DRAFT – NOT FOR CIRCULATION

UKIBC – techUK- NASSCOM

Joint Position Paper on Enabling UK-India Cross Border Data Transfers

[Date] October 2021

On behalf of our members, we respectfully submit the following joint position paper on enabling cross-border data transfers between United Kingdom and India. This paper suggests recommendations for the governments of India and the United Kingdom to consider when negotiating the UK-India Free Trade Agreement and when considering reforms to domestic rules on international data transfers and provide guidance to discussions between India-EU.

---

techUK is an industry association for the technology sector in the United Kingdom. Established in 2015, techUK has over 800 members in the United Kingdom.

The UK-India Business Council (**UKIBC**) is a not-for-profit industry association to foster bilateral trade between India and the United Kingdom. Established in 1993, UKIBC has over 90 members in India and the United Kingdom.

National Association for Software and Service Companies (**NASSCOM**) is a not-for-profit industry association for IT/ITeS industry in India. Established in 1988, NASSCOM has over 3000 member companies, including Indian organisations, multinational organisations and United Kingdom (**UK**) information technology organisations that have a presence in India.

Section A
Introduction

A central driver of modern global commerce is the free movement of data across borders. By accessing the internet and transferring data across borders, businesses – from large multi-national conglomerates to small and medium enterprises – have been able to access global marketplaces and supply chains, reduce trade costs, increase productivity, and scale operations globally.

With the COVID-19 pandemic forcing life into remote operating environments, global trade witnessed the trend towards accelerated electronic commerce. As per UNCTAD, the share of electronic commerce in global retail trade surged during the pandemic, jumping from 14% in 2019 to 17% in 2020.[1] This shift has made international data transfers a basic feature of doing business today. Considering this, policies restricting such transfers have become significant barriers on

[1] *See* UNCTAD, '*How COVID-19 triggered the digital and e-commerce turning point',* March 15 2021, *available at* https://unctad.org/news/how-covid-19-triggered-digital-and-e-commerce-turning-point (last accessed on October 20, 2021).

access to services and digital products, impeding the ease of doing of business, dampening innovation, and hindering global trade and investment.

Governments, for whom informational privacy has become a key policy imperative in recent years, may take different regulatory approaches to protecting personal information. Consequently, to uphold their domestic regimes, governments may consider it necessary to restrict or impose conditions to transfer of personal information to overseas territories. However, as such restrictions and conditions are built up across multiple jurisdictions, they can have the unintended impact of leading to legal uncertainty and incompatibilities across regimes. This can make digital trade unnecessarily cumbersome, have an adverse effect on competition, or restrict digital trade altogether. The result is suboptimal outcomes for consumers whose personal data is sought to be protected by their governments.

Our members are key participants in digital trade in the economies of India and the UK. While we recognise the need to protect and uphold the informational privacy of consumers, we are also aware of the importance that international data transfers hold for global trade generally and, more specifically, for bilateral trade between UK and India. This is especially significant when we consider that the ambitious target, set by both nations, of more than doubling India-UK trade by 2030, has put us on a course to unlock the full potential of our bilateral commercial relationship.[2]

A common message across several conversations with our members is that the capacity of the information technology sectors in India and the UK to contribute to this goal shall be better realised by policies that recognise that informational privacy and digital trade are not mutually exclusive objectives and that different data protection regimes may look to be mutually compatible.

