CITP
CENTRE FOR INCLUSIVE TRADE POLICY

@centre4itp

The UK's data governance regime and the (challenging) data partnership with Indonesia

Phoebe Li, Minako Morita-Jaeger, Javier Ruiz, Arif Perdana, Saru Arifin

Published 29 July 2024

CITP Briefing Paper 15

Key Points:

- Data governance interoperability is key to digital trade. However, fragmentation in regulations and levels of data protection remain hurdles to digital trade.
- The UK's emerging data governance regime aims to include an international data hub, going forward, it is imperative to retain the data adequacy decision from the EU.
- The UK is also developing external data partnerships with the Association of Southeast Asian Nations countries. Yet the Indo-Pacific tilt in data governance requires careful assessment to bridge the gap between countries with different levels of data governance.
- Taking the UK-Indonesia *data partnership* as an example, both countries are currently undergoing major reforms in data governance. Whereas the UK remains a top performer in all metrics of data governance, there are significant gaps between the two countries' levels of data governance. Indonesia's new legal framework for data governance appears sufficient on paper but will require effective implementation.
- Even without a new data protection bill in the UK, UK ministers have extensive powers to facilitate international data transfer. Yet, extending data sharing to countries that exhibit significant gaps in data protection may jeopardise the UK's data adequacy decision granted by the EU.

Data has been the new currency for digital services trade. However, variations in approaches to data governance pose significant challenges to international harmonisation and interoperability. In this Briefing Paper, we describe the UK's and Indonesia's different approaches to data governance and the challenges that arise from attempts to bring them closer together, which would arguably facilitate the fledgling bilateral trade in digitally-delivered services.

UK's data governance reform

Since the vote to leave the EU, the various Conservative British Governments consistently tried to change the UK data regime inherited from the EU. The main focus of those reforms, as set out in the 2020 National Data Strategy and related consultations, was to use the ability to depart from EU policy to establish a 'pro-growth and trusted data regime'.

That policy direction included promoting 'the free flow of data to and from the UK', with global partners beyond the EU, to promote digital trade. To facilitate international data transfers, the UK Government sought to expand the number of countries with which the executive can decide to allow unrestricted flows of personal data, provided certain requirements are met. Under the EU GDPR regime, these are called *adequacy* decisions. In the UK, these are now renamed as *data partnerships* but remain essentially the same. Countries on the immediate priority list for British data partnerships include the United States (US), Australia, and Singapore, while Indonesia is on the long-term priority list, together with India, Brazil, and Kenya (2021 DCMS). None of those new data partnerships were completed by the Conservative governments, with the partial exception of the 2023 UK-US 'Data Bridge'. This was initially touted as a unique arrangement but eventually, it just meant extending the US-EU Data Protection Framework to cover the UK.

The most fundamental changes to UK data policy were meant to take place through legal reforms in the Data Protection and Digital Information Bill (DPDIB). The DPDIB was in the advanced stages of discussion and approval in the British Parliament, but it was dropped due to the 2024 general election. The DPDIB aimed at amending the General Data Protection Regulation (UK GDPR) inherited from the EU, including making it easier for ministers to create new *data partnerships*.

The DPDIB specifically proposed a subtle but important shift in the criteria for awarding these decisions. This was towards an assessment of 'material' privacy risks for the UK, rather than establishing the 'essential equivalence' of the legal regime - on data privacy but also fundamental human rights.[1] The language of 'essential equivalent' protections was introduced by the Court of Justice of the EU (CJEU) and later adopted in the GDPR. At heart it means that any interferences with fundamental rights, as enshrined in the EU Charter of Fundamental Rights, must pass established human rights tests.[2] This apparent simplicity unleashed a torrent of complex legal doctrine. The human rights test would appear to be easy to pass for any modern democracy, and possibly not directly relevant to commercial data transfers, but in practice, it is more complicated. The context of the CJEU discussions was Edward Snowden's whistleblowing over mass surveillance programmes by the US National Security Agency and their partners, including the UK and many advanced democracies. This surveillance was shown to rely heavily on various forms of access to commercial internet services and infrastructure.

In this context, the equivalence approach requires some legal contortions that may not hold scrutiny, as shown by the CJEU's repeated rejection of decisions by the European Commission to allow US data transfers. Given the UK's desire to enable data transfers to many more countries and to escape the EU's legal framework, it is understandable that a more practical route was sought. However, relying on practical risks and mitigations without the need for legal alignment and a human rights test could weaken the main attractiveness of adequacy: that the government underwrites a bulletproof legal certainty for data transfers without the need for additional due diligence and lawyers' fees.

