CIPL Response to the Department for Science, Innovation and Technology's Call for Evidence: Data Flows You Can Trust

I. Introduction

The Centre for Information Policy Leadership[1] (CIPL) welcomes the opportunity to respond to DSIT's call for evidence, *Data flows you can trust*. CIPL has worked on international data transfers for many years and is a long-standing proponent of a risk-based, accountability-based and interoperable approach to cross-border data flows.

International data transfers are a defining feature of the modern digital economy and one of its principal engines of growth. While the trade in goods is flattening, data flows and data-enabled services are growing rapidly and reshaping global trade.[2] It is therefore imperative that data can flow safely and responsibly, as restricting cross-border data flows hampers trade, hinders productivity, impacting individuals and raising downstream prices.[3] Most importantly, with the transformative power of AI, it is imperative for every country to enable AI adoption in all aspects of the AI stack and lifecycle – from training and development to deployment, from infrastructure to AI as a service. Critically, in order to build AI systems that are robust, accurate, fair and representative, and that mitigate discriminatory outcomes, it will be necessary to have large volumes of relevant and representative data and share data across borders. AI adoption depends on access to data and on the ability to move it. Every country and organisation therefore has an interest in fair access to data, and in participating in data sharing, so that AI works for them and reflects their society. This is why data flows policy is becoming intrinsically linked to AI competitiveness and AI adoption. Data will continue to flow across borders as a matter of economic and technological reality. The question for policymakers is therefore not whether to permit those flows, but how to enable them in a way that is trusted, responsible and workable.

CIPL has long argued that accountability is the key to enabling trusted data flows. Cross-border transfers are best enabled *ex-post (*without prior authorisation*)*, with organisational accountability as the backstop: the transferring organisation remains responsible for the personal data regardless of where it is processed, and ensures that it is protected at the original level

[1] The Centre for Information Policy Leadership (CIPL) is a global privacy and data policy think tank within the Hunton law firm that is financially supported by 85+ member companies that are leaders in key sectors of the global economy and by other private and public sector stakeholders through consulting and advisory projects. CIPL's mission is to engage in thought leadership and develop best practices for the responsible and beneficial use of data in the modern information age. CIPL's work facilitates constructive engagement between business leaders, data governance and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at www.informationpolicycentre.com. Nothing in this document should be construed as representing the views of any individual CIPL member company or Hunton. This document is not designed to be and should not be taken as legal advice.

[2] McKinsey, Digital Globalization: The New Era of Global Flows, 2016; Globalisation in Transition, 2019; Global Flows: The Ties That Bind, 2022

[3] International Data Transfer Expert Council report, Nov 2023

wherever it travels. Transfers should be regulated in a risk-based way rather than a "zero-risk" regime – one that requires safeguards proportionate to the actual risk of a given transfer rather than the elimination of every theoretical one.[4]

The UK is uniquely placed to create its own distinctive path, and create its own rules that work in practice, bridging different approaches and acting as a promoter of multilateral approaches to trusted data flows. International data transfers cannot be addressed in a vacuum. To move forward in an increasingly fragmented world, the UK must also continue to engage externally with like-minded countries to build the interoperable, trusted arrangements that allow data to move responsibly across borders. The recommendations that follow are offered in that spirit.

This response distils positions CIPL has developed and advocated over more than 25 years, so rather than respond question by question, we structure our response around five ideas that we believe should guide the UK's approach – preserving the risk-based, accountability-based foundation of the current regime, and the UK's high standards of protection, while reforming the mechanisms through which data flows and the way their safeguards operate:

- **Lead on multilateral, accountability-based transfers.** The UK should embrace and build upon the Global CBPR Forum – the only genuinely multilateral transfer mechanism. It should move from associate to full membership and broker its convergence with the GDPR, while also making fuller and more flexible use of adequacy, including partial adequacy.
- **Reimagine binding corporate rules and recognise certifications.** BCR should evolve and be made accessible to organisations of all sizes, and certification to recognised technical and international standards should be recognised as a valid and interoperable transfer tool.
- **Make the transfer assessment risk-based and workable.** The data protection test should remain genuinely risk-based rather than zero-risk. The country-level legal and government-access analysis should be centralised, so that organisations need only assess the risk of their own transfer rather than each conducting a private adequacy determination
- **Privacy Enhancing Technologies (PETs) for data sharing and transfers must be incentivised and supported.** The promise of PETs will only be realised when these techniques are made more available, applied in a risk-based manner, afforded legal certainty, and incentivised by policymakers and regulators as a true demonstration of accountability and as risk-reducing safeguards.
- **Address sovereignty and security directly, not through localisation.** Localisation harms security, resilience and growth rather than improving protection; trust is better built by addressing government access directly – building on the emerging international consensus on trusted government access – and by approaching data sovereignty through a holistic, security-aware lens. Digital sovereignty may be justifiable in specific

[4] T. Christakis, The "Zero Risk" Fallacy: International Data Transfers, Foreign Governments' Access to Data and the Need for a Risk-Based Approach, 2024

cases, and may have to co-exist with DFFT (Data Free Flow with Trust), but it should be an exception, rather than a rule. Like-minded countries should encourage digital solidarity over digital sovereignty.

We expand on each below.

II. Transfer mechanisms – the UK's opportunity to lead on international data transfers policy and on the Global CBPR

The Global Cross-Border Privacy Rules (CBPR), together with the Global Privacy Recognition for Processors (PRP), are a multilateral and accountability-based mechanism for transferring personal data across borders, and the only transfer mechanism that offers a genuinely multilateral solution.[5] Because it is accountability-based, it can offer a form of protection that other transfer mechanisms do not: a comprehensive and independently assured privacy management programme, comparable to BCRs, with controls, policies and technologies applied throughout the data lifecycle. Unlike a contractual mechanism, the protection it secures travels with the data across every participating jurisdiction, in addition to applicable national law. The potential of the CBPR as a one-stop-shop multilateral mechanism, and its capacity to evolve and attract further countries and companies, is considerable. It offers an opportunity to support DFFT at a scale that bilateral arrangements or individual contracts cannot reach.

The UK, as an Associate member of the Global CBPR Forum (the first jurisdiction to be admitted on that basis), is well placed to help shape its development into a widely used mechanism for cross-border data flows. Associate status has its limits, however: it allows the UK to participate in and contribute to the Forum's work, but not to take part in its decision-making, and it does not yet permit UK organisations to certify under, or to rely on, the CBPR as a transfer mechanism. That step requires full membership.

Considering the opportunity that CBPR presents to the UK and other countries as a mechanism for DFFT, the UK should work towards fully embracing CBPR and becoming a full member. While the EU does not at present recognise CBPR as affording an equivalent level of protection for onward transfers of EU personal data, the UK can still fully embrace CBPR as other adequate jurisdictions have done. For instance, Japan and Korea have each built safeguards into their adequacy arrangements (through supplementary rules) that keep EU personal data protected by restricting its onward transfers based on CBPR. The UK is, if anything, better placed than either, beginning from far closer alignment with the GDPR. It can therefore seize the opportunity the CBPR presents and become a full member, recognising the CBPR for its own and other data flows while, as Japan and Korea have done, keeping EU-origin data within its adequacy framework.

Furthermore, the EU's position has not been revisited since the Global CBPR Program Requirements were substantially strengthened in March 2026. When CIPL mapped the updated

[5] CIPL, CBPR–GDPR Mapping, Apr 2026

Program Requirements against the EU GDPR in 2026, we found that 72% of the CBPR requirements align fully with the GDPR, rising to more than 75% in the case of the PRP. We also concluded that EU participation faces no significant obstacle from an enforcement perspective.[6]

This is the moment to embrace CBPR as the EU is itself reviewing its digital rulebook, including the GDPR, and has not yet reassessed the CBPR in light of the recent updates of the program requirements. The UK would be uniquely placed to lead that conversation and bridge with the European Commission, so that in time a single certification can be trusted across the UK, the EU and the wider CBPR Forum.

