GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

RESPONSE TO UNITED KINGDOM DEPARTMENT FOR SCIENCE INNOVATION AND TECHNOLOGY

CONSULTATION ON *DATA FLOWS YOU CAN TRUST*

July 2026

The Global Data Alliance (GDA)[1] is pleased to respond to the June 2026 consultation of the Department for Science Innovation and Technology (DSIT), entitled "*Data Flows You Can Trust.*" The United Kingdom has long been an international leader in showing that strong data protection can coexist with innovation, trade and growth. GDA welcomes the Government's practical, proportionate and business-friendly approach to enabling secure data flows.

The GDA is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. GDA member companies are active in all industrial sectors and depend on cross-border access to information and data transfers to create jobs across the United Kingdom. GDA members are active across the agriculture, automotive, aviation, energy, finance, health, hospitality, manufacturing, media, software, telecommunications, transportation, and other sectors in the UK.

GDA Recommendations

The United Kingdom begins from a strong position. Its data-bridge programme, flexible transfer mechanisms and practical ICO guidance make it one of the more forward-looking jurisdictions on international transfers. This approach supports businesses of all sizes and public interests including cybersecurity, research, health and resilience. The Government should preserve the toolkit and pursue targeted improvements, not broad restrictions. Trust is best advanced through accountability, security, enforceable rights and interoperable mechanisms - not data localisation.

The absence of interoperability results in reduced performance capabilities, with significant follow-on consequences for reduced access to knowledge, scientific collaboration, sharing of ideas, commercial opportunity, and other benefits of seamless cross-border data transfers. For example, in today's research and educational environments, AI and machine learning capabilities depend on access to global compute infrastructure and cross border data flows for model training, inference, and improvement. Data localisation requirements that fragment this infrastructure directly impair the ability to realize the benefits that knowledge exchange and computational data analytics can bring.

1. Awareness and Behaviour Around International Transfers

Organisations should understand their data flows, the parties involved, relevant processing purposes, destination jurisdictions, and applicable safeguards. In practice, multinational enterprises maintain this oversight through data inventories, records of processing, vendor-management systems, contractual subprocessor notices, technical access controls, and periodic risk reviews.

In modern distributed cloud environments, however, requiring organisations to trace the physical location of every transient data element at every moment would be technically infeasible and of limited value to individuals. Regulation should focus on meaningful accountability: who controls or processes the data, for what purpose, under which legal obligations, and subject to which technical and organisational protections. Privacy and security outcomes depend principally on the effectiveness of those controls, rather than the physical location of infrastructure.

The Government and ICO should provide worked examples covering cloud hosting, global cybersecurity monitoring, human-resources administration, remote technical support, intra-group services, and AI development and deployment. Guidance should distinguish restricted transfers from direct collection by an overseas organisation and explain the treatment of remote access. Standardised subprocessor and destination disclosures would improve recordkeeping, and tools should be usable by smaller organisations without large legal teams.

2. Use of International Transfer Mechanisms

First, adequacy frameworks—once adopted—are highly efficient data-transfer mechanisms because they provide economy-wide legal certainty and avoid duplicative, transaction-level assessments. At the same time, economy-by-economy adequacy review and approval processes are often lengthy and resource-intensive. To realise the full benefits of adequacy, the UK should continue expanding data bridges with trusted partners while preserving stable and frictionless UK-EU and UK-US data flows. Partial or sectoral adequacy arrangements can also be useful where their scope is clear, their legal basis is durable, and their application is readily understandable to businesses and individuals.

Second, the UK could make fuller use of certification and interoperable accountability mechanisms. GDA supports deeper UK engagement with the Global Cross-Border Privacy Rules Forum and arrangements enabling UK organisations to use recognised Global CBPR and Privacy Recognition for Processors certifications. These independently verified systems can provide scalable, multilateral support for trusted data transfers and reduce the need for businesses to navigate multiple duplicative compliance frameworks.

Third, the ICO has explained at a high level how approved certifications and codes of conduct could operate as safeguards for restricted transfers. However, no such UK transfer mechanisms are currently operational, and businesses still lack the detailed implementation guidance needed to use these alternatives in practice. The ICO should prioritise finalising this guidance and supporting the development and approval of workable certification schemes and codes of conduct.

Fourth, the UK should continue improving interoperability between its contractual transfer mechanisms and those used in other jurisdictions. The UK Addendum already enables organisations to adapt the EU Standard Contractual Clauses for UK transfers, but the ICO could further reduce compliance burdens by publishing a consolidated, clause-by-clause comparison of the EU SCCs, the UK Addendum and the standalone International Data Transfer Agreement. This comparison should identify equivalent obligations, material differences and areas in which common documentation or contractual language can satisfy both UK and EU requirements.