We also note here a recent paper from the World Bank.[3] It finds that a regulatory approach that combines a regime with few or no restrictions on international data transfers with strong domestic safeguards for the protection of personal data during processing appears to be the most conducive to enabling trade in digital services, characterised as software-intensive services by the World Bank. Such a regulatory approach enables data to move freely across borders whilst also creating trust through safeguards on processing operations. The paper also finds that countries with compatible data processing and transfer regimes tend to have a higher level of digital services trade between them as compared to trading partners with different data regimes. This highlights the importance of framing and operationalising policies that are cognisant of implications of restrictions on international data transfers for digital trade. A specific dimension worth considering is the potentially disproportionate impact of such restrictions on small and medium enterprises (**SMEs**) and start-ups. The Internet has enabled SMEs and start-ups to take

[2] Ministry of External Affairs, Joint Statement on India-UK Virtual Summit (Roadmap 2030 for a Comprehensive Strategic Partnership), May 4, 2021, available at: https://mea.gov.in/bilateral-documents.htm?dtl/33837/Joint_Statement_on_IndiaUK_Virtual_Summit_Roadmap_2030_for_a_Comprehensive_Strategic_Partnership (last accessed on October 20, 2021).

[3] *See* M. Ferracane, E. Marel, *Regulating Personal Data: Data Models and Digital Services Trade,* Background Paper, World Development Report 2021, World Bank Group, March 2021, available at https://openknowledge.worldbank.org/bitstream/handle/10986/35308/Regulating-Personal-Data-Data-Models-and-Digital-Services-Trade.pdf (last accessed on October 20, 2021).

part in cross-border commerce and serve as (what some have called) "micro-multinationals" firms that are born global.[4] India and UK are among the world's largest start-up ecosystems.[5] Over the long-term, both countries can benefit from connecting each other's SME and start-up ecosystems and from enabling their participation in bilateral digital trade. A common objective of enabling unimpeded international data transfers may be seen as valuable from this perspective as well.

Against this backdrop, we congratulate the decision of Governments of India and the United Kingdom to negotiate a Free Trade Agreement (**FTA**).[6] We note that the FTA negotiations begin at a time when both governments are reviewing their existing legal regimes on the protection and cross-border transfers of personal information. Currently in India, a Joint Parliamentary Committee (**JPC**) is reviewing a draft of a comprehensive new law - the Personal Data Protection Bill of 2019 (**PDP Bill**).[7] The UK has recently announced the decision to take its current framework on data regulation in '*a new direction'.* It has released a consultation paper considering several reforms needed to secure a '*pro-growth and trusted data regime*' (**DCMS 2021 Consultation**).[8]

The FTA negotiations, taking place alongside these domestic reform exercises, present a unique opportunity for both governments to establish a visionary approach at both the bilateral and domestic level. We urge both governments to capitalise on this opportunity and mutually establish an approach to data regulation that moves beyond seeing unimpeded international data transfers and the protection of personal information as mutually exclusive. They may also firmly recognise that data protection regimes – even if predicated upon different approaches - may look to find common ground and encourage compatible frameworks to international data transfers.

In this position paper, we offer recommendations to both governments that set out the elements of such a future-oriented approach. In Section B, we suggest how both governments may embed these elements in an India-UK FTA. Thereafter, in Section C, we offer suggestions on their data protection regimes. In Section D, we conclude by shifting to a long-term perspective and discussing how we can work towards building an India-UK data adequacy partnership.

---

[4] *See* S. Lund, J. Manyika, *How Digital Trade is Transforming Globalisation,* E15 Initiative, International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum, January 2016, available at https://e15initiative.org/wp-content/uploads/2015/09/E15-Digital-Lund-and-Manyika.pdf (last accessed on October 20, 2021).

[5] London (ranked second) and Bengaluru (ranked twenty-third) both figure in the top thirty global start-up ecosystems, while Mumbai ranks at the top as an emerging global start-up ecosystem. *See* Startup Genome LLC, *The Global Startup Ecosystem Report 2021,* September 2021, available at: https://startupgenome.com/reports/gser2021 (last accessed on October 20, 2021).

[6] India UK Virtual Summit, Prime Minister's Office, Press Information Bureau, Government of India, May 4, 2021, available at: https://pib.gov.in/PressReleseDetail.aspx?PRID=1715968#:~:text=As%20part%20of%20the%20ETP,jobs%20in%20both%20the%20countries (last accessed on October 20, 2021).