Although CIPL believes that the adequacy model is not sustainable in the long term, based on bilateral adequacy findings, the UK should also make fuller, and more flexible, use of adequacy. Full adequacy will not always be achievable; for instance, a country may provide strong protection in some sectors, but not others, or for some categories of data but not others, yet the absence of a full adequacy decision need not mean the absence of trusted flows. The UK should therefore explore partial and conditional adequacy: sector-specific adequacy for particular industries within a country, or adequacy subject to additional conditions for particular categories of data. Approached in an outcomes-focused and risk-based way, this would extend the benefits of adequacy to the UK's trading partners while reserving the more demanding transfer mechanisms for the situations that genuinely warrant them. Priority countries and sectors could be identified by reference to their economic significance and the practical complexity organisations face in transferring to them.[7] To remain workable, this flexibility should be designed to avoid unnecessary fragmentation, so that a more granular adequacy landscape stays clear and usable for the organisations relying on it.

Finally, the UK is well positioned to lead on international data transfers policy and support the initiatives of DFFT, originated by Japan and also pursued through the OECD. As part of its commitment to the value of preserving international data transfers, the previous UK government established the Expert Council for International Data Transfers, with diverse global experts called to provide steer and advice to HMG on data flows policy. The work of the Council culminated in a report *Towards a sustainable, multilateral, and universal solution for international data transfers*. The report provided many workable short- and mid-term recommendations and is even more relevant today. The new government must continue this work and re-establish the Council, with renewed focus and solutions. This is not a political or party issue, but an essential aspect of industrial, AI and competitiveness policy for the UK that HMG must lead on.

III. Re-imagining binding corporate rules and recognising certifications as transfer tools

Binding corporate rules (BCR) are widely regarded as the gold standard of cross-border transfer mechanisms: they require an organisation to put in place a comprehensive data protection

[6] CIPL, CBPR–GDPR Mapping Report, Apr 2026
[7] CIPL, Response to UK Data Strategy, 2020

programme and compliance infrastructure and are, in essence, an accountability mechanism that ensures the continued protection of personal data wherever it travels.

BCR's potential, however, remains largely unrealised. The approval process is prescriptive, costly and lengthy, requiring prior approval by a regulator, which favours large and sophisticated multinationals and places BCR beyond the practical reach of most organisations. In the EU, for instance, the approval process has become progressively more demanding and narrowing[8] with expectations that go beyond what the framework requires and that add limited protective value in practice. This discourages accountable organisations from embarking on the BCR process at all, and leads them instead to settle for less protective and more administratively burdensome contractual measures (SCCs). All of this has led to a strikingly low take-up of BCR, a mechanism that only a handful of organisations have the resources and time to obtain and ultimately a lost opportunity.[9]

Therefore, BCR should be reimagined so that their value as an accountability mechanism is realised in practice rather than lost at the approval stage. The most significant change would be to move away from mandatory prior approval by a regulator to a self -declaration or a third-party assured declaration. Rather than requiring an authority to review and approve each set of rules, a demand that strains limited regulatory capacity and generates lengthy backlogs, BCR could instead be reviewed by a recognised third party. The CBPRs are also based on third-party certifiable and assured reviews, and the SCCs are just bilateral contracts which are not audited nor reviewed by a third party. Now is the time to re-imagine BCR in light of the other mechanisms. Reforming BCR in this way would remove the principal barrier to their uptake and make them affordable, scalable and accessible to organisations of all sizes, including the SMEs for whom they are at present effectively out of reach.

The value of BCR should also be more fully recognised and incentivised by policy makers and regulators.

a) They could be recognised as a valid certification of an organisation's entire privacy management programme, reflecting what they already are in substance and adding to their value to organisations.
b) Their adoption should be recognised as a mitigating factor in enforcement, consistent with their status as a genuine demonstration of accountability.
c) Organisations with approved BCR should be able to transfer data between each other without having to rely on any additional transfer tool, since they already meet the highest data protection standards – a rationale that should extend equally to transfers between BCR-approved organisations and certified organisations or those adhering to an approved code of conduct.[10]

[8] European Data Protection Board (EDPB) proposal restricts reliance on BCRs for the initial transfer of personal data into a BCR-covered group, limiting BCRs' ability to function as a comprehensive end-to-end transfer mechanism - EDPB, Draft Recommendations 1/2026 on Binding Corporate Rules for Processors, January 2026

[9] GDPR Six Years On, May 2024

[10] CIPL, National Data Strategy response, Dec 2020

d) There should be further bridges built between CBPR and BCR and tangible benefits for organisations that already have one of these mechanisms in place to obtain the other one. The previous work on CBPR – BCR referential demonstrated the art of the possible and should be resumed and recast in the light of new imperatives for DFFT.