Finally, Binding Corporate Rules remain a valuable mechanism for multinational groups, but the approval process could be made faster, more predictable and more transparent. The ICO could publish indicative review timelines and anonymised statistics on approval durations, and provide BCR guidance in both modular and consolidated, searchable formats.

3. Balancing Compliance with Accountability

We recognise that many organisations operating in the UK also rely on the continued free flow of personal data from the EU and EEA. On 19 December 2025 the European Commission renewed the UK's two adequacy decisions through 27 December 2031, having concluded — after reviewing the DUAA reforms — that the UK continues to offer a level of protection essentially equivalent to that of the EU. Crucially, the very measures at issue here, including the "not materially lower" data protection test and the streamlined transfer regime, formed part of the framework the Commission assessed before renewing. Efficient, risk-based compliance and continued EU adequacy are therefore not in tension; they were affirmed together.

We accordingly encourage DSIT and the ICO to pursue the streamlining measures above in a manner that remains demonstrably within that essentially-equivalent envelope. The reforms we advocate — reusable country risk information, category- and group-level assessments, material-change triggers for re-assessment, and worked examples — are operational and procedural refinements to how organisations assess and document transfers. They do not lower the substantive standard of protection, and are fully compatible with the transparent, principled safeguards on which the UK's adequacy status rests.

Finally, because the renewed decisions remain subject to ongoing Commission monitoring, and because the European Data Protection Board's October 2025 opinion identified areas to keep under review, we would welcome guidance that is clear and well-documented enough to demonstrate — to both UK organisations and EU counterparts — that a more proportionate UK regime continues to deliver robust, real-world protection.

4. Ensuring Trust in the Face of a Changing World

It is widely recognised that data security depends principally on the quality of technical, organisational, contractual, and governance controls – not the location of a server. Cross-border data access and visibility can also strengthen security by enabling global threat detection, fraud prevention, rapid patching, resilience, redundancy, and disaster recovery.

Conversely, localisation concentrates risk, reduces access to advanced security services, fragments monitoring, and creates single points of failure. It also cuts against the geographic redundancy that operational-resilience frameworks – including those the UK's own financial regulators promote – treat as a security asset rather than a liability.

This approach is also consistent with the UK's own binding commitments. Through its accession to the CPTPP (in force since 15 December 2024) and its digital trade agreements, the UK has committed not to require data localisation as a condition of doing business, subject only to narrow, non-discriminatory public-policy exceptions. The Government should therefore define "data sovereignty" in terms of effective control, lawful access, resilience, portability, and accountability, rather than domestic storage. Any special controls for genuinely national-defence or critical government datasets should be narrowly defined, evidence-based, technology-neutral, and no more restrictive than necessary. They should not become a general localisation requirement for commercial, health, research, or industrial data.

Stated concerns about foreign-government access should be addressed through principled assessments of necessity, proportionality, independent oversight, redress, transparency, and rule-of-law safeguards. The OECD Declaration on Government Access to Personal Data (Trusted Government Access) – adopted by the 38 OECD members and the EU – provides a useful common framework and seeks to increase confidence in cross-border flows among countries committed to democratic values and the rule

of law. We continue to urge all OECD adherents, including the UK, US, and EU member states, to lead by example – and would welcome the UK being among the first to publish a mapping of its own national access regime against the OECD's Trusted Government Access principles.

Conclusion

The UK can strengthen trust and innovation by remaining the globe's preeminent leader in adaptable, agile, and responsible approaches to regulating and facilitating cross-border data transfers. GDA recommends preserving a diverse transfer toolkit; growing the UK's network of data bridges; enabling certification for cross-border data transfers; simplifying low-risk assessments; and concentrating scrutiny on genuinely high-risk transfers (among other reforms). This approach will protect individuals, improve cybersecurity and resilience, and support the cloud, AI, research, and cross-border services on which the UK's growth increasingly depends.

---

[1] The GDA is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to access and transfer information across borders to innovate and create jobs. GDA member companies are active in the accounting, agriculture, automotive, aerospace and aviation, biopharmaceutical, consumer goods, energy, film and television, finance, healthcare, hospitality, insurance, manufacturing, medical device, natural resources, publishing, semiconductor, software, supply chain, telecommunications, and transportation sectors. For more information, see https://www.globaldataalliance.org