NASSCOM®

To: The European Data Protection Board (**EDPB**)

From: National Association of Software and Service Companies (**NASSCOM**)

Subject: Comments on the Draft Guidelines on the Interplay between Article 3 and Chapter V of the GDPR

Date: January 31st, 2022

About this document

NASSCOM welcomes this opportunity to offer our comments to the EDPB on the draft Guidelines 05/2021[1] on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the General Data Protection Regulation (**Draft Guidelines**).

The Indian IT – BPM industry processes data for several industries in over 100 countries, including those in the European Union (**EU**). We are acutely aware of the need to establish stable, practical, and balanced regimes on international personal data transfers for the digital economy. In our view, these Draft Guidelines can serve as a step towards the establishment of such a regime.

Through this submission, we aim to positively contribute to the EDPB's thinking and guidelines on the regulation of international data transfers in and out of the EEA under the General Data Protection Regulation (**GDPR**).

Executive summary

- The Draft Guidelines identify cumulative criteria for when a processing qualifies as a transfer to a third country, based on the CJEU's decision in *Bodil Lindqvist*. However, *Lindqvist* does not definitely set out these criteria; it is limited to one particular scenario – a website hosted on an EEA server that is accessible from any third country. We therefore request more clarity on the meaning and scope of transfer.
- As a general principle, we submit that the intent of a sender to provide access to personal data be considered while determining whether processing constitutes a transfer, in line with EPDS suggestions.
- In particular, the Draft Guidelines offer a notion of a transfer based on two key phrases – "*disclosure by transmission*" and "*making available*" of personal data – but miss the opportunity to clarify what these phrases mean. We request guidance and illustrations on what these cover and exclude. We request a more nuanced understanding in two scenarios:
- First, the EDPB should look to define its understanding of "remote access" in more concrete and technical terms. Not all scenarios of "remote access" need to be regarded as a "transfer" necessitating a transfer tool. For example, where the personal data stays on a server in the EU

[1] EDPB, *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*, (19th November 2021), available at https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf (**Draft Guidelines**).

and is only processed by an overseas processor who cannot export or download the personal data, and the data is encrypted in transit.

- Alternatively, if the concept of a "transfer" is interpreted so broadly as to capture all scenarios currently considered as "remote access", then the EDPB should regard certain nuanced scenarios as situations meriting lower protections/safeguards and specify security measures to ensure that the GDPR protections are not undermined.
- Second, the concept of a "transfer" should be interpreted in a manner that excludes transit scenarios involving intermediate entities, through whom personal data passes, where such entities cannot access or manipulate the personal data whilst it is in transit between the exporter and importer.

Detailed Comments on the Draft Guidelines

Need for guidance on the concept of transfer

1. The Draft Guidelines set out three cumulative criteria for when a processing activity qualifies as a "transfer" [2]:

- A controller or processor is subject to the GDPR. In other words, it is sufficient if the processing in question falls within the territorial scope of the GDPR pursuant to Article 3.
- The controller or processor ("**exporter**") "discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor" ("**importer**").
- The importer is in a third country or is an international organization, irrespective of whether the importer is subject to the GDPR.[3]

2. From the criteria and the guidance in the Draft Guidelines, we understand that:

- For a transfer to take place, the exporter and importer must be separate and distinct organizations.[4]
- The status of the exporter under the GDPR is relevant in determining whether or not a processing activity is a transfer.[5]
- The status of the importer is not relevant in determining whether a processing activity is a transfer or not. It is a transfer whenever the importer is in a third country, even if that recipient is subject to the GDPR by virtue of Article 3(2).

3. While these are helpful principles, the Draft Guidelines only provide limited guidance. They do not provide guidance on the phrases "disclosure by transmission" and "making available personal data" – which are key to the meaning of transfer.