A lower hurdle for adequacy may also complicate onward data transfers from the EU if those countries remain subject to more stringent standards and cannot meet EU adequacy standards. The latest EU adequacy decisions show the growing concerns over the tangled web of data and trade agreements that may enable onward transfers to third countries. Changes to UK adequacy requirements may even risk the UK's adequacy decision from the EU, or at least trigger demands from the EU for additional safeguards. For example, the EU adequacy decision on Japan required specific commitments from Japanese authorities to create a separate regime for EU data, although experts and rights groups caution that this approach may not be enough if subjected to a legal challenge at the CJEU.

It is highly improbable that the DPDIB will become law now that the UK general election resulted in a change of government. The Labour leadership also sees economic growth as a priority, and given the centrality of data and digital technologies such as AI to society and the economy, they will probably try to bring forward new laws on data,

[1] This risk approach was novel among countries using the adequacy framework for data transfers. For example, the Japanese data protection law APPI requires "equivalent" protections (Art 24), while Brazil's LGPD requires levels of protection that are "appropriate" (Art 33).

[2] See Drechsler, L., & Kamara, I. (2022). "Chapter 13: Essential equivalence as a benchmark for international data transfers after Schrems II". In *Research Handbook on EU Data Protection Law*. Cheltenham, UK: Edward Elgar Publishing. Retrieved Jul 9, 2024, from https://doi.org/10.4337/9781800371682.00022.

but this may take time. With the large Labour majority in Parliament, the Government could try to blitz through some speedy reforms, but this may be unwise. The complexity of these issues requires a deliberate, inclusive, and participatory process.

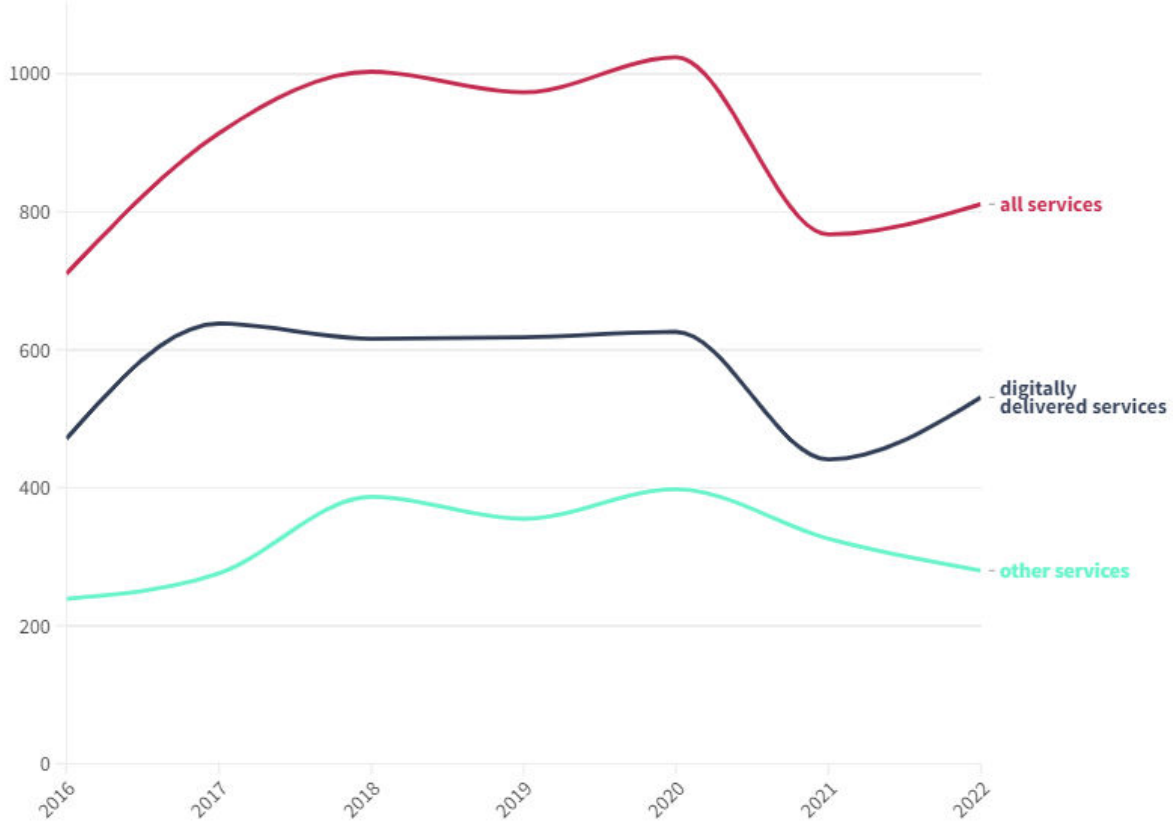
The UK Government should clearly lay out and seek diverse views on their own approaches to growth, digital rights, and trust before starting the formal track of policy drafting, legal consultation, and eventually finding a slot in the legislative schedule for a bill.