IV. Safeguards – a risk-based and workable transfer assessment

The safeguards that accompany a transfer should be proportionate to the actual risk it presents, rather than calibrated to a "zero-risk" standard that the law does not require and that would be practically impossible to meet.[11] However, the transfer risk assessment (TRA) has become one of the heaviest compliance burdens organisations face and a source of what has been described as internal "data transfer fatigue".[12] This requirement in effect requires each organisation to conduct its own private-sector "adequacy" determination of a destination country's laws and its government-access regime. In practice, organisations often cannot accurately foresee future risks associated with a transfer, even where rigorous assessments and state of the art controls have been put in place. This challenge is compounded by the fact that organisations frequently rely on complex processor, sub-processor and third-party ecosystems over which visibility and auditability may be limited. There is a real question of whether the requirement to conduct a TRA is actually workable in practice and capable of full compliance – both for large organisations that undertake thousands of international data transfers daily for different purposes, systems and business functions - where a TRA for each becomes unworkable, as well as for SMEs and startups that carry single-digit transfers but have no means, expertise, nor information to conduct TRAs in practice.

The single most effective step the Government could take to make the assessment workable is to centralise the country-level legal analysis on which every transfer risk assessment rests.[13] This part of the analysis does not vary from one exporter to the next, yet each exporter is presently expected to reach its own conclusions on the same questions, at considerable cost and with no corresponding benefit to individuals. The Government, working with industry and other stakeholders, could develop and publish practical, sector- or industry-specific country-level legal analysis on which organisations can rely as part of their TRAs.[14] The approach is not without precedent: Japan's data protection authority already publishes country-by-country assessments of foreign data protection regimes, including their government-access safeguards, on which organisations rely when framing their transfers. Centralising the country-level legal analysis in this way leaves organisations to assess the specific risks of their own transfer, taking into consideration

[11] T. Christakis, The "Zero Risk" Fallacy: International Data Transfers, Foreign Governments' Access to Data and the Need for a Risk-Based Approach, 2024

[12] CIPL, GDPR Six Years On, May 2024

[13] This includes the content of the destination country's data protection framework; the laws and practices under which its public authorities may access personal data for law enforcement and national security purposes; the conditions, thresholds and independent authorisation or oversight that govern such access; the existence and independence of a supervisory authority; and the redress available to individuals who are neither nationals nor residents of that country.

[14] CIPL, GDPR Six Years On, May 2024

the data types, volume and purpose of the transfer, while sparing them the task of each creating this resource each time they conduct a TRA.

Another option is to remove the prescriptive requirement altogether and continue with an outcomes-based, accountability-based requirement for a data exporter to ensure adequate protection for data and address any risks, based on severity and likelihood. This would enable organisations to achieve the policy objectives and regulators to focus on those that do not demonstrate their accountability and where actual harm due to international data transfer occurs.

The UK's future transfer framework should focus on being technologically neutral and reflect real-world operating models. Data is increasingly processed through cloud infrastructure, remote access arrangements, and globally distributed operations. Future transfer rules should recognise these operational realities and ensure that related obligations are workable in increasingly complex data environments.

V. Privacy-enhancing technologies as the solution

A transfer risk assessment that is genuinely risk-based must give full credit to the technical measures that reduce the risk of a transfer, and privacy-enhancing technologies (PETs) are among the most effective of these. Technologies such as encryption, homomorphic encryption, secure multi-party computation, differential privacy and trusted execution environments can keep data protected from any recipient, including a foreign public authority, throughout its processing. Because they do so, they speak directly to the government-access concern that lies at the heart of the transfer risk assessment.[15] The EDPB has itself recognised secure multi-party computation as an effective supplementary measure for international transfers.[16]

The value of PETs in this context, however, extends well beyond making a given transfer safer. A defining feature of this family of technologies is that they allow organisations to derive value from data collaboratively without the raw data ever having to move or be exposed. Federated learning enables multiple parties to train a shared model on their respective data sets while that data remains in place; and we found in our research that organisations turn to it precisely where transfers are "not allowed or convenient", including because of data-sovereignty or localisation requirements.[17] Homomorphic encryption similarly allows organisations in different countries to collaborate on training AI models without either revealing its underlying data. Understood in this way, PETs are not merely a means of de-risking a transfer; they are a means of achieving the outcomes that cross-border data flows are meant to deliver while reducing, and sometimes removing, the transfer itself.