4. Further, to frame the concept of a "transfer", the Draft Guidelines rely on findings from the decision of the Court of Justice of the European Union (**CJEU**) in *Bodil Lindqvist* (**Lindqvist**).[6] In *Lindqvist*, the CJEU found that it is not a "transfer" if a person in the EU uploads personal data on to a website, which is accessible by anyone who connects to the internet, including by persons

---

[2] *Supra* note 1 at Paras 6 & 7, Page 4.
[3] *Supra* note 1 at Para 7, Page 4.
[4] *Supra* note 1 at Example 5, Page 6.
[5] *Supra* note 1 at Para 12, Example 1, Page 5 & 6.
[6] As noted in footnote 7 of the Draft Guidelines. *Supra* note 1 at Para 7, page 4. *Also see Bodil Lindqvist* v. *Åklagarkammaren i Jönköping*, Case C-101/01, ECLI:EU:C:2003:596 (**Lindqvist**).

in third countries.[7] *Lindqvist* notes that the concept of a "transfer" should be interpreted in a manner that avoids the special regime of data transfers becoming "*a regime of general application, as regards operations on the internet*".[8] Clearly, the CJEU also recognized the challenges that arise from having an over-broad conception of this term and took into account the consequences of finding a particular operation as a transfer or not.[9]

5. However, the *Lindqvist* decision does not offer any assistance in interpreting the concept of transfer. In the past, the European Data Protection Supervisor (**EDPS**) has pointed out that the conclusion of the CJEU on the concept of "*transfer*" should not be "*simply and automatically be applied to cases with different characteristics".*[10] Moreover, since the *Lindqvist* decision is from 2003, it is difficult to accept that this judgement is sufficiently nuanced to cover different scenarios in modern networking environments.

6. None of the other cases before the CJEU, such as those in *EU-Canada PNR*[11] opinion, or in *Schrems I*[12] or Schrems *II*[13] - deal with the scope or meaning of a "transfer".

Recommendation:

7. **Given that the CJEU or other courts are yet to rule on the scope of 'transfer', we request that the Draft Guidelines provide clarity on the scope or meaning of transfer. This is crucial because there is no guidance on how the key phrases that are core to a transfer, namely, "*disclosure by transmission*" or the "*making available*" of personal data, are to be interpreted and applied in different contexts and at a technical level.**

8. **Further, to determine situations that qualify as transfer, we also recommend incorporating EDPS's suggestion on considering the intent of the sender to provide access to personal data. The EDPS said that the concept of transfer should be one of "*communication, disclosure or otherwise making available of personal data, conducted with the knowledge or intention of a sender subject to the Regulation that the recipient will have access to it".*[14]**

9. **In particular, we recommend a more nuanced understanding of transfer in two situations: (1) 'remote access' and (2) mere transit scenarios, as we discuss below.**

Analyzing "remote access" vis-à-vis "transfer"

10. Earlier documents released by the EDPB assume that "remote access" scenarios always constitute a transfer. For example, in the recommendations on supplementary measures post

[7] *Id* at Para 71.
[8] *Id* at Para 69.
[9] Some have considered this approach of the CJEU considering the consequences of finding that some conduct amounts to a "transfer" before doing so as an approach that involved the application of a "reasonableness test" and that was worth appreciating as a suitable method to address legal issues arising from rapidly evolving technologies. *See* D. J. B. Svantesson, *Privacy, Internet and Transborder Data Flows, Masaryk University Journal of Law and Technology*, 16, (2010), available at https://journals.muni.cz/mujlt/article/view/2554/2118
[10] *See* European Data Protection Supervisor, *The transfer of personal data to third countries and international organizations by EU institutions and bodies,* Position Paper, Page 6, (14th July 2014), available at https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf
[11] *See* CJEU, *Opinion 1/15 on the EU – Canada PNR Sharing Agreement*, (26th July 2017), available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62015CV0001(01)&from=EN.
[12] *Maximillian Schrems* v. *Data Protection Commissioner*, Case C - 362/14, ECLI:EU:C:2015:650, (**Schrems I**).
[13] *Data Protection Commissioner* v. *Facebook Ireland and Maximillian Schrems*, Case C-311/18, ECLI:EU:C:2020:559, (**Schrems II**).
[14] *Supra* note 10 at Page 7

