UKIBC – techUK- NASSCOM

Joint Position Paper on Enabling Data Transfers for India-UK Digital Trade

May 2022

*We respectfully submit this joint position paper on enabling data transfers between India and the United Kingdom (**UK**) to deepen their digital trade relationship. To this end, we offer recommendations for both nations to consider when negotiating the India-UK Free Trade Agreement and to help inform their efforts to reform domestic regimes on personal data protection and data transfers or to engage in discussions on data adequacy.*

---

techUK is a not-for-profit industry association for the technology sector in the UK. It aims to prepare and empower the UK for what comes next, delivering a better future for people, society, the economy, and the planet. Established in 2013, techUK has over 850 members in the UK.

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

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.

Section A
Introduction: Digital Trade and the India-UK FTA

As representatives for the information technology sectors in India and the UK, we congratulate the recent decision of both governments to negotiate a Free Trade Agreement (**FTA**).[1] This has put us on a course towards unlocking the full potential of our bilateral trade relationship and achieving the ambitious target, set by both nations, of doubling India-UK trade by 2030.[2]

Designing an FTA for the world of 2022 and beyond requires a forward-thinking approach to trade. In the modern global economy, which is characterised by hyperconnectivity and increasing reliance on digital technologies, this necessarily means accounting for digital trade – a phenomena that has expanded to not just cover online sale of goods and services but also a wide range of economic activities that constitute the digital economy.[3]

Given the global nature and future potential of digital trade, an impetus towards convergence on regulatory policies is desirable. In some areas, such as the recognition of electronic commerce,[4] much progress has been made in terms of arriving at an internationally accepted baseline.[5] In others, such as the protection of personal data or the regulation of international data flows, there is tremendous scope for harmonisation and co-operation between nations. Achieving this is crucial to avoid the unintended effect of regulatory uncertainty and inconsistencies, viz., dampening trade and investment, ultimately leading to suboptimal economic outcomes for consumers and nations.

India and the UK are two of the world's most digitally evolved economies and hosts to the world's leading digital service suppliers. India-UK tech trade goes back a long way. Indian tech industry has invested in the UK in many ways, such as by employing and upskilling the local talent. There are over 100 UK-based Capability Centres in India leveraging India's digital talent, innovation capabilities and scale to drive enterprise competitiveness and solving complex problems. Both

---

[1] 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 May 6, 2022).

[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 May 6, 2022).

[3] There is no single accepted definition of "digital trade". For this paper, we adopt the following understanding: that it *"encompasses digitally enabled transactions in trade in goods and services which can be either digitally or physically delivered and which involve consumers, firms and governments".* See J. Lopez-Gonzalez, M. Jouanjean, *Digital Trade: Developing a Framework for Analysis*, OECD Trade Policy Papers, No. 205, 2017, available at: https://www.oecd-ilibrary.org/trade/digital-trade_524c8c83-en (last accessed on May 6, 2022).

[4] The terms 'electronic commerce' and 'digital trade' have been used interchangeably in this paper.

[5] *See* the UNCITRAL Model Law on Electronic Commerce, (1996) adopted by the General Assembly of the United Nations by resolution A/RES/51/162 dated January 30th, 1997 available at: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf (last accessed on May 6, 2022).

India and UK are among the world's largest start-up ecosystems.[6] Over a long-term, both countries can benefit from connecting each other's start-up and Small and Medium Enterprise (**SME**) ecosystems and from enabling their participation in bilateral digital trade. Considering this, we believe that an imperative for both governments is to leverage the FTA to build a shared approach to digital trade.

Accordingly, **we recommend the inclusion of a dedicated digital trade chapter in the proposed FTA.** Such a chapter may cover several topics, including protection of privacy and personal information, international data flows, paperless trading, electronic signatures, electronic contracts, source code disclosure, online consumer protection, unsolicited commercial communications, cooperation on fintech, data innovation and artificial intelligence. We believe both governments are ready to, and would benefit from, adopting a forward-thinking approach. Through a series of submissions, we intend to offer suggestions on these and other topics on digital trade to both governments as they negotiate the FTA.

The rest of this paper serves as the first in that series. It focuses on two areas of digital trade related regulation that industry and nations consider as priorities: the protection of personal data and the regulation of international data flows. Digital trade is inextricably linked to the exchange of information, and hence a regime for data transfers along with protection of personal information is crucial. We begin by offering recommendations in *Section B* below on potential commitments on these areas in the proposed FTA.