[7] *See* the Personal Data Protection Bill of 2019, available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf (last accessed on October 20, 2021).

[8] Department for Digital, Culture, Media & Sport, *Consultation on data: a new direction,* September 10, 2021, available at: https://www.gov.uk/government/consultations/data-a-new-direction (last accessed on October 20, 2021).

Section B
Recommendations for an India-UK FTA

With respect to the FTA, we start with three desired outcomes from both governments:

I. Establish robust legal regimes on the protection of personal information in accordance with internationally accepted principles and guidelines.[9]

II. Not prohibit or unduly restrict businesses from transferring information, including personal information, by electronic means across borders.

III. Ensure that rules that impact cross-border information transfers, are precise, non-discriminatory, and designed in a proportionate manner tied to legitimate public policy objectives.

Similar outcomes are already embedded in existing trade agreements executed by the UK with other countries, such as in those on electronic commerce contained in the UK-Japan Comprehensive Economic Partnership Agreement (**CEPA**).[10] Our members encourage the UK to advance the progress made in the CEPA into its FTA negotiations with India.

We recognise that the national priorities and strategic interests of different governments can vary. There can be scenarios where governments may seek to introduce data regulations with conditions on international data transfers or mandate for domestic location of computing facilities.[11] In India, for example, regulators for the financial services industries have already required financial service providers to store specific categories of information, such as data relating to payment systems[12] or records of insurance policies and claims[13], on computing facilities located only in India. These requirements are presumably introduced with the objective of ensuring continued access to information required for supervising those industries. However, it is important that introduction of such requirements is accompanied with appropriate guidance explaining that the required access would not have been guaranteed through less restrictive means. Governments may also seek to introduce such conditions/ mandates for the purposes of government procurement, or for the purposes of storing or processing information relating to the State.

---

[9] For examples of such principles, *see* the OECD Privacy Framework of 2013 available at: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf; the APEC Privacy Framework of 2015 available at: https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015) (last accessed on October 20, 2021).

[10] *See* Article 8.84 and 8.85 on "location of computing facilities", CEPA available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/929181/CS_Japan_1.2020_UK_Japan_Agreement_Comprehensive_Economic_Partnership__v1.pdf (last accessed on October 20,2021).

[11] By the term '*computing facilities*', we refer to computer resources, including servers or storage devices, that may be used for processing or storing information for commercial use.

[12] *See* RBI Directive on Storage of Payment Systems Data issued under Sections 10(2) read with Section 18 of the Payment and Settlement Systems Act, 2007 available at: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244

[13] *See* Regulation 3(9), IRDAI (Maintenance of Insurance Records) Regulations, 2015 available at: https://www.irdai.gov.in/admincms/cms/frmGeneral_Layout.aspx?page=PageNo2604&flag=1

We recognise that such requirements can be imposed in furtherance of such legitimate objectives. From the perspective of the FTA, we suggest that such legitimate objectives be well-defined and cast within a set of clear principles.

Keeping in mind the above, we offer below specific recommendations for the FTA. We refer to each government as "**Party**" and both together as "**Parties**".

1. Dedicated chapter on digital trade or on electronic commerce may be included in the FTA. Amongst other issues, the chapter may include articles requiring a robust legal regime on the protection of personal information, international data transfers and location of computing facilities. To make early progress, we submit that these may also be included in the proposed Early Harvest Agreement scheduled for March 2022.[14]

2. Articles on the protection of personal information may impose obligations on Parties to:

   2.1. Recognise the dual importance of the protection of personal information for the digital economy and for facilitating digital trade.
   2.2. Adopt or maintain a comprehensive legal regime on the protection of personal information that accounts for globally accepted principles and guidelines and that each Party may consider adequate.
   2.3. Ensure that all users of digital trade are afforded protection of their privacy and access to remedies against violations occurring within their territories equally and in a non-discriminatory manner, irrespective of the residence of those users.
   2.4. Ensure that information on the requirements and regulatory mechanisms under the legal regime for personal information protection are made easily accessible to the public, including on how businesses may comply and how individuals may pursue remedies.
   2.5. Ensure that any measures introduced to protect personal information or personal privacy are not used as an indirect method to impose sector-specific requirements that conflict with the principles set out in clause 5 below.
   2.6. Develop mechanisms that promote the compatibility or interoperability of their data protection regimes. Such mechanisms may include, for example, privacy certification schemes or codes of practice.

