC decided Standard Contractual Clauses it in principle deems duplicating GDPR provisions, and where relevant relate this to some of the examples given earlier and/or give addtional specific examples?

Separately under article 46(2)(d) competent supervisory authorities, with approval from the EC, can determine Standard Contractual Clauses.
Could EDPB orchestrate such determination together with the individual competent authorities in the interest of consistency and present an “EDPB version” for approval to the EC, also in light of article 46(4) not requiring this?

Transmission of data from a third country to the Union by third country controllers.
In case a controller or processor subject to GDPR in a third country transmits data (back) to a data subject or another controller or processor in the Union, would (one of) these controllers or processors have to conduct an impact assessment related to these transmissions, either based on various general provisions in GDPR or based on Chapter V provisions?
To what extent should such an impact assessment be enhanced to include access by public authorities, including those in individual member state countries?

Uber B.V.

Data Protection Office
Mr. Treublaan 7, 1097 DP,
Amsterdam, The Netherlands
Registration No. 56317441

The latter access is not inconceivable, given the fact that intelligence services in EU member states either by law or in practice may be inclined to treat data originating from outside the Union differently from data in the Union and/or may find themselves at issue with adequate independent oversight of data processing conducted in the context of national security. The latter for instance may be found in EU member states that have not yet been able to ratify Convention 108+[1] for reasons related to provisions with respect to independent oversight over (all) data processing conducted for national security purposes.

The interpretation of the last sentence of article 44.

Article 44 last sentence states (italics added) “All provisions in this Chapter *shall be applied* in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.” Yet the equally valid Dutch and French versions of article 44 (quoted below) in their last sentence could be read as stating this as the first condition of the “conditions laid down in this Chapter” [that] “are complied with” rather than as an obligation to apply other provisions.
This can be interpreted as leaving room to first assess whether the level of protection is not undermined, based on demonstrable compliance with all provisions of GDPR outside Chapter V addressed in light of the application of GDPR in (the legal context of) a third country. Based on such demonstrable compliance, the condition of non-undermining (the last sentence of article 44) could be considered to be met to subsequently consider the rest of Chapter V to not be applicable to the data processing in scope.
Such interpretation also seems better in line with the conclusion that direct transmission of data by a data subject to a controller in a third country does not require the further conditions in Chapter V to be met, while all other provisions of GDPR remain fully applicable.

Could EDPB adopt this, admittedly creative, reading of Article 44 to be valid and in doing so arrive at a reading irrespective of the actual transmission path, leading to more logic and consistency in its guidelines, without compromising on continued and effective protection?

“Alle bepalingen van dit hoofdstuk *worden toegepast* (translates as “are applied”, rather than “shall be applied”/“dienen te worden toegepast”) opdat het door deze verordening voor natuurlijke personen gewaarborgde beschermingsniveau niet wordt ondermijnd.” and “Toutes les dispositions du présent chapitre *sont appliquées* (translates as “are applied” rather than

[1] For example on 9 December 2021 the Dutch Minister of Interior sent a letter to the Dutch Senate regarding ratification of Convention 108+. The Dutch government disclosed it decided to postpone ratification, pending external advice sought regarding a sustainable oversight system in light of latest jurisprudence, suggesting there may be systemic issues to resolve in order to be able to ratify.

Uber B.V.

Data Protection Office
Mr. Treublaan 7, 1097 DP,
Amsterdam, The Netherlands
Registration No. 56317441

"shall be applied"/"doivent être appliquées") de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis."

The role of communications service providers factually conducting the transfers as exporters and importers operating on behalf of controllers and processors.
Almost every controller or processor in the Union will engage a communication service provider (CSP) via the local establishment of the CSP in order to perform data transfers by disclosing data via transmission to recipients in third countries. The CSP liaises with its own establishments and/or other CSPs in potentially multiple third countries to sequentially disclose the data by transmission and other intermediary data processing operations, between the various local establishment(s) of, in most cases, multiple CSPs until it is disclosed by transmission to its final recipient along a dynamically changing route potentially traversing multiple third countries and multiple CSP establishments.
Applying the three criteria found by EDPB to this, results in observing a cascade of onward transfers, with independent CSPs and their establishments as factual exporters and importers of the data transmitted via disclosure, while operating on behalf (as a processor or (partial) controller) of the originating controller or processor.