Notably, the FTA negotiations are expected to run in parallel with efforts by both governments to review their domestic legal regimes governing these areas. At the time of writing, in India, the Ministry of Electronics and Information Technology (**MEITY**) is currently considering the latest iteration of a comprehensive draft data protection law, the Data Protection Bill of 2021 (**DPB 2021**)[7] that has been released by a Joint Parliamentary Committee (**JPC**) that was reviewing an earlier version called the Personal Data Protection Bill of 2019 (**PDP Bill**).[8] The DPB 2021 may soon be tabled in Parliament for its passage. The UK has also recently concluded a consultation process on taking its current framework on data regulation in '***a new direction'*** by considering several reforms needed to secure a '*pro-growth and trusted data regime*' (**DCMS 2021 Consultation**).[9] Further, the UK has also set up an Expert Council on International Data Transfers

[6] 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 May 6, 2022).

[7] *See* the (Draft) Data Protection Act of 2021 contained in the Annexure in the Report of the Joint Parliamentary Committee on the Personal Data Protection 2019, available at http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf (last accessed on January 24, 2022).

[8] *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 May 6, 2022).

[9] 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 May 6, 2022).

that shall look to reduce barriers to cross-border flows and promote a risk-based, trust-focused approach to international data transfer policy.[10]

We consider these parallel exercises as being timely. They afford an opportunity for both nations to arrive at a shared approach at the international level and reflect that in their domestic legal regimes, thereby taking steps towards building mutually compatible legal approaches in these two areas. Therefore, in *Section C*, we offer suggestions on the domestic data protection regimes of India and UK respectively. In *Section D*, we conclude by shifting to a long-term perspective and discussing the path towards an India-UK data adequacy partnership.

[10] *See* Department for Digital, Culture, Media & Sport, *International Data Transfers Expert Council*, January 25 2022 available at https://www.gov.uk/government/news/global-data-experts-fire-up-governments-plans-to-promote-free-flow-of-data (last accessed on May 6, 2022).

Section B
Recommendations: Potential Commitments on Data in an India-UK FTA

International data flows enable businesses operating at all scales to take part in global markets and supply chains. They make it possible to offer services across borders or engage in digital trade. By transferring data over the internet, start-ups and SMEs can take part globally and become "micro-multinationals".[11] Several new technologies need access to data located in more than one territory. Examples include cloud computing, outsourcing of services, or artificial intelligence.[12] We hope to include more information on the impact on industry of potential data commitments including restrictions on cross-border transfer of data, based on the results of a survey being undertaken by us.

The impact of the COVID-19 pandemic has underlined the importance of international data flows. As the United Nations Conference on Trade and Development (**UNCTAD**) recently noted, restrictions on movement induced by the pandemic triggered a dramatic rise in electronic commerce, increasing the share of online retail sales of total retail sales from 16% to 19% in 2020.[13] This accelerated an upward trend that was already underway. Before the pandemic, global electronic commerce sales had increased the year before to $26.7 trillion in 2019 up by 4% from 2018. The bulk of this value (82%) was contributed by business-to-business sales.[14]

Considering the above, policies that unduly restrict international data flows are likely to inhibit digital trade. In recent years, governments have increasingly started considering policies and rules aimed at impacting international data flows as necessary to uphold their domestic data protection regimes. However, it is not necessary to presume that international data flows must be at odds with privacy and data protection imperatives.

A recent paper from the World Bank is instructive.[15] It finds that trading partners looking to bolster bilateral trade in digital services should look to adopt a shared approach to the regulation of personal data processing and international data flows. Such an approach should combine a regime with few or no restrictions on international data flows along with strong domestic safeguards for the protection of personal data. This could enable safe processing of data in either jurisdiction while allowing it to move between those jurisdictions. Such a

[11] *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 May 6, 2022).
[12] *See* J. Lopez-Gonzalez, M. Jouanjean*, supra* note *3.*
[13] *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 May 6, 2022).
[14] *See* UNCTAD, 'Global e-commerce jumps to $26.7 trillion, COVID-19 boosts online sales', May 3 2021, available at https://unctad.org/news/global-e-commerce-jumps-267-trillion-covid-19-boosts-online-sales (last accessed on May 6, 2022).
[15] *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 May 6, 2022).

combination can potentially bolster such bilateral trade in digital services without either jurisdiction having to compromise on data protection safeguards.