3. Articles on international data transfers may impose obligations on Parties to:

   3.1. Recognise that each Party may have its own regulatory requirements regarding the transfer of information by electronic means.
   3.2. Allow the cross-border transfer of information by electronic means, including personal information, when this activity is in furtherance of conducting business.
   3.3. Recognise that each Party may be afforded an exception to adopt or maintain measures inconsistent with clause 3.2., where such measures are for the purposes of government

[14] R. Jayaswal, *Free trade pact: India-UK to sign early harvest deal by March 2022,* the Hindustan Times, September 15, 2021, available at https://www.hindustantimes.com/business/indiauk-to-sign-early-harvest-deal-by-march-2022-101631618015781.html (last accessed on October 20, 2021).

procurement or for the storing or processing of information by, or on behalf of, a Party, or for the Party to impose measures related to that information.

3.4. Recognise that each Party may be afforded, in addition to the exception under clause 3.3., an exception to adopt or maintain measures inconsistent with clause 3.2., but only if all the following conditions are met:

3.4.1. The measure is intended to achieve a legitimate public policy objective.

3.4.2. The measure is not applied in an arbitrary or unjustifiably discriminatory manner or does not amount to a disguised trade restriction.

3.4.3. The measure does not impose restrictions that are greater than as required to achieve the objective.

4. Articles on the location of computing facilities may impose obligations on Parties to:

4.1. Recognise that each Party may have its own regulatory requirements regarding the use of computing facilities.

4.2. Not to require businesses to use or locate computing facilities in the territory of a Party as a condition for conducting business in that territory.

4.3. Recognise that each Party may be afforded an exception to adopt or maintain measures inconsistent with clause 4.2., where such measures are for the purposes specified in clause 3.3., or where such measures meet all the conditions under clause 3.4. above.

5. Articles on specific sectors, if included in the FTA (such as those for the financial sector), may ensure that the rules for such sectors are substantially equivalent as those generally applicable to international data transfers or to the location of computing facilities. If Parties seek to impose requirements for domestic location of computing facilities for specific sectors, then such measures may be adopted only if all the following conditions are met:

5.1. The measure is intended for the objective of securing sufficient and timely access to information to regulators for monitoring, regulation, or supervision in cases where such access is otherwise not guaranteed.

5.2. The measure may be imposed only after affected service providers are provided reasonable opportunities to remediate any lack of access to the necessary information.

5.3. The measure does not impose restrictions that are greater than as required to achieve the objective.

5.4. The measure may only be imposed by a regulator or a Party on a service provider located in the territory of the other Party after the latter Party or its relevant regulator is consulted.

Section C
Recommendations towards mutual interoperability of transfer regimes

India and the UK are two of the world's largest economies. By introducing an FTA with the commitments and obligations outlined in Section B, they can deliver a powerful example for building a multilateral consensus on the future direction for international data regulation. From this perspective, the UK-India FTA can have not just bilateral, but global implications.

However, setting such an example is best achieved if both governments also work towards reflecting those commitments and obligations in their domestic legal regimes. By building on our recommendations on the FTA in Section B, both governments can take steps towards establishing mutually compatible regulatory regimes.