Consider for example data transmitted from the Union to India, or Japan routed via countries in the Middle East, Egypt in particular, or routed in the other direction via the US. Consider data transmitted from continental Europe to Ireland routed via the UK, or data exchanged between the Union and Sub-Saharan countries via satellite links.

Does the EDPB agree with this observation and subsequent application and interpretation of the criteria in the Guidelines?
If yes: how should the originating controller or processor in the Union realistically in practice adhere to the provisions in Chapter V, given the, by reasoned design, dynamic nature of these disclosures by transmission?
If no: why not and how is it to be ensured GDPR is not undermined and data remains protected when the data is transmitted via disclosure to intermediary establishments in third countries, who may be and in many cases are subject to access requirements by government authorities?

In both cases: Would the EDPB for example consider these "mere conduits" to not be part of (a cascade of) "disclosure by transmission" processing operations and to not be included in the notion of a "transfer"? Or alternatively could EDPB arrive at a conclusion that these disclosures by transmission do not result in a requirement to engage in provisions under Chapter V, in case both exporter and importer can demonstrate protection is not undermined by engaging in an

“enhanced” risk assessment and “enhanced” mitigations. This for instance could result in applying technological and organisational measures that render the data unintelligible en route by engaging in strong encryption such that only the importer and the exporter have access to the cryptographic keys.

The role of Data Protection Officers

WP29 as a predecessor of the EDPB in its opinion on Data Protection Officers stated the DPO “is a cornerstone of accountability” and “appointing a DPO can facilitate compliance” while “GDPR recognises the DPO as a key player in the new data governance system”.

Could EDPB therefore please elaborate on the role and tasks of a Data Protection Officer in the context of the interplay between article 3 and Chapter V, i.e. in those cases where a data controller in a third country is not subject to the requirements in GDPR related to the designation of a DPO? To what extent is a DPO an element in considering essential equivalence and/or GDPR to not be undermined when designated (voluntary or not) by a controller or processor in a third country subject to GDPR? Does EDPB consider the designation of a DPO by a controller/processor in a third country an additional safeguard complementing appropriate safeguards under article 46 for controllers/processors?

Elements that come to mind to consider are:

Designation

- Controllers and processors in third countries, subject to article 3(1) and/or 3(2), in accordance with article 37 and 37(1)(b) in particular, in most cases need to designate a DPO.
- Controllers and processors in third countries, not directly subject to GDPR receiving data, subject to the conditions in Chapter V, in particular SCCs under article 46, are not subject to any obligation to designate a DPO, potentially creating an undermining effect.

Position

- Controllers and processors, including those in third countries, need to ensure the DPO is involved in matters of data protection.
  This includes international data flows, data transfers and, for controllers and processors in third countries subject to GDPR, any further processing and onward transfers.
- In compliant organisations, DPOs carefully consider risks to data subjects, conduct their tasks independently, in a confidential manner, without conflicts of interest, while reporting to highest management and receiving their full support.
  This enables a high level of internal supervision of the data processing operations of a

controller or processor in a third country subject to GDPR, at a level not found in controllers or processors in third countries not subject to GDPR.

- DPOs cannot receive instruction with regard to their tasks.
  Yet, this does not stand in the way of DPOs receiving requests from controllers and processors regarding the exercise of their tasks and in particular related to international data flows.
- DPOs, also those appointed by controllers and processors in third countries, may be contacted by all data subjects with regard to issues related to processing of their data. This provides data subjects access to a statutory officer with a mandate in order to raise issues with respect to transparency and lawfulness and an avenue to initiate redress.

Tasks

- DPOs inform and advise, in particular with respect to data processing operations with potential high risks.
  This includes risks such as international data flows, data transfers and the associated Data Protection and Transfer Impact Assessments and Prior Consultations;
- DPOs monitor for compliance, which, if they decide and commit to do so, can include monitoring of data processing activities performed by third country data controllers and processors subject to GDPR leading up to disclosures to public authorities;
- DPOs, including those designated by third country data controllers and processors subject to GDPR, are obliged to cooperate and consult and act as point of contact for supervisory authorities, enabling these to effectively supervise controllers and processors in third countries;