For India and the UK, this suggests that both countries stand to gain from adopting such a shared regulatory approach. This could be achieved by including commitments in a dedicated digital trade chapter under the FTA that are aimed at the following desired outcomes:

I. Establish robust legal regimes on the protection of personal data in accordance with internationally accepted principles and guidelines.[16]
II. Not prohibit or unduly restrict businesses from transferring data, including personal data, by electronic means across borders.
III. Ensure that rules impacting international data flows are tied to legitimate public policy objectives and are precise, non-discriminatory, and proportionately designed.
IV. Ensure that rules for specific sectors impacting international data flows are substantially equivalent to the principles set out in the rules on digital trade.

Similar outcomes are already embedded in existing trade agreements being executed by different trading partners across jurisdictions. We provide an illustrative list of such trade agreements in Annexure I below. A notable example is the UK-Japan Comprehensive Economic Partnership Agreement (**CEPA**).[17] We encourage the UK to advance the progress made in the CEPA into its FTA negotiations with India.

Keeping in mind the above, we offer below recommendations on specific articles that may be considered for inclusion in the FTA. To make early progress, we submit that these may also be included in the proposed Early Harvest Agreement scheduled for March 2022.[18] We refer to each government as "**Party**" and both together as "**Parties**". We also use the term "information" to refer to the concept of data, thus adopting the approach followed in the CEPA.

1. <u>Commitments on the protection of personal information</u>

We encourage both governments to commit to the protection of personal information as a key regulatory priority in the digital economy. FTA should include commitments to do so via a comprehensive legal regime that either government may consider adequate. Beyond this, such articles should also include commitments to ensure citizens of both Parties are afforded equal access to protections and remedies under, and adequate information on the operation of, such legal regimes. Both Parties should also ensure these legal regimes form the baseline across sectors. Suggested text to these ends is in Table 1.

[16] 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 May 6, 2022).
[17] *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 May 6, 2022).
[18] 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 May 6, 2022).

Table 1: Articles on the Protection of Personal Information

1. Protection of personal information. *Parties shall:*

1.1. Recognise the importance of the protection of personal information for the digital economy and for facilitating digital trade.

1.2. 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.

1.3. 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.

1.4. 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.

1.5. Develop mechanisms that promote the compatibility or interoperability of their regimes for personal information protection. Such mechanisms may include, for example, privacy certification schemes or codes of practice.

1.6. Cooperate on the protection of personal information. Such cooperation may include technical assistance in the form of exchange of information and experts and the establishment of joint programmes and projects.

2. Commitments on international data flows and location of computing facilities

International data flows become onerous on account of measures that mandate conditions on transferring data across borders or that require the domestic location of computing facilities.[19]

Therefore, it is suggested that the governments consider measures that are least onerous while pursuing legitimate objectives. Examples of such objectives can include processing of personal information for the purposes of national security requirements, government procurement, the protection of consumers' privacy, etc.

In other cases, such measures may be introduced for ensuring the continued access to information required for regulators to supervise certain industries. 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

[19] 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.

systems[20] or records of insurance policies and claims[21], on computing facilities located only in India.

Such measures aimed at the pursuit of legitimate objectives should be cast within a principled framework. This is to ensure that they are not excessively restrictive and that the design, introduction, and operation of such measures does not take place in an arbitrary, uncertain, or discriminatory manner. Beyond this, both governments may consider recognising a general set of principles – of permitting international data flows and not requiring the local storage or processing of data. Suggested text to these ends is in Table 2.

Table 2: Articles on international data flows and location of computing facilities

2. ***International data transfers.*** *Parties shall:*

2.1. Recognise that each Party may have its own regulatory requirements regarding the transfer of information by electronic means.

2.2. Allow the cross-border transfer of information by electronic means, including personal information, when this activity is in furtherance of conducting business.

2.3. Recognise that each Party may be afforded an exception to adopt or maintain measures inconsistent with clause 2.2., where such measures are for the purposes of government 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.

2.4. Recognise that each Party may be afforded, in addition to the exception under clause 2.3., an exception to adopt or maintain measures inconsistent with clause 2.2., but only if all the following conditions are met:

2.4.1. The measure is intended to achieve a legitimate public policy objective or national security or strategic interests.

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

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

3. ***Location of computing facilities.*** *Parties shall:*

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

[20] *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

[21] *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

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

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 specified in clause 2.3., or where such measures meet all the conditions under clause 2.4. above.