Schrems II, the EDPB states that remote access from a third country is considered as a transfer.[15] This position comes from a set of FAQs which stated that "*even providing access to data from a third country, for instance for administration purposes, also amounts to a transfer*".[16] However, across all these documents, the EDPB does not formally set out its understanding of the concept of "remote access" itself. The EDPB does not delve into why remote access from a third country, in all or specific scenarios, should be regarded as a "transfer". It does not provide a risk assessment of different scenarios that may be considered as falling under this concept.

11. The Draft Guidelines note that if an employee of the EEA-based controller remotely accesses the data while physically in a non-EEA region, the processing does not constitute transfer, because the employee is part of the EEA-based controller and not a separate data importer.[17] This is helpful, but it does not provide additional guidance on the concept of "remote access". Further, the Draft Guidelines offer no guidance on how "remote access" should be understood vis-à-vis the phrases *"disclose by transmission" or "making available".*

12. We find that the concept of remote access is implicitly being understood by the EDPB as covering scenarios where the personal data being processed remains on a host computer system located in the physical territory of the EU. Instead of any transmission, an overseas importer connects to that host computer system over a network. However, in such remote access scenarios, the EDPB does not analyze the nature and extent of access to personal data. This becomes challenging when we consider more nuanced scenarios. For example:

Personal data is made available by a controller in the EU to a processor in India. The processor in India can only view or process the data via a platform that prevents all files and data from being exported or downloaded. The data is only stored in the EU.

13. Since personal data remains in the EU in the above example, it would be difficult to regard this as a form of "*disclosure by transmission*".

14. The Draft Guidelines also make it clear that a transfer would capture any scenario involving the "*making available"* of personal data. The phrase is overly broad that it may be construed to cover any processing operation of any kind without any link back to identifiable risk that the EDPB wishes to preclude. This is a slippery slope, making the form of remote access outlined in the above example falling within this catch-all phrase. Since there is no end to what can be captured, we are again faced with the challenge recognized in *Lindqvist* – of the transfer regime becoming generally applicable.

15. We find that, in relation to the above example, the level of risk of the GDPR protections being undermined is particularly low – to the extent where it is not necessary for such a scenario to be regarded as a "transfer" necessitating the application of the provisions of chapter V. This is because there are no data flows to any territory outside the EU, and the controller continues to be in the EU.

Recommendation:

[15] See EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, available at https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf
[16] *See* EDPB, *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, 5, (23rd July 2020), available at https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf
[17] *Supra* note 1 at Example 5, Page 6.

16. **We submit that the EDPB should reconsider its understanding of "remote access". They should clarify which "remote access" scenarios are being considered as transfers on the basis of degree of risk.[18] It would also be useful to examine different technical operations where personal data is accessed remotely and evaluate the risk of GDPR protections being undermined on a case-to-case basis. This is to determine whether the provisions of chapter V should apply.**

17. **We recommend that cases where the risk is low or negligible should not be regarded as "transfer". This does not mean that other protections will not be made applicable on the overseas processor by the controller. The controller could, through Article 32 and the data processing agreement under Article 28, introduce several measures to minimize risks. For instance, if personal data is being made available by an EU based controller to a processor in India, who can only view or process the data, the controller could deploy technological measures to ensure that copies of files or data being viewed or processed are not created, and that the data is encrypted in transit.**

18. **We also recommend that, if at all 'remote access' falls within the scope of transfer, the EDPB should consider such scenarios requiring lower forms of protections/safeguards and simpler forms of transfer tools. The EDPB could assist by setting out measures needed to ensure that the GDPR protections are not undermined**.