UK- Indonesia digital trade relations and data partnerships

Indonesia is the largest Southeast Asian economy, a member of the Association of Southeast Asian Nations (ASEAN), and an important strategic partner for the UK in its Indo-Pacific tilt strategy. Yet, the share of the UK's services exports to Indonesia accounts for only 0.16% (or $811 million) of its total services exports to the world in 2022.

The value of global 'digitally delivered services exports' exceeded that of 'other services exports' as early as 2008 according to the WTO. In the case of the UK's services exports to Indonesia (Figure 1), the value (US dollars) of the UK's 'digitally-delivered services exports' to Indonesia (2016-2022) were much more stable than 'other services exports'. Although the volume of 'digitally deliverable services exports' does not show an increase from 2017, after a huge drop in 2021, it nearly bounced back to its 2020 level.

Figure 1: UK's services exports to Indonesia (million US dollars)

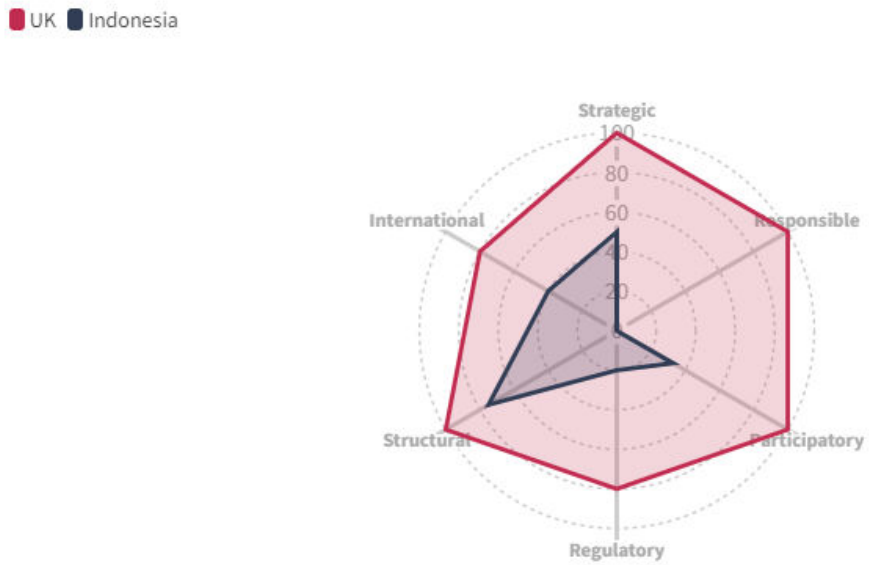


Data source: WTO, authors' representation using data.

Note: We classified the digitally deliverable services in accordance with reference of the Handbook on Measuring Digital Trade and World Trade Organisation Statistics Portal dataset (see Appendix: List of digitally deliverable services) .

The UK and Indonesia are taking different approaches to data governance. According to the Global Data Governance Project, Indonesia's data governance regime is classified as being weaker than that of the UK with regard to each of the constituent elements: (Responsible, Regulatory, Participatory, International, and Strategic)[3] as can be seen in Figure 2. Indonesia's data governance appears to be ranked as especially weak for the categories 'responsible' and 'regulatory'. Hence, with regard to the latter, Indonesia does not have an open data law for the proactive release of government information and the right to data portability. With respect to the former, Indonesia does not have a data charter, a public sector data ethics framework, a trust framework for digital identity management, or non-governmental data sharing guidelines.

Figure 2: A comparison of data governance between the UK and Indonesia



Source: Global Data Governance Mapping Project 2024: authors' representation.