3. Commitments in relation to specific sectors

The above commitments, which would be included in a dedicated chapter on digital trade, would operate horizontally. However, articles may be included in trade agreements for specific (and often highly regulated) sectors, such as the financial or telecommunications sectors. If this route is adopted for the FTA, then both governments should ensure that rules for such sectors impacting international data flows are substantially equivalent to those generally applicable to international data flows or to the location of computing facilities. Any exemptions for specific sectors vis-à-vis horizontal rules should only be adopted in accordance with well-defined principles. Suggested text to these ends is in Table 3.

Table 3: Articles in relation to specific sectors

4. Articles in relation to specific sectors. *Parties shall:*

4.1. 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 below.

4.2. Measures impacting international data transfers or requiring the location of computing facilities may only be adopted if all the following conditions are met:

4.2.1. 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.

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

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

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 outlined in Section B, we believe 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, such an example is best set if both governments also work towards reflecting such commitments in their domestic legal regimes and delivering mutually compatible rules.

The governments of India and the UK are at different points in their journeys to reform their domestic legal regimes on personal data protection and international data flows. The DPB 2021 in India and the current UK data protection laws do share much in common. However, there are several differences in their respective regimes for international data flows. This area is a valuable starting point for both governments to consider for convergence. 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 flows to take place between India and the UK. We welcome these initiatives and hope to engage deeply with the UK Government on international data transfer policy in the coming months. We offer the following suggestions as starting points for further discussion:

    1.1. **A risk-based understanding of a 'restricted transfer' should be developed.** We believe that, with the constitution of the Expert Council on International Data Transfers, the UK has a key opportunity to frame a modern understanding of what a 'restricted transfer' is.

    At present, this concept is not given a formal legal definition under the UK GDPR. As a result, it can be difficult to determine its scope and meaning. So far, we have only seen a one-size-fits-all approach, where this concept captures a wide range of processing operations without distinction, regardless of the technical or practical risks across different operations.

    For example, in the context of the EU GDPR, the European Data Protection Board (**EDPB**) has continuously stated that 'remote access' is a form of transfer but has never offered much guidance on the meaning of 'remote access' or why the physical hosting location of personal data is irrelevant to the concept of a restricted transfer.[22]

[22] For instances where "remote access" is discussed in the context of international data transfers, *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 ; 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 .

If personal data continues to be hosted on a server within UK, and an overseas processor connects to that server over a network, then, we submit, that a risk-based approach would factor in the absence of any actual transmission of personal data, and then test for other risk factors to determine whether such a case should be regarded as a restricted transfer. Currently, such a risk-based evaluation does not take place, thereby ignoring the potential for security safeguards, such as technical restrictions to prevent personal data from being exported or downloaded by that overseas processor or to prevent the personal data from being compromised in transit, to act as mitigating factors.

We have seen that, in the past, the UK Information Commissioner's Office (**ICO**) has, in its guidance, offered examples of '*restricted transfers*' that indicate a more pragmatic risk-based approach to interpreting international data transfer restrictions. For example, the ICO notes that "*transfer does not mean the same as a transit*", thereby excluding scenarios where personal data merely moves through different jurisdictions *en route* to its destination.[23] This is an understanding informed by technical considerations and is worth building upon. Scenarios posing less risk where sufficient security safeguards are installed may not be regarded as restricted transfers at all, or, alternatively, be regarded as scenarios meriting simpler transfer tools.

1.2. **The set of transfer mechanisms should be expanded to include certification schemes and codes of practice.** 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 developing certification schemes and codes of conduct that can also function as viable transfer mechanisms. These are valuable tools that may be framed by industry associations or sectoral groups to define data protection rules at the sectoral level.[24] In this regard, we welcome the proposals in the DCMS 2021 Consultation aimed at making transfer mechanisms more practical and flexible, including by introducing a more flexible approach to certifications and encourage the UK Government to similarly explore codes of conduct to enable future international data flows.[25] We support an approach whereby transfer mechanisms can operate at a sectoral level – making transfers to specific sectors in other territories possible (for example, HR data, data used to identify financial fraud, etc.). Such an approach can be leveraged to enable the information technology sectors in the UK and India to build a safe corridor to share data across borders. We also welcome the proposal to permit the accreditation of overseas

[23] In its guidance on restricted transfers, the ICO offers the following 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. *See*, ICO, *Guide to the GDPR*, (2021) 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/

[24] *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 May 6, 2022).

[25] *See* DCMS 2021 Consultation, *supra* note 8 at page 94.

certification bodies to run UK-approved international transfer schemes. We recommend the UK Government to adopt criteria that support Indian certification bodies to participate in such a scheme.