Analyzing the "transit" scenario vis-à-vis "transfer"

19. In situations where personal data is routed through a computer system located in a third country, but the transfer is between EU based exporter and importer, this is a mere transit and should not be considered as transfer.

20. This is also in line with the interpretation suggested by the EDPS, which noted that "*the mere fact that information might or will cross international borders to its destination due to the way in which networks are structured would not automatically trigger the concept*".[19]

21. While evaluating whether processing will constitute a transfer, the Information Commissioner's Office in the United Kingdom (**UK ICO**) concluded that "transfer does not mean same as transit".[20] It suggested that the intention to access or manipulate the data in a non-EEA region is relevant in considering if processing is a transfer. In particular, the UK ICO mentioned the following example to clarify:

[18] It is to be noted that the lack of clarity on the concept of "remote access" has been raised before by other stakeholders as well. *See*, *for example,* Norwegian Institute of Public Health and the University of Oslo, *Comments on the Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, (2020), available at: https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/comments_from_niph_and_uio_on_recommendations_01-2020_on_measures_that_supplement_transfer_tools.pdf

[19] *Supra* note 10 at Page 7.

[20] See, the UK ICO guidance on restricted transfers, example: A UK company sells holidays in Australia. It sends the personal data of customers who have bought the holidays to the hotels they have chosen in Australia in order to secure their bookings. This is a restricted transfer. Transfer does not mean the same as transit. If personal data is just electronically routed through a non-UK country but the transfer is actually from one UK organisation to another, then it is not a restricted transfer, available at, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/

Personal data is transferred from a controller in the UK to another controller in the UK via a server in Australia. There is no intention that the personal data will be accessed or manipulated while it is in Australia. Therefore, there is no restricted transfer.[21]

22. In the UK ICO example, we may consider the Australian server as an example of an intermediate entity through whom data passes. As per the Draft Guidelines, the concept of a transfer includes the phrase "*disclosure by transmission"* and the catch-all phrase "*making available".* A strict interpretation of these phrases would result in the transmission being broken into two stages: (1) from the EU exporter to the server in Australia, and (2) from that server to the EU importer. Both these stages could be regarded as separate transfers, triggering Chapter V provisions.

23. Such an interpretation could lead to the provisions of chapter V being made applicable across a wide variety of transmissions across networks with no analysis of whether the actual risk of the GDPR protections not being applicable is being realized or not. By not accounting for such scenarios of "transit" in the Draft Guidelines, the challenge of the concept of "transfer" becoming generally applicable across the board - first recognized in *Lindqvist* – rises.

24. Note that non-applicability of Chapter V would not mean that other protections under the GDPR will not be applicable. Controllers could be required to ensure that as part of their obligations under Article 32, effective technical measures are implemented. These include ensuring data in transit is encrypted, that no intelligible access or decryption keys are afforded to any intermediate entities through whom data passes. This could ensure that, while in transit, such personal data is not accessed or manipulated by an intermediate entity and the key risk of access of such personal data by non-EU law enforcement agencies can be alleviated. We limit this suggestion to only a "transit" scenario, where an entity is only performing a transit function to pass the personal data forward and with only incidental and transitory storage to facilitate such transit.

Recommendation:

25. **We recommend that the EDPB's guidelines reflect EDPS's suggestion on considering the intent of a sender to provide access in determining whether transit qualifies as transfer.**[22] **Accordingly, we recommend that the EDPB clarify that mere transit scenarios should be excluded from being considered transfers.**

The National Association for Software and Service Companies (**NASSCOM**) is a not-for-profit industry association for the information technology industry in India. Established in 1988, NASSCOM has over 3000 members comprising Indian and foreign organisations, including those from UK that have a presence in India.

For any queries or clarifications regarding this submission, please contact Ashish Aggarwal (Asaggarwal@nasscom.in), Varun Sen Bahl (varun@nasscom.in), or Apurva Singh (apurva@nasscom.in).

***

[21] *Supra* note 20
[22] *Supra* note 10 at Page 7.