[3] According to the Mapping Project, the six dimensions of the index have the following definition: ***Strategic*** (data strategy, public administration data strategy, AI strategy and strategy for data in society 5.0); ***Regulatory*** (personal data protection law, open data law for the proactive release of government information, freedom of information act, righto to be protected from automated decision-making, and right of data portability); ***Responsible*** (data charter, public sector data ethics framework, responsible AI initiatives, trust framework for digital identity management, and non-governmental data sharing guidelines); ***Structural*** (personal data protection body, open data portal, open data coordinating body, and public sector data governance body); ***Participatory*** (public consultation on data, government response to consultation and multistakeholder advisory body); ***International*** (Convention 108+, open government partnership, OECD AI principles, binding trade agreements on cross-border data flows, and Budapest convention). See the methodology in detail in "Data Governance Mapping Project Year 4".

Since the UK became an ASEAN Dialogue Partner in 2021,[4] the British Government has been supporting information and communication technology (ICT) and digital integration within ASEAN. To enhance cooperation in trade and investment relations, the British and Indonesian Governments adopted the UK-Indonesia Partnership Roadmap 2022 to 2024 (April 2022). The UK-Indonesia Joint Economic Trade Committee (JETCO) was launched as the forum to explore the future trade relationship, including a potential free trade agreement. Under the roadmap, cooperation on the digital economy defined several areas of focus, including supporting the development of ICT infrastructure and digital transformation in Indonesia, business-to-business cooperation in digitally-enabled sectors, and exploring opportunities for deeper future cooperation in digital technologies and the creative economy. It also aims to promote the UK's engagement in the digital economy in ASEAN and the Asia-Pacific region.

Indonesia's data governance reform

As mentioned above, Indonesia has been identified as one of the UK's 'Longer Term Priorities' in Data Partnerships. The UK-Indonesia Partnership Roadmap emphasises the commitment to strengthening bilateral cooperation across various domains, including digital and data partnerships. Specifically, the roadmap highlights efforts to enhance digital transformation, ICT infrastructure, and cooperation in digitally-enabled sectors. The roadmap also outlines ambitions to shape future technologies with shared democratic values, promoting business-to-business cooperation and training in digital technologies.

To strengthen the legal framework for data protection, Indonesia recently enacted the Personal Data Protection Law (UU PDP), aligning with the rollout of the National Data Center (PDN), which consolidated over 2,700 data centers from 630 institutions. The UU PDP emphasizes the protection of personal data across both public and private sectors, mandating compliance to safeguard citizens' fundamental rights. This regulation is a catalyst for broader public sector reform and public service enhancement.

Another aspect of data governance is reflected in the commitment to transparency and accountability of AI governance, which mandates the disclosure of source code or software. These disclosure requirements ensure that AI systems operate fairly, ethically, and without bias. They allow for independent verification of AI algorithms, promoting trust and accountability. However, these mandates must be balanced with the protection of intellectual property such as trade secrets. Effective regulations can enhance international trade by ensuring that AI technologies are following the principles of AI governance. Indonesia's regulatory framework for source code and software disclosure (particularly under Regulation 71/2019, GR71), imposes data localisation requirements and mandates source code disclosure for companies engaging with public-sector entities. Although the disclosure of source code is critical for the requirement of 'transparency' in AI governance, this requirement, along with burdensome local content rules and opaque licensing (Regulation 80/2019, GR80), poses significant market entry barriers for foreign firms. Notably, the data localization requirement was relaxed to include only public bodies' data whereas banking and financial data operated by public bodies are exempt.

In addition, Indonesia has enacted an extensive array of regulations pertaining to technology. These include Information and Electronic Transactions (ITE, Law No. 19 of 2016, amending Law No. 11 of 2008); the Protection of Personal Data Law (No. 27 of 2022); the implementation of electronic systems and transactions (Government Regulation No. 71 of 2019); and Minister of Communication and Information Regulation concerning electronic certificates (No. 10 of 2021). These new laws aim at enhancing data governance, ensuring data security, and building trust in electronic transactions. They are intended to create a more robust digital framework that aligns with international standards. Implementation and enforcement, however, require technical support and monitoring to ensure fairness in international trade.

Indonesia's new data laws align with UK standards on principles, data subject rights, breach notifications, and cross-border transfers. In comparison to the previous legal framework, which was based on traditional legal approaches

[4] ASEAN has established Dialogue Partnerships with the following countries: Australia, Canada, China, EU, India, Japan, New Zealand, Korea, Russia, UK, and US. https://asean.org/our-communities/asean-political-security-community/outward-looking-community/external-relations/ (accessed 8 July 2024).

such as the ITE Acts, criminal law, and Public Information Acts, the present Indonesian legal framework regarding digital activities has been significantly enhanced. Personal data protection, for example, was primarily derived from the GDPR. Yet there is one remaining task: the preparation of the technical regulation and its infrastructure in order to implement the PDP Act. In addition to the advantages conferred by the data governance provisions that are specifically aligned with the UU PDP, Indonesia faces a significant challenge in integrating the diverse institutions responsible for data protection under the control of the data protection body. This is due to persistent government bureaucracy. Furthermore, it is imperative to have well-trained personnel who can oversee the implementation of data protection.