2. Recommendations to the Government of India: The current provisions in DPB 2021 on regulating international data flows[26] can benefit from modifications to improve compatibility with regimes in other territories and trading partners. Currently, the DPB 2021 carves out two subsets of personal data: "sensitive personal data" (**SPD**) and "critical personal data" (**CPD**). It then requires the local storage of SPD and local processing of CPD by default. While SPD and CPD can, in principle, be transferred across borders, this is only permitted on highly limited grounds and only after the prior authorisation of both the Indian Government and the proposed Data Protection Authority is received. This approach may create the following challenges:

    - It may undermine the ability of businesses to carry out key operations that necessarily involve processing data from multiple jurisdictions. For instance, to detect frauds in online payments in real time, entities need to examine unusual payment patterns across jurisdictions at high speeds – at odds with granular authorisation exercises.[27]
    - It may undermine the ability of Indian organisations to leverage emerging technologies that rely on distribution of data, such as cloud computing, data analytics or applications of artificial intelligence.
    - It would require the creation of additional storage systems, which may increase costs for organisations operating in India. For SMEs and start-ups, this could limit their global competitiveness since they would be forced to bear these costs at a time when they are trying to start out and launch their digital services.[28]

    To recalibrate towards a less restrictive approach that can help grow cross border trade while meeting the Government's legitimate public policy objectives, we offer the following suggestions:

    2.1. **The current taxonomy of data categories may be narrowed and better defined.** The concept of SPD may be narrowed to exclude certain categories. For instance, official identifiers and financial data may be excluded while the definition of health data may be narrowed to only cover data about the health status of a person. The concept of CPD may be linked to the requirements of national security by introducing a definition and a

[26] *See* Sections 33 and 34, DPB 2021, *supra* note 6.
[27] *See* A. Chander, M.F. Ferracane, *Exploring International Data Flow Governance,* World Economic Forum, December 2019, available at https://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf (last accessed on May 6, 2022).
[28] *See* A. Chander, M.F. Ferracane, *Exploring International Data Flow Governance,* World Economic Forum, December 2019, available at https://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf (last accessed on May 6, 2022); Centre for Information Policy Leadership and Data Security Council of India, *Enabling Accountable Data Transfers from India to the United States under India's Personal Data Protection Bill (No. 373 of 2019),* August 2020, available at *https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-dsci_report_on_enabling_accountable_data_transfers_from_india_to_the_united_states_under_indias_proposed_pdpb__8_september_2020_.pdf* (last accessed on May 6, 2022).

regulatory process to determine its contents based on clear parameters of 'criticality'. We also recommend introducing a clarification that SPD and CPD are subsets of personal data, so that provisions that merely mention personal data also apply to SPD and CPD.

2.2. **The requirement for an additional round of consent for transferring SPD may be reviewed.** The DPB 2021 currently requires that a data principal must provide explicit consent before SPD may be transferred. This is even after the data principal already provides consent for processing SPD. The need to collect an additional round of consent for one aspect of processing (international data transfer) may unduly burden data principals and increase the potential for consent fatigue without affording them additional protection.

2.3. **The requirement for specific prior authorisation of each transfer may be reviewed.** The DPB 2021 currently contemplates that each transfer or scheme for transferring SPD will be individually approved by the Central Government and the Authority. This approach can impose undue regulatory burden on consumers, industry, and on public administrations – and is also out of sync with the approaches in other jurisdictions. We recommend instead introducing tools and safeguards that are in line with equivalents recognised in other jurisdictions, including in the UK and in the EU, such as model contracts, certifications, and codes of conduct, and do not require specific prior authorisation in every instance. The DPB 2021 does recognise that the Authority is empowered to frame codes of practice (**COP**) for international data flows, but does not specifically provide that such COPs can cover transfer tools.[29] At present, it is unclear whether such COPs can be used to create transfer tools, such as model contracts, or what the scope and purpose of such COPs may be.

2.4. **The operation of the exemption for data processors dealing with foreign residents' personal data may be afforded greater clarity.** Currently, the DPB 2021 includes an enabling clause for such an exemption.[30] However, the way this exemption shall operate is unclear. Its applicability is dependent on the Central Government passing a notification. The DPB 2021 does not clarify the contents of such a notification. As a result, there is a risk that, due to the exemption, foreign residents may not be able to access remedies in India in relation to the processing of their personal data by Indian data processors. This could reduce the confidence of foreign data controllers seeking to rely on Indian data processors in the future. This exemption clause may be reviewed to provide upfront clarity on its scope and operation to ensure that the processing of the personal data of foreign residents may not have to be bound by certain India-specific rules, such as those on

[29] *See* Section 50(q), the DPB 2021, *supra* note *6*.
[30] Section 37, the DPB 2021, *supra* note *6*, 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.*

transferring data to overseas territories[31] or barring the processing of biometric data[32] on having to comply with access requests for non-personal data from the Government of India[33], but that foreign data principals may still be offered remedies in India.