[15] CIPL, Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age, 2023

[16] Recommendations 01/2020 on measures that supplement transfer tools (final version adopted 18 June 2021), Annex 2, Use Case 5

[17] CIPL, PETs and PPTs in AI, Mar 2025

In CIPL's PETs papers, we tracked key use cases of PETs in the data sharing and international data flows context. For instance, multiple hospitals and medical centres have jointly trained a cancer-detection model without sharing sensitive pathology images, by combining federated learning with trusted execution environments; several insurers have collaborated on a fraud-detection model using federated learning and synthetic data; and independent parties have jointly analysed highly sensitive neuro-imaging data through secure multi-party computation without either disclosing its raw data or its model.[18] Each is a form of cross-organisational data collaboration that a localisation-based or transfer-restriction-based approach would tend to frustrate, and that PETs make possible.

The case for PETs is not, however, solely an organisational one. Trusted data flows depend on public confidence, and ICO research has found that fear of personal data being stolen or misused remains among the most significant public concerns about how organisations store and share data.[19] PETs answer that concern at a technical level: where data is encrypted in use, aggregated under differential privacy, or processed within a trusted execution environment, what is exposed in a compromise cannot readily be attributed back to identifiable individuals. PETs thus enable organisations to maximise the value of data while minimising risk, by making potentially sensitive data less vulnerable to unauthorised sharing or breach[20] and in doing so support individuals' willingness to allow their data to be used and shared, including across borders.

Equally, PETs are an important element to ensure trusted data flows in respect of both personal data and data more broadly, especially given the economic value of data and data being a major asset for any company or government that also needs to be protected and secured from unwanted sharing and access. As such, PETs are an essential component of any data strategy and can also present solutions for digital solidarity and legitimate digital sovereignty concerns.

To realise this potential, the UK should actively incentivise the use of PETs in the transfer context by:

a) Issuing clear, practical guidance on the circumstances in which PET-protected data will be treated as falling outside the transfer restrictions, and more generally reduce the legal uncertainty that currently deters investment in and adoption of PETs;
b) Recognise and reward the good-faith adoption of PETs, both as a demonstrable element of accountability and as a mitigating factor in enforcement, and afford PET-protected processing a degree of legal certainty equivalent to a "safe harbour"; and
c) Support interoperability by encouraging the development of technical standards for PETs, and promote adoption through published case studies, practical implementation guidance and experimentation in regulatory sandboxes.

[18] ibid
[19] ICO, Information Rights Strategic Plan: Trust and Confidence
[20] CIPL, Understanding PETs and PPTs, Dec 2023

VI. Sovereignty, localisation and cyber security

When reflecting on whether the UK should take a more explicit position on the 'sovereignty' of UK data, and whether there would be merits or risks in more tightly managed controls of UK datasets for security or wider national benefit, it is worth examining the actual risks of such policies. The consultation defines data sovereignty as the degree of control and access that organisations and governments have over data – legal, technical, contractual, governance and infrastructure. Understood in these terms, sovereignty is a function of who controls and can access data, and of how well the systems that hold it are secured and governed – not of where the data physically sits.

There may indeed be some occasions where digital sovereignty or data localisation may be justifiable. On these occasions, any transfers should co-exist with DFFT (free data flows with trust). However, this should be an exception, rather than a rule. Like-minded countries should encourage digital solidarity over digital sovereignty. An approach that neither disadvantages domestic organisations relative to imported technology, nor treats sovereignty as a synonym for localisation, is the surest way to reconcile the UK's legitimate security and sovereignty interests with its ambition to remain an open and trusted hub for international data flows.