We note that the governments of India and the UK are at different points in their journey to reform their domestic legal regimes for the protection of personal information. Even though the PDP Bill and current UK data protection laws share several principles and frameworks in common, a key area where the two regimes differ is that of the regimes for international data transfers. We consider this area to be a valuable starting point for both governments to consider alignment on. In this context, we offer the following recommendations:

1. Recommendations to the Government of the UK: We encourage the UK Government to explore avenues for enabling international data transfers to take place between India and the UK, particularly through transfer tools that can operate at a sectoral level. In this regard, we agree with a recent consultation paper from the UK Government that notes that transfer mechanisms under the current UK data protection law can be made more practical and flexible for organisations to utilise.[15] In this regard, we offer the following suggestions:

    1.1. **Two transfer tools – certification schemes and codes of practice – may be leveraged as equally viable alternatives to standard contractual clauses (SCCs).** Currently, SCCs are the most used transfer tool and operate at the level of individual organisations. However, the UK GDPR also recognises the possibility of using certification schemes and codes of conduct as transfer mechanisms. These are valuable alternatives to SCCs that may be framed by industry associations or sectoral groups to define data protection rules at the sectoral level.[16] We support leveraging these transfer tools to enable the information technology sectors in the UK and India to build a safe corridor to share data across borders. In this regard, we welcome the proposals in the DCMS 2021 Consultation aimed at introducing a more flexible approach to certifications and encourage the UK Government to similarly explore codes of conduct to enable future international data transfers. We also welcome the proposal to permit the accreditation of overseas certification bodies to run UK-approved international transfer schemes. We

[15] *See* DCMS 2021 Consultation, *supra* note 8 at page 94.
[16] *See* DCMS 2021 Consultation, *supra* note 8 at page 98; *also see* European Data Protection Board, *Guidelines 04/2021 on codes of conduct as tools for transfers,* July 7 2021, available at https://edpb.europa.eu/system/files/2021-07/edpb_guidelinescodesconducttransfers_publicconsultation_en.pdf (last accessed on October 20, 2021).

encourage the UK Government to adopt criteria that support Indian certification bodies to participate in such a scheme.

1.2. **Organisations may be permitted to create or identify their own transfer tools.** We endorse an approach which maximises the flexibility available to organisations in relation to meeting transfer conditions and using transfer tools. We therefore welcome the proposal from the UK Government to permit organisations with complex data transfer requirements to design and use bespoke contracts to enable international data transfers. This has much potential for encouraging international data transfers. However, we would recommend that the UK Government and the ICO set out the minimum expectations to be met by organisations seeking to explore this route. This may be set out in accompanying ICO guidance in the event this proposal is accepted.

2. Recommendations to the Government of India: The current framework for international data transfers under the PDP Bill[17] shall also benefit from modifications to improve its compatibility with the regimes in other countries. In this regard, we offer the following suggestions:

2.1.1. **The approach to imposing conditions on international data transfers may not be more restrictive than necessary.** The following reforms may be examined:

2.1.1.1. The list of data categories being considered as "sensitive personal data" may be narrowed to exclude official identifiers and financial data and to limit the scope of the definition of health data to data about the health condition of a person. This is to ensure that organisations are not handicapped from meeting regulatory requirements or routine business needs, such as employee onboarding or customer management, that necessitate the collection of such data on a routine basis.

2.1.1.2. The concept of 'critical personal data' may be refined by introducing clear parameters and standards of 'criticality' that are closely linked to requirements of national security.

2.1.1.3. Instead of imposing a local storage requirement by default with respect to sensitive and critical personal data, the Bill may permit the use of transfer tools to assess the risk of, and thereupon permit, transferring such data to overseas territories. Additional safeguards may be adopted for the transfer of 'critical personal data'. These improvements may help grow cross border trade while meeting the Government's "legitimate public policy objective", in a relatively transparent manner.