2.5. The DPB 2021 should provide for a strong and independent oversight mechanism. The Data Protection Authority, proposed to be established under the DPB 2020, shall be a key determinant of success of the DPB 2021. Given that it will be regulating both the private sector and public institutions, it should be afforded sufficient autonomy for it to remain impartial. This requires redesigning its appointment process, and ensuring it is at arms-length from the Central Government. It shall also have to supervise and respond to rapid technological changes across a wide range of sectors – and should be afforded sufficient resources to ensure it has sufficient technical and functional capacity.

Section D
Setting the stage for a data adequacy partnership

The UK Government has recently listed India as a priority destination for a future data adequacy partnership.[34] We consider this expression of intent to create an open corridor for cross-border data transfers as highly valuable. We would welcome the opportunity to assist in building this partnership.

The process of concluding adequacy decisions has, in the past, taken a significant amount of time. However, the UK Government has a unique opportunity to inform the Government of India of its expectations from an adequacy perspective at a time when the latter is introducing a more comprehensive data protection regime. The timing of the FTA negotiations also aligns well with the recent signalling of intent by the UK Government to chart its own course on adequacy assessments and "*focus on risk-based decision-making and outcomes".*[35]

Considering the above, **we encourage the UK Government to leverage the FTA negotiations to kick-start the conversation on a data adequacy partnership with India.** For instance, the UK Government could set out the criteria, in terms of technical assessments and real-world practices, it considers relevant to an adequacy assessment. In a recent consultation paper, it was suggested that these criteria are currently under development.[36]

We encourage the Government of India to enact the DPB Bill after duly considering our suggested modifications. Enacting the DPB Bill soon would be a timely step to take to leverage the FTA as a starting point towards establishing a data adequacy partnership with

[31] *See* Sections 33 and 34, the DPB 2021, *supra* note *6*.
[32] *See* Section 93, the DPB 2021, *supra* note *6*.
[33] *See* Section 92, the DPB 2021, *supra* note *6*.
[34] *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 May 6, 2022).
[35] *See* DCMS 2021 Consultation, *supra* note 8 at page 89.
[36] *Id.*

the UK. However, as a recent study by NASSCOM reveals, this would only be one of the steps needed to prepare the Indian legal system for an adequacy assessment.[37] A separate set of reforms will be needed to ensure that modern safeguards and protections can be introduced into the laws and regulations currently empowering government agencies to access data for preventing, detecting, investigating, or prosecuting criminal offences, including threats to national security. These reforms are not restricted to the DPB 2021 and require the relevant provisions of other laws, such as the Information Technology Act of 2000, the Code of Criminal Procedure of 1973, and the Indian Telegraph Act of 1885, to be revisited.

NASSCOM's study finds that, while the Indian regime is broadly favourable from an adequacy standpoint, certain laws – those that contain rules used to engage in lawful surveillance or by law enforcement agencies to access data from private entities[38] - could benefit from a review to better meet the expectations of other countries from the perspective of the protection of personal data. This is likely to enhance the overall evaluation vis-à-vis adequacy with the UK or with the European Union**.** 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 this paper with our recommendations to both governments on the UK-India FTA negotiations from a digital trade perspective.

The focus of this paper was on presenting commitments on the protection of personal data and the regulation of international data flows that may be included in the upcoming FTA in a dedicated chapter on digital trade. Such commitments should be considered to best achieve the mutual target of doubling bilateral trade between India and the UK. They may form part of early harvest discussions. We also presented suggestions for both governments to consider aligning their domestic rules with our suggested FTA commitments. These may be followed up by efforts to build a data adequacy partnership in due course.

It is hoped this paper is of value to both governments in their bilateral negotiations. We intend to follow up this paper with additional work aimed at enabling bilateral digital trade between India and the UK. Such work would look to examine other issues, beyond the protection of personal data and the regulation of international data flows, that we believe should also form part of any chapter on digital trade in the FTA.

Please write to Jana Psarka (jana.psarska@techuk.org), Meghna Mishra (Meghna.misra-elder@ukibc.com), or Ashish Aggarwal (asaggarwal@nasscom.in) with any questions or comments that you may have.