In reality, data localisation is increasingly presented as a solution to digital sovereignty and also for greater protection. The proposition that data kept within the country is data kept under control is largely mistaken, and pursuing sovereignty through localisation carries real risks.[21] Localisation does not, in itself, improve the protection of personal data; and in a borderless digital world, in which data moves seamlessly and automatically across jurisdictions, it is extremely difficult and in practice unviable. What protects data is the controls placed on it and the resilience of the systems that govern it – the very legal, technical, contractual, governance and infrastructure controls the call for evidence associates with sovereignty. This is borne out in the cloud context in particular. Global cloud services will often provide a superior, state-of-the-art level of security that many organisations could not achieve on their own, including encryption engineered in by default, the capacity to absorb and repel large-scale attacks, and a globally distributed architecture that allows a provider to detect a threat in one region and apply the defence everywhere. Requiring that data instead remain on local servers can therefore deprive organisations of the very security that localisation is intended to deliver.[22]

Data localisation can have real proven impact, for instance it can raise the cost of hosting data by between 30% and 60%.[23] Our research on the real harms of data localisation policies found that localisation can actually degrade cybersecurity, as cloud providers generate trillions of threat signals from data sets worldwide to identify botnets, malware and other malicious activity, and cutting them off from cross-border flows leaves defenders blind to threats that themselves respect no borders. It can also undermine fraud prevention as anti-money-laundering, counter-

[21] CIPL, The Real Life Harms of Data Localisation, Mar 2023; IDT Expert Council report, Nov 2023
[22] CIPL, From Barriers to Bridges: Cloud Computing in Support of Privacy and Security, Sept 2024
[23] ibid

terrorist-financing, anti-bribery and know-your-customer controls depend on personal data analysed across jurisdictions, and walling that data off risks turning localising countries into safe havens for bad actors. It can also obstruct life-critical research, as researchers in the EU and EEA withdraw from a cancer research consortium led by the US National Institutes of Health's National Cancer Institute rather than make the cross-border transfers the collaboration required. And it can weaken the very security it is invoked to protect: on the eve of Russia's 2022 invasion, Ukraine amended its own localisation rules so that critical government, banking, tax and education data could be moved to the cloud and distributed safely abroad, rather than left on domestic servers facing physical destruction. At the end of this submission is an overview of the other sectors that data localisation policies can impact, as found in our research.[24]

One of the reasons for promoting digital sovereignty and data localisation is the possible risk of governmental access to data in the country where data are transferred. If the aim is trusted data flows, the more effective lever is not where data is stored but the conditions under which governments may access it. Government access for national security and law enforcement purposes cannot be treated in isolation from data flows, but it is equally hard for organisations to impact government processes and data use decisions. Addressing that access directly, rather than through the blunt instrument of localisation or data protection transfer restrictions, is therefore central to enabling trusted flows. The constructive path is to build on the growing international consensus on the conditions for trusted government access. The OECD's Declaration on Government Access to Personal Data Held by Private Sector Entities sets out common principles,[25] and the UK is well placed to champion this consensus. For instance, it is among the few countries to have placed the use of personal data for law enforcement and national security purposes on a clear statutory footing (under Parts 3 and 4 of the Data Protection Act 2018).[26]

Graphic 1: A list of areas that could be affected by data localisation policies

[24] CIPL and Tech, Law & Security Program, The "Real Life" Harms of Data Localization Policies, Mar 2023
[25] OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, Dec 2022
[26] IDT Expert Council report, Nov 2023

The "Real Life" Harms of Data Localization Policies

Discussion Paper I

Before continuing down the path of data localization, it is vital for policymakers to recognize the consequences of such policies, and to better understand the economic and societal harms that terminating or severely limiting cross-border data flows could bring about. **Impacts of data localization include:**

Business Operations

- **Cyber security-related tools and services;**
- **Human resources systems;**
- **Fraud prevention services;**
- **Manufacturing operations; and**
- **Customer service.**

Products & Services

- **Cloud computing services;**
- **Financial services;**
- **E-commerce;**
- **5G telecommunications;**
- **Streaming entertainment;**
- **Modern farming technology.**

Communication Platforms

- **Social media services and communication tools**, including video conferencing, audio translation, and content moderation, that allow people across the world to communicate and connect.

Education, Medicine, & Research

- **Educational and medical tools and services and research** all rely on cross-border data flows, including personal data.