2.1.1.4. The requirement for seeking an additional express prior consent for any international data transfer involving sensitive personal data is likely to present certain unintended outcomes. Given that express prior consent is required to process sensitive personal data, the need to collect an additional round of consent for one aspect of processing – a transfer to an overseas territory – may

[17] *See* Sections 33 and 34, PDP Bill, *supra* note 7.

not afford an additional protection to the consumer. Instead, this may unnecessarily burden data principals and increase the potential for consent fatigue. We also note that this consent requirement is sought to be applied even for international data transfers to territories deemed adequate by the Government of India. This would create a situation where data principals must still consent to an international data transfer to territories with data protection regimes that their government considers as providing an equivalent level of data protection as their own. This has the potential to undermine the value of an adequacy decision by the Government of India. Given this, the requirement of this additional may be reviewed.

2.1.2. **The current available set of transfer mechanisms may be expanded in line with international practice.** The Government of India may consider formally recognising additional transfer mechanisms, such as certifications and codes of conduct, under the scheme of the Bill. This would bring the Bill in line with the data protection regimes in other jurisdictions including the UK GDPR. The design and operation of such additional transfer mechanisms may draw from international frameworks (such as under the APEC Cross Border Privacy Rules) or from data protection regimes of other governments (including those currently provided for in the UK data protection law or in the EU GDPR). We note here that the Bill does recognise the potential for this – by recognising that the Authority may draw up codes of practice for the purposes of international data transfers[18] – but does not correspondingly reflect this in the specific provisions governing international data transfers.

2.1.3. **The framework to exempt data processors dealing with foreign nationals' data may be afforded greater certainty and enablement.** We appreciate the fact that the PDP Bill explicitly recognises the need for such an exemption.[19] However, there is scope to better clarify the manner of its operation. Currently, even with this exemption, the Bill may still require Indian data processors personal data of foreign nationals from having to comply with the restrictions on retaining personal data,[20] on transferring data to overseas territories,[21] on not processing biometric data[22] and on having to comply with access requests for non-personal data from the Government of India.[23] These can lead to conflicts with contractual obligations binding those Indian data processors in their contracts with overseas data fiduciaries. To preclude

[18] *See* Section 50(q), the PDP Bill, *supra* note 7.
[19] Section 37, the PDP Bill, *supra* note 7, which states:

> 37. *Power of Central Government to exempt certain data processors.*
> *The Central Government may, by notification, exempt from the application of this Act, the processing of personal data of data principals not within the territory of India, pursuant to any contract entered into with any person outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law.*

[20] *See* Section 9, the PDP Bill, *supra* note 7.
[21] *See* Sections 33 and 34, the PDP Bill, *supra* note 7.
[22] *See* Section 92, the PDP Bill, *supra* note 7.
[23] *See* Section 91, the PDP Bill, *supra* note 7.

these, the existing exemption may explicitly incorporate upfront exemptions from these provisions. In addition, it may also permit the Government of India to issue notifications exempting Indian data processors processing the personal data of foreign nationals from the operation of any other provisions of the Bill to prevent conflicts with obligations being imposed on such data processors by the personal data protection regimes applicable to the personal data of those foreign nationals or to the relevant processing operation.

2.1.4. **The grounds for processing sensitive personal data may also incorporate reasonable purposes.** We note here that an overly restrictive approach to restricting the grounds of processing can have the unintended effect of impeding international data transfers for routine purposes. The Bill only recognises explicit consent as a valid legal basis for processing sensitive personal data.[24] However, businesses may also need to process sensitive personal data for reasonable purposes in scenarios where the collection of consent may not be possible or practical – such as for the purposes of complying with a court order, where the relevant data principal that may be unwilling to provide such consent. To this end, we submit that the grounds for processing sensitive personal data may be expanded to include some reasonable purposes for which consent is not required. Such purposes may include processing to comply with the law and with orders from judicial or quasi-judicial bodies; for the purposes of emergencies; or for recruitment and employment purposes.

[24] *See* Sections 13 read with 11 and 12, the PDP Bill, *supra* note 7.