---

[37] *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 May 6, 2022).

[38] These include the Information Technology Act of 2000, the Indian Telegraph Act of 1885, the Code of Criminal Procedure, 1973. This study also examined the relevant provisions of the PDP Bill that concern government access to data. The relevant findings are also applicable to the DPB 2021. *Id*.

Annexure 1

Illustrative List of Trade Arrangements incorporating Commitments on Data

S. No.	Trade Agreement	Relevant Excerpt
1.	**India – UAE Comprehensive Economic Partnership Agreement**	**ARTICLE 9.10** **Personal Data Protection** 1. The Parties recognise the economic and social benefits of protecting the personal data of persons who conduct or engage in electronic transactions and the contribution that this makes to enhancing consumer confidence in digital trade. 2. To this end, each Party shall endeavour to adopt or maintain a legal framework that provides for the protection of the personal data of the users of digital trade. ln the development of any legal framework for the protection of personal data, each Party shall endeavour to take into account principles and guidelines of relevant international organisations. 3. Each Party shall endeavour to publish information on the persona! Data protection it provides to users, including how: a. individuals can pursue remedies; and b. businesses can comply with any legal requirements. 4. The Parties shall endeavour to cooperate, to the extent possible, regarding the protection of personal information or personal data transferred from a Party. **Footnote:** For greater certainty, a Party may comply with the obligation in this paragraph by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, and sector-specific laws covering privacy. **ARTICLE 9.11** **Cross-Border Flow of Information** The Parties recognise the importance of the flow of information in facilitating trade, and acknowledge the importance of protecting personal data. As such, the Parties shall endeavour to promote electronic information flows across borders subject to their laws and regulatory frameworks.
2.	**UK – EU Trade and Cooperation Agreement**	**Article 201** **Cross-border data flows** 5. The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end,

		cross-border data flows shall not be restricted between the Parties by a Party: a. requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a Party; b. requiring the localisation of data in the Party's territory for storage or processing; c. prohibiting the storage or processing in the territory of the other Party; or d. making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties' territory or upon localisation requirements in the Parties' territory. 6. The Parties shall keep the implementation of this provision under review and assess its functioning within three years of the date of entry into force of this Agreement. A Party may at any time propose to the other Party to review the list of restrictions listed in paragraph 1. Such a request shall be accorded sympathetic consideration. **Article 202** **Protection of personal data and privacy** 1. Each Party recognises that individuals have a right to the protection of personal data and privacy and that high standards in this regard contribute to trust in the digital economy and to the development of trade. 2. Nothing in this Agreement shall prevent a Party from adopting or maintaining measures on the protection of personal data and privacy, including with respect to cross-border data transfers, provided that the law of the Party provides for instruments enabling transfers under conditions of general application for the protection of the data transferred. 3. Each Party shall inform the other Party about any measure referred to in paragraph 2 that it adopts or maintains.
3.	**UK – Japan Comprehensive Economic Partnership Agreement**	**Article 8.63** **Financial information** 1. A Party shall not restrict a financial service supplier of the other Party from transferring information, including transfers of data into and out of the former Party's territory by electronic or other means, where such transfers are relevant for the

		conduct of the ordinary business of the financial service supplier. 2. Subject to paragraph 3, a Party shall not require, as a condition for conducting business in its territory, a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory. 3. A Party has the right to require a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory, where it is not able to ensure access to information that is appropriate for the purposes of effective financial regulation and supervision, provided that the following conditions are met: a. to the extent practicable, the Party provides a financial service supplier of the other Party with a reasonable opportunity to remediate any lack of access to information; and b. the Party or its financial regulatory authorities consults the other Party or its financial regulatory authorities before imposing any requirements to a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory. 4. Nothing in paragraph 3 shall be construed to grant a Party access to information or to require a financial service supplier of the other Party to use or locate financial service computing facilities in the former Party's territory, in a manner beyond what is appropriate for the purposes of effective financial regulation and supervision. 5. Nothing in this Article restricts the right of a Party to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as that right is not used to circumvent Sections B to D and this Sub-Section. **Article 8.80** **Personal information protection** 1. The Parties recognise the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce. 2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies. 3. Each Party shall endeavour to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction.