While some provisions exist, the requirements for national data protection authority and appointing a data protection officer could be more detailed and comprehensive, similar to the GDPR's stringent criteria. Ensuring the independence and authority of the data protection regulatory body is crucial for unbiased enforcement and building international trust. Developing sector-specific guidelines and best practices for data protection can also help align Indonesia's policies more closely with the comprehensive approach seen in the UK.

The new legal framework has shown a positive move towards improving the level of data governance in Indonesia; however, the implementation and enforcement of these regulations will still need robust technical support and will need to be closely monitored to ensure impartiality in international digital trade transactions. In light of this, Indonesia is continuing to enhance its legal capabilities to facilitate the implementation of its digital activities that are pertinent to international advancements.

Conclusion

Current and future legal reforms in both countries could bring their levels of data governance closer together, which might facilitate a UK-Indonesia data partnership. Addressing these regulatory issues and improving the clarity and fairness of the laws are crucial to attracting foreign investment and supporting the growth of the digital economy.

The UK's approach to Indonesia reflects an awareness of the gaps in data protection, but also some strategic differences that prevailed when the UK was deciding on those priorities, particularly with regard to the policy to keep public body data within Indonesian data centres, which the UK sees as inimical to digital trade. Whereas the two governments are promoting economic cooperation, the level of data governance in the UK is currently much higher than in Indonesia, although the UK is at a turning point for data protection and data governance, with the first rotation of the governing political party in 15 years. Fundamental shifts are unlikely though. The UK DPDI Bill failed to be fast-tracked for approval mainly because of domestic controversies, including new powers for government to access bank accounts. Pro-business policies, such as facilitating international transfers and digital trade, are broadly supported by all main parties.

The design and implementation of new data governance policies in both Indonesia and the UK will face a new test to remain satisfactory across the five metrics of the Global Data Governance Mapping Project: Responsible, Regulatory, Participatory, International, Participatory and Strategic (see Figure 2). This challenge is compounded by the danger that any movement by the UK towards Indonesia—and Asia-Pacific more generally—may jeopardise the UK's data adequacy decision vis-a-vis the EU. It remains to be seen whether the UK-Indonesia data partnership is promising or going nowhere under the new UK Government.

Despite this unpredictable landscape, the agenda for collaboration between the UK and Indonesia could advance in the absence of new legal reforms. The current regime already gives UK ministers extensive powers to facilitate international data transfers, as compared with their EU counterparts. The incoming executive could choose to make use of these powers in the short-term, instead of waiting for a future Bill.

Appendix

In accordance with reference Of the World Trade Organisation Statistics Portal dataset, we classified the following sectors as digitally deliverable services: BOP6 - SC4 - Postal and courier services, BOP6 - SD - Travel, BOP6 - SDA - Business, BOP6 - SDB - Personal, BOP6 - SDB1 - Health-related, BOP6 - SDB2 - Education-related, BOP6 - SF - Insurance and pension services, BOP6 - SF1 - Direct insurance, BOP6 - SF2 - Reinsurance, BOP6 - SF3 - Auxiliary insurance services, BOP6 - SF4 - Pension and standardized guaranteed services, BOP6 - SG - Financial services, BOP6 - SG1 - Explicitly charged and other financial services, BOP6 - SG2 - Financial intermediation services indirectly measured (FISIM), BOP6 - SH - Charges for the use of intellectual property n.i.e., BOP6 - SI - Telecommunications, computer, and information services, BOP6 - SI1 - Telecommunications services, BOP6 - SI2 - Computer services, BOP6 - SI3 - Information services, BOP6 - SJ - Other business services, BOP6 - SJ1 - Research and development services, BOP6 - SJ2 - Professional and management consulting services, BOP6 - SJ21 - Legal, accounting, management consulting, and public relations services, BOP6 - SJ211 - Legal services, BOP6 - SJ212 - Accounting, auditing, bookkeeping, and tax consulting services, BOP6 - SJ213 - Business and management consulting and public relations services, BOP6 - SJ22 - Advertising, market research, and public opinion polling services, BOP6 - SJ3 - Technical, trade-related, and other business services, BOP6 - SJ31 - Architectural, engineering, scientific, and other technical services, BOP6 - SJ311 - Architectural services, BOP6 - SJ312 - Engineering services, BOP6 - SJ313 - Scientific and other technical services, BOP6 - SJ323 - Services incidental to mining, and oil and gas extraction, BOP6 - SJ33 - Operating leasing services, BOP6 - SJ34 - Trade-related services, BOP6 - SJ35 - Other business services n.i.e., BOP6 - SK - Personal, cultural, and recreational services, BOP6 - SK1 - Audiovisual and related services, BOP6 - SK2 - Other personal, cultural, and recreational services.

Other sectors are classified as 'Other services', such as BOP6 - SOX - Commercial services, BOP6 - SPX4 - Goods-related services, BOP6 - SA - Manufacturing services on physical inputs owned by others, BOP6 - SB - Maintenance and repair services n.i.e., BOP6 - SC - Transport, BOP6 - SC1 - Sea transport, BOP6 - SC11 - Passenger (Sea), BOP6 - SC12 - Freight (Sea), BOP6 - SC13 - Other (Sea), BOP6 - SC2 - Air transport, BOP6 - SC21 - Passenger (Air), BOP6 - SC22 - Freight (Air), BOP6 - SC23 - Other (Air), BOP6 - SC3 - Other modes of transport, BOP6 - SDA1 - Acquisition of goods and services by border, seasonal, and other short-term workers, BOP6 - SDA2 - Other (Business), BOP6 - SDB3 - Other (Personal), BOP6 - SOX1 - Other commercial services, BOP6 - SE - Construction, BOP6 - SE1 - Construction abroad, BOP6 - SE2 - Construction in the reporting economy, BOP6 - SJ11 - Work undertaken on a systematic basis to increase the stock of knowledge, BOP6 - SJ111 - Provision of customized and non-customized research and development services, BOP6 - SJ112 - Sale of proprietary rights arising from research and development, BOP6 - SJ12 - Other research and development services, BOP6 - SJ321 - Waste treatment and de-pollution, BOP6 - SJ322 - Services incidental to agriculture, forestry and fishing, BOP6 - S - Memo item: Total services, BOP6 - SPX1 - Memo item: Other services, BOP6 - SL - Memo item: Government goods and services n.i.e.

Digitally Deliverable Services
BOP6 - SC4 - Postal and courier services
BOP6 - SD - Travel
BOP6 - SDA - Business
BOP6 - SDB - Personal
BOP6 - SDB1 - Health-related
BOP6 - SDB2 - Education-related
BOP6 - SF - Insurance and pension services
BOP6 - SF1 - Direct insurance
BOP6 - SF2 - Reinsurance

BOP6 - SF3 - Auxiliary insurance services

BOP6 - SF4 - Pension and standardized guaranteed services

BOP6 - SG - Financial services

BOP6 - SG1 - Explicitly charged and other financial services

BOP6 - SG2 - Financial intermediation services indirectly measured (FISIM)

BOP6 - SH - Charges for the use of intellectual property n.i.e.

BOP6 - SI - Telecommunications, computer, and information services

BOP6 - SI1 - Telecommunications services

BOP6 - SI2 - Computer services

BOP6 - SI3 - Information services

BOP6 - SJ - Other business services

BOP6 - SJ1 - Research and development services

BOP6 - SJ2 - Professional and management consulting services

BOP6 - SJ21 - Legal, accounting, management consulting, and public relations services

BOP6 - SJ211 - Legal services

BOP6 - SJ212 - Accounting, auditing, bookkeeping, and tax consulting services

BOP6 - SJ213 - Business and management consulting and public relations services

BOP6 - SJ22 - Advertising, market research, and public opinion polling services

BOP6 - SJ3 - Technical, trade-related, and other business services

BOP6 - SJ31 - Architectural, engineering, scientific, and other technical services

BOP6 - SJ311 - Architectural services

BOP6 - SJ312 - Engineering services

BOP6 - SJ313 - Scientific and other technical services

BOP6 - SJ323 - Services incidental to mining, and oil and gas extraction

BOP6 - SJ33 - Operating leasing services

BOP6 - SJ34 - Trade-related services

BOP6 - SJ35 - Other business services n.i.e.

BOP6 - SK - Personal, cultural, and recreational services

BOP6 - SK1 - Audiovisual and related services

BOP6 - SK2 - Other personal, cultural, and recreational services

UKRI Economic and Social Research Council