Section D
Setting the stage for a data adequacy partnership

We note that the UK Government has recently listed India as a priority destination for a future data adequacy partnership.[25] We consider this expression of intent to create a corridor for both countries to engage in free and open international data transfers as highly valuable and would welcome the opportunity to assist the UK Government in building such a partnership.

We also note that the process of concluding adequacy decisions and partnerships have, in the past, taken a significant amount of time. However, the UK Government has a unique opportunity to set forth its expectations from an adequacy perspective to the Government of India at a time when the latter is transitioning to a more comprehensive data protection regime. This is especially significant considering that the UK Government has signalled its intent to approach adequacy assessments with "*a focus on risk-based decision-making and outcomes"* and to chart its own course on adequacy assessments.[26]

Considering that the timing of the FTA negotiations aligns well with the intent to approach adequacy assessments with a fresh perspective, **we encourage the UK Government to leverage the FTA negotiations to kick-start the conversation on a data adequacy partnership.** The FTA negotiations could be leveraged to initiate the 'gatekeeping stage' outlined in its recent consultation paper.[27] The UK Government may also, for instance, set out the technical assessment criteria as well as the real-world outcomes and practices it considers relevant to determining how other countries achieve a high standard of data protection.

In the Indian context, the Government of India has an opportunity to leverage the FTA as a starting point to establishing a data adequacy partnership. By incorporating the changes suggested in this paper, and enacting the PDP Bill so revised, the Government of India can take a timely step towards leveraging the benefits of commitments on digital trade in the FTA. **We encourage the Government of India to enact the PDP Bill with the suggested modifications soon.**

The PDP Bill shall be a key step forward for the Indian legal system in relation to adequacy assessments by other governments. However, such assessments shall also involve examinations of India's surveillance regime since this has equal bearing on the protection of personal information. Here, a recent study by NASSCOM is instructive.[28] It finds the Indian regime to be

---

[25] *See* Department for Digital, Culture, Media & Sport, *Guidance on international data transfers: building trust, delivering growth and firing up innovation,* August 26, 2021, available at: https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation (last accessed on October 20, 2021).

[26] *See* DCMS 2021 Consultation, *supra* note 8 at page 89.

[27] *Id.*

[28] *See* NASSCOM, *Implications of Schrems II on EU-India Data Transfers,* August 2021, available at: https://community.nasscom.in/sites/default/files/blog/attachments/202108_NASSCOM_schremsIIStudyFinal.pdf (last accessed on October 20, 2021).

broadly favourable to an adequacy assessment and highlights a few laws that can benefit from a review from a lens of adequacy assessments by other countries.[29]

The study also suggests narrowing the scope of existing provisions in the PDP Bill that vest broad powers with the Central Government to exempt Government agencies from the application of the provisions of the Bill. These provisions may be based on legitimate state objectives of national security. This is likely to enhance the overall evaluation vis-à-vis adequacy with the EU. In sum**, the Government of India may take steps to prepare for future adequacy partnerships.**

On behalf of our members, we at techUK, UKIBC and NASSCOM appreciate this opportunity to present our recommendations via this submission to both governments on the UK-India FTA negotiations from a digital trade perspective.

The focus of this submission was on examining the issue of international data transfers as a component of any chapter on digital trade that may be included in the FTA. We also sought to offer suggestions on connected efforts to establish data regulations in the interest of aligning commitments at the international level with rules at the domestic level.

To briefly reiterate, in this submission, we presented that if we want to achieve a mutual target of doubling bilateral trade between India and the UK, then we could leverage the upcoming FTA to commit to measures aimed at enabling international data transfers. These may form part of early harvest discussions and may be followed up by efforts to build a data adequacy partnership in due course.

It is hoped this submission is of value to both governments in their bilateral negotiations. It is our intent to follow up this submission with additional works aimed at enabling bilateral digital trade and at examining further avenues for both countries to align their approach to regulating data.

Please contact us at any time with any questions or comments you may have. [insert contact details].

[29] *Id.*