		4. Each Party shall publish information on the personal information protections it provides to users of electronic commerce, including how: a. individuals can pursue remedies; and b. business can comply with any legal requirements. 5. Recognising that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall endeavour to exchange information on any such mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them. **Article 8.84** **Cross-border transfer of information by electronic means** 1. A Party shall not prohibit or restrict the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person. 2. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 1 to achieve a legitimate public policy objective, provided that the measure: a. is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and b. does not impose restrictions on transfers of information greater than are required to achieve the objective. 3. This Article does not apply to: a. government procurement; or b. information held or processed by or on behalf of a Party, or measures by a Party related to that information, including measures related to its collection. **Article 8.85** **Location of computing facilities** 1. A Party shall not require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory. 2. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 1 that are necessary to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which

		would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade. 3. This Article does not apply to: a. government procurement; or b. information held or processed by or on behalf of a Party, or measures by a Party related to that information, including measures related to its collection.
6.	**Regional Comprehensive Economic Partnership Agreement**	**Article 12.8: Online Personal Information Protection** 1. Each Party shall adopt or maintain a legal framework which ensures the protection of personal information of the users of electronic commerce. 2. In the development of its legal framework for the protection of personal information, each Party shall take into account international standards, principles, guidelines, and criteria of relevant international organisations or bodies. 3. Each Party shall publish information on the personal information protection it provides to users of electronic commerce, including how: a. individuals can pursue remedies; and b. business can comply with any legal requirements. 4. The Parties shall encourage juridical persons to publish, including on the internet, their policies and procedures related to the protection of personal information. 5. The Parties shall cooperate, to the extent possible, for the protection of personal information transferred from a Party. **Article 12.14: Location of Computing Facilities** 1. The Parties recognise that each Party may have its own measures regarding the use or location of computing facilities, including requirements that seek to ensure the security and confidentiality of communications. 2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that Party's territory. 3. Nothing in this Article shall prevent a Party from adopting or maintaining: a. any measure inconsistent with paragraph 2 that it considers necessary to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or b. any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties.

		Article 12.15: Cross-border Transfer of Information by Electronic Means 1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means. 2. A Party shall not prevent cross-border transfer of information by electronic means where such activity is for the conduct of the business of a covered person. 3. Nothing in this Article shall prevent a Party from adopting or maintaining: c. any measure inconsistent with paragraph 2 that it considers necessary to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; or d. any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties. Explanation: For the purposes of this subparagraph, the Parties affirm that the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party. **Article 9: Transfers of Information and Processing of Information (Financial Services)** 1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information and the processing of information. 2. A Party shall not take measures that prevent: e. transfers of information, including transfers of data by electronic or other means, necessary for the conduct of the ordinary business of a financial service supplier in its territory; or f. processing of information necessary for the conduct of the ordinary business of a financial service supplier in its territory. 3. Nothing in paragraph 2 prevents a regulatory authority of a Party, for regulatory or prudential reasons, from requiring a financial service supplier in its territory to comply with its laws and regulations in relation to data management and storage and system maintenance, as well as to retain within its territory copies of records, provided that such requirements shall not be used as a means of avoiding the Party's commitments or obligations under this Agreement. 4. Nothing in paragraph 2 restricts the right of a Party to protect personal data, personal privacy, and the confidentiality of individual records and accounts including in accordance with its laws and regulations, provided that such a right shall not

		be used as a means of avoiding the Party's commitments or obligations under this Agreement. 5. Nothing in paragraph 2 shall be construed to require a Party to allow the cross-border supply or consumption abroad of services in relation to which it has not made commitments, including to allow non-resident suppliers of financial services to supply, as a principal, through an intermediary or as an intermediary, the provision and transfer of financial information and financial data processing as referred to in subparagraph (b)(xv) of Article 1 (Definitions).
7.	**EU-Mexico Global Trade Agreement**	**Review clause on Data Flows** The Parties shall reassess within three years of the date of entry into force of this Agreement the need for inclusion of provisions on the free flow of data into this Agreement.
8.	**UK – Chile Association Agreement**	**Article 30** **Data protection** 1. The Parties agree to cooperate on the protection of personal data in order to improve the level of protection and avoid obstacles to trade that requires transfers of personal data. 2. Cooperation on personal data protection may include technical assistance in the form of exchange of information and experts and the establishment of joint programmes and projects.
9.	**UK – Vietnam FTA**	**Article 8.45** **Data Processing – Financial Services** 1. Each Party shall adopt or maintain appropriate safeguards to protect personal data and privacy, including individual records and accounts. 2. No later than two years from the date of entry into force of this Agreement, each Party shall permit financial service suppliers of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service suppliers. 3. Nothing in this Article restricts the right of a Party to protect personal data and privacy, so long as such right is not used to circumvent this